sistem de interoperabilitate tehnologică cu statele membre UE (SITUE)

Specificații de integrare

Cuprins

[1 Introducere 2](#_Toc144154055)

[1.1 Contextul actual 2](#_Toc144154056)

[1.2 Scopul documentului 4](#_Toc144154057)

[1.3 Termeni si definitii 4](#_Toc144154058)

[2 Arhitectura logică 6](#_Toc144154059)

[2.1 Prezentare eIDAS 6](#_Toc144154060)

[2.2 Actori 8](#_Toc144154061)

[2.3 Procese 9](#_Toc144154062)

[2.3.1 Descriere 9](#_Toc144154063)

[2.4 Funcționalități 10](#_Toc144154064)

[3 Arhitectură integrare SP și IDP 11](#_Toc144154065)

[3.1 Furnizori de servicii (SP) 11](#_Toc144154066)

[3.1.1 Înrolarea 11](#_Toc144154067)

[3.1.2 Autentificarea 11](#_Toc144154068)

[3.2 Furnizori de identitati (IdP) 26](#_Toc144154069)

[3.2.1 Descriere generală 26](#_Toc144154070)

[3.2.2 Scenariu de implementare 31](#_Toc144154071)

# Introducere

## Contextul actual

La 1 iulie 2016 a intrat în vigoare REGULAMENTUL (UE) NR. 910/2014 AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE. Regulamentul se aplică tuturor statelor membre, fără a fi nevoie de o lege națională care să îl adopte. Statele membre trebuie să desemneze organismele responsabile de implementarea Regulamentului UE 910/2014 și să definească modul acestora de lucru.

Regulamentul UE 910/2014 acoperă două domenii principale: Identificarea electronică și Servicii de încredere. În limitele definite prin prezentul proiect, sistemul dezvoltat va răspunde cerințelor Cap. II (Electronic Identification) al Regulamentului.

Cu privire la Identificarea electronică, sunt definite 3 niveluri de siguranță: scăzut, substanțial și ridicat. Statele membre notifică Comisia Europeană cu privire la sistemele de identificare electronică naționale, incluzând nivelurile de securitate și emitentul sau emitenții mijloacelor de identificare electronică din cadrul sistemului.

Interoperabilitatea dintre sistemele de identificare notificate de statele membre se realizează prin noduri (noduri eIDAS) ce reprezintă puncte de legătură care fac parte din arhitectura de interoperabilitate pentru identificarea electronică. Un nod este implicat în autentificarea transfrontalieră a persoanelor și are capacitatea să recunoască și să prelucreze sau să transmită mai departe datele către alte noduri, prin faptul că face posibilă comunicarea dintre infrastructura națională de identificare electronică a unui stat membru și infrastructurile naționale de identificare electronică ale altor state membre.

Regulamentul eIDAS obligă statele membre să notifice către celelalte state și către CE serviciile de e-guvernare naționale și mecanismele de autentificare la acestea pe cele 3 niveluri de identificare: scăzut, substanțial și ridicat.

Descrierea cerințelor minime privind nivelul de asigurare este prezentat în regulamentul de punere în aplicare (UE) 2015/1502 al Comisiei din 8 septembrie 2015 de stabilire a unor specificații și proceduri tehnice minime pentru nivelurile de asigurare a încrederii ale mijloacelor de identificare electronică în temeiul articolului 8 alineatul (3) din Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă.

Obiectivul proiectului este realizarea de către Autoritatea Contractantă – Autoritatea pentru Digitalizarea României - a Sistemului de Interoperabilitate Tehnologică cu Statele Membre UE (SITUE) care va avea la baza construcția nodului eIDAS pentru România si va realiza interconectarea acestuia cu nodurile eIDAS ale celorlalte state membre și cu furnizorii de identitate si servicii electronice din România.

SITUE va fi utilizat pentru autentificarea națională și transfrontalieră a solicitanților in relația cu furnizorii de servicii de e-guvernare și va face posibilă comunicarea dintre infrastructura națională de identificare electronică și infrastructurile naționale de identificare electronică ale altor state membre UE.

