Fact Sheet

Cogito Group

Jellyfish Token Support

The Challenge

Modern digital security is built on digital keys and unique credentials. To ensure the safety of systems and information, cryptographic tokens such as smartcards or HSMs are used to protect keys. These keys need to have protection commensurate with what they protect. The challenge is ensuring the security of an organisation's keys while being able to use, monitor and control them efficiently. Cogito Group's Jellyfish Command and Control Platform is purpose-built to improve how you manage current security components, such as token management and enhance future capabilities to support these tokens.

The Solution

Cogito Group's Jellyfish is a complete and integrated cyber security platform that responds to this need for holistic identity, credential, and access management. It enhances your security through increased visibility, greater control, stronger protection, and seamless authentication in one centralized management interface.

Jellyfish provides a one-stop-shop to manage your organisation's tokens and keys. Jellyfish supports a wide range of soft keys, hard tokens like smartcards and FIDO tokens, as well as HSMs. It also has the agility to add support for more. Jellyfish can be deployed on-premises or as-a-service subscription to control and manage your tokens. It is purpose-built to be customisable, modular, and scalable - adapting to an organisation's individual requirements.

Figure 1 - Token on Jellyfish Mobile Platform

Jellyfish Token Support

Fact Sheet

Jellyfish Smartcard Support

What are Smartcards?

Smartcards are cards that have an embedded, integrated circuit or 'chip' in them. They are used to improve security when accessing information, locations, or equipment. Smartcards are often used as a replacement for traditional physical access control methods, allowing one Smartcard to replace numerous keys, cards, and PIN entry systems. Smartcards provide additional assurance when securing digital transactions or gaining logical access to systems.

Jellyfish manages the full lifecycle of smartcards. Configure, personalise, renew, cancel, and control access of a user via a smartcard - all from the Jellyfish platform.

If the smartcard has cryptographic token interface standard PKCS #11 or PIV, Jellyfish can support it. Jellyfish also supports the use of other platforms like using YubiKey as a Smartcard (this is explored later in this factsheet) or a FIDO token.

Figure 2 - Traditional Form Factor Smart Card

Current card support:

- AB Corp: JCOP ID 180ABC_PIV
- Athena: IDProtect - deprecated
- Datacard: DK330 - deprecated
- Feitian: A22CR, ePass, K9, K40
- Giesecke+Devrient: SCF 7.1 P60, SmartCafe Expert 64K
- Gemalto: ID Prime MD 840/930
- HID: Crescendo
- IDEMIA/Oberthur: ID-One PIV 2.4, ID-One PIV 2.4.2
- NXP: JCOP 3 SecID P60 CS, JCOP 4 P71
- PIVKey C910, C920, T800
- Placard: P60, P71
- SafeNet: 4100, 4300 - deprecated
- SafeNet: 5110
- SafeNet AT (previously Safenet): SC650
- Yubico: Yubikey v4 and v5 (PIV, FIDO in all form factors)

Given Cogito Group's strong partnership with Thales who now own the Gemalto, Gemplus and Safenet brands, Jellyfish already supports this family of cards. Some family of cards work the same way as those listed, meaning Jellyfish is interoperable with a wider number of cards.

Cogito can also configure access to a pre-existing Physical Access Control System (PACS) in Jellyfish. As mentioned, Jellyfish is purpose-built to be customisable. Custom solutions are available to fit specific use-cases.

Jellyfish Token Support

Fact Sheet

Jellyfish HSM Support

What is an HSM?

A Hardware Security Module (HSM) is a dedicated crypto processor. HSM's are tamper-resistant devices that protect the crypto key life cycle. HSMs act as trust anchors and protect some of the most security-conscious organisations in the world. They do this by managing, processing, and storing cryptographic keys. HSMs are also optimised for key transactions giving greater performance where secure key transactions are performed.

Thales Utimaco Entrust

Figure 3 - Jellyfish Compatible HSMs

Jellyfish provides a centralized management interface to integrate with these devices. Organisations can install the Jellyfish platform on their servers locally or connect remotely into the Cogito Group servers. Jellyfish can support an organisation holding their own key (HYOK) or Cogito Group can hold it for them in their HSM (BYOK).

Bring Your Own Key (BYOK) allows clients to use keys not related from their cloud services vendor. They can generate their own key or use a third-party key provider. Hold Your Own Key (HYOK) allows customers to keep their key in an on-premises service and manage all encryption and decryption with their own hardware.

Jellyfish HSMaaS (HSM as a Service) also known as usCrypto provides:

- Key Generation
- Key Deletion
- Key Usage such as:
  - Signing of: Digests, PDF Documents, Executables (Code Signing) and ePassports (SODs)
  - Encryption
- Key Import
- Key Export such as:
  - Azure BYOK
  - AWS BYOK
  - Salesforce BYOK
- Key Management through the Jellyfish interface

Current HSM Support:

- Entrust (formerly nCipher and Thales) nShield Connect 1500/6000, XC
- Entrust (formerly nCipher and Thales) nShield Edge

- Gemalto (see Thales)
- nCipher (see Entrust)
- Safenet G5 (yes, see Thales)
- Safenet Luna v4, v5, 6 (see Thales)
- Thales (formerly Gemalto and Safenet) Luna v7
- Utimaco SE12, 52, 500, 1500
- Yubico YubiHSM2 (new)

Jellyfish also supports Luna and nShield for use with Smartcard management for the storage of the master (factory and customer) keys.

Jellyfish YubiKey Support

What is a YubiKey?

Yubico's award-winning security key, the YubiKey, is a hardware authentication token. It is a type of cryptographic token used to gain access to an electronically restricted resource. They are used in addition to or in place of a password - like an electronic key.

Figure 4 - Yubikey 5 Series USB Smart Card

With Jellyfish, users can manage their entire organization's YubiKeys in one central place. Keys can be issued to a user, credentials can be added, modified, and deleted, and the YubiKey token and related credentials can be cancelled all from within Jellyfish. The Jellyfish platform brings together features such as Identity Management, Configuration Management Databases and Token Management Services. Jellyfish and YubiKeys allow for relationships to be built between Yubico devices, other devices, services, and users, as well as the credentials held on the Yubico devices. Full reporting is also available and can be customized to focus on multiple or single aspects of the token use.

Jellyfish works with the following compatible YubiKeys:

- YubiKey 4/5 Series (PIV and FIDO)
- YubiKey Bio Series
- YubiKey FIPS Series
- Security Key Series
- Legacy YubiKeys

Jellyfish Token Support

Fact Sheet

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.