Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Australian Information Security Evaluation Program

Certification Report

Cogito Jellyfish Certificate Authority Version 7.0

Version 1.0, 29 April 2026

Document reference: AISEP-CC-CR-2026-EFV-T002-CR-V1.0
(Certification expires five years from certification report date)

Table of contents

Executive Summary

This report describes the findings of the IT security evaluation of Cogito Jellyfish Certificate Authority V7.0 against Common Criteria approved Protection Profile (PP).

The TOE is the Cogito Jellyfish Certificate Authority (hereby known as Jellyfish CA), a web based certificate authority that handles the generation, request and revocation of digital certificates across government and commercial environments. The Jellyfish CA provides interfaces to Hardware Security Modules (HSM) for the management of multiple cryptographic key types supporting certificates.

This report concludes that the Target of Evaluation (TOE) has complied with the following *PP [4]:*

- Protection Profile for Certification Authorities Version 2.1, 01 December 2017 (PP_CA_V2.1)

No PP-Configurations were used for this evaluation.

The evaluation was conducted in accordance with the Common Criteria and the requirements of the Australian Information Security Evaluation Program (AISEP). Viden Labs performed the evaluation activities with the final Evaluation Technical Report (ETR) submitted on 28 April 2026.

With regard to the secure operation of the TOE, the Australian Certification Authority recommends that administrators:

- ensure that the TOE is operated in the evaluated configuration and that assumptions concerning the TOE security environment are fulfilled
- configure and operate the TOE according to the vendor's product administrator guidance and pay attention to all security warnings
- maintain the underlying environment in a secure manner so that the integrity of the TOE Security Function is preserved
- verify the version of any downloaded software, as presented in the Security Target and Admin Guide
- the system auditor should review the audit trail generated and exported by the TOE periodically
- configure certificate templates and certificate authorities to support selections claimed in the ST
- the system auditor should review the audit trail generated and exported by the TOE periodically
- enable certificate-based smart card multi-factor authentication
- Non-TOE software listed in ST is installed as a dependency in the system.

Potential purchasers of the TOE should review the intended operational environment and ensure that they are comfortable that the stated security objectives for the operational environment can be suitably addressed.

This report includes information about the underlying security policies and architecture of the TOE, and information regarding the conduct of the evaluation.

It is the responsibility of the user to ensure that the TOE meets their requirements. For this reason, it is recommended that a prospective user of the TOE refer to the Security Target and read this Certification Report prior to deciding whether to purchase the product.

Introduction

Overview

This chapter defines the purpose of this document and contains information to identify the Target of Evaluation (TOE).

Purpose

The purpose of this Certification Report is to:

- report the certification of results of the IT security evaluation of the TOE against the requirements of the *Common Criteria [1,2,3]* and Protection *Profile [4]*
- provide a source of detailed security information about the TOE for any interested parties.

This report should be read in conjunction with the TOE's *Security Target [8],* which provides a full description of the security requirements, and specifications that were used as the basis of the evaluation.

Identification

The TOE is the Cogito Jellyfish CA version 7.0.

Description	Version
Evaluation scheme	Australian Information Security Evaluation Program
TOE	Cogito Jellyfish CA version 7.0
Software version	7.0
Hardware platforms	N/A
Security Target	Jellyfish CA Security Target, Version 11.0, 24 April 2026
Evaluation Technical Report	Jellyfish CA Evaluation Technical Report 7.0, dated 28 April 2026 Document reference EFV-T002-REP-001 - Jellyfish CA Evaluation Technical Report (ETR) – v7.0
Criteria	Common Criteria for Information Technology Security Evaluation Part 2 Extended and Part 3 Conformant, April 2017, Version 3.1 Rev 5
Methodology	Common Methodology for Information Technology Security, April 2017 Version 3.1 Rev 5
Conformance	Protection Profile for Certification Authorities, Version 2.1, 01 December 2017 [PP_CA_V2.1]

Developer	Cogito Group Suite 3, 9 Sydney Avenue Barton ACT 2600 Australia
Evaluation facility	Viden Labs Unit 63, 10 Lonsdale Street Braddon ACT 2612 Australia

Target of Evaluation

Overview

This chapter contains information about the Target of Evaluation (TOE), including a description of functionality provided, its architectural components, the scope of evaluation, its security policies and its secure usage.

Description of the TOE

The TOE is the Jellyfish CA which is an enterprise class Public Key Infrastructure (PKI) certificate authority built on a collection of microservices allowing the issuance and life cycle management of public key certificates of the type specified in the X.509 v3 standard (RFC 5280). Jellyfish CA functionalities can be accessed through web interfaces or APIs and utilises NIST-compliant encryption algorithms.