Proiectul are următoarele obiective specifice:

a) Integrarea SITUE in rețeaua europeana eIDAS

b) Interconectarea SITUE cu furnizorii de servicii eGuvernare din România

c) Testarea specifică a interoperabilității tehnice asigurate de SITUE

Soluția va implementa mijloace tehnice pentru implementarea modalităților de suspendare sau de revocare a întregului sistem de identificare sau de autentificare ori a părților compromise din aceste sisteme.

Proiectul ține seama de toate deciziile publicate pe situl comisiei europene cu privire la regulamentul 910, pentru semnătura, de exemplu DECIZIA DE PUNERE ÎN APLICARE (UE) 2015/1506 A COMISIEI din 8 septembrie 2015 de stabilire a specificațiilor referitoare la formatele semnăturilor și sigiliilor electronice avansate care trebuie recunoscute de către organismele din sectorul public în temeiul articolului 27 alineatul (5) și al articolului 37 alineatul (5) din Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă sau DECIZIA DE PUNERE ÎN APLICARE (UE) 2015/1505 A COMISIEI din 8 septembrie 2015 de stabilire a specificațiilor tehnice și a formatelor pentru listele sigure în temeiul articolului 22 alineatul (5) din Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă.

Realizarea nodului eIDAS presupune implicarea minim a următoarelor tipuri de entități: Sisteme ce oferă servicii electronice de eguvernare (Service providers :ADR, ANAF- Ministerul Finantelor, CNAS, ONRC, MAI), furnizorii de identități electronice (Identity Providers – ROEID implementat prin proiectul PSCID-Platforma Software Centralizată pentru Identificare Digitală), nodurile eIDAS ale celorlalte state membre UE. Într-un context transfrontalier se va utiliza un set minim de date de identificare personală care desemnează în mod unic o persoană fizică sau juridică. Aceste atribute sunt definite în legislația secundară de implementare a Regulamentului UE 910/2014.

Pentru orice alt beneficiar sistemul va pune la dispoziție, in condițiile recomandate de rețeaua de cooperare, toate mecanismele tehnice pentru conectare: interfete, documentatie, proceduri)

Pentru acces transfrontalier, SITUE va opera cu următorul set minim de date pentru o persoană fizică, care conține toate atributele obligatorii de mai jos:

1. numele de familie actual(e);
2. prenumele actual(e);
3. data nașterii;
4. un identificator unic, care este alcătuit de către statul membru expeditor în conformitate cu specificațiile tehnice privind identificarea transfrontalieră și care are o durată de viață cât mai mare.

Setul minim de date pentru o persoană fizică poate conține unul sau mai multe din atributele suplimentare de mai jos:

1. prenumele și numele de familie la naștere;
2. locul nașterii;
3. adresa actuală;
4. sexul.

## Scopul documentului

Acest document este elaborat pentru a oferi informaţii şi detalii de interes pentru entitatile care doresc sa se integreze cu nodule eIDAS din România, din perspectiva furnizorilor de servicii electronice (SP) și a furnizorilor de identități electronice.

## Termeni si definitii

| **Termen** | **Definitie** |
| --- | --- |
| IDP | Identity Provider - Furnizor de identitate si autorizare – sistemul care autentifica utilizatorul |
| SSO | Single Sign On |
| JWT  | JSON Web Token - token in format json care contine datele despre utilizatorul autentificat |
| PSCID | Platforma Software Centralizată pentru Identificare Digitală |
| eIDAS | electronic IDentification, Authentication and trust Services |
| Nod-eIDAS:  | entitate operațională implicată în autentificarea transfrontalieră a persoanelor. |
| SM expeditor (de trimitere) | stat membru a cărui schemă eID este utilizată în procesul de autentificare și trimitere ID autentificat către statul membru receptor. |
| SM receptor | stat membru în care se găseşte partea care solicită autentificarea unei persoane |
| SP | Service Provider – Sistem informtic care oferă servicii publice de încredere |
| SM | stat reglementat de regulamentul eIDAS, un stat membru al Uniunii Europene și/sau al Zonei Economice Europene |

