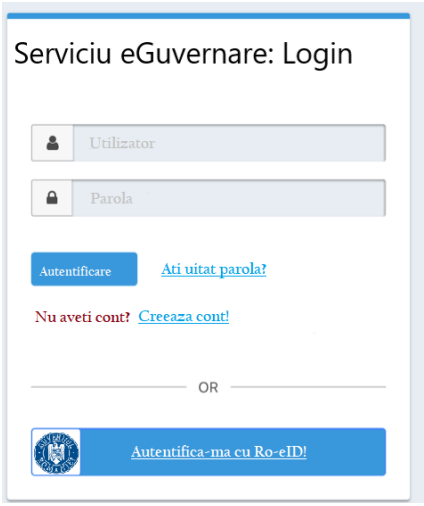
Inrolarea in PSCID a furnizorilor de servicii eGuvernare

Prin implementarea *„Platformei Software Centralizata pentru Identificare Digitala” („PSCID”)* Autoritatea pentru Digitalizarea Romaniei (denumita în continuare și ADR) urmareste ca obiectiv general al proiectului imbunatatirea si automatizarea modalitatii de acces a serviciilor electronice guvernamentale de catre cetateni si asigurarea **identitatii electronice unice** ale fiecarui cetatean care utilizeaza servicii electronice de eGuvernare.



Obiectivele specifice ale proiectului sunt:

- Constituirea **Registrului Electronic National de Identitati Electronice** in cadrul caruia se vor regasi Identitatile Electronice ale tuturor consumatorilor de servicii electronice de eGuvernare;
- Interconectarea cu portalul de acces unitar si securizat la serviciile electronice de eGuvernare si inrolarea cetatenilor la serviciile dorite;
- Interconectarea cu Catalogul Serviciilor Electronice de eGuvernare la care cetatenii se vor inrola prin intermediul PSCID;
- Cresterea gradului de utilizare a serviciilor de eGuvernare printr-o modalitate consecventa si simplificata de autentificare si accesare (inclusiv SSO – Single Sign ON);
- Inrolarea in cadrul PSCID a sistemelor si serviciilor electronice de eGuvernare din Romania;
- Inrolarea in cadrul PSCID a furnizorilor de identitate (publici si privati) existenti;
- Interconectarea PSCID cu nodul eIDAS national;
- Reducerea riscului in utilizarea serviciilor de eGuvernare si diminuarea posibilitatii si impactului de furt de identitate.

PSCID va asigura toate aspectele mai-sus mentionate si in plus isi propune sa implementeze si instrumente de detectare a posibilelor furturi de identitate.

Pentru a putea realiza un management eficient al identitatilor electronice trebuie sa fie identificate serviciile de eGuvernare electronice actuale, consumatorii acestora si modalitatile de identificare si autentificare a utilizatorilor (credentialele). Referitor la credentialele utilizate pentru accesarea serviciilor eGuvernare, prin intermediul PSCID vor fi asigurate:

- instrumente de emitere, gestionare si de personalizare a credentialelor de tip parole;
- instrumente de emitere si gestionare tokenuri virtuale (software) de tip one-time- password (OTP);
- suportul pentru integrarea cu credentialele de tip certificate digitale emise de terti:
  - calificate emise de furnizori autorizati;
  - necalificate emise de institutiile statului (STS, MAI);

Avantajele modelului de autentificare centralizat

- **Imbunatatirea experientei de utilizare a Serviciilor de eGuvernare**

  Prin utilizarea autentificarii centralizate, cetatenii vor putea sa se autentifice o singura data pentru toate Serviciile inrolate. In acest mod, utilizatorii nu vor mai retine mai multe credentiale de autentificare catre deverse servicii, iar modul de accesare poate fi facut printr-un singur click din portalul comun de e-identitate.

- **Securitate imbunatatita**

  Prin existenta unui singur mecanism securizat de autentificare, cetatenii vor pastra intr-un singur loc credentialele de acces. De asemenea, autentificarea poate fi imbunatatita prin mecanisme suplimentare de securitate cum ar fi: certificate digitale, cod de confirmare trimis prin SMS sau email, etc.

