AUTOMATING CERTIFICATE MANAGEMENT WITH CERTACCORD™ ENTERPRISE

How to deploy certificate enrollment and automatic renewal across your entire network without needing PKI expertise

A Guide for IT Managers from Revocent Inc.

CONTACT US

sales@revocent.com | +1-408-638-9323 | revocent.com

Table of Contents

Overview

A core part of the cybersecurity infrastructure of many large enterprises is a Public Key Infrastructure (PKI) solution based on Microsoft Active Directory Certificate Services (ADCS). Such a PKI provides comprehensive security across the network and automates most aspects of managing a PKI including certificate provisioning and lifecycle management.

What's more, even for networks involving tens of thousands of users and systems within an Active Directory domain, day-to-day PKI management is easily accomplished by a small number of IT administrators thanks to the automation and integration ADCS provides. The situation is much different, however, for systems and applications outside the Microsoft eco-system. To take advantage of the Microsoft PKI, IT administrators must manually track, enroll, and renew certificates and keys on their own. This is not only inefficient and expensive, but opens the door to errors, missed renewals, and system outages.

CertAccord™ Enterprise by Revocent solves these problems by extending certificate enrollment, renewal, and trust of a Microsoft Certificate Authority (CA) to computers running Linux, MacOS, UNIX, and Windows. CertAccord Enterprise™ also does not just drop certificates onto the filesystem and walk away. It automates the integration and provisioning of X.509 certificates with applications, even Java applications on Windows. This eliminates the manual process of requesting, installing, and renewing certificates leading to reduced IT labor costs, fewer errors, elimination of missed renewals, improved security through consistent policy implementation, and scalability to support thousands or even tens of thousands of endpoints.

The growth of PKI in enterprises

Within enterprises, PKI has evolved from a means to protect websites to now sit at the heart of digital management functions within cybersecurity operations. It is used to manage digital identities of people and machines, applications, and devices within companies. It is also being adopted and deployed by IT teams to combat a growing variety of cybersecurity threats, ranging from stopping distributed denial of service (DDoS) attacks to thwarting malware, and phishing attempts to the preventing hacking of internet of things (IoT) devices.

While PKI is an integral part of keeping enterprises safe, deploying and managing a PKI can be a resource-intensive process, particularly as digital infrastructures and the role of PKI have continued to grow.

Adding to the value of automation, certificate lifetimes are getting shorter. Starting September 1, 2020, all browsers will only trust certificates that are no older that one year (398 days). To overcome the challenge presented by this additional workload, automated certificate monitoring and renewal is absolutely essential to keep your PKI up and running without interruption.

This white paper looks at the mandate for end-to-end certificate full lifecycle management and automation, key features of CertAccord Enterprise and its architecture, the certificate creation process from Linux and MacOS and the use of Certificate Appliers™ to automate application integration.

Role of Microsoft ADCS and PKI in Enterprises Today

Microsoft's Active Directory (AD) is by far the most widely used enterprise repository for digital identities. Microsoft Active Directory Certificate Services (ADCS) is a Windows server designed to issue digital certificates and is an optional, integrated component of AD. So, it's no surprise that ADCS has been widely embraced by enterprises around the world. Certificates have proven to be more secure and easier to use than passwords, and are far easier to deal with when certificate management is integrated into AD.

Microsoft realized this and developed ADCS to give Microsoft IT administrators the tools they needed to take advantage of all the security and usability benefits of PKI. Organizations running on Microsoft environments use their Microsoft CA to distribute certificates to domain-connected devices through group policies. An additional benefit is that Microsoft CA services are "free" because they're included with the Windows server.

For organizations operating an AD environment, the ability to leverage the certificate template information already included in Microsoft certificate services can make running a Microsoft CA extremely appealing. Since AD and Microsoft certificate services are connected, you can seamlessly register and provision certificates to all domain-connected objects based on group policies. Auto enrollment and silent installation make certificate enrollment and renewal easy for IT administrators and end users alike. There is no denying the benefits of integrating your certificate management processes with AD. What is needed then is a way to extend the benefits of ADCS to your entire network, not just systems joined to AD.