# Arhitectura logică

## Prezentare eIDAS

Soluția eIDAS permite cetățenilor din statele membre să dovedească și să verifice identitatea lor atunci când accesează servicii online în alte state membre. Această soluţie permite cetățenilor să se autentifice folosind eID-urile lor și conectându-se cu furnizorul lor de identitate (IdP) din țara acestora. Un proces descris la nivel înalt este următorul:

1. Un cetățean solicită accesul la un serviciu on-line într-un stat membru.
2. Cetăţeanul este rugat să se autentifice prin serviciul on-line.
3. În etapa de autentificare, devine evident că cetățeanul are un eID din alt stat membru.
4. Solicitarea de autentificare este trimisă în țara cetățeanului pentru autentificare, prin soluția eIDAS, către Furnizorul de Identitate (IdP) al cetățeanului unde are loc autentificarea.
5. Rezultatul autentificării este returnat furnizorului de servicii.
6. Autentificarea este completă, iar cetățeanul poate continua cu accesarea serviciului.

Soluția eIDAS face interoperabile între ele diferite protocoale naționale eID. Soluția folosește protocolul eIDAS pentru a traduce datele naționale de identificare într-un format comun care este înțeles și utilizat de statele membre.

Acest lucru duce la interoperabilitatea și acceptarea eID ale statelor membre în alte state membre, deschizând noi posibilități și oportunități pentru cetățeni de a utiliza serviciile transfrontaliere.

Imaginea de mai jos ilustrează modul în care utilizarea protocolului eIDAS și implementarea nodurilor eIDAS permit comunicarea între arhitecturile naționale independente ale schemelor eID, susținând autentificarea transfrontalieră fără probleme.



Un nod eIDAS poate acționa fie ca solicitant, fie ca furnizor de autentificare transfrontalieră. Statul membru care solicită autentificarea se numește statul membru receptor, în timp ce statul membru care furnizează autentificarea se numește statul membru expeditor.

Un stat membru se poate regăsi în una dintre următoarele situaţii:

1. Solicită o autentificare transfrontalieră.

Atunci când un serviciu online (Furnizor de servicii) conectat la o schemă națională eID (Furnizor de identitate electroncă) întâlnește un utilizator dintr-un alt stat membru (în etapa de identificare a utilizatorului), acesta emite o cerere de autentificare în țara de origine a cetățeanului. Această solicitare este tradusă în protocolul eIDAS. Acesta este apoi direcționat prin nodul eIDAS al țării furnizorului de servicii (statul membru receptor) pentru a solicita autentificarea transfrontalieră prin nodul eIDAS al țării utilizatorului (statul membru expeditor). Componenta eIDAS-Node utilizată pentru a face cereri pentru autentificări transfrontaliere se numește eIDAS-Connector.

2. Furnizează o autentificare transfrontalieră

După ce un utilizator solicită un serviciu într-un alt stat membru, nodul eIDAS din țara de origine a utilizatorului (statul membru expeditor) va furniza autentificarea transfrontalieră prin serviciul eIDAS.

Datorită naturii unor sisteme eID, fără o componentă centrală, schemele eID corespunzătoare pot fi integrate în rețeaua eIDAS prin modelul de integrare middleware.

**Rolul protocolului eIDAS**

Protocolul permite comunicarea între diferitele noduri eIDAS ale rețelei eIDAS. Principalul avantaj al acestei soluții este că statele membre sunt libere să păstreze și să dezvolte propriile protocoale de autentificare la nivel național. Astfel, soluția de interoperabilitate eIDAS nu necesită nicio modificare a infrastructurii naționale (de exemplu, a comunicației dintre Furnizorii de servicii locali și Furnizorii de identitate).

