Microsoft AD CS Connector

Introduction

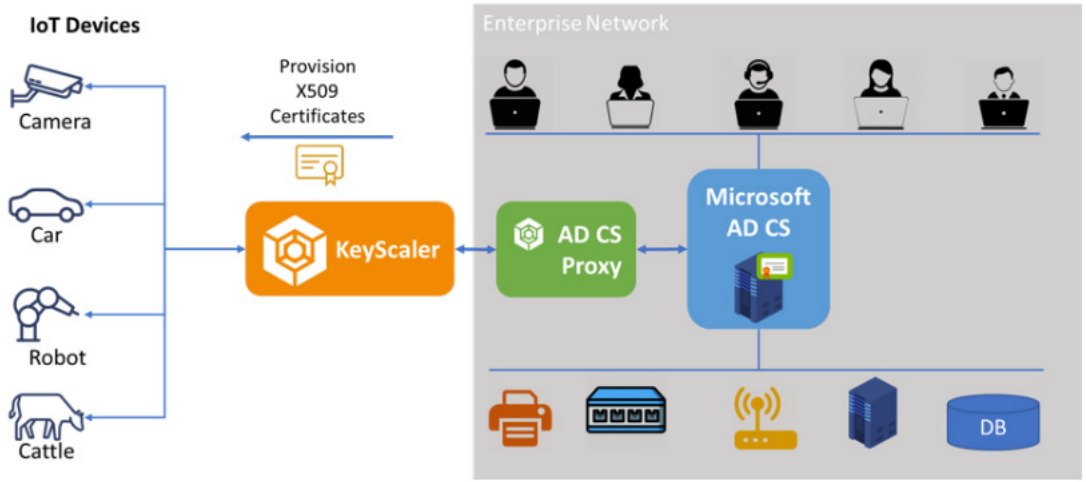
Today in enterprise networks there are a number of existing connections, such as users and network peripherals to an Active Directory Certificate Services (AD CS) server which provides the public key infrastructure (PKI) functionality; such as create, validate and revoke public key certificates for internal uses of an organization.

With the proliferation of the Internet of Things (IoT), many new types of devices, for example security cameras, connected cars, and industrial robots in manufacturing or hospital environments, also need access to the AD CS server. But as these devices are external to the enterprise network, they cannot connect to the AD CS server directly and managing the security for them is difficult and can be complex.

This connectivity and device security management can be solved with Device Authority's KeyScaler AD CS connector to provide the PKI functionality such as private certificate signing service from AD CS Server.

What is it?

The KeyScaler AD CS service connector is designed to provide public certificate signing service from Microsoft AD CS Server leveraging the existing Active Directory (AD) infrastructure and existing investments made in AD CS PKI infrastructure service.
This connector enables integration with existing Microsoft Active Directory Certificate Services to deliver signed X.509 certificates to IoT devices. This effectively enables KeyScaler platform to behave as a Registration Authority (RA) for Microsoft's private Certificate Authority (CA) service.



What are the benefits?

• Improve operational efficiency by leveraging existing investments in Microsoft infrastructure by including IoT devices that would not be normally part of the Enterprise network and provide public key cryptography

• Enhanced IoT device security by binding the device identity with corresponding digitally signed certificates

• Gain enhanced visibility of their device within enterprise services

• Extend & leverage AD CS features for IoT devices e.g. group policies making it easy to implement role or attribute-based access control

• Automated certificate provisioning and lifecycle management for Enterprise IoT devices

How does it work?

The KeyScaler AD CS service connector is an installable Windows service that acts as a connection proxy between KeyScaler and the Active Directory Certificate Services. It can be installed on the AD CS server itself, or on a separate Windows machine within the domain. The proxy application acts like a gate keeper which receives the requests from KeyScaler and then translates them into a format that Microsoft AD CS can interpret, for certificate signing, and revocation.

Step 1: Administrator configures the AD CS connector setting up KeyScaler as a Registration Authority.

Step 2: When a device powers up, it connects to KeyScaler and registers to the platform (assuming it is an authentic device)

Step 3: KeyScaler check the policies for the device to see what certificates it needs. In this example the device must go through a certificate provisioning process.

Step 4, 5 and 6: KeyScaler generates a CSR and send it to AD CS server via the Proxy application to get signed.

Step 7 and 8: The AD CS signed certificate is returned to the device via KeyScaler.

Interested in Learning More? Contact Us!

www.deviceauthority.com

info@deviceauthority.com

DEVICE AUTHORITY™