



Certificatenbeheer Vlaamse overheid

Veelgestelde vragen bij de migratie van Vo-DCB naar Vo-DCBaaS



INHOUDSOPGAVE

Inhoudsopgave.....	2
Versiegeschiedenis van het document.....	2
Lijst van gebruikte afkortingen.....	3
1 Context en doel van dit document.....	4
2 FAQ bij de migratie.....	5

VERSIEGESCHIEDENIS VAN HET DOCUMENT

Versie	Datum	Wijzigingen
1.0	28/01/2021	Eerste publieke versie



LIJST VAN GEBRUIKTE AFKORTINGEN

Afkorting	Betekenis
CN	Common Name, eigenschap van een certificaat die doorgaans de domeinnaam of gewoon de naam van de toepassing of server is waarvoor je een bepaald certificaat gebruikt. Het aanvragen van de CN is de eerste stap in het aanvragen van een certificaat in Vo-DCB en Vo-DCBaaS.
CSR	Certificate Signing Request, een bestand waarmee je in Vo-DCB en Vo-DCBaaS een nieuw certificaat kan aanvragen
CRL	Certificate Revocation List, een lijst van certificaten die herroepen zijn door de <i>certificate authority</i> voor hun vervaldatum is bereikt en dus niet meer vertrouwd mogen worden
Vo-DCB	Vlaamse overheid - Digitaal Certificaten Beheer, de huidige toepassing die gebruikt wordt om certificaten aan te maken en te beheren
Vo-DCBaaS	Vlaamse overheid - Digitaal Certificaten Beheer as a Service, de nieuwe toepassing die Vo-DCB gaat vervangen
Vo-PKI	Vlaamse overheid - Private Key Infrastructure, de achterliggende infrastructuur waarmee toepassingen zoals Vo-DCB en Vo-DCBaaS certificaten aanmaken en ondertekenen. De Vlaamse overheid heeft een eigen (private) PKI-infrastructuur. Deze bestaat uit een <i>root certificate authority</i> en een <i>issuing certificate authority</i> . Vo-DCB en Vo-DCBaaS hebben elk hun eigen (aparte) PKI-infrastructuur.
VOICA2.2018	Vlaamse overheid – Issuing Certificate Authority, de oude <i>issuing certificate authority</i> waarmee Vo-DCB-certificaten aanmaakt en ondertekent
VOICA2.2020	Vlaamse overheid – Issuing Certificate Authority, de nieuwe <i>issuing certificate authority</i> waarmee Vo-DCBaaS certificaten aanmaakt en ondertekent
VORCA.2012	Vlaamse overheid – Root Certificate Authority, de <i>root certificate authority</i> van VOICA2.2018 (en dus Vo-DCB, de huidige toepassing)

1 CONTEXT EN DOEL VAN DIT DOCUMENT

De huidige Vo-DCB-toepassing en haar achterliggende PKI-infrastructuur zijn verouderd en voldoen niet meer aan de functionele en veiligheidsvereisten van de Vlaamse overheid. Om die reden hebben we ervoor gekozen om een nieuwe toepassing te bouwen (Vo-DCBaaS) en ook de achterliggende PKI-infrastructuur volledig te moderniseren.

Op die manier kunnen we een hogere veiligheid en betrouwbaarheid leveren en kunnen we blijven inspelen op de vragen van klanten. In de nieuwe toepassing (Vo-DCBaaS) staat selfservice centraal en wordt het veel gemakkelijker voor gebruikers om certificaten aan te vragen, zonder afhankelijkheden van de centrale administratie. De nieuwe PKI-infrastructuur (hardware en de nieuwe sleutelhiërarchie) biedt ondersteuning voor nieuwe cryptografische standaarden (b.v. SHA3 en Elliptic-curve) en legt de basis voor nieuwe ontwikkelingen in de toekomst (b.v. aanvragen van certificaten via API en hoge volumes van certificaten in functie van IOT).

De huidige Vo-DCB-toepassing en haar achterliggende PKI-infrastructuur zijn gebouwd op servers in het datacenter COLT/NMC4. De sluiting van dit datacenter in Q2-2021 zorgt ervoor dat we de overstap en migratie van Vo-DCB naar Vo-DCBaaS versneld moeten doorvoeren in de loop van 2021.

Deze overschakeling naar de nieuwe Vo-DCBaaS-toepassing heeft impact op alle klanten die Vo-PKI-certificaten gebruiken. In dit document beantwoorden we veelgestelde vragen van klanten bij de migratie van Vo-DCB naar Vo-DCBaaS.

Dit document zal verder aangevuld worden met nieuwe informatie gedurende het migratietraject. Al deze laatste informatie vind je ook steeds terug op onze website bij [publicaties](#), onder de hoofding 'Ik heb vragen over Vo-DCB of VoDCBaaS'.