Protocolul eIDAS este destinat doar pentru autentificarea transfrontalieră. Orice utilizare a acestuia în infrastructura națională nu este recomandată sau acceptată.

## Actori

Diagrama de mai jos ilustrează principalii actori și componente ale arhitecturii eIDAS. Nodurile eIDAS comunică între ele prin translatarea protocoalelor naționale ale statelor membre A și B în protocolul eIDAS.



Actorii sunt tipurile de utilizatori care interacționează cu sistemul. Actorii pot fi utilizatori umani sau alte sisteme:

1. Două state membre
2. Un utilizator (persoană fizică sau juridică).
3. Un furnizor de servicii (administrație publică sau furnizor de servicii electronice) - SP
4. Sunt implicate nodurile eIDAS ale ambelor state membre, fiecare constând din (părțile specifice statelor membre vor fie implementate de fiecare stat membru pentru a se face trecerea între protocoalele naționale ale schemei eID și protocolul eIDAS):
	1. un conector, inclusiv partea specifică statului membru;
	2. un serviciu proxy sau un serviciu middleware, inclusiv partea specifică statului membru;
	3. unul sau mai multe servicii Middleware ale statelor membre pentru comunicarea cu țările Middleware.
5. Un furnizor național de identitate care furnizează informații eID la autentificarea cu succes a utilizatorului. Procedura de autentificare a utilizatorului are loc între utilizator și Furnizorul de Identitate (este în afara Rețelei eIDAS) - IdP

## Procese

Descrierea detaliata a proceselor sistemului se regaseste in documentatia de specificații funcționale ale sistemului.

Nodurile eIDAS Europa sunt de două tipuri, în funcţie de modele tehnice adoptate: Proxy sau Middleware. Nodul naţional realizat prin proiectul SITUE este de tip proxy şi se va conecta la un nod eIDAS de tip proxy (Franța) şi la un nod eIDAS de tip middleware (Germania).

### Descriere

Datorită distincției dintre nodurile eIDAS de tip proxy și nodurile eIDAS de tip middleware, există patru combinații diferite posibile în ceea ce privește solicitarea și furnizarea de autentificare transfrontalieră:

1. Proxy - Proxy: un utilizator dintr-o țară bazată pe o schemă proxy care accesează un serviciu într-o altă țară bazată pe o schemă proxy.
2. Middleware - Proxy: un utilizator dintr-o țară bazată pe o schemă de middleware care accesează un serviciu într-o țară bazată pe o schemă proxy.
3. Proxy - Middleware: Un utilizator dintr-o țară bazată pe o schemă proxy care accesează un serviciu într-o țară bazată pe o schemă middleware.
4. Middleware - Middleware: Un utilizator dintr-o țară bazată pe o schemă de middleware care accesează un serviciu într-o altă țară bazată pe o schemă de middleware.

## Funcționalități

SITUE asigură interoperabilitatea cu nodurile eIDAS din alte state membre și cu furnizorii de servicii (Service Providers), astfel:

1. Utilizatorul din statul membru A solicită acces la serviciile din statul membru B
2. Furnizorul de servicii din statul membru B transmite cererea nodului eIDAS din țara sa
3. Nodul eIDAS din statul membru B cere utilizatorului informații cu privire la țara din care acesta provine
4. După ce utilizatorul furnizează informațiile privind țara de origine nodul eIDAS din statul membru B trimite cererea către nodul eIDAS din statul membru A
5. Nodul eIDAS din statul membru A transmite cererea către Furnizorul de identitate în vederea autentificării. Utilizatorul se autentifică folosind identitatea sa electronică iar după autentificare identitatea este transmisă către nodul eIDAS
6. Nodul eIDAS din statul membru A transmite răspunsul către nodul eIDAS din statul membru B care îl transmite către Furnizorul de servicii
7. Furnizorul de servicii permite accesul utilizatorului

In rolul statului membru A sau B vor fi, pe rând, Romania/Franța, Romania/Germania, Franta/Romania, Germania/Romania.