This allows the issuance of public key certificates for different purposes, including:

- System management functions (e.g., security audit, configuration management, archive)
- Key generation/storage in the Operational Environment
- Certificate generation, modification, re-key, renewal, and distribution
- Certificate revocation list (CRL) generation and distribution
- Key escrow and recovery
- Directory management of certificate related items
- Certificate token initialization/programming/management

Public Key Cryptography commonly uses digital certificates in order to authenticate users. Given the complex nature of the issuance and management of the digital certificate lifecycle, organisations that want to carry out these types of operations typically require Certificate Authority applications to ensure effective registration, revocation and renewal of certificates.

TOE Functionality

The TOE functionality that was evaluated is described in section 1.4 of the *Security Target [8].*

TOE Physical Boundary

The TOE physical boundary consists of the following items:

- Jellyfish CA Codebase
- Consul API
- Postgresql database

The firmware version reflects the detail reported for the components of the Jellyfish CA as described in the *ST [8]*

The physical boundary for the Cogito Jellyfish CA is shown in the figure below.

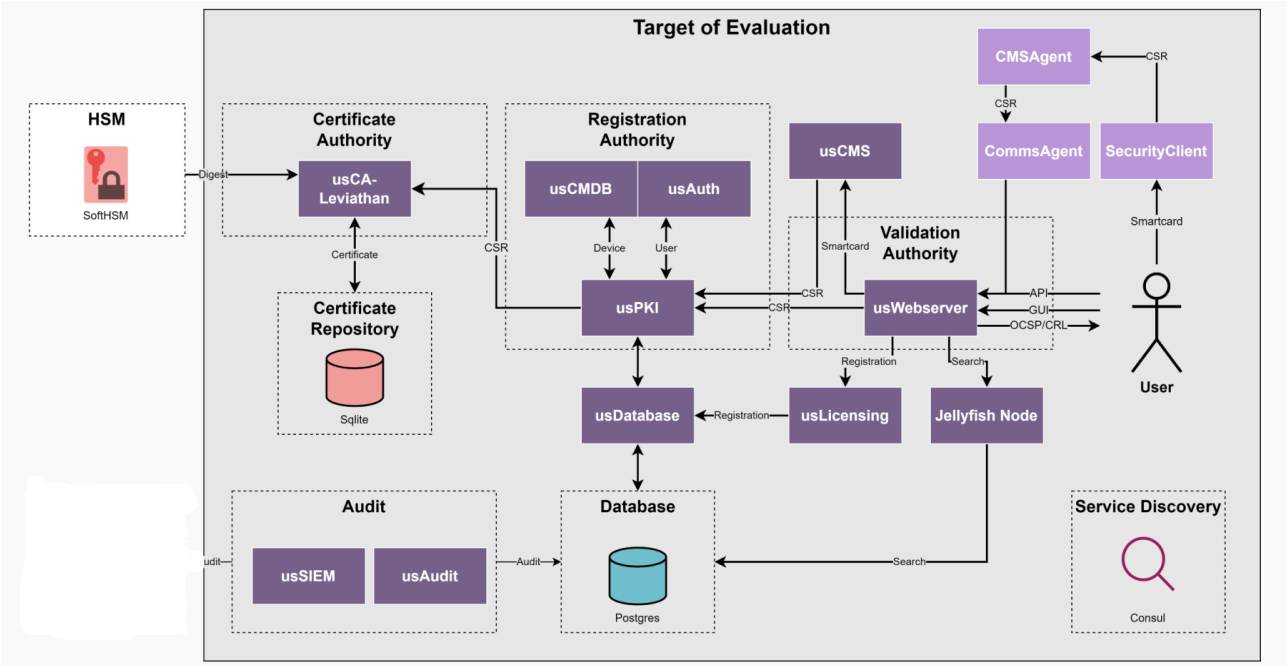

Figure 1: TOE Boundary

Architecture

Each instance of the TOE consists of the following major architectural components:

- The Jellyfish CA Application is series of services via a Graphical User Interface (GUI) provided by React FrontEnd and API accesses for various CA functionality.
- The webserver (usWebserver) implements HTTPS for the provision of GUI and API interactions for users. Furthermore, the webserver utilises standard Go cryptographic libraries for TLS and HTTPS functionality in the TOE.
- Hashicorp Consul is a middleware service mesh allowing for secure communication through Mutual Transport Layer Security (mTLS) and serivce access for all microservices running on Jellyfish CA.
- The database on the Jellyfish CA is used to store audit events associated with the system, system objects including certificate requests, certificates, certificate metadata and CRLs, store user credentials and roles, profiles used for certificate generation and storing configurations relating to CA functionality.

