

1. Prezentare generală

VOGO eBS PKI este infrastructura internă de chei publice a suitei VOGO eBS. Emite, reînnoiește, revocă și validează certificatele interne ale organizației — pentru servicii, echipamente, autentificare tehnică și semnături interne necalificate — și se instalează integral în infrastructura beneficiarului, fără dependență de un serviciu extern.

Componenta folosește biblioteci open EJBCA, cu suport enterprise asigurat de Ofertant pe întreaga perioadă de implementare și de garanție. Nu se substituie prestatorilor calificați de servicii de încredere: certificatele calificate ale persoanelor rămân emise de aceștia și sunt utilizate separat, prin agentul local de semnare.

Produs dezvoltat de VOGO TECHNOLOGY (denumire anterioară VIPTES) parte a suitei VOGO eBS, înregistrată la ORDA în Registrul Național al Programelor pentru Calculator cu certificatul seria 478196BV nr. 13869, sub marca Uniunii Europene VOGO.me înregistrată la EUIPO cu nr. 019103505 / 15.04.2025 - <https://euipo.europa.eu/eSearch/#details/trademarks/019103505>.

Produs	VOGO eBS PKI
Suita	VOGO eBS — Enterprise Business Suite
Bază tehnologică	Biblioteci open EJBCA, cu suport enterprise asigurat de Ofertant
Domeniu de emiterie	Certificate interne: servicii, echipamente, autentificare tehnică, semnături necalificate
Ce NU emite	Certificate calificate ale persoanelor — acestea rămân la prestatori calificați
Instalare	On-premises sau cloud privat, fără conectivitate externă obligatorie
Publicare stare	Liste de revocare și răspuns OCSP publicate în perimetrul organizației

2. Ierarhia și ciclul de viață al certificatelor

- ▶ Autoritate rădăcină păstrată offline și autorități intermediare de emiterie pentru fiecare categorie de utilizare.
- ▶ Profile de certificat distincte: servicii și servere, echipamente, autentificare de utilizator, semnare necalificată, sigiliu tehnic.
- ▶ Cereri de emiterie manuale sau automate, cu validarea identității solicitantului și aprobarea pe rol.
- ▶ Reînnoire programată înainte de expirare, cu notificarea titularului și a administratorului.
- ▶ Revocare cu motiv consemnat, cu efect imediat în lista de revocare și în răspunsul OCSP.
- ▶ Evidența completă a certificatelor emise, cu titular, utilizare, perioadă de valabilitate și stare curentă.

3. Publicarea stării și validarea

- ▶ Publicarea listelor de revocare la intervale configurabile și la fiecare revocare cu efect imediat.
- ▶ Răspuns OCSP pentru verificarea în timp real a stării unui certificat.
- ▶ Distribuirea automată a certificatului rădăcină și a lanțului de încredere către componentele suitei și către stațiile de lucru.
- ▶ Validarea lanțului, a perioadei de valabilitate și a stării la fiecare utilizare, cu rezultatul consemnat.

4. Utilizarea certificatelor în suită

Identitatea serviciilor	Certificate pentru comunicația între componente, cu autentificare reciprocă
Criptarea în tranzit	Certificate pentru TLS pe interfețele web, API-uri și conectori
Semnături interne	Semnături necalificate pentru circuite interne, distincte de semnătura calificată a persoanei
Sigiliu instituțional	Certificat aplicat automat de sistem la înregistrare, la emitere și la arhivare
Marcare temporală	Asocierea unei mărci de timp la semnare, pentru validare pe termen lung

5. Protecția cheilor și securitatea operării

- ▶ Cheile autorităților sunt protejate în module criptografice hardware sau în magazine de chei echivalente, cu acces pe rol și cu aprobare multiplă pentru operațiile critice.
- ▶ Cheia privată a unui certificat de persoană nu părăsește stația sau dispozitivul criptografic al titularului.
- ▶ Separarea rolurilor: administratorul autorității, ofițerul de înregistrare, auditorul și operatorul sunt roluri distincte.
- ▶ Jurnalizarea completă a emiterilor, reînnoirilor, revocărilor și a accesului administrativ, cu transmiterea evenimentelor către componenta de securitate.
- ▶ Proceduri documentate de pornire, rotație a cheilor, recuperare și continuitate.

