Fact Sheet

Cogito Group

SCEP

Simple Certificate Enrolment Protocol - SCEP

The next generation of Certificate Automation

Simple Certificate Enrolment Protocol (SCEP) is an open-source protocol that allows devices to easily enrol certificates from a PKI using a securely encrypted URL. It is widely used to make digital certificate issuance at large organisations easier, more secure, and scalable.

Cogito Group's implementation of SCEP, through Jellyfish, is fully compliant with RFC 8894, and the Cryptographic Message Syntax defined within.

Why SCEP?

There are some key use cases for an organisation to the SCEP protocol. This includes:

- Wifi Authentication
- VPN Authentication
- Client/Server authentication
- Secure Email
- Access to Managed Company Resources

Distributing certificates to managed devices can be overwhelming and time consuming. There are a lot of moving parts that need to be accounted for. This includes:

- Device authentication
- PKI integration
- Establishment of a gateway
- Configuration policies
- Certificate enrolment

SCEP streamlines the certificate enrolment process on managed devices. An administrator can automatically enrol every managed device for a client certificate without requiring any end user interaction.

Primary Method of Automatic Enrolment

SCEP is the primary method of automatic enrolment for devices deployed through Microsoft Intune, Autopilot and Company Portal software. SCEP is also favoured among Linux, Mobile, and 'Internet of things' devices like Office Phones and Printers.

SCEP

Fact Sheet

Jellyfish Intune Security

Cogito Jellyfish Intune SCEP Connector provides the highest level of security possible within the Microsoft Intune implementation of the Simple Certificate Enrolment Protocol (SCEP).

Intune supports use of the Simple Certificate Enrolment Protocol (SCEP) to authenticate connections to your apps and corporate resources. SCEP uses the Certification Authority (CA) certificate to secure the message exchange for the Certificate Signing Request (CSR).

The process involves a three step 'handshake' in which the device:

1. Determines the capabilities of the SCEP server.
2. Verifies the authenticity of the servers SCEP certificate.
3. Submits a CSR for issuance to the CA.

The authentication and validation procedure of this flow is implemented through an API request from usSCEP to the Microsoft Graph API. This request is a sequence of two subsequent requests, the first request reads the Service Principal Endpoints for the Intune 'Azure Application', this provides an address for which to submit a SCEP challenge request.

In the Microsoft Intune SCEP request flow, validation of the device or app occurs after the CSR is generated, but before the CSR is signed.

The Jellyfish Microsoft Intune SCEP procedure is outlined in the diagram below.

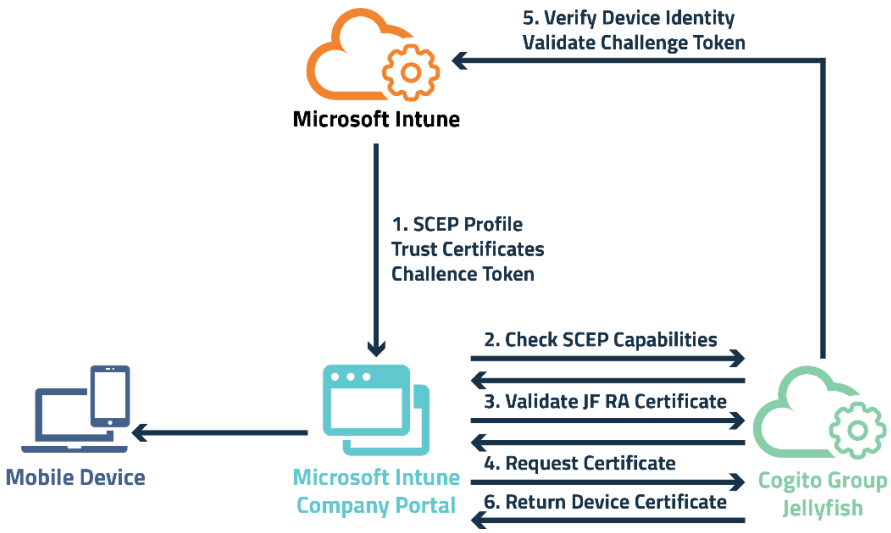

Figure 1 - Jellyfish SCEP Intune Verification Process

Azure Intune uses the whole Certificate Signing Request (CSR) as the 'challenge'. This is a distinction from the Simple SCEP implementation in which a 'pre-shared secret' is used as validation.

SCEP

Fact Sheet

The SCEP certificate Device Configuration Profile (SCEP profile) takes the form of an exact match whitelist. The SCEP profile defines exactly which Subjects, Subject Alternatives Names, Key Usages, Extended Key Usages, Key Sizes, Hash Algorithms, and more MUST be included in a CSR intended for enrolment using this SCEP Profile. The SCEP Profile is permissioned against a set of Included and Excluded Azure Active Directory Users or Groups.

Cogito and the Jellyfish Software are not involved in the validation procedure beyond requesting validation of a CSR.

Why SCEP over NDES?

NDES is the Microsoft Network Device Enrolment Service based on the Simple Certificate Enrolment Protocol (SCEP). Basically, NDES is the Microsoft implementation of SCEP.

Using NDES over standard SCEP forces you to use Microsoft products as IIS (host for the NDES service) and ADCS.

Whereas, if you don't use NDES you can use CAs and PKI infrastructure from other vendors.

NDES also requires a lot of installations and configurations, whereas the Jellyfish SCEP connector requires none.

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.