A PKI Ecosystem at a Glance

Microsoft ADCS allows companies to implement a complete PKI and to make effective use of public key cryptography. A PKI is what provides confidence that a public key found for any entity does indeed belong to that entity and not an attacker. As shown in **Figure 1**, a certificate authority sits at the core of any PKI. The CA is a trusted entity responsible for issuing, revoking, and publishing digital certificates.

Certificates are standardized using the X.509 format. Upon issuing a digital certificate the CA will use its private key to digitally sign it. An X.509 digital certificate that has been signed using cryptographic means includes information about who the certificate was issued to and when and how it was issued, among other details.

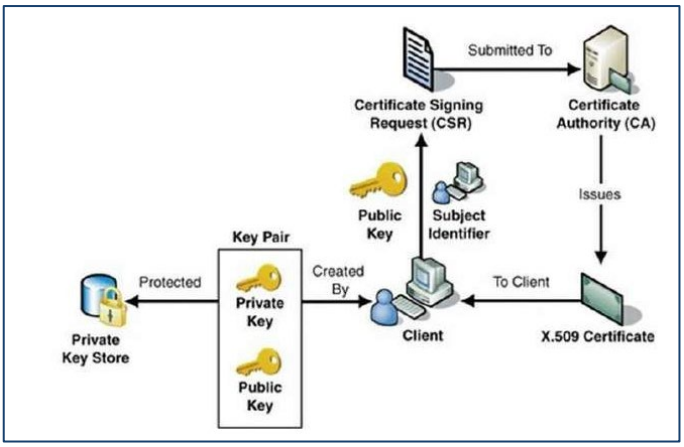

Figure 1. *A Certificate Authority (CA) sits at the core of a PKI*

Extending the Microsoft CA beyond Windows

The greatest advantage of the Windows PKI solution is automation, but that advantage does not extend to endpoints outside the Windows environment. Unfortunately, there are no free Linux or UNIX clients available today that provide auto-enrollment or integrate with the Microsoft PKI like the one built into Microsoft Windows.

Within enterprise networks, Linux is often used for critical services that require X.509 trusted certificates. One typical need is for an SSL/TLS Server Authentication certificate, commonly known as a web server certificate, on Red Hat Enterprise Linux (RHEL), Ubuntu server, or other Linux distributions.

The traditional process of creating a trusted certificate on Linux involves Linux IT admins using OpenSSL to create a private key and certificate signing request (CSR), emailing the request to the Microsoft PKI administrator, receiving back the certificate, and installing the certificate and key properly. Then you have to have some kind of out-of-band reminder to repeat this process before the certificate expires. Most of this process is usually done manually by IT staff.

This might be manageable for a dozen or so systems, but this scales very poorly. The usual results are certificates with long expiration times that exceed widely accepted safe durations. This can create a future potential vulnerability and/or certificates can expire without being renewed, thus causing a service outage. Using long, multi-year expiration times is far from ideal because the longer a certificate is valid, the more it is susceptible to weakened cryptography. Using shorter expiration times shortens the exposure to susceptible cryptography but comes at the cost of more frequent certificate renewals.