Kom je een vraag tegen over je toepassing of de migratie? Contacteer ons op vodcb@vlaanderen.be.



2 FAQ BIJ DE MIGRATIE

2.1 Vragen bij de context van de migratie van Vo-DCB

2.1.1 **Waar wordt de nieuwe Vo-DCBaaS-toepassing (en achterliggende PKI-infrastructuur) gehost?**

De Vo-DCBaaS-toepassing zal gehost worden op een door ons beheerde omgeving op Amazon Web Services (AWS). Voor de PKI-infrastructuur hebben we voor een oplossing van GlobalSign gekozen. Voor beide omgevingen werden de nodige veiligheidsmaatregelen getroffen, conform de vereisten van de Vo-informatieclassificatie en de GDPR-regelgeving. De *root certificate authority* staat offline en is fysiek beveiligd binnen de gebouwen van de Vlaamse overheid.

2.1.2 **Ga je Vo-DCBaaS-certificaten kunnen gebruiken op publieke websites (voor burgers)?**

Neen. We maken gebruik van infrastructuur van GlobalSign, maar de PKI-infrastructuur achter Vo-DCBaaS is nog steeds een private PKI (net zoals dat het geval was met zijn voorganger Vo-DCB). Het *root* certificaat van onze PKI-infrastructuur is dus niet standaard geïnstalleerd op laptops en desktops van burgers. Vo-DCBaaS-certificaten zijn dus niet geschikt om te gebruiken voor b.v. het SSL-verkeer van een website die publiek toegankelijk is voor burgers.

2.2 Fase 1: “Voorbereiding nieuwe dienstverlening Vo-DCBaaS”

Timing: < 01/03/2021

2.2.1 **Waarom worden enkel de CN's gemigreerd naar de nieuwe Vo-DCBaaS toepassing (niet de CSR's, de eigenlijke certificaten, enz.)?**

De nieuwe Vo-DCBaaS-toepassing gebruikt een nieuwe PKI-infrastructuur. Bestaande Vo-DCB-certificaten kunnen dus niet zomaar gemigreerd worden naar de nieuwe toepassing om ze daar te beheren. Dat kan enkel nog in de oude Vo-DCB-toepassing.

2.2.2 **Waarom worden niet alle CN's gemigreerd (enkel met een actief certificaat of vervallen binnen het laatste jaar)?**

CN's die al zolang niet gebruikt zijn om een certificaat mee te genereren worden in de praktijk niet meer gebruikt. Het heeft geen zin om ze nog te migreren.

2.2.3 Kan ik tijdens fase 1 nog CN's en certificaten aanvragen in de Vo-DCB-toepassing

Je kan nog certificaten aanvragen in de Vo-DCB-toepassing tot 22/02/2021. Dan wordt de Vo-DCB-toepassing permanent bevroren en is het niet meer mogelijk om nog nieuwe CN's of certificaten aan te vragen. Je kan wel nog steeds bestaande certificaten downloaden, herroepen, enz.

2.2.4 Wie beheert de toegangsrechten (voor mijn organisatie) tot de nieuwe Vo-DCBaaS-toepassing?

Toegangsrechten tot de Vo-DCBaaS-toepassing worden beheerd in het Gebruikersbeheer (IDM) door de lokale beheerder van uw organisatie. Via de "[Mijn Profiel](#)"-toepassing van het Gebruikersbeheer (IDM) kan u nagaan wie de lokale beheerder van uw organisatie is.

2.3 Fase 2: "Vo-DCBaaS is beschikbaar + start migratie"

Timing: 01/03/2021 – 30/06/2021

2.3.1 Wat kan ik tijdens fase 2 nog in de Vo-DCB-toepassing doen?

Tijdens fase 2 blijft de Vo-DCB-toepassing beschikbaar, maar enkel voor het beheren van bestaande Vo-DCB-certificaten (b.v. downloaden, herroepen, enz.). Je zal geen nieuwe certificaten kunnen maken. Je zal ook nog steeds meldingen ontvangen van te vervallen Vo-DCB-certificaten.

2.3.2 Is er een handleiding van Vo-DCBaaS beschikbaar?

De eindgebruikershandleiding is momenteel in opmaak. Van zodra ze beschikbaar is zullen we ze communiceren en zullen we hier de link plaatsen.

2.3.3 Bij wie kan ik terecht om nieuwe Vo-DCBaaS certificaten aan te maken?

Bij de door uw organisatie toegewezen certificaatbeheerder(s). Uw lokale beheerder in het Gebruikersbeheer (IDM) kan u aangeven wie deze functie invult binnen uw organisatie. Via de "[Mijn Profiel](#)"-toepassing van het Gebruikersbeheer (IDM) kan u nagaan wie de lokale beheerder van uw organisatie is.