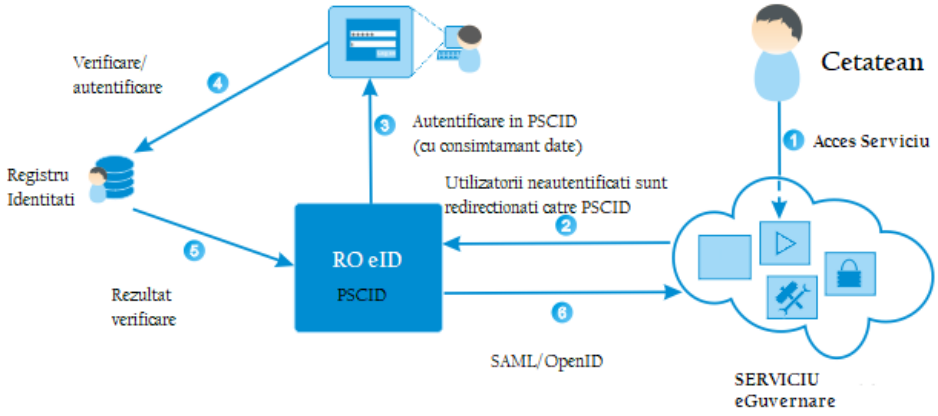
- **Simplificarea managementului utilizatorilor in cadrul platformelor**

  Prin centralizarea sistemului de acces, managementul ciclului de viata al utilizatorilor cade in sarcina unui furnizorului de identitate si anume al platformei PSCID.

Inrolarea in PSCID a furnizorilor de servicii eGuvernare

- **Adoptarea modelului de incredere Federalizat**

In vederea realizarii parteneriatului intre platforma PSCID si Furnizorii de Servicii de eGuvernare, este necesara stabilirea unor acorduri / protocoale de colaborare pentru asigurarea increderii si transferului de identitati si credentiale de autentificare intre Platforma PSCID si sistemele eGuvernare. Incheierea acestor acorduri / protocoale va permite Furnizorilor de Servicii eGuvernare sa ia decizii privind accesul in sistemele proprii pe baza nivelului de incredere definit in cadrul Platformei PSCID.



- **Federalizarea autentificarii Single Sign-On (SSO)**

Federalizarea accesului Single Sign-On (SSO) presupune o relație între doua sau mai multe părți interesate in ceea ce priveste **autentificarea și autorizarea utilizatorilor** și care depășește diferențele tehnologice între diferite entități.

Platforma PSCID reprezintă in cadrul acestui sistem de incredere federalizat entitatea ***Furnizor de Identitate (Identity Provider - IdP)*** fiind responsabilă pentru gestionarea identităților și garantarea identității utilizatorilor. ***Furnizorii de Servicii eGuvernare (denumiți Service Provider - SP)*** autorizează accesul la serviciile oferite pe baza informațiilor despre utilizator primite de la Furnizorul de Identitate (respectiv PSCID).

Tranzacțiile dintre partenerii care formează Federația SSO permit:

- Schimb sigur de informații de identificare a utilizatorilor între parteneri.
- Stabilirea unei relații între identitatea utilizatorului din partea Furnizor de Identitate (PSCID) și identitatea utilizatorului în sistemul Furnizorului de Servicii eGuvernare.
- Funcționalitate de conectare unică între site-urile web ale partenerilor din cadrul Federației SSO.
- Controlul accesului la resursele Furnizorului de Servicii eGuvernare pe baza informațiilor primite de la Furnizorul de Identitate.
- Interoperabilitate între medii eterogene

Federalizarea autentificarii SSO poate fi realizată prin implementarea oricăruia dintre următoarelor două standarde de comunicare securizate / protocoale de autentificare:

- ✓ ***Security Assertion Markup Language (SAML)***
- ✓ ***OpenID Connect***

Protocolul Security Assertion Markup Language (SAML)

SAML este un protocol dezvoltat de OASIS (Organization for the Advancement of Structured Information Standards). SAML este un cadru XML destinat schimbului de date de autentificare și autorizare. SAML folosește o asertiune (SAML Token) pentru a face schimb de informații de identificare a utilizatorului între entități. Tokenul este semnat criptografic, criptarea este opțională. Asertiunile SAML pot fi:

- Asertiune de autentificare – confirmă autentificarea utilizatorului, timpul de conectare și metoda de autentificare
- Asertiune de autorizare – oferă informații despre utilizator: dacă utilizatorul este autorizat să utilizeze serviciul sau dacă Identity Provider a respins cererea din cauza autentificării incorecte
- Asertiunea atributului - trimite anumite atribute SAML către Service Provider (informații suplimentare despre utilizator)

Protocolul SAML asigură un proces de autentificare și autorizare în mediul în care se stabilește Federația SSO între entități.