Moreover, IT administrators are human. They can forget things. They change jobs or move to a different company. They don’t always document their work. One thing they often forget or fail to document are the expiration dates for certificates. This leads to service outages and the associated $250,000 per hour average cost of such outages. Even if your IT admins have the memory of an elephant and the discipline of a Zen master, the labor costs of creating and managing large numbers of certificates in this manner is huge.

```
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:California
Locality Name (eg, city) []:San Jose
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Acme Inc
Organizational Unit Name (eg, section) []:IT
Common Name (e.g. server FQDN or YOUR name) []:www.my.com
Email Address []:it@my.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

Using OpenSSL to create a Certificate Signing Request (CSR) requires knowledge of enterprise PKI policies for keys and certificates and filling in lots of details by hand.

The high cost of rip and replace

Looking across the industry landscape, third-party tools are available that can automate the certificate process. Such tools require a large-scale rip and replace. You have to deeply integrate each Linux system with Active Directory, including switching your system user authentication over as well. This requires massive changes to existing Linux and Microsoft infrastructure, extensive staff re-training, and significant software licensing costs. The replacement approach also requires implementation time frames of three months to more than three years and can have a price tag starting at $250,000 for an entry level implementation to several million dollars for large organizations.

Enter CertAccord Enterprise

Introduced in 2016, CertAccord is the first product to solve these problems. CertAccord Enterprise brings auto enrollment with the Microsoft PKI Certificate Authority to Linux, Mac, Unix (Solaris), non-AD-joined Windows systems and the ability to automate certificate provisioning and management with virtually any application.

CertAccord enterprise is designed to be easy to use by Linux administrators who only need to run a simple command to create certificates. Once created, the certificates are managed and renewed throughout their lifecycle. In addition, the certificate creators only have to provide the purpose of the certificate without having to know what the company PKI configuration policies are for creating a private key or certificate. Instead, the policies have already been configured by enterprise PKI experts and can be executed with one simple CertAccord command.

The Microsoft PKI administrators in turn use nearly all the same tools and interfaces to manage Certificate Templates (policies) with the addition of the CertAccord Enterprise Management Console (CMC) web GUI.

The CMC allows PKI administrators to configure Microsoft ADCS access and templates. It provides centralized policies and settings for endpoints. The CMC also allows PKI administrators to deploy certificates to a single endpoint or to groups of endpoints using AD groups.

It is easy to install because it’s designed as a “bolt-on” to your existing Microsoft PKI and Linux infrastructure. There is no Certificate Authority to standup or change. You do not integrate your Linux systems directly with AD, so it is a simple installation. All this means is you do not have to spend a year implementing it and it won’t cost you most of your annual budget. It is by far the easiest and most capable solution of its kind available today.

How CertAccord Enterprise Works

CertAccord Enterprise consists of a Server and an Agent component as shown in **Figure 2** below. The Server communicates with a Microsoft ADCS or GlobalSign CA using native APIs. Agent software is installed on each end-node device (web servers, application servers, etc.) on which certificates will be installed and managed. The Server runs on Microsoft Windows Server 2012 (or later) and is typically installed on-premise on a physical or virtual machine (VM) guest.

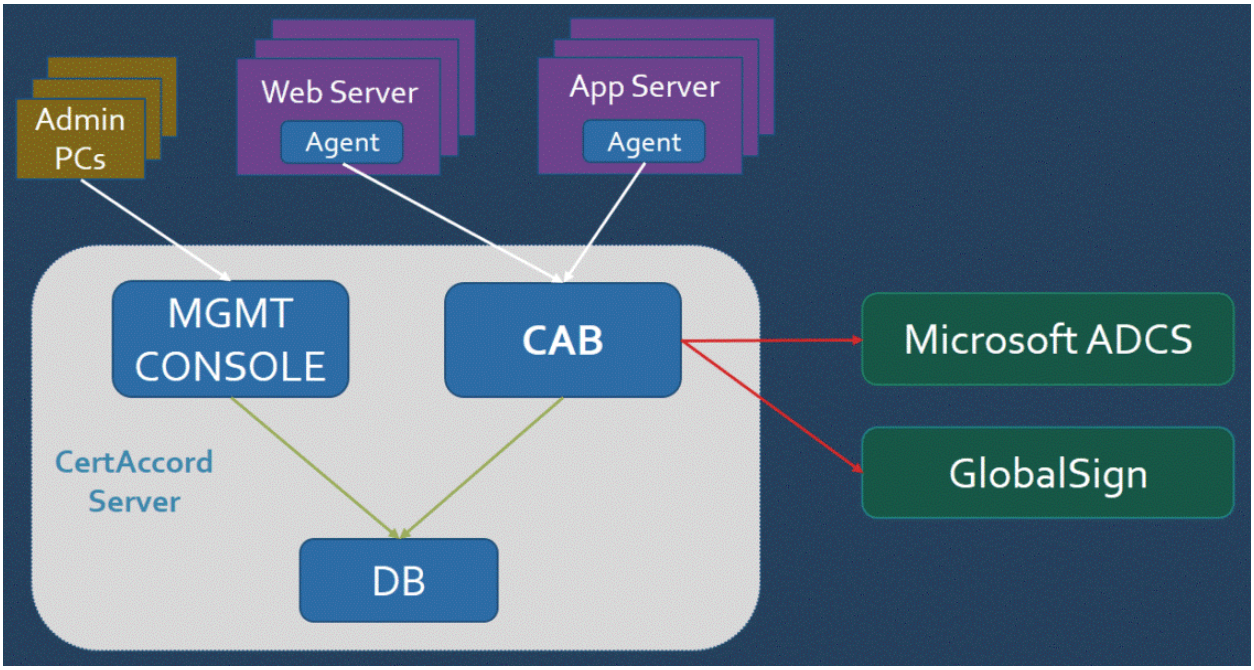

Figure 2. *CertAccord Enterprise consists of server and agent components.*

The Server consists of three sub-components:

1. Certificate Authority Bridge (CAB). Integrates and communicates with CAs. Communicates and controls Agents.
2. Management Console (MGMT CONSOLE). Web-based GUI which is typically used by CertAccord product administrators to configure the product.
3. Product Database (DB). A Microsoft SQL Server database installed locally on the server or on a different network-accessible server supplied by the customer.

The end-node computer running the CertAccord Agent communicates with a CertAccord Server using a REST API. The Agents never communicate directly with any CA or any other Microsoft infrastructure service. This has the advantage of greatly simplifying the installation of CertAccord since you do not have to domain join end-points in AD.

The Agent has a daemon or service process that starts automatically at system boot. The Agent daemon is responsible for checking in with a Server to look for updated policy and configurations. It is also responsible for checking and performing automatic renewals of certificates. The CertAccord IT system administrator can

also run the Agent to request a new certificate quickly and easily or perform other tasks. Certificate creation is as simple as running:

