Factsheet

Cogito Group

Cloud Certificate Management Comparison

Cloud Certificate Management

Cloud based certificate management is offered by each of the major cloud vendors. The level of certificate management capability provided by these vendors varies and is usually limited to the certificate used within the services provided by the cloud provider.

This factsheet provided a comparison of the capabilities provided by the cloud providers and compares those to the capability provided by Cogito Group's Jellyfish product and SecureSME platform.

The Platforms

GCP Certificate Manager (GCP CM)

GCP Certificate Manager is a fully managed service from Google Cloud Platform (GCP) that helps you provision, manage, and deploy TLS/SSL certificates for your applications running on GCP. It was created to simplify and automate how certificates are handled for services like load balancers, cloud run services, and Google Kubernetes Engine (GKE) clusters.

Azure Key Vault (AKV)

Azure Key Vault is a cloud service offered by Microsoft Azure that provides a secure and centralized platform to manage cryptographic keys, secrets (such as API keys, passwords), and certificates. It is designed to help safeguard cryptographic keys and secrets used by cloud applications and services, ensuring that sensitive information is stored securely and that access is tightly controlled and monitored.

Microsoft Cloud PKI (MCPKI)

Microsoft Cloud PKI is a cloud-based service for Microsoft Intune that simplifies and automates certificate lifecycle management for Intune-managed devices. It provides a dedicated PKI for an organization without requiring on-premises servers, NDES, Intune certificate connectors, or customer-managed hardware. Microsoft Cloud PKI supports private certificate issuance, renewal, revocation, SCEP-based certificate registration, cloud-hosted CRL and AIA endpoints, reporting, RBAC, and deployment models using either Microsoft Cloud PKI root and issuing CAs or bring-your-own CA (BYOCA) anchored to an existing private CA.

AWS Certificate Manager (ACM)

AWS Certificate Manager is a service by Amazon Web Services that enables users to easily provision, manage, and deploy public and private TLS/SSL certificates for securing websites and applications. ACM handles much of the heavy lifting involved in managing certificates—including issuing, renewing, and deploying them—especially across services like Elastic Load Balancing (ELB), CloudFront, and API Gateway.

Active Directory Certificate Services (ADCS)

Active Directory Certificate Services (ADCS) is a Windows Server role developed by Microsoft that provides a customizable Public Key Infrastructure (PKI) for issuing and managing digital certificates. ADCS enables organizations to create and manage their own certificate authority (CA) hierarchy for use within their enterprise network.

Although ADCS is primarily an on premise CA solution it is included here for completeness as a CA with a large deployment footprint.

Factsheet

Cogito Group

Cloud Certificate Management Comparison

Feature Comparison Matrix

Feature	SecureSME (Cogito aaS)	Jellyfish (Cogito on Premises Software)	Azure Key Vault	Microsoft Cloud PKI	GCP Certificate Manager	AWS Certificate Manager (ACM)	AD CS
Cloud-Native Integration	✅ Cloud service delivery, supports multi-cloud & hybrid auth	✅ Integrates with all major clouds + on-prem	✅ Azure-native	✅ Intune-native	✅ GCP-native	✅ AWS-native	❌ On-prem only or VM in cloud as not cloud native
AWS Services Support	✅ Supported	✅ Supported	❌ No Support	❌ No Support	❌ No Support	✅ Supported	❌ No Support
Azure Services Support	✅ Supported	✅ Supported	✅ Supported	❌ No. Intune only	❌ No Support	❌ No Support	❌ No Support
Highly Available Configuration	✅ Supported	✅ Supported	✅ Supported	✅ Supported	✅ Supported	✅ Supported	❌ No Support
Post Quantum Support	✅ Supported	✅ Supported	❌ No for standard ✅ Yes for HSM	❌ No Support	✅ Supported	✅ Supported	❌ No Support
Multiple CAs hosted on one software instance	✅ Supported	✅ Supported	✅ Supported	❌ No Support	✅ Supported	✅ Supported	❌ No Support
Full Certificate Lifecycle Management	✅ Supported	✅ Supported	❌ No Support	❌ No Support	❌ No Support	✅ Supported	❌ No Support
Key Management (KMS)	✅ Uses certs for identity/access enforcement, integrates with trusted key stores	✅ Supports external and internal key sources including HSM (FIPS 140-2)	✅ With Azure Key Vault Keys	✅ Microsoft-managed CA keys; HSM-backed with licensed service	✅ Uses Cloud KMS	✅ KMS + CloudHSM	✅ With HSMs