The following table represents the evaluated configuration of the TOE against *CA_PP_v2.1*.

Component	Description/Identifier
Jellyfish CA	V7.0
Operating System	Linux Ubuntu 22.04

Hashicorp Consul Community	V1.21 – network and security mesh for microservices used in the system.
Node.js	V22.17 – Javascript framework used to support queries to the usDatabase microservice.
Postgresql	v15.13 - relational database storing TOE relevant information
Build Procedures	Build_Guide-Jellyfish_Linux_All-In-One_Common Criteria_v1.51
Administrative Procedures	Jellyfish Client Admin Guide_v7.6.121
VMWare ESXi	Version 11 - a bare metal hypervisor used to host virtual machines.
SoftHSM	V2.6 - software-based HSM used to represent the HSM functionality of the system.

The Jellyfish CA, operating as a microservices platform, which is independent of hardware and operating system. The ACA can only provide assurance for an evaluated configuration based on evaluation activities conducted by the AISEF. For the purposes of this evaluation, Ubuntu Linux was selected for the evaluation activities against the TOE.

Clarification of Scope

The evaluation was conducted in accordance with the Common Criteria and associated methodologies.

The scope of the evaluation was limited to those claims made in the *Security Target [8].*

Evaluated Functionality

Functional tests performed during the evaluation were taken from the Protection Profile and sufficiently demonstrate the security functionality of the TOE. Some of the tests were combined for ease of execution.

Non-TOE Hardware/Software/Firmware

Additional hardware and software components are required to operate the system. A server or Virtual Machine (VM) running Ubuntu Linux (22.04) with the minimum recommended specification of 2 Cores, 4GB RAM and 30GB HDD.

The TOE relies on the provision of the following items in the operational environment:

- Source Files copied to the Virtual Machine:
  - Hashicorp Consul Community v1.21
  - Node.js v22.17
  - PostgreSQL v15.13
  - SoftHSM v2.6
- System hardware
- Operating System
- Hardware Security Module

Non-evaluated Functionality and Services

Potential users of the TOE are advised that some functions and services have not been evaluated as part of the evaluation. Potential users of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration.

Australian Government users should refer to the *Australian Government Information Security Manual* [5] for policy relating to using an evaluated product in an unevaluated configuration.

The following components are considered outside of the scope of the TOE:

- the microservices usCMDB, usCMS and usLicense as they do not support or implement trusted security functionality to the TOE
- SIEM forwarding features of the TOE by usSIEM
- system hardware
- operating system
- Hardware Security Module (HSM)

It is important to note the HSM itself is excluded from the scope of the evaluation, however the cryptographic functionality the HSM provides through the operational environment has been evaluated.

Security Policy

The TOE Security Policy is a set of rules that defines the required security behaviour of the TOE; how information within the TOE is managed and protected. The Security Target [8] contains a summary of the functionality that is evaluated.

Secure Delivery

The Jellyfish CA is provided to customers in two forms:

- Software-As-A-Service offering
- Self-Hosted Deployment.

In order to access the evaluated product in a secure manner as a Software-as-a-Service offering, customers are instructed to use the Uniform Resource Locator provided by Cogito and ensure that the TLS certificate matches the domain prior to login.

For Self-Hosted Deployment, customers are to access the product from the online storage service provided by Cogito using TLS and verify the download using instructions in the administration guide. The folder is listed as:

- Jellyfish-AIO-Linux-7.0.x.x

Installation of the TOE

For Software-as-a-Service (SaaS) deployment of Jellyfish CA, no user installation is required. Cogito manages this in the role of the trusted administrator.

For Self-Hosted Deployment, users are to follow the guidance in the user and administration guide to ensure the complete installation of Jellyfish CA.

Version Verification

To ensure the product is the evaluated version, customers are to ensure that the version number listed on the user interface of the TOE is the same as that described within the Security Target [8] and guidance documentation [6].

Documentation and Guidance

It is important that the TOE be used in accordance with guidance documentation [6] in order to ensure secure usage. The following documentation is available to the consumer when the TOE is purchased. The evaluated configuration guide (System Admin Guide) documents for the Cogito Jellyfish CA version 7.0 is available for download via the Uniform Resource Locator (SaaS) or online storage service (self-hosted deployment) provided by Cogito. The title is:

- *Build Guide Jellyfish Linux All-In-One Common Criteria, Version 1.51.2, Pub. 24 April 2026*
- *Jellyfish Client Admin Guide, Version 7.6.121, Pub. 20 April 2026*

All Common Criteria guidance material is available at *https://www.commoncriteriaportal.org* [1, 2, 3, 12].

