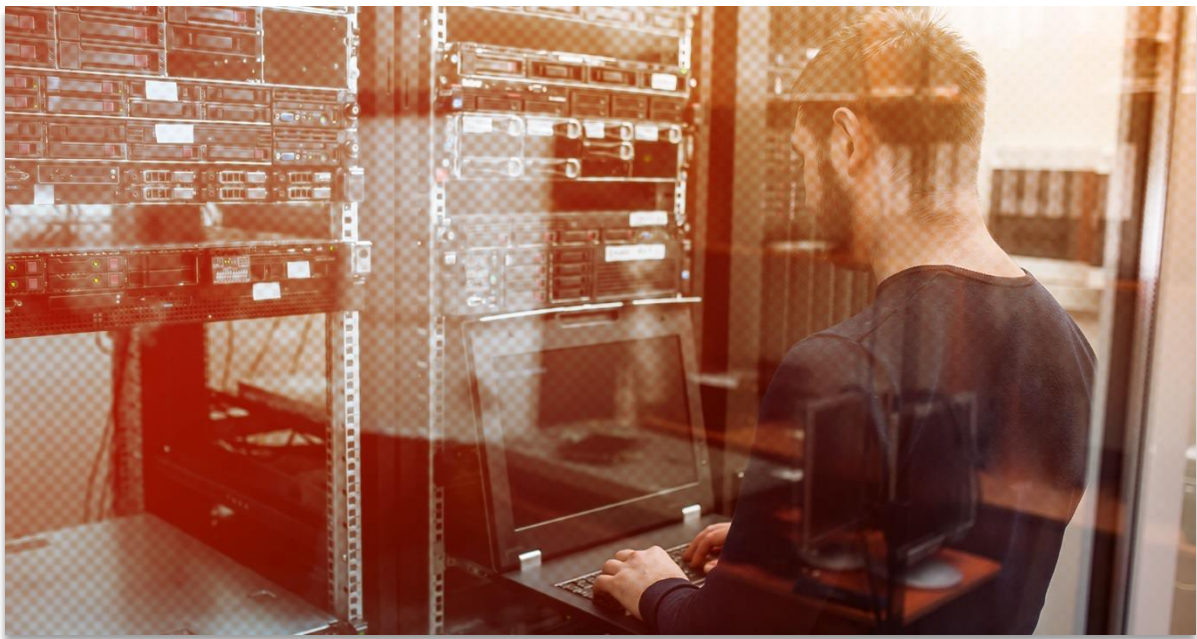


Whitepaper

Securing a cloud-based IT Infra for 30,000+ devices

The world is changing rapidly and the acceleration is increasing every decade. Modern companies and organizations are adapting to an IT infrastructure that is fully scalable and accessible from anywhere via the internet, so that employees can work and collaborate from anywhere in the world.



Contents

The Challenge.....	3
The Solution.....	3
The Hurdles.....	4
KeyTalk.....	4
KeyTalk – Intune – SCEP connector	4
Customer Reporting.....	5
The Result.....	6

The Challenge

A large globally operating customer, faced the challenge 3 years ago to operate securely without the facilities of the parent company. This meant building a flexible IT infrastructure that would be able to support 30,000+ users worldwide in a short period of time.

Given this enormous challenge, the company chose to design a new fully 'Cloud'-based IT Infrastructure that can quickly and securely provide all employees, at home or at one of the thousand locations in the world, with a workplace. A key challenge was creating secure network access without the hassle of cumbersome password management.

The Solution

The company opted for 802.1x EAP/TLS certificate-based authentication, where each approved corporate device gains access to the global corporate network based on a short-lived authentication certificate and cryptographic key pair for securely encrypted access.

GlobalSign was chosen as a Certificate Authority provider of both the private authentication and server certificates and the publicly trusted server certificates (TLS/SSL) with all certificates being issued by GlobalSign's modern and fully certified, high volume Atlas issuance platform. As a result, the company is assured of meeting strict CAB Forum control and compliance rules in the field of PKI. By choosing a short-lived authentication certificate, she ensured that all devices are periodically validated in order to maintain secure access to the company network.

