Fact Sheet

Cogito Group

JellyFish Integrations

Supported Integrations

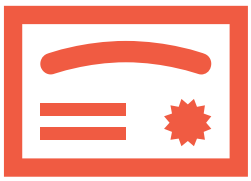
This list is not exhaustive, as there would be many more products and services that will work with our standards compliant integration points if they also comply with those standards. This is just the list of products and services that have been tested to work with Jellyfish.

Automatic Certificate Enrolment Protocols

- ACME
- ACME+ (Cogito expanded protocol)
- AEX (Modern Windows AutoEnroll protocol)
- API
- SCEP and Intune SCEP

Certificate Authority

- Jellyfish Leviathan CA
- ACM
- AD CS (Microsoft Windows CA)
- AWS Private CA*
- Azure Key Vault
- CFSSL*
- DigiCert
- EJBCA
- Entrust Authority Security Manager
- Let's Encrypt
- UniCERT



Certificate Lifecycle Management

- Generic: All supported Certificate Authorities
- Generic: Jellyfish can support manual or automated import of any certificate meeting the X.509 standards
- ACM (AWS Certificate Manager allows support of other solutions such as Elastic Load Balancing, Cloudfront, Cognito and Elastic Beanstalk. See the ACM Integration Services link for more supported products.
- AWS Private CA
- Azure Key Vault
- Linux
- Microsoft Windows
- Network Discovery of Certificates
- ServiceNow

**Coming soon*

JellyFish Integrations

Fact Sheet

Cloud Services

- Generic/Protocol Based Services: BYOK
- AWS - ACM, EKS, etc
- Azure Key Vault
- Cloudflare
- Google Cloud Platform
- Salesforce
- ServiceNow

CMDB

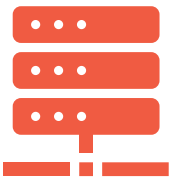
- Network Discovery of Devices
- CSV Export and Import of Devices

CMS

- Generic: Contact and Contactless Encoding
- Generic: MIFARE DESFire Smartcard Read/Write
- Generic: PIV Smartcard Encoding
- Printer: Evolis - Smartcard Printer
- Printer: Fargo HID - Smartcard Printer
- For more on Smartcard and Hardware Token Support - please see our separate list in Jellyfish_TokenSupport_Cogito_Group.pdf

DB- Certificate Support

- Key DB/Redis - In Memory DB/Cache
- Maria DB
- Microsoft SQL
- My SQL
- Oracle RDBMS
- Postgres



Hardware Security Modules

- Generic HSMs support - PKCS11
- Entrust - nShield
- Thales - Luna 4, 5, 6, 7
- Yubico - YubiHSM 2
- Utimaco - Security Server

Identity and Authentication

- API Key
- Certificate Logon
- CSV Export and Import of Users
- FIDO
- Key DB/ Redis - In Memory DB/Cache
- LDAP/S such as AD LDS, View DS and Open LDAP
- Microsoft AD
- Microsoft AAD
- MidPoint
- OTP - TOTP and HOTP
- SCIM
- Smartcard and Tokens such as Yubikey and Titan

JellyFish Integrations

Fact Sheet

Key Management

- AWS - Generation, Wrapping and Archive/Restore
- Azure - Generation, Wrapping and Archive/Restore
- BYOK
- GCP - Generation, Wrapping and Archive/Restore
- Salesforce
- SSH keys - Discovery, Alerting, Monitoring, Reporting, Enrolment, Auto-Enrolment, Rotation

Infrastructure Supporting Services

- Generic: Anything supporting our standard protocols such as AEX, ACME and SCEP
- Consul - Service Discovery
- Graylog - SIEM
- HA Proxy
- Linux - OS: REHL, Ubuntu, etc
- Key DB/Redis - In Memory DB/Cache
- Kubernetes - Container Orchestration
- Nagios - monitoring and Alerting
- Proxmox - OS and HyperVisor
- Rabbit MQ - Message Queue
- Windows Desktop - OS
- Windows Server - OS and HyperVisor

Networking Infrastructure Support

- Generic: Anything supporting protocols such as SCEP
- Cisco - Firewalls, Switches, Routers, Access Points
- Draytek - Firewalls, Switches, Routers
- F5 - Big-IP
- Fortinet - Firewalls
- Netgear - Switches, Routers, Access Points
- Palo Alto - Firewalls
- Sonic Wall - Firewalls
- TP-Link - Firewalls, Switches, Routers, Access Points
- Ubiquiti - Switches, Routers, Access Points

PACs/EACs

- Gallagher PACs
- Lenel
- Protege PACs
- WHO's On Location Visitor Management
- Vecos/Vidak Locker Management

IT Service Management

- BMC/Remedy
- Service Now

Standards and Protocols

Protocols

- ACME
- ACME+ (Cogito expanded protocol)
- FIDO CTAP 2.1
- Microsoft Autoenrol - MS-WCCE: Windows Client Certificate Enrollment Protocol
- Microsoft Autoenrol - MS-WSTEP: WS-Trust X.509v3 Token Enrollment Extensions
- Microsoft Autoenrol - MS-XCEP: X.509 Certificate Enrollment Policy Protocol
- MIFARE DESFire
- PIV (Personal Identification Verification)
- PKCS1 (RSA Standard)
- PKCS5 (Password-based cryptography standard)
- PKCS7 (Signed-Data/SOD standard)
- PKCS8 (Private Key standard)
- PKCS10 (CSRs/Certificate Signing Requests standard)
- PKCS11 (HSM comms protocol)
- PKCS12 (P12s/PFX standard)
- RADIUS
- RadSec
- Redis
- SCEP
- SECG 1 (ECC Standard)
- SCIM
- Syslog
- W3C Web Authentication Level 3 used for FIDO

Main RFCs

- RFC-2315 - PKCS7 RSA standard
- RFC-2986 - PKCS10 CSRs standard
- RFC-3394 - AES wrapping spec
- RFC-5208 - PKCS8 standard
- RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- RFC 5652 - Cryptographic Message Syntax (CMS)
- RFC-5639 - Brainpool Elliptic Curve Cryptography standard
- RFC-7292 - PKCS12 standard
- RFC-8017 - PKCS1 standard
- RFC-8018 - PKCS5 Password-Based Cryptography standard)
- RFC 8812 - CBOR Object Signing and Encryption used with FIDO
- RFC 8555 - Automatic Certificate Management Environment (ACME)
- RFC 8894 - Simple Certificate Enrollment Protocol
- RFC-6960 - X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP

Tooling & Infrastructure

Audit /Logging

- Graylog
- RabbitMQ
- Syslog
- Syslog feeds

Configuration and Availability

- Consul centralised microservice configuration
- HA Proxy
- Key DB

Database- Data Storage

- Dgraph/GraphQL
- Key DB/Redis - In Memory DB/Cache
- PostgreSQL

About Cogito Group

Cogito Group is an award-winning, Australian owned and operated ICT company, specialising in authentication, cloud security, identity management and data protection. Cogito Group protect the authentication methods used to access information through the use of Identity and other security technologies. Cogito Group protect data not only from unauthorised access and disclosure, but also from being altered by an unauthorised third party or a trusted insider with malicious intent. This assists in the detection and prevention of fraud or other malicious activities by third parties or trusted insiders.