# Arhitectură integrare SP și IDP

## Furnizori de servicii (SP)

### Înrolarea

Modalitatea de comunicare a datelor între furnizorii de servicii (SP) și SITUE se stabilește de comun acord în cadrul procesului de înrolare.

Pentru înrolare in platforma SITUE este necesara parcurgerea următorilor pași:

1. SITUE cat si SP-ul de interes vor genera cate o pereche de chei (publica si privata). După generarea acestor chei se va realiza un schimb de chei publice intre cele doua entități.
2. Pe lângă cheia publica, SP-ul va alege un identificator unic reprezentativ serviciului lor (Ex.: pentru ghiseul.ro identificatorul poate fi "GHISEUL"). De preferat sa fie in format UPPERCASE iar cuvintele separate prin cratima ("-").
3. SITUE va comunica SP-ului un identificator de eIDAS (un URL de recunoaștere a acestuia).

### Autentificarea

Cererea de autentificare se bazează pe JWT, standard definit in RFC7519: <https://www.rfc-editor.org/rfc/rfc7519>. Pentru implementarea acestui standard poate fi folosita orice librarie disponibila: <https://jwt.io/libraries>.

Token-urile JWT reprezintă un important mod de a transmite securizat informații intre doua entități. Deoarece se pot semna (folosind chei publice sau private) , token-urile asigura identificarea sigura si unica a „partenerului de discuție”. Se verifica inclusiv ca informația transmisa nu a fost alterata prin implicarea in semnare a antetului si a conținutului mesajului. In momentul in care se transmit informații, acestea se semneaza pentru a valida corespondentul; aceasta validare se realizează prin intermediul unei semnături digitale.

Semnătura se poate realiza folosind tehnici criptografice. Exista tehnologii care implementează aceste semnături digitale la nivel programatic cu scopul de a valida conținutul in concordanta cu corespondentul. Atuul JWT se regăsește in aceste semnături utilizate in procesul de validarea a cererii si a răspunsului.

JWT este utilizat pe scara larga in industrie, fiind ușor de implementat si învățat, ceea ce permite oricărui furnizor de servicii, care dorește sa adere la EIDAS, sa implementeze procesul de integrare cu ușurința si rapiditate.

JWT se traduce prin JSON Web Token, si respecta următoarea forma: <header>.<payload>.<signature>

Fiecare componenta reprezintă un sir de caractere de tip Base64 compatibil URL (Standard RFC4648 Secțiunea 5, Tabel 2).

Informația din "header" reprezintă un JSON care contine algoritmul utilizat pentru criptare, ex: header = base64UrlEncoding('{"alg":"ES512","typ":"JWT"}');

Informatia din "payload" este reprezentata de un JSON care reprezinta continutul mesajului, ex: payload = base64UrlEncoding('{"name":"Popescu"}');

Informatia din "signature" este un sir de octeti ce contine semnatura criptografica a informatiei "<header>.<payload>", ex:

signature = base64UrlEncoding(ES512('<header>' + '.' + '<payload>', privateKey));

ES512 este un algoritm de criptare asimetrica folosind o curba eliptica P-521 reprezentat printr-un hash unic folosind SHA512. Fiind asimetric, necesita o cheie privata pentru semnătura si o cheie publica pentru validarea acesteia, in concluzie validarea semnăturii se face cu cheia publica. Standardul RFC7518 secțiunea 3.1 oferă o lista de algoritmi disponibili.

#### Diagrama flux



Pasul 1 - Pregătire cerere semnata de catre SP;

Pasul 2 - Citire cerere si validare semnătura de catre conectorul SITUE, daca totul este in regula se transmite mai departe pentru autentificare catre IdP-ul din nodul eIDAS al statului membru;
Pasul 3 - Autentificare cetățean străin;

Pasul 4 - SITUE primește un răspuns la cererea de autentificare din partea nodului eIDAS al statului membru, pe care o procesează, adaugă o semnătură si o trimite mai departe catre SP;

Pasul 5 - SP-ul primește răspunsul final semnat. SP-ul poate sa valideze răspunsul si sa il proceseze.

