|  |  |
| --- | --- |
|  | Anbud  Nyinstallation av AD CS med nyckelskydd från thales  {{ \_\_datestring }}  {{ customer.name }} |
|  | |  | | --- | | Atea Sverige AB  Spannmålsgatan 7  291 32 Kristianstad  ,  Organisationsnr: 556448-0282 | |

# Sammanfattning

Detta dokument innehåller ett lösningsförslag för {{ customer.simple\_name }} av en nyinstallation av *Microsoft Active Directory Certificate Services (AD CS)* med nyckelskydd baserat på *Thales Luna 7*.

Syftet med systemet är att tillhandahålla en tjänst för utgivning av digitala certifikat.

Lösningsförslaget beskriver mer ingående hur systemet kommer att fungera, vilka komponenter som ingår i lösningen, förutsättningarna för att systemet ska kunna installeras, samt en kostnadsberäkning.

# Introduktion till Public Key Infrastructure

*Public Key Infrastructure (PKI)* består av policies, personal och mjukvara för att hantera digitala certifikat.

## Användningsområden

Certifikat är en viktig komponent i de flesta säkerhetslösningar eftersom de tillhanhåller en mekanism för att etablera tillit mellan användare och datorer.

Några användingsområden där certifikat används är:

1. Autentisering i TLS-protokollet genom klient- och servercertifikat
2. Signering och kryptering av mail
3. Kodsignering
4. Certifikat på smartkort för tvåfaktorautentisering vid inloggning

## Syftet med Active Directory Certificate Services

AD CS är en del av Windows Server och tillhandahåller den mjukvara som behövs för att utfärda och återkalla certifikaten. Utfärdandet kan ske manuellt eller per automatik med exempelvis *Autoenrollment* om certifikatet ska utfärdas till domänanslutna användare eller datorer, eller via *Network Device Enrollment Service (NDES)* och *Intune* om certifikatet ska utfärdas till mobiler och surfplattor.

Microsoft Autoenrollment styrs via gruppolicy vilket gör att det lämpar sig bäst i en ren Windowsmiljö, medan Intune är en molnbaserad tjänst som tillhandahålls av Microsoft, designad för att även kunna fungera med iOS, OS X och Android-enheter.

Att kunna återkalla certifikat är viktigt om den privata nyckeln för certifikatetinte längre är betrodd, till exempel för att den är kompretterad eller för att certifikatet har utfärdats till en användare som har slutat på arbetet. Revokering tillhandahålls med hjälp av *spärrlistor (CRLer)* som distribueras via HTTP.

## CA-hierarki

Av säkerhetsskäl finns det två utfärdare, en *root CA* och en *issuing CA* som tillsammans bildar en *CA-hierarki*. På grund av en teknisk begränsning i AD CS måste varje utfärdare installeras på en separat installation av Windows.

Root CA-maskinen med tillhörande nyckelpar är bortkopplad under normal drift. Om en obehörig person har fått tillgång till issuing CA-maskinen kan certifikatet för denna utfärdare återkallas genom att koppla på root CA-maskinen och återkalla utfärdarens *CA-certifikat*.

## Nyckelskydd

För att systemet skall vara säkert är det viktigt att utfärdarens privata nyckel inte hamnar i obehöriga händer. Detta säkerställs enklast genom att generera och spara nyckeln i en säkerhetsmodul (HSM). I detta lösningsförslag används en nätverksbaserad säkerhetsmodul från tillverkaren Thales som sparar den privata nyckeln för både root CA- och issuing CA-maskinen.

Nyckeln för root CA-maskinen sparas på en separat partition i säkerhetsmodulen. Det gör att man kan inaktivera den privata nyckeln när root CA-maskinen inte är i drift.

När den privata nyckeln är aktiv kan AD CS hämta ut digitala signaturer från säkerhetsmodulen, men har aldrig tillgång till den privata nyckeln i klartext.

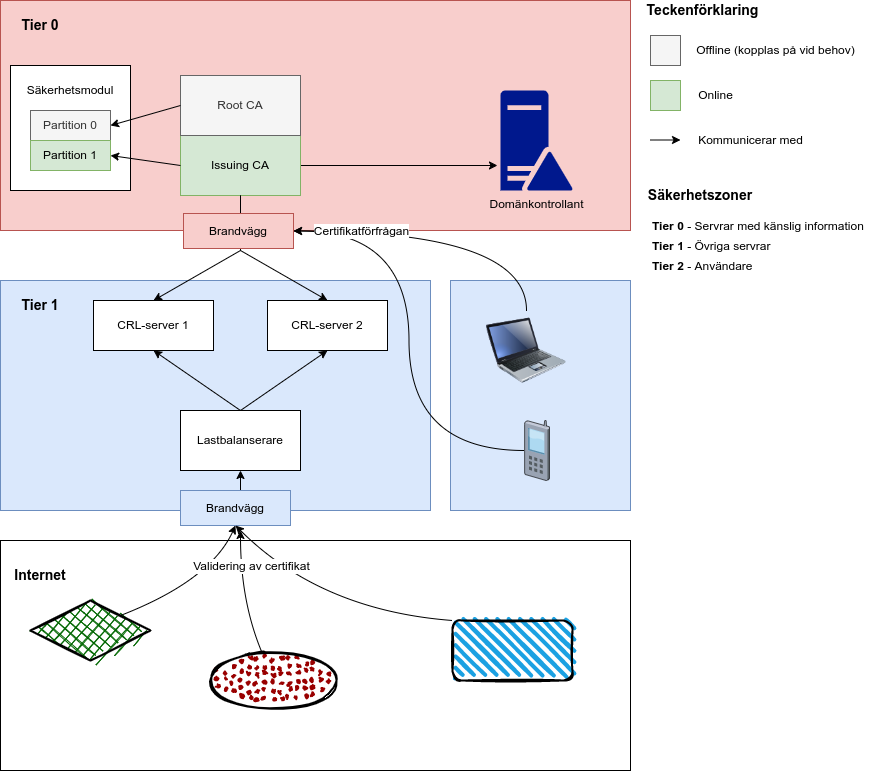
## Viktigt med redundans för spärrlistor