2.3.4 Moet ik nog steeds eerst een CN aanvragen via vodcb@vlaanderen.be om een nieuw certificaat aan te maken?

Neen, in de nieuwe Vo-DCBaaS-toepassing kan een certificaatbeheerder de CN in de toepassing zelf aanvragen. Er moet geen aanvraag meer gebeuren via vodcb@vlaanderen.be. De goedkeuringsstromen gebeuren volledig via de toepassing. In de meeste gevallen zal er ook geen goedkeuring meer nodig zijn (door de introductie van het nieuwe concept "domein").

Certificatenbeheer Vlaamse overheid

2.3.5 Moet ik al mijn Vo-DCB certificaten vervangen?

Ja, alle Vo-DCB-certificaten zullen na 15/12/2021 niet meer vertrouwd zijn en dus praktisch onbruikbaar worden, ongeacht van hun vervaldatum. Je moet ze dus vervangen door nieuwe Vo-DCBaaS-certificaten.

2.3.6 Hoeveel tijd heb ik om al mijn Vo-DCB-certificaten te vervangen?

Je hebt tijd tot 15/12/2021 om al je Vo-DCB-certificaten te vervangen door Vo-DCBaaS-certificaten. Wij raden echter aan om de vervanging al te doen vóór 30/06/2021. Na die datum is het nog steeds mogelijk, maar dan wordt het moeilijker en betalend om bestaande Vo-DCB-certificaten te herroepen.

2.3.7 Wat is precies het voordeel van al je Vo-DCB-certificaten vóór 30/06/2021?

Je Vo-DCB-certificaten zullen sowieso vertrouwd blijven tot 15/12/2021, maar na de stopzetting van de Vo-DCB-toepassing (30/06/2021) ga je b.v. geen meldingen meer krijgen van te vervallen Vo-DCB-certificaten. Als je een Vo-DCB-certificaat wil herroepen, dan ga je ook een nieuw manueel proces moeten volgen dat betalend is. Zolang de Vo-DCB-toepassing nog beschikbaar is kan je dat gewoon nog daar doen.

2.4 Fase 3: “Vo-DCB is stopgezet + afronden migratie”

Timing: 01/07/2021 – 15/12/2021

2.4.1 Waarom blijven de oude Vo-DCB-certificaten nog vertrouwd na de stopzetting van de Vo-DCB-toepassing op 30/06/2021?

We houden deze certificaten vertrouwd (tot 15/12/2021) om klanten meer tijd te geven om de overschakeling te maken naar nieuwe Vo-DCBaaS-certificaten.

2.4.2 Krijg ik nog notificaties over te vervallen Vo-DCB-certificaten na de stopzetting van de Vo-DCB-toepassing?

Neen, de notificaties over Vo-DCB-certificaten werden uitgestuurd door de Vo-DCB-toepassing. Aangezien de toepassing wordt stopgezet op 30/06/2021 zullen ook de meldingen stoppen. De nieuwe Vo-DCBaaS-toepassing zal enkel meldingen uitsturen voor nieuwe Vo-DCBaaS-certificaten.

2.4.3 Wat moet ik precies doen om mijn Vo-DCB-certificaat te herroepen na 30/06/2021?

We zijn momenteel een nieuw manueel proces aan het maken die het mogelijk moet maken om nog Vo-DCB-certificaten te herroepen (zonder de Vo-DCB-toepassing). Zo kan je het oude certificaat herroepen nadat je het vervangen hebt door een Vo-DCBaaS-certificaat. Op die manier kan je ook snel ingrijpen

wanneer b.v. je private sleutel zou gecompromitteerd worden (en je dus dringend je certificaat moet herroepen).

Wanneer het manueel proces volledig is uitgewerkt zullen we hierover communiceren en dit FAQ-item updaten.

2.4.4 Wordt de CRL van de oude PKI-infrastructuur nog geactualiseerd met de manuele herroepingen in fase 3?

Ja, de CRL van de oude PKI-infrastructuur zal nog steeds geactualiseerd worden en zal beschikbaar blijven op zijn huidige plaats.

2.4.5 Wat gebeurt er precies na 15/12/2021 met mijn Vo-DCB-certificaat?

Op 15/12/2021 gaan we het *root* en *intermediate* certificaat van de oude PKI-infrastructuur van Vo-DCB herroepen. Hierdoor is de sleutelhiërarchie van een Vo-DCB-certificaat niet vertrouwd en zal het certificaat zelf dus ook niet meer vertrouwd zijn. Andere toepassingen die b.v. met jouw toepassing gegevens uitwisselen zullen dus je certificaat niet meer aanvaarden.

