

V O G O D I G I T A L

FIȘĂ TEHNICĂ

VOGO eBS
VOGO-ROEID
AUTENTIFICARE ROEID

VERSIUNEA 2.4

Produs	VOGO-ROEID
Domeniu	Autentificare ROeID
Scop	Identificarea electronică sigură a cetățenilor prin roeid
Interfețe	Web responsive, API și aplicație mobilă, după profilul modulului
Execuție	On-premises, cloud privat sau hibrid; containere OCI ori mașini virtuale

1. Prezentare generală

VOGO-ROEID are rolul principal de a asigura identificarea electronică sigură a cetățenilor prin ROeID și revenirea controlată în serviciul public inițiat.

Modulul asigură

- Fallback administrativ controlat pentru situațiile de indisponibilitate a serviciului extern.
- Acces unitar la informații și servicii, cu experiență coerentă pe web și mobil.
- Date și documente urmărite de la inițiere până la închidere.
- Modulul asigură validarea identității prin ROeID prin următoarele funcționalități:
- Identifică cetățeanul care accesează serviciile platformei online prin identitatea electronică validată.
- Interfață în limba română, responsive și adaptată rolului utilizatorului.
- Automatizează integral crearea contului și a profilului utilizatorului.
- Automatizează accesul la serviciile online prin înrolarea utilizatorului care a interacționat anterior cu instituția, de exemplu prin existența unui bun impozabil în evidența UAT-ului.
- API REST documentat și servicii securizate pentru integrare.
- Webhook-uri și evenimente pentru sincronizarea cu sisteme terțe.
- Conectori pentru e-mail, fișiere, baze de date și servicii web.
- Importă utilizatori din Active Directory.
- Separarea atribuțiilor administrative și verificarea accesului la nivelul serviciilor.
- Oferă integrare nativă cu sistemele Microsoft Active Directory și Keycloak.
- Verificarea identității utilizatorilor și a sistemelor care interacționează cu API-ul este primul pas în securizarea acestuia.
- Metodele comune includ:
- Oferă suport implicit pentru autentificare multi-factor, atât pentru conectarea la sistem, cât și pentru ridicarea drepturilor utilizatorilor.
- Backup periodic pentru date, configurații și documente.
- Monitorizarea serviciilor, capacității, erorilor și performanței.
- Instruirea utilizatorilor și administratorilor pe roluri.
- Asigură autentificarea cetățenilor prin ROeID și corelarea identității electronice cu profilul utilizatorului din portal.
- Permite revenirea securizată în serviciul inițiat după finalizarea fluxului de identificare ROeID.

2. Beneficii și rezultate

În VOGO-ROEID, beneficiile operaționale rezultă din reducerea verificărilor manuale de identitate și reutilizarea unei identități electronice validate în serviciile online.

Modulul asigură

- Reducerea timpului de procesare și a operațiunilor manuale repetitive.

3. Experiența utilizatorului și fluxul operațional

Experiența de lucru din VOGO-ROEID acoperă redirecționarea utilizatorului către autentificarea ROeID, preluarea rezultatului și continuarea solicitării inițiate în portal.

Modulul asigură

- Corelarea identității validate cu profilul și dosarul digital al solicitantului.
- Pași clari, validări la introducerea datelor și mesaje explicite de succes sau eroare.
- Căutare, filtrare, sortare și export pentru listele operaționale.
- Extinderea controlată cu noi formulare, fluxuri, rapoarte și integrări.

4. Date, configurare și administrare

Administrarea funcțională a VOGO-ROEID asigură administrarea parametrilor de conectare, mapării atributelor de identitate, profilurilor și regulilor de asociere a conturilor.

Modulul asigură

- Configurare unitară, cu păstrarea informațiilor într-un flux integrat.
- Notificări configurabile la evenimente, termene și schimbări de stare.
- Nomenclatoare, tipuri, stări, termene și reguli configurabile.
- Metadate obligatorii și opționale, cu validări și valori controlate.
- Versionarea configurațiilor și promovarea lor între medii.
- Administrare separată pe organizație, structură și rol.
- Suportă autentificarea biometrică disponibilă pe dispozitivul mobil, inclusiv prin amprentă și recunoaștere facială.
- Jurnal complet pentru autentificare, consultare, creare, modificare, aprobare, transmitere și administrare.
- Notificări configurabile prin canalele active în proiect.
- Administrare unitară și autentificare unică (single sign-on).
- Baze de date relaționale și stocare configurabilă, cu portabilitatea datelor.
- Actualizări controlate, posibilitate de revenire și note de versiune.

5. Integrare și interoperabilitate

Interoperabilitatea VOGO-ROEID acoperă schimbul securizat de date de autentificare între ROeID, portal, serviciile online și infrastructura de identitate VOGO eBS.