#### Initierea cererii de autentificare catre SITUE

SP-ul isi va adauga in sectiunea publica a aplicatiei propria un buton care va permite autentificarea prin eIDAS, similar cu cel din imagina de mai jos:



Dupa accesarea butonului va fi necesar ca SP-ul sa solicite selectarea naționalității utilizatorului (ex. FR/DE):



După selectarea naționalității se va lansa o cerere care SITUE prin intermediul unui formular:

<form action="[https://<url\_eidas\_node>/SpecificConnector/ServiceProvider](https://srodev.patrix.tech/SpecificConnector/ServiceProvider)" method="post">

 <input type="hidden" id="SMSSPRequest" name="SMSSPRequest" value=”<jwt\_request>”/>

 <input type="submit" value="Submit"/>

</form>

Valoarea SMSSPRequest trebuie sa conțină o cerere in format JWT.

Exemplu:

**eyJhbGciOiJFUzUxMiIsInR5cCI6IkpXVCJ9.eyJhdXRoZW50aWNhdGlvbl9yZXF1ZXN0Ijp7ImF0dHJpYnV0ZV9saXN0IjpbeyJ0eXBlIjoicmVxdWVzdGVkX2F0dHJpYnV0ZSIsIm5hbWUiOiJGYW1pbHlOYW1lIiwicmVxdWlyZWQiOnRydWV9LHsidHlwZSI6InJlcXVlc3RlZF9hdHRyaWJ1dGUiLCJuYW1lIjoiRmlyc3ROYW1lIiwicmVxdWlyZWQiOnRydWV9LHsidHlwZSI6InJlcXVlc3RlZF9hdHRyaWJ1dGUiLCJuYW1lIjoiRGF0ZU9mQmlydGgiLCJyZXF1aXJlZCI6dHJ1ZX0seyJ0eXBlIjoicmVxdWVzdGVkX2F0dHJpYnV0ZSIsIm5hbWUiOiJHZW5kZXIiLCJyZXF1aXJlZCI6ZmFsc2V9LHsidHlwZSI6InJlcXVlc3RlZF9hdHRyaWJ1dGUiLCJuYW1lIjoiUGVyc29uSWRlbnRpZmllciIsInJlcXVpcmVkIjp0cnVlfV0sInJlcXVlc3RlZF9hdXRoZW50aWNhdGlvbl9jb250ZXh0Ijp7ImNvbXBhcmlzb24iOiJtaW5pbXVtIiwiY29udGV4dF9jbGFzcyI6WyJBIl19LCJjaXRpemVuX2NvdW50cnkiOiJJVCIsImNyZWF0ZWRfb24iOiIyMDIyLTExLTAzVDIxOjE1OjU1LjQxMyswMjowMCIsImZvcmNlX2F1dGhlbnRpY2F0aW9uIjp0cnVlLCJpZCI6ImFiOTM4Nzk3LTgwNWItNDNlNC1hNjFmLWQ4MjUxYTFlYzFlMyIsInByb3ZpZGVyX25hbWUiOiJTT01FLVNQLVJPIiwicmVxdWVzdGVyX2lkIjoiaHR0cDovL2VpZGFzLmV1L0VpZGFzTm9kZS9SZXF1ZXN0ZXJJZF9STyIsInNlcnZpY2VVcmwiOiJodHRwczovL3lvdXIuc3AuaG9zdC9TUC9SZXR1cm5QYWdlIiwic3BfdHlwZSI6InB1YmxpYyIsInZlcnNpb24iOiIxIn19.ALNwl5UNVKSqG7dTXKv1ihXPW7o6TDg82uD4maN9-16YcX\_KJJ0TnNJAxmqHg\_HHXXW8UITOEkOpelPTyKd77kSwAO53nFIFn5rzfC7w