Cloud Certificates Comparison

Factsheet

Feature	SecureSME (Cogito aaS)	Jellyfish (Cogito on Premises Software)	Azure Key Vault	Microsoft Cloud PKI	GCP Certificate Manager	AWS Certificate Manager (ACM)	AD CS
Certificate Issuance (Public)	✅ Validates external certs for user access, mutual TLS	✅ Supports public cert chains and trust store integration	⚠️ Limited (via partners)	❌ Private device certificates only	❌ Requires external CA	✅ Fully managed public certs	❌ Not built-in
Certificate Issuance (Private)	✅ Uses Jellyfish as source of truth for trusted issuers	✅ Full certificate lifecycle platform for internal PKI	✅ With Azure Managed CA	✅ Issues SCEP certs to Intune-managed devices	✅ GCP Private CA	✅ AWS Private CA	✅ Core feature
Certificate Auto-Renewal	✅ Maintains access rules based on active/valid certs	✅ Full automation with policy-driven renewal and expiry notifications	✅ For Azure resources	✅ For Intune SCEP profiles	✅ For Google-managed certs	✅ For AWS workloads	⚠️ Manual/scripting
Support for External PKI / CA	✅ Federates trust across environments; client CA chains validated at auth	✅ Import/export support; root/intermediate management; CA hierarchy controls	⚠️ Limited	✅ BYOCA anchors to AD CS or private CA	✅ Supports external bundles	✅ Import trust bundles	✅ Native AD trust support
HSM Support	✅ Uses Jellyfish's key management and validation engine	✅ Yes, FIPS 140-2 certified HSMs for key storage	✅ Azure Managed HSM / BYOK	✅ Azure Managed HSM-backed CA keys; trial CAs use software keys	✅ Cloud HSM / External CA	✅ CloudHSM, BYOK	✅ With integration
Audit Logging & Monitoring	✅ Daily review of all logs/events, feeds SIEM	✅ Comprehensive audit trail + SIEM integration	✅ Azure Monitor	✅ Intune dashboards + admin audit actions	✅ Cloud Audit Logs	✅ AWS CloudTrail	⚠️ Event logs only
API / SDK Access	✅ Full API exposure for identity management	✅ RESTful APIs for integration with	✅ REST, PowerShell, SDKs	⚠️ Primarily Intune admin centre and	✅ REST, gcloud CLI	✅ REST, SDKs	⚠️ Limited

Cloud Certificates Comparison

Factsheet

Feature	SecureSME (Cogito aaS)	Jellyfish (Cogito on Premises Software)	Azure Key Vault	Microsoft Cloud PKI	GCP Certificate Manager	AWS Certificate Manager (ACM)	AD CS
	and session enforcement	DevOps, SCEP, ACME, and more		device profiles			
Role-Based Access Control (RBAC)	✅ Access policies enforce RBAC at per-service and per-user level	✅ Multi-tenant RBAC, delegated admin, policy templates	✅ Azure AD-based	✅ Intune RBAC + scope tags	✅ GCP IAM	✅ IAM policies	✅ AD-based
Policy Enforcement (Expiry, Key Length)	✅ Session duration, cert validity, role restrictions configurable	✅ Enforces minimum key length, allowed issuers, expiry windows	⚠️ Basic expiry and renewal rules	✅ SCEP profile controls for validity, renewal, EKU and key size	✅ Templates and policy sets	⚠️ Basic expiration controls	✅ Via templates
Multi-Cloud/On-Prem Management	✅ Designed for external multi-cloud user access and control	✅ Native support for hybrid + multi-cloud environments	❌ No	⚠️ Intune endpoint focused; BYOCA only, not general lifecycle	❌ No	❌ No	⚠️ On-prem focused only
Non-Repudiation / mTLS / Cert-Based Auth	✅ Yes, used for all user/service access – built for non-repudiation compliance	✅ Supports mTLS, mutual auth, cert mapping, and transaction signing	⚠️ Limited support	⚠️ Enables device client auth; not full non-repudiation platform	❌ No	❌ No	⚠️ Configurable
Compliance / Governance Support	✅ Aligned with DISP, Gatekeeper, and Zero Trust governance	✅ Designed to support ISM, DISP, ISO27001, Gatekeeper	✅ SOC2, ISO, etc.	✅ Microsoft cloud controls; tenant governance dependent	✅ Compliance-aligned	✅ Compliant services	⚠️ Depends on deployment