Modulul asigură

- Import și export controlat pentru inițializare, migrare și interoperabilitate.
- Identificatori stabili, idempotency și mecanisme de reluare a operațiunilor.
- Jurnalizarea schimburilor și reconcilierea erorilor de integrare.
- Autentificare integrată cu serviciile de identitate configurate pentru organizație.
- Permite integrarea cu ROeID și PDURo.

6. Identitate, acces și securitate

Mecanismele de identitate și acces din VOGO-ROEID asigură validarea identității, tokenurilor și sesiunilor și aplicarea drepturilor corespunzătoare profilului autentificat.

Modulul asigură

- Autentificare unică prin ROeID, bazată pe identitatea electronică a cetățeanului.
- Consimțământ explicit, minimizarea datelor și jurnalizarea autentificărilor.
- Salvare intermediară, reluare controlată și istoric al operațiunilor.
- Permite accesul securizat la serviciile online prin autentificare ROeID.
- Permite accesul la funcționalitățile autorizate ale platformei imediat după autentificare.
- Control al accesului pe roluri, structură, operație și obiect de business.
- Principiul privilegiului minim, delegare temporară și revocare explicită.
- Criptarea comunicațiilor și protejarea datelor sensibile.
- JWT (JSON Web Tokens): Token-uri care conțin afirmații sau declarații despre o entitate, oferind autentificare și schimb de informații securizate.

7. Audit, trasabilitate și conformitate

Trasabilitatea VOGO-ROEID acoperă jurnalizarea autentificărilor, răspunsurilor ROeID, asocierilor de cont, sesiunilor și evenimentelor de securitate.

Modulul asigură

- Păstrarea autorului, momentului, motivului și valorilor relevante pentru fiecare schimbare.
- Politici de retenție și acces la dovezi pentru controale și audit.
- Protecția datelor conform principiilor GDPR, inclusiv minimizare și acces justificat.
- Export de audit și rapoarte de conformitate cu păstrarea integrității înregistrărilor operaționale.
- Istoric al notificărilor și dovada transmiterii.

8. Raportare, notificări și analiză

Funcțiile de raportare și notificare din VOGO-ROEID asigură monitorizarea autentificărilor reușite sau respinse, erorilor de integrare, sesiunilor și alertelor de securitate.

Modulul asigură

- Tablouri de bord operaționale și indicatori configurați pe rol.
- Rapoarte filtrabile și exportabile.
- Indicatori de volum, durată, stare, termen și excepție.

9. Arhitectură, deployment și scalabilitate

Arhitectura VOGO-ROEID susține operarea conectorului ROeID prin componente securizate și scalabile, integrate cu serviciile de identitate ale platformei.

Modulul asigură

- Deployment on-premises, în cloud privat sau în arhitectură hibridă.
- Operare pe infrastructura virtualizată sau containerizată configurată pentru proiect.
- Separarea mediilor de dezvoltare, testare, acceptanță și producție.
- Scalare orizontală a componentelor stateless, conform arhitecturii proiectului.
- Punct unic de contact, ticketing și escaladare pe niveluri de severitate.

10. Continuitate, backup și operare

Continuitatea operațională a VOGO-ROEID asigură menținerea autentificării prin monitorizare, backup al configurației, restaurare și proceduri de recuperare a integrității.

Modulul asigură

- Restaurare testată și proceduri documentate de recuperare.
- Politici de disponibilitate și recuperare adaptate criticității modulului.

11. Livrare, suport și evoluție

Livrarea și operarea asistată a VOGO-ROEID includ configurarea conectorului, documentarea parametrilor, instruirea administratorilor, suportul și actualizarea controlată.

Modulul asigură

- Instalare, configurare, integrare și documentație tehnică și de utilizare.
- Actualizări de securitate și corecții pe perioada de suport.

12. Alte funcționalități

Modulul asigură:

1. Fallback administrativ controlat pentru situațiile de indisponibilitate a serviciului extern.
2. Acces unitar la informații și servicii, cu experiență coerentă pe web și mobil.
3. Date și documente urmărite de la inițiere până la închidere.
4. Modulul asigură validarea identității prin ROeID prin următoarele funcționalități:
5. Identifică cetățeanul care accesează serviciile platformei online prin identitatea electronică validată.
6. Interfață în limba română, responsive și adaptată rolului utilizatorului.
7. Automatizează integral crearea contului și a profilului utilizatorului.
8. Automatizează accesul la serviciile online prin înrolarea utilizatorului care a interacționat anterior cu instituția, de exemplu prin existența unui bun impozabil în evidența UAT-ului.
9. API REST documentat și servicii securizate pentru integrare.
10. Webhook-uri și evenimente pentru sincronizarea cu sisteme terțe.
11. Conectori pentru e-mail, fișiere, baze de date și servicii web.
12. Importă utilizatori din Active Directory.
13. Separarea atribuțiilor administrative și verificarea accesului la nivelul serviciilor.
14. Oferă integrare nativă cu sistemele Microsoft Active Directory și Keycloak.
15. Verificarea identității utilizatorilor și a sistemelor care interacționează cu API-ul este primul pas în securizarea acestuia.
16. Metodele comune includ:
17. Oferă suport implicit pentru autentificare multi-factor, atât pentru conectarea la sistem, cât și pentru ridicarea drepturilor utilizatorilor.
18. Backup periodic pentru date, configurații și documente.
19. Monitorizarea serviciilor, capacității, erorilor și performanței.
20. Instruirea utilizatorilor și administratorilor pe roluri.
21. Asigură autentificarea cetățenilor prin ROeID și corelarea identității electronice cu profilul utilizatorului din portal.
22. Permite revenirea securizată în serviciul inițiat după finalizarea fluxului de identificare ROeID.
23. Reducerea timpului de procesare și a operațiunilor manuale repetitive.
24. Corelarea identității validate cu profilul și dosarul digital al solicitantului.
25. Pași clari, validări la introducerea datelor și mesaje explicite de succes sau eroare.
26. Căutare, filtrare, sortare și export pentru listele operaționale.
27. Extinderea controlată cu noi formulare, fluxuri, rapoarte și integrări.
28. Configurare unitară, cu păstrarea informațiilor într-un flux integrat.
29. Notificări configurabile la evenimente, termene și schimbări de stare.
30. Nomenclatoare, tipuri, stări, termene și reguli configurabile.
31. Metadate obligatorii și opționale, cu validări și valori controlate.
32. Versionarea configurațiilor și promovarea lor între medii.
33. Administrare separată pe organizație, structură și rol.
34. Suportă autentificarea biometrică disponibilă pe dispozitivul mobil, inclusiv prin amprentă și recunoaștere facială.
35. Jurnal complet pentru autentificare, consultare, creare, modificare, aprobare, transmitere și administrare.
36. Notificări configurabile prin canalele active în proiect.
37. Administrare unitară și autentificare unică (single sign-on).
38. Baze de date relaționale și stocare configurabilă, cu portabilitatea datelor.
39. Actualizări controlate, posibilitate de revenire și note de versiune.
40. Import și export controlat pentru inițializare, migrare și interoperabilitate.
41. Identificatori stabili, idempotency și mecanisme de reluare a operațiunilor.

42. Jurnalizarea schimburilor și reconcilierea erorilor de integrare.
43. Autentificare integrată cu serviciile de identitate configurate pentru organizație.
44. Permite integrarea cu ROeID și PDURo.
45. Autentificare unică prin ROeID, bazată pe identitatea electronică a cetățeanului.
46. Consimțământ explicit, minimizarea datelor și jurnalizarea autentificărilor.
47. Salvare intermediară, reluare controlată și istoric al operațiunilor.
48. Permite accesul securizat la serviciile online prin autentificare ROeID.
49. Permite accesul la funcționalitățile autorizate ale platformei imediat după autentificare.
50. Control al accesului pe roluri, structură, operație și obiect de business.
51. Principiul privilegiului minim, delegare temporară și revocare explicită.
52. Criptarea comunicațiilor și protejarea datelor sensibile.
53. JWT (JSON Web Tokens): Token-uri care conțin afirmații sau declarații despre o entitate, oferind autentificare și schimb de informații securizate.
54. Păstrarea autorului, momentului, motivului și valorilor relevante pentru fiecare schimbare.
55. Politici de retenție și acces la dovezi pentru controale și audit.
56. Protecția datelor conform principiilor GDPR, inclusiv minimizare și acces justificat.
57. Export de audit și rapoarte de conformitate cu păstrarea integrității înregistrărilor operaționale.
58. Istoric al notificărilor și dovada transmiterii.
59. Tablouri de bord operaționale și indicatori configurați pe rol.
60. Rapoarte filtrabile și exportabile.
61. Indicatori de volum, durată, stare, termen și excepție.
62. Deployment on-premises, în cloud privat sau în arhitectură hibridă.
63. Operare pe infrastructura virtualizată sau containerizată configurată pentru proiect.
64. Separarea mediilor de dezvoltare, testare, acceptanță și producție.
65. Scalare orizontală a componentelor stateless, conform arhitecturii proiectului.
66. Punct unic de contact, ticketing și escaladare pe niveluri de severitate.
67. Restaurare testată și proceduri documentate de recuperare.
68. Politici de disponibilitate și recuperare adaptate criticității modului.
69. Instalare, configurare, integrare și documentație tehnică și de utilizare.