För att klienter skall kunna använda certifikaten måste spärrlistorna vara tillgängliga. Därför är det viktigt med redundans på denna del av systemet. Detta löses genom att utfärdaren publicerar spärrlistorna till flera olika servrar. Servrarna är tillgängliga över en lastbalanserad publik URL, så kallad *CRL Distribution Point* *(CDP*)*.* Det räcker då att åtminstone en server går att nå för att klienten ska kunna validera certifikatet.

# Design

Det är vanligt att dela upp nätverket i olika säkerhetszoner. Framför varje säkerhetszon ska det finnas en brandvägg som begränsar åtkomst till resurser i zonen. I detta fall förutsätter vi att det finns tre säkerhetszoner som vi kallar tier 0, tier 1 och tier 2[[1]](#footnote-0).

Tier 0 har den högsta säkerhetsnivån med servrar som innehåller känslig information. Här placeras säkerhetsmodulen, root CA-maskinen och issuing CA-maskinen. Tier 1 har den näst högsta säkerhetsnivån och här placeras CRL-servrarna som exponeras mot internet. I tier 2 finns vanliga datorer. Dessa kan komma åt issuing CA-maskinen i tier 0 för att hämta ut certifikat.



## Existerande komponenter

För att kunna sätta upp systemet enligt ovan krävs det att kunden har följande komponenter på plats:

|  |  |  |
| --- | --- | --- |
| Komponent | Krav | Rekommendation |
| Virtualiseringsmiljö | VMware ESXi med 26 GB ledigt RAM, 6 vCPUer och 256 GB ledigt diskutrymme | 512 GB ledigt diskutrymme |
| Licenser för Windows Server | 4 st | Windows Server 2022 eller Windows Server 2019 |
| Lediga portar i switch | 2 st för Luna 7 |  |
| Lediga uttag för el | 2 st för Luna 7 |  |
| Rack | 1U för Luna 7 |  |
| Förvaring av nyckelmaterial | Låst utrymme | Kassaskåp eller bankfack |
| Lastbalanserare | 1 st | 2 st |
| Domänkontrollant | 1 st |  |

## Nya komponenter

Detta lösningsförslag omfattar följande komponenter:

* Installation och konfiguration av 1 st root CA
* Installation och konfiguration av 1 st issuing CA
* Installation och konfiguation av 2 st servrar för distribution av spärrlistor
* Konsultation för uppsättning av roller på Luna 7
* Installation, konfiguration och säkerhetskopiering av 1 st Luna 7
* Konfiguration av domänkontrollant:
  + Gruppolicy för Microsoft Autoenrollment
  + Design och konfiguration av certifikatmallar
* Dokumentation för installation, drift och underhåll av systemet
* Test av systemet innan driftsättning

## Komponenter som ej omfattas av lösningsförslaget

Lösningsförslaget omfattar inte:

* Uppsättning av nya maskiner i VMware ESXi
* Konfiguration av brandväggar
* Konfiguration av lastbalanserare
* Konfiguration av VPN för fjärråtkomst

Vid behov kan Atea hjälpa till med dessa tjänster för en ytterligare kostnad.

# Kostnadsberäkning

I tabellen nedan visas de olika kostnadsposterna.

Notera att installation och konfiguration av säkerhetsmodulen måste göras på plats hos kunden. Installation och konfiguration av AD CS kan göras antingen på plats eller på distans över VPN enligt överrenskommelse. Reseersättning, fraktkostnader av hårdvara och eventuella kostnader för kost och logi tillkommer separat.

|  |  |
| --- | --- |
| Kostnadspost | Kostnad (SEK) |
| 1 st Thales Luna 7 A700 | 196000 |
| 3-års supportkontrakt med Thales | 106000 |
| 1 st Luna B700 backupenhet | 65000 |
| 2 st Luna 7 klientlicenser | 24000 |
| 2 st elkablar | 500 |
| 1 par Luna 7 räls | 2200 |
| 1 st shortage fee | 31500 |
| Installation, konfiguration och dokumentation av AD CS | 82000 |
| Installation och konfiguration av säkerhetsmodul hos kund | 40000 |
| **Totalt** | **547200** |



Bastian Fredriksson  
Senior Consultant

+46 4 426 96 48

1. Microsoft Docs - Enterprise Access Model, https://docs.microsoft.com/en-us/security/compass/privileged-access-access-model [↑](#footnote-ref-0)