```
cmbagent cert create purpose=webserver
```

The Agent automates the generation of a local private key using policy data obtained from a server. It generates a CSR and signs it, then sends the CSR to a Server and waits for a response. Once the response is received, the new certificate is stored on the local filesystem. If a Certificate Applier is available, then it is executed to perform application-specific actions.

Certificate purposes

CertAccord Enterprise is designed to provide a friction-free and easy to understand and manage connection to CAs. One of the ways it does that is through the use of Certificate Purposes that act as a tag to both simplify the certificate creation request process and to ensure that PKI administrators have a controlled process for issuing the proper identity certificates.

In CertAccord Enterprise, Certificate Purposes are used to configure Certificate Policy Bindings, Subject Bindings, and more. A usage value like ServerAuthentication alone cannot tell a PKI administrator how a certificate is intended to be used or what its subject should contain. A purpose like WebServer, however, indicates that a certificate is intended to be used with a web server such as Apache HTTPD. In addition to the built-in purposes, you can create your own purposes for such things as certificates for VPN devices and users.

Why is managing digital certificates so important?

Research by IDC shows that the number of businesses using PKI as part of their broader security programs, beyond TLS for websites, has more than doubled in the last decade.

A recent IDC Data Services for Hybrid Cloud Survey, which included interviews with more than 400 chief information security officers (CISOs), security architects, IT security and data management specialists in Europe and North America, shows that PKI is increasingly viewed by security leaders as essential in securing digital transformation initiatives across a variety of business use cases.

As PKI deployments grow, proper management of digital certificates is critical. IDC research found that the **average cost of downtime industrywide is $250,000 per hour**, and one unmanaged digital certificate that expires can hurt the bottom line.

Source: https://futurecio.tech/study-shows-growing-use-of-pki-for-enterprise-security/

Using CertAccord Enterprise to create certificates

The CertAccord Enterprise Agent is managed through a Command Line Interface (CLI) and allows Linux system administrators to make swift work of installing certificates on Linux systems. The steps involved are similar whether you are working on MacOS, Unix, or Windows systems. The process is simple, easy, and doesn't take a PKI expert.

This example assumes your enterprise PKI experts have already installed the CertAccord Enterprise Server.

STEP 1 – Install CertAccord Enterprise Agent

If you don't already have the CertAccord Agent installed, you can install it by copying the CertAccord Agent installer to your Linux system. Then run the installer:

```
chmod +x ./cmbagent-1.0-linux-x64.run
./cmbagent-1.0-linux-x64.run --mode unattended
```

This command will install the Agent into the default location of `/usr/local/cmbagent`. On Linux you can also install from a ".rpm" and ".deb" package.

STEP 2 – Register Agent

```
export PATH=/usr/local/cmbagent/bin:$PATH
cmb register server=myserver
```

Change *myserver* to be the hostname of the CertAccord Enterprise Server.

When you run this command, the Agent will download the CA trust information from the Server, generate a private key (configured to adhere to the policies given by the server), and submit the registration request to the server.

STEP 3 – Create Certificate

To create a web server certificate for use with Apache HTTPD or other web server, run the following command:

```
cmb cert create purpose=webserver
```

This command will automatically create a CSR, submit it to the enterprise CA, and install the certificate once issued. This is all done using the PKI policies configured on the CertAccord Enterprise Server and your enterprise CA. No knowledge of these policies or configuration requirements are needed by the Linux system administrator when running this command.

Here is the example output:

```
Creating Certificate PURPOSES: [WebServer]
Created certificate 634RJ65d [SUBJECT: "dune.contoso.com" PURPOSES: WebServer
EXPIRES: Jul 14 2021 13:52:14 PDT]
Saved certificate 634RJ65d [SUBJECT: "dune.contoso.com" PURPOSES: WebServer
EXPIRES: Jul 14 2021 13:52:14 PDT] to AgentProfile
```