But how can such an authentication certificate be requested quickly and easily in the right way, rolled out to the right device and then managed and replaced in time? Microsoft Intune for both corporate and Bring Your Own (BYO) devices was chosen as the foundation of the solution given the MS Azure experience of the IT team.

The Hurdles

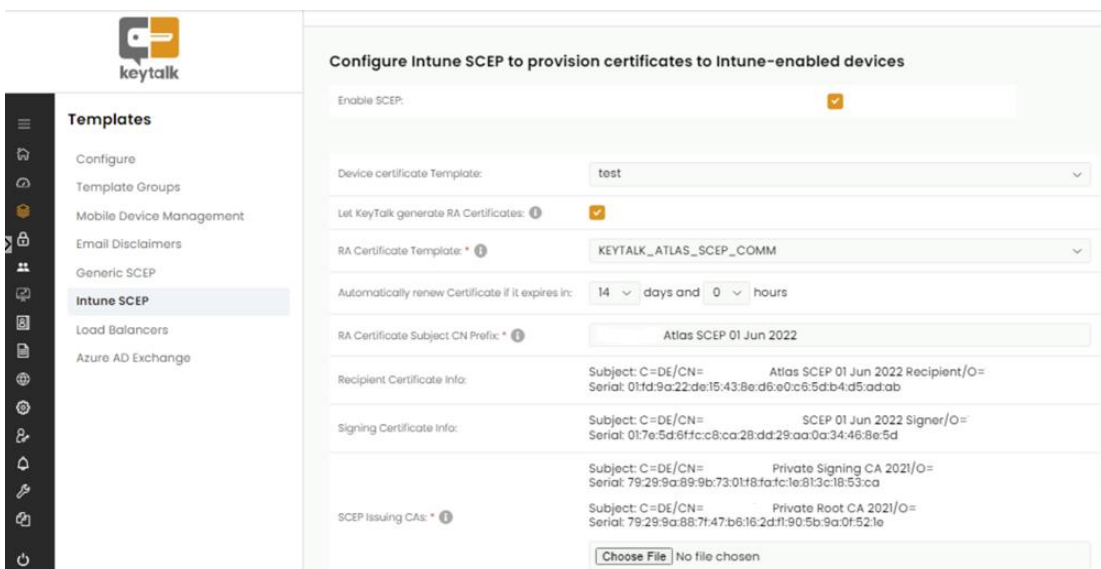
But how does an Intune-managed device request an authentication certificate from a public CA such as GlobalSign, so that it is clear at any time which devices;

- Successfully obtained a certificate;
- Expected to renew their authentication certificate in the coming days;
- Have not received a certificate and why not;
- Have not renewed their authentication certificate in time;
- Are not yet provided with a valid authentication certificate.

KeyTalk

For this, the KeyTalk Certificate & Key Management System (CKMS), hosted on the private Azure cloud platform, has been chosen as the critical solution for processing and managing the certificate requests from 30,000+ devices. The KeyTalk CKMS servers are installed in an N+1 Active-Active configuration across multiple global regions in conjunction with Azure LoadBalancers, Cloud-based Utimaco HSMs, and a robust and fully scalable Azure MySQL database that encrypts all device certificate management information.

KeyTalk – Intune – SCEP connector



The screenshot displays the KeyTalk web interface for configuring Intune SCEP. The left sidebar shows a navigation menu with 'Intune SCEP' selected. The main content area is titled 'Configure Intune SCEP to provision certificates to Intune-enabled devices'. The configuration includes:

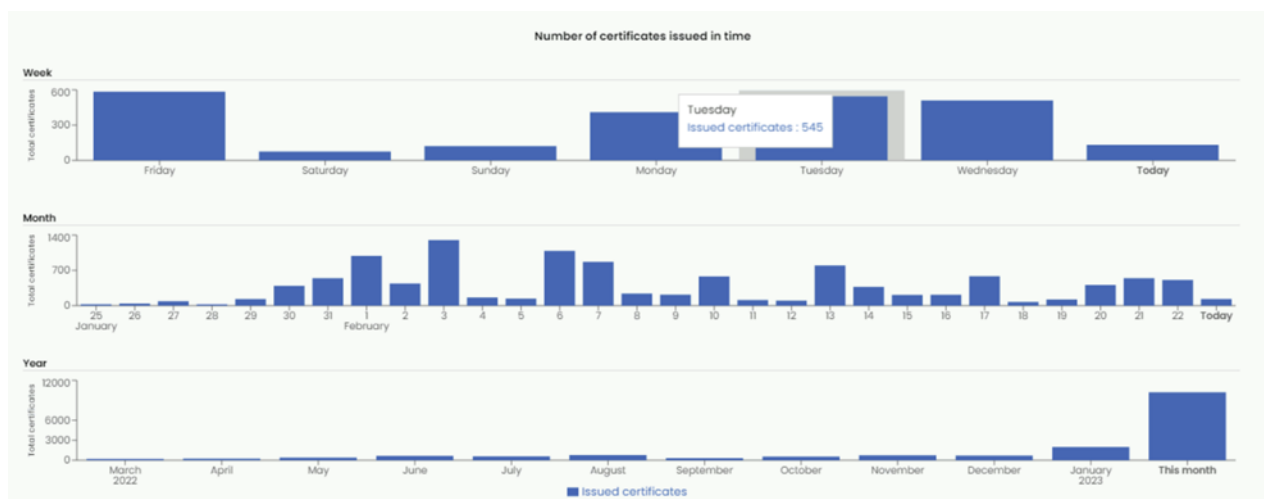
- Enable SCEP:** A checkbox that is checked.
- Device certificate Template:** A dropdown menu set to 'test'.
- Let KeyTalk generate RA Certificates:** A checkbox that is checked.
- RA Certificate Template:** A dropdown menu set to 'KEYTALK_ATLAS_SCEP_COMM'.
- Automatically renew Certificate if it expires in:** A field set to '14' days and '0' hours.
- RA Certificate Subject CN Prefix:** A text field containing 'Atlas SCEP 01 Jun 2022'.
- Recipient Certificate Info:** A text field showing 'Subject: C=DE/CN= Atlas SCEP 01 Jun 2022 Recipient/O= Serial: 01:fd:9a:22:de:15:43:8e:d6:e0:c6:5d:b4:d5:ad:ab'.
- Signing Certificate Info:** A text field showing 'Subject: C=DE/CN= SCEP 01 Jun 2022 Signer/O= Serial: 01:7e:5d:61:fc:c8:ca:28:dd:29:aa:0a:34:46:8e:5d'.
- SCEP Issuing CAs:** A section with two entries: 'Private Signing CA 2021/O=' and 'Private Root CA 2021/O='.
- Choose File:** A button labeled 'Choose File' with the text 'No file chosen'.

After all profiles have been rolled out and applied to the devices via MS Intune, the devices are instructed to retrieve an authentication certificate from the KeyTalk servers based on [the Intune SCEP protocol](#). The KeyTalk service acts like a SCEP proxy for GlobalSign Atlas, first verifying the request with MS Intune. Once Intune confirms authorization, the original SCEP-based Certificate Signing Request (CSR) is sent to GlobalSign Atlas, which then returns a signed certificate, or an error message if the CSR does not meet GlobalSign's requirements.

The KeyTalk service has meanwhile stored a copy of the issued and signed certificate in the encrypted KeyTalk database and forwards the certificate to MS Intune, which in turn forwards it to the relevant device where the public key is again linked with its own private key to a unique pair, where for Windows OS based devices the private key is stored on the local TPM chip, and then the correct Wifi 802.1x EAP/TLS profile is applied.

Customer Reporting

On a daily basis, this customer receives automated reports from the KeyTalk service about the progress of the certificate requests and rollout, so that the Workplace team can intervene quickly if reports of unsuccessful requests are received.



The Result

This results in a fully automated cloud-based authentication certificate management process for all devices that need to securely connect to their global IT network. If you have any questions about this modern and excellently working application in the cloud, [please contact us](#).

KeyTalk IT Security Software
website: keytalk.com
email: info@keytalk.com

Central office:

Maanlander 47
3824 MN Amersfoort
The Netherlands

Phone: +31 88 539 82 55