6. Delimitarea față de serviciile calificate

Componenta nu se prezintă și nu funcționează ca prestator calificat de servicii de încredere. Certificatele calificate ale persoanelor sunt emise de prestatori calificați și sunt folosite prin agentul local de semnare, care accesează magazinul de certificate al stației și dispozitivele criptografice fără exportul cheii private. VOGO eBS PKI acoperă exclusiv nevoile interne ale organizației.

7. Funcționalitățile în aplicație

Certificatele interne sunt folosite direct în circuitul documentelor și al fluxurilor platformei VOGO eBS.

Semnarea documentelor:

- ▶ **Furnizorii de semnătură se configurează în platformă, pentru certificate interne și pentru certificatele calificate ale utilizatorilor.**
- ▶ **Cererile de semnare au participanți, ordine și stare, iar fiecare semnătură produce un artefact semnat.**
- ▶ **Documentele Word și PDF se semnează individual sau în masă, în formatele PAdES, CAdES și XAdES.**

Validare și marcare temporală:

- ▶ **Fiecare semnătură este validată, inclusiv prin OCSP, iar rezultatul validării rămâne la document.**
- ▶ **Marca temporală se asociază semnăturii și se păstrează ca metadată arhivistică.**
- ▶ **O semnătură invalidă este semnalată și blochează pașii următori ai fluxului.**

Sigiliu și expediere:

- ▶ **Sigiliul instituțional se aplică automat la înregistrare, la emitere și la arhivare.**
- ▶ **Documentele semnate se expediază cu dovada expedierii păstrată la document.**

8. Livrare, suport și operare

VOGO livrează și integrează componenta, profilele de certificat, politicile de emitere, configurațiile, imaginile de container și documentația de administrare, împreună cu procedurile de inițializare a ierarhiei, de rotație și de recuperare.

Modelul de suport operațional este asigurat de VOGO pe întreaga perioadă de implementare și de garanție — instalare, configurare, actualizări de securitate, remediarea incidentelor, documentare, compatibilitate cu infrastructura

beneficiarului și transfer operațional. Absența costului de licență pentru componentele open-source integrate nu diminuează niciuna dintre aceste obligații.

9. Suport enterprise

Suportul pentru VOGO eBS PKI este un serviciu enterprise asigurat de Ofertant pentru întreaga stivă livrată, inclusiv pentru componentele open-source integrate, pe toată perioada de implementare și de garanție. Beneficiarul are un singur punct de contact pentru toate componentele produsului, indiferent de originea lor.

Disponibilitate	24 × 7 × 365, pentru incidentele critice; program extins pentru solicitările de nivel funcțional
Call center	Punct unic de contact telefonic și prin e-mail, în limba română, cu preluare și înregistrare a fiecărei solicitări
Ticketing	Sistem de ticketing pus la dispoziția beneficiarului, cu portal web, înregistrare, clasificare, urmărire, istoric complet și rapoarte periodice
Niveluri de suport	Nivel 1 în call center, nivel 2 tehnic pe produs, nivel 3 la echipa de dezvoltare a Ofertantului, cu escaladare automată pe severitate
Acord de nivel al serviciului	Timpi de răspuns și de restabilire asumați pe clase de severitate, conform nivelurilor din contract
Acoperire	Produsul, modulele sale și componentele open-source integrate; absența costului de licență nu diminuează niciuna dintre obligațiile de suport

Serviciul include, fără costuri suplimentare pe perioada acoperită:

- ▶ Preluarea, clasificarea și soluționarea incidentelor, cu notificarea beneficiarului la fiecare schimbare de stare.
- ▶ Actualizări de securitate și corecții de defecte, testate de Ofertant și livrate cu note de versiune și procedură de aplicare.
- ▶ Mentenanță preventivă, verificări periodice de stare și recomandări de optimizare a configurației.
- ▶ Asistență la operațiunile planificate: actualizări de versiune, migrări, extinderi de capacitate, exerciții de restaurare.
- ▶ Documentație de administrare și operare, actualizată la fiecare versiune livrată.
- ▶ Instruirea administratorilor beneficiarului și transfer operațional la finalul perioadei de garanție.
- ▶ Rapoarte periodice de disponibilitate, incidente, timpi de soluționare și acțiuni corective.