Protocolul OpenID Connect

OpenID Connect este o actualizare a protocolului OAuth 2.0, care permite autentificarea federalizata. Spre deosebire de specificațiile SAML care se bazează pe XML, OpenID Connect se bazează pe JSON și folosește JSON Web Token (JWT). Protocolul este conceput astfel încât să poată fi utilizat în toate tipurile de aplicații client, inclusiv în aplicații JavaScript (aplicații care rulează doar într-un browser web), precum și în aplicații native (aplicații Android, iOS, Windows, Linux). Tokenul este semnat criptografic, criptarea este opțională.

Înrolarea Serviciilor de eGuvernare (Service Provider) in platforma PSCID.

Procesul de autentificare prin PSCID

Prin inrolarea serviciilor de eGuvernare in platforma PSCID, cetatenii vor avea la dispozitie un catalog de servicii la care au sau doresc sa aiba acces prin SSO.

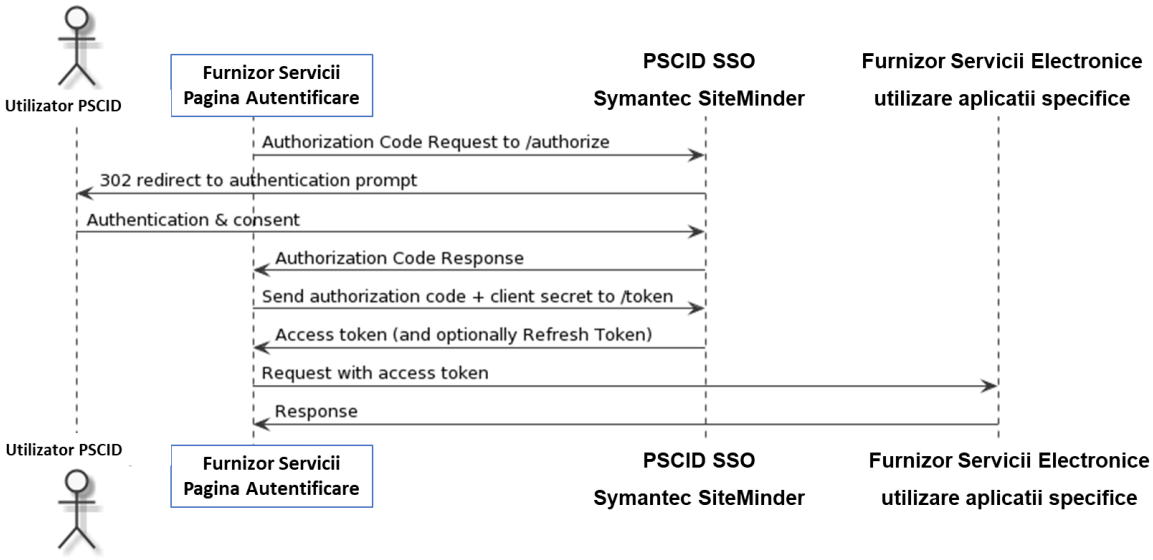
In cazul in care cetatenii vor accesa un serviciu prin modul de autentificare PSCID, acestia vor fi identificati cu utilizatori existenti deja (prin potrivirea unui atribut unic de identificare) sau vor fi trecuti printr-un proces transparent de inrolare pe baza atributelor livrate de catre procesul de autentificare. Se va avea in vedere o uniformizare a necesarului de atribute pentru inrolare in serviciile publice de eGuvernare astfel incat procesul de inrolare intr-un serviciu sa se faca fara un aport suplimentare de date solicitate cetatenilor.

In vederea inrolarii in serviciul solicitat, cetatenii vor trebui sa acorde un consintamant privind transferul de date.