```
Apply Certificate 634RJ65d [SUBJECT: "dune.contoso.com" PURPOSES: WebServer
EXPIRES: Jul 14 2021 13:52:14 PDT]
Exported Certificate 634RJ65d [SUBJECT: "dune.contoso.com" PURPOSES: WebServer
EXPIRES: Jul 14 2021 13:52:14 PDT] to /var/cmb/cert/dune.contoso.com-webserver.crt
Exported PrivateKey Grq8jB3h [RSA 2048] to /var/cmb/cert/dune.contoso.com-
webserver.key
Applying certificate to Apache HTTP Web Server: ID: 634RJ65d PURPOSE: WebServer
COMMAND [/usr/sbin/service apache2 reload] ran successfully
Reloaded Apache HTTP Web Server
Apply certificate to Apache HTTP Web Server: ID: 634RJ65d RESULT: Succeeded
```

The output shows that a certificate was created, saved to the local Agent database, and a copy of the certificate was exported to `/var/cmb/cert/dune.contoso.com-webserver.crt`. The Apache HTTPD server was also reloaded so that it re-read its configured certificate files.

As this example illustrates, the CertAccord Enterprise Agent is a much easier and simpler means of creating trusted certificates on Linux and other servers and clients. It can lower IT costs through automated certificate creation and life-cycle management, improve security by reducing errors in creation and renewals, and be implemented as a simple add-on to your existing enterprise PKI.

CertAccord Enterprise Application Integration

One of the most important advantages of using CertAccord Enterprise is that it takes full advantage of the automation provided by Microsoft ADCS. The Agent extends this automation through to the application level with the use of Certificate Appliers.

Offering a command-level API for application integration, Certificate Appliers are executable scripts or programs that allow applications to receive notifications whenever a certificate is created or renewed, so the application can decide what actions to execute.

An example of an applier is the Apache HTTP applier which is built into the Agent. Whenever a certificate with purpose of WebServer is created (or renewed), the Apache HTTP Certificate Applier is called and given the certificate information so that it can reload the Apache HTTP processes with the new certificate.

Using the Certificate Applier's executable API, users can create their own custom Certificate Appliers to automate whatever application integration is needed. Examples of this could include integrating with a VPN client or integrating with a JKS application like Tomcat or JBoss.

The Certificate Applier process is shown in **Figure 3** below. The Agent starts the process by searching for applier scripts in the filesystem. When an applier is found, the Agent provides updated certificate information and the applier script or binary performs any actions required for the application to start using the certificate and establish itself as a trusted entity on the network.

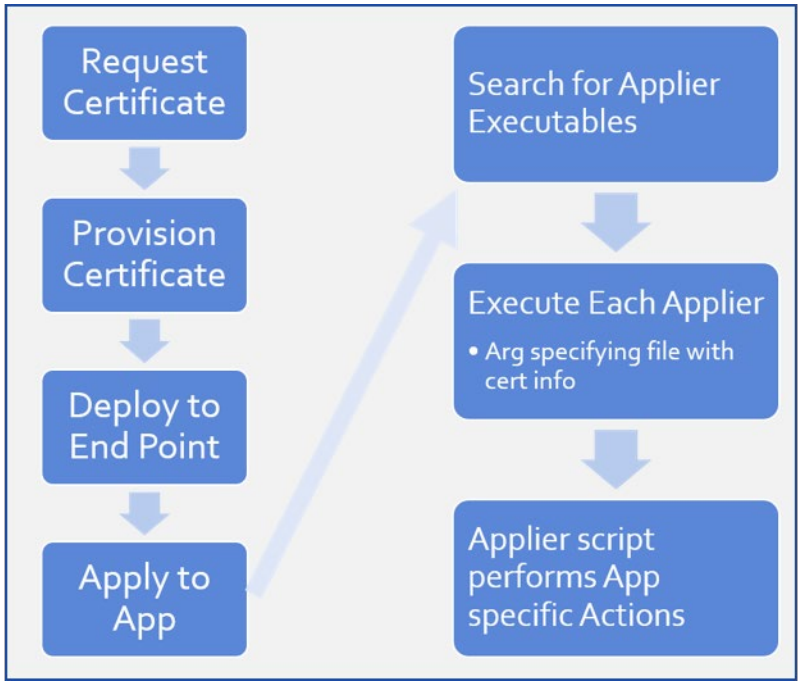

Figure 3. *Certificate applier process in CertAccord Enterprise*

Is CertAccord Enterprise right for you?

One of the top five power utilities in the U.S. is using CertAccord to overcome the challenges of certificate management. As your enterprise has likely done, this utility explored multiple options for automating certificate management across its network before deciding to deploy CertAccord Enterprise. Now the CertAccord Agent is a part of every new Linux deployment, and concerns about expiring certificates are effectively eliminated.

With the certificate lifetimes already getting shorter, and threats like quantum computing looming, the need for automated certificate management has never been greater. While ADCS addresses the automation challenge within the Active Directory environment, far too many enterprises are still relying on manual processes for non-Microsoft systems and applications.

CertAccord installs into your existing environment in minutes and computer administrators can easily request certificates using a simple command line interface. With the cost of a single outage averaging more than $250,000 hour, it doesn't take many outages due to expired certificates to justify an investment in CertAccord Enterprise. The labor savings alone make for a rapid ROI while helping to keep your network safer and more stable.

For more information or a hands-on demo, call us +1 408-638-9323 or send email to info@revocent.com.

CertAccord Enterprise At A Glance

- Automatic certificate creation and installation
- Automatic certificate integration with applications
- Automatic certificate renewals without manual action
- Create enrollment policies and automate client enrollment from the CertAccord Web Management Console
- Request certificates via simple command line on end-nodes without being a PKI genius
- Push certificates to devices by group using the Management Console
- Easily installs into existing Microsoft and Linux environments in minutes
- Web based management console
- IT administrators on Linux devices can initiate certificate requests using simple commands or a CertAccord administrator can push a certificate to any registered device.