Cloud Certificates Comparison Factsheet

Multi-Environment Certificate Management Capability Matrix

Platform	Multi-Cloud / On-Prem Management	Key Highlights
Azure Key Vault	❌ Primarily for Azure. No direct multi-cloud or on-premise certificate lifecycle management. Export/import for certs is limited to un-managed certs.	Great for Azure-native services.
Microsoft Cloud PKI	⚠️ Primarily for Intune-managed Android, iOS/iPadOS, macOS, and Windows devices. Can anchor to existing private CAs using BYOCA, but is not a general multi-cloud workload certificate lifecycle platform.	Cloud-hosted PKI in Intune with SCEP registration authority, HSM-backed CA keys, CRL/AIA hosting, reporting, RBAC, and revocation for issued leaf certificates.
GCP Certificate Manager	❌ Designed only for Google Cloud workloads. No direct cross-cloud support.	Suitable for GCP-managed certs, but lacks external integrations.
AWS ACM	❌ AWS-centric. Public certs can't be exported; private certs can be, with limitations.	Excellent for AWS workloads but not usable elsewhere without external integration.
AD CS	✅ Yes, via Group Policy, SCEP, and scripting. Supports on-prem and can be adapted for cloud use with effort.	Requires manual configuration or external automation tools.
Jellyfish (Cogito)	✅ Yes. Designed to manage certificates across hybrid, multi-cloud, and secure enclaves. Integrates with AD CS, Azure Key Vault, AWS, and GCP. Supports cert issuance, renewal, and role-based access.	Policy-driven, fully auditable PKI and certificate management platform. Integrates with HSMs and external CAs.
SecureSME (Cogito)	✅ Yes. Extends Jellyfish's capabilities to customer-facing services. Provides authentication (incl. cert-based), enforcement of certificate trust chains, revocation, and reporting.	Designed for secure service delivery. Supports mutual TLS, client cert auth, and federation.

Key Observations

- Jellyfish fills a major gap in cross-platform certificate management — none of the native cloud tools can manage external certs across environments.
- SecureSME builds on Jellyfish's authority to enforce trust, access, and identity rules in customer-facing or federated environments.
    - Microsoft Cloud PKI reduces AD CS, NDES, and Intune connector overhead for Intune-managed device certificates, but remains endpoint-focused.
    - Native cloud tools, including Microsoft Cloud PKI, are optimized for their own management planes; Jellyfish is broader where central policy, audit, and lifecycle management must span clouds, on-premise environments, and secure enclaves.
- Tools like AWS ACM, Azure Key Vault, Microsoft Cloud PKI, and GCP Certificate Manager are optimized primarily for their own clouds or management planes.
- AD CS remains flexible on-prem, but lacks automation and cloud awareness.

How Jellyfish and SecureSME Stand Out

Jellyfish

- Purpose-Built for Hybrid Environments: Integrates with cloud-native CAs (Azure, AWS, GCP), on-prem AD CS, and third-party PKIs.
- Certificate Lifecycle Management: Full automation for issuance, renewal, revocation, suspension, with policy enforcement.
- API & UI Driven: Rich REST API and role-based web interface.
- Key Features:
    - Federation-ready
    - SCIM and SAML support
    - Certificate profiling and templating
    - Detailed logging and audit for compliance
    - HSM-backed key storage (FIPS 140-2)
    - Multi-tenancy with delegated administration

SecureSME

- **Designed for Externalization:** Provides secure, certificate-backed access control to customer environments and services.
- **Supports Federated Identity:** Works with Azure AD, Entra ID, and third-party IdPs. Offers SAML, OpenID Connect, and certificate-based login.

- **Built-In Certificate Trust Chains:** Validates external and internal certificates, supports CRLs and OCSP.
- **Security Features:**
    - TLS mutual auth for APIs and service endpoints
    - Certificate-based non-repudiation for transactions
    - Audit integration with SIEM
    - Managed session controls and MFA

When to use Jellyfish, SecureSME

Use Case	Recommended Platform
Certificate management across AD CS, AWS, Azure, GCP, and other environments	Jellyfish
Automated renewal of server/client certs	Jellyfish
Providing secure certificate-based user access	SecureSME
Integrating PKI into Zero Trust architecture	Jellyfish + SecureSME
Meeting ISM/IRAP or DISP compliance for certs	Jellyfish (backed by HSM)
Federation with external agencies	SecureSME

Summary

Microsoft Cloud PKI is a useful managed option for Intune-managed device certificate issuance, particularly where an organisation wants to reduce AD CS, NDES, and connector dependencies. However, only a few platforms — notably Jellyfish and SecureSME — offer complete multi-cloud and on-premise certificate lifecycle management with the flexibility, compliance, and control required in regulated or hybrid environments. They are especially suitable where:

- You need central control but operate across multiple clouds and datacentres.
- Compliance (e.g., ISM, IRAP, DISP) mandates strict visibility and audit of certificates.
- Certificate-based non-repudiation, federation, or mTLS is critical.
- You require orchestration of certificate lifecycle, trust enforcement, and audit across multiple environments.

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.