Pentru înrolarea în PSCID, după încheierea protocoalelor / acordurilor inter-instituționale, trebuie parcurse următoarele etape tehnice:

- Furnizorul de Servicii eGuvernare și Platforma PSCID trebuie să agreeze unul dintre protocoalele SAML sau OpenID in vederea interconectarii.
- Furnizorul de Servicii de eGuvernare si Platforma PSCID vor agrea:
    - Nivelul de autentificare necesar Serviciului de eGuvernare (scazut, mediu sau ridicat)
    - Detaliile procesului de autentificare, conform protocolului utilizat (OpenID / SAML)
    - Atributele transmise de PSCID catre Servciu de eGuvernare dupa consimtamantul utilizatorului si autentificarea cu succes a acestuia, precum si elementul unic prin care utilizatorul să fie identificat în ambele sisteme informatice (identificatorul unic al utilizatorului). **Pentru ca Platforma PSCID să poată fi gestionată odată cu creșterea numărului de servicii de eGuvernare înrolate, identificatorul unic al utilizatorului trebuie să fie același pentru toate serviciile de eGuvernare înrolate** (exemplu: cod CNP / nume+prenume+data nasterii)
- Furnizorul de Servicii eGuvernare va implementa protocolul ales pentru realizarea autentificarii SSO între sistemele proprii si Platforma PSCID, cu asistenta specialistilor implicati in dezvoltarea platformei PSCID.
- Testarea Autentificarii SSO între Platforma PSCID ca Furnizor de Identitate (Identity Provider - IdP) și Furnizorul de Servicii eGuvernare ca Service Provider.

Procedura autentificare utilizator PSCID la un serviciu de eGuvernare utilizând protocol OpenID:



Pas 1. Utilizatorul apelează funcția/butonul ”Autentificare PSCID / ROeID) de pe pagina de autentificare a furnizorului de Servicii Electronice (Service Provider)

Pas 2. Solicitarea de autentificare este retransmisă/preluată de Symantec SiteMinder (PSCID SSO) și utilizatorului i se prezintă pagina de autentificare PSCID/ROeID

Pas 3. Utilizatorul se autentifică utilizând username + parola + OTP/certificat digital și confirma acordul privind transmiterea datelor personale către Service Provider

Pas 4. În cazul autentificării cu succes a utilizatorului, Symantec SiteMinder (PSCID SSO) transmite către browser (componenta de autentificare a Serviciului Electronic) un cod de autorizare

Pas 5. Componenta de autentificare a Serviciului Electronic transmite înapoi către Symantec SiteMinder (PSCID SSO) codul de autorizare primit + identificatul propriu.

Nota: La înrolarea unui Furnizor de Servicii Electronice (Service Provider) în PSCID, pentru fiecare Serviciu Electronic (aplicație) oferit, se configurează în Symantec SiteMinder un identificator unic. Daca un Service Provider oferă mai multe Servicii Electronice (aplicații), fiecare Serviciu Electronic va avea configurat un identificator unic propriu.

Pas 6. Symantec SiteMinder (PSCID SSO) transmite către componenta de autentificare a Serviciului Electronic un Access Token ce include atributele/datele agreate ale utilizatorului și faptul că este autentificat