The *Australian Government Information Security Manual* is available at *https://www.cyber.gov.au/ism [5].*

Secure Usage

The evaluation of the TOE took into account certain assumptions about its operational environment. These assumptions must hold in order to ensure the security objectives of the TOE are met.

The TOE is assumed to be physically secured within its operational environment, protected from physical attacks that could compromise its security or interfere with its physical connections and correct operation. This level of protection is expected to be sufficient to safeguard the device and the sensitive data it handles.

The TOE is expected to provide Public Key Infrastructure (PKI) functionality as its primary purpose and should not offer any general-purpose computing capabilities, such as running compilers or user applications unrelated to its PKI, key and token management functions. This ensures that the device remains focused solely on its intended security role.

The TOE administrator(s) are assumed trustworthy, acting in the best interests of the organisation's security. This includes being well-trained, adhering to established policies, and following all *guidance documentation [6].* Administrators are responsible for ensuring that passwords and credentials used within the TOE are strong and

secure. The TOE is not expected to protect against a malicious administrator who deliberately seeks to bypass or compromise its security features.

For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store (aka 'root store', ' trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification).

The TOE's firmware and software are assumed to be regularly updated by an administrator, particularly in response to newly discovered vulnerabilities. This ensures that the TOE remains protected against emerging threats.

The credentials (such as private keys) used by administrators to access the TOE must be securely protected on any platform where they are stored. Administrators must also ensure that sensitive residual information, including cryptographic keys, keying material, PINs, and passwords, is not accessible to unauthorized individuals when equipment is discarded or removed from service.

Evaluation

Overview

This chapter contains information about the procedures used in conducting the evaluation, the testing conducted as part of the evaluation and the certification result.

Evaluation Procedures

The criteria against which the Target of Evaluation (TOE) has been evaluated are contained in the relevant *Protection Profile [4]* and *Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 5, Parts 2 and 3 [1, 2].*

Testing methodology was drawn from *Common Methodology for Information Technology Security, April 2017 Version 3.1 Revision 5 [3]*.

The evaluation was carried out in accordance with the operational procedures of the *Australian Information Security Evaluation Program [10].*

In addition, the conditions outlined in the Arrangement on the Recognition of *Common Criteria Certificates in the field of Information Technology Security [9]* and the document *CC and CEM addenda, Exact Conformance, Selection-Based SFRs, Optional SFRs* [12] were also upheld.

Functional Testing

All functional tests performed by the evaluators were taken from the *Protection Profile [4]* and. The tests were designed to provide the required testing coverage for the security functions claimed by the TOE.

Entropy Testing

The entropy design description, justification, operation and health tests are assessed and documented in a *separate report [12].* The cryptographic module used by the TOE, BoringSSL/BoringCrypto, is covered by NIST CMVP Certificate #4407. All cryptographic operations evaluated were implemented using this validated module.

Penetration Testing

The evaluators performed the evaluation activities for vulnerability assessment specified by the *CA_PP Protection Profile Document [4]* that expects the evaluation lab to survey open sources to discover what vulnerabilities have been identified for the TOE.

The evaluators conducted a review of public vulnerability databases to determine potential flaw hypotheses using searches that include TOE device name and components, protocols supported by the TOE and terms relating to the device type of the TOE. These searches were conducted up to the **11 December 2025** coinciding with the conclusion of the evaluation.

In addition, the evaluation team devised two tests to check for potential vulnerabilities within the TOE's web application and access control. The evaluation team also conducted tool-generated vulnerability testing of the TOE.

Based on the results of this testing, the evaluators determined that the TOE is resistant to an attacker possessing a basic attack potential.

Certification

Overview

This chapter contains information about the result of the certification, an overview of the assurance provided and recommendations made by the certifiers.

Assurance

This certification focuses on the evaluation of product compliance with Protection Profile that cover the technology area of Certificate Authority devices. Organisations can have confidence that the scope of an evaluation against an ASD-approved Protection Profile covers the necessary security functionality expected of the evaluated product and known threats will have been addressed.

The analysis is supported by testing as outlined in the PP Documents and a vulnerability survey demonstrating resistance to penetration attackers with a basic attack potential. Compliance also provides assurance through evidence of secure delivery procedures. Certification is not a guarantee of freedom from security vulnerabilities.

The effectiveness and integrity of cryptographic functions are also within the scope of product evaluations performed in line with the Protection Profiles (PPs). PPs provide assurance by providing a full Security Target, and an analysis of the Security Functional Requirements in that Security Target, guidance documentation, and a basic description of the architecture of the TOE.

Certification Result

Viden Labs **has determined** that the TOE upholds the claims made in the *Security Target [8]* and **has met** the requirements of the *Protection Profile CA_PP_V2.1 [4].*

After due consideration of the conduct of the evaluation as reported to the certifiers, and of the *Evaluation Technical Report [7]*, the Australian Certification Authority **certifies** the evaluation of the Cogito Jellyfish CA performed by the Australian Information Security Evaluation Facility, Viden Labs.

The Australian Certification Authority certifies that the *Security Target [8]* have met the requirements of the Certification Authority *Protection Profile [4].*

Certification is not a guarantee of freedom from security vulnerabilities.

Recommendations

Not all of the evaluated functionality present in the TOE may be suitable for Australian Government users. For further guidance, Australian Government users should refer to the *Australian Government Information Security Manual [5].*

In addition to ensuring that the assumptions concerning the operational environment are fulfilled, and the guidance document is followed, the Australian Certification Authority also recommends that users and administrators:

- ensure that the TOE is operated in the evaluated configuration and that assumptions concerning the TOE security environment are fulfilled
- configure and operate the TOE according to the vendor's product administrator guidance and pay attention to all security warnings

- maintain the underlying environment in a secure manner so that the integrity of the TOE Security Function is preserved
- verify the version of any downloaded software, as presented in the Security Target and Admin Guide
- the system auditor should review the audit trail generated and exported by the TOE periodically
- configure certificate templates and certificate authorities to support selections claimed in the ST
- the system auditor should review the audit trail generated and exported by the TOE periodically
- enable certificate-based smart card multi-factor authentication
- Non-TOE software listed in ST is installed as a dependency in the system.

Annex – References and Abbreviations

References

1. *Common Criteria for Information Technology Security Evaluation Part 2: Security functional components April 2017, Version 3.1 Revision 5*
2. *Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components April 2017, Version 3.1 Revision 5*
3. *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, April 2017, Version 3.1 Revision 5*
4. Protection Profile: Protection Profile for Certification Authorities, Version 2.1, 01 December 2017 (PP_CA_V2.1)
5. *Australian Government Information Security Manual:* https://www.cyber.gov.au/ism
6. Guidance documentation:
    a) *Build Guide Jellyfish Linux All-in-One Common Criteria, Version 1.51.2, 24 April 2026*
    b) *Jellyfish Client Admin Guide, Version 7.6.121, 20 April 2026*
7. *Jellyfish CA Evaluation Technical Report Version 7.0, dated* 28 April *2026* (Document reference EFV-T002-ETR 7.0)
8. *Jellyfish CA Security Target, Version 11.0,* 24 April *2026.*
9. *Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, 02 July 2014*
10. *AISEP Policy Manual (APM):* https://www.cyber.gov.au/sites/default/files/2019-03/AISEP_Policy_Manual.pdf
11. Entropy Documentation:
    a) *FIPS 140-3 Non-Proprietary Security Policy - BoringCrypto for Google, LLC, Version 0.2, 19 July 2024*
12. CC and CEM addenda, Exact Conformance, Selection-Based SFRs, Optional SFRs 30 September 2021, Version 2.0, CCDB-013-v2.0

Abbreviations

AISEP	Australian Information Security Evaluation Program
API	Application Programming Interface
ASD	Australian Signals Directorate
ASIC	Application Specific Integrated Circuit
CA	Certificate Authority
CCRA	Common Criteria Recognition Arrangement
CMVP	Cryptographic Module Validation Program
CRL	Certificate Revocation List
HSM	Hardware Security Module
HTTPS	Hypertext Transfer Protocol Secure
mTLS	Mutual Transport Layer Security
NIST	National Institute of Standards and Technology
PKI	Public Key Infrastructure
PP	Protection Profile
RFC	Internet Engineering Task Force Request for Comment – technical specifications for internet and networking technologies
RSA	Rivest Shamir Adleman
SaaS	Software-as-a-Service
SIEM	Security Information and Event Management
SSH	Secure Shell
SSL	Secure Sockets Layer
TLS	Transport Layer Security
TOE	Target of Evaluation
VM	Virtual Machine
X.509	ITU format for public key certificates

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

For more information, or to report a cyber security incident, contact us:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

Australian Government

Australian Signals Directorate