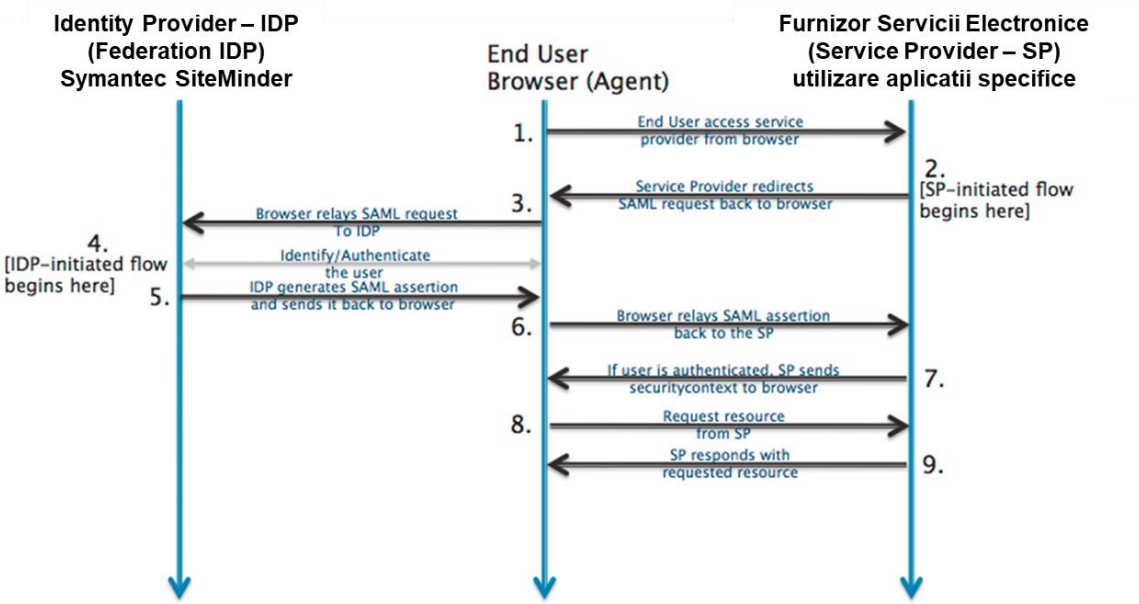
Pas 7. Componenta de autentificare a Serviciului Electronic autentifică utilizatorul în aplicația specifică utilizând token-ul (respectiv atributele/datele) primit de la Symantec SiteMinder.

Pas 8. Aplicația specifică a Serviciului Electronic verifică datele utilizatorului primite și autorizează utilizatorul conform drepturilor de acces proprii. Utilizatorul poate utiliza Serviciul Electronic conform drepturilor existente în acesta.

În cazul utilizării OpenID, comunicația dintre Componenta de autentificare a Serviciului Electronic și Symantec SiteMinder se realizează prin OpenID Claims în tehnologie JSON.

Pentru integrarea OpenID în aplicațiile existente (daca acestea nu suporta nativ OpenID) sunt disponibile pe Internet, gratuit, librării specifice diverselor tehnologii – de exemplu la https://openid.net/developers/certified/

Procedura autentificare utilizator PSCID la un serviciu de eGuvernare utilizând protocol SAML:



Pas 1. Utilizatorul apelează funcția/butonul ”Autentificare PSCID / ROeID) de pe pagina de autentificare a furnizorului de Servicii Electronice (Service Provider)

Pas 2. Solicitarea de autentificare este preluată de Clientul SAML din cadrul Componentei de autentificare a Serviciului Electronic și redirecționată către Identity Provider, respectiv către Symantec SiteMinder (PSCID SSO)

Pas 3. Symantec SiteMinder prezintă utilizatorului pagina de autentificare specifică PSCID/ROeID

Pas 4. Utilizatorul se autentifică utilizând username + parola + OTP/certificat digital și confirma acordul privind transmiterea datelor personale către Service Provider

Pas 5. Symantec SiteMinder (PSCID SSO) generează SAML assertion și o transmite către browser-ul utilizatorului. În cazul autentificării cu succes a utilizatorului, SAML assertion conține atributele/datele utilizatorului (SAML assertion include rezultatul autentificării utilizatorului).

Pas 6. Browser-ul utilizatorului transmite SAML assertion către componenta de autentificare a Serviciului Electronic (SAML client).

Pas 7. Daca utilizatorul este autentificat, componenta de autentificare a Serviciului Electronic autentifică utilizatorul în aplicația specifică utilizând atributele/datele din SAML assertion.

Pas 8. Aplicația specifică a Serviciului Electronic verifică datele utilizatorului primite și autorizează utilizatorul conform drepturilor de acces proprii – utilizatorul poate utiliza Serviciul Electronic confirm drepturilor existente în acesta.

În cazul utilizării OpenID, comunicația dintre Componenta de autentificare a Serviciului Electronic și Symantec SiteMinder se realizează prin SAML assertions în tehnologie HTTPS.

Clienți SAML (SAML toolkit) pentru diverse tehnologii sunt disponibili la https://www.samltool.com/toolkits.php

Mai multe informații privind SAML sunt disponibile la https://wiki.oasis-open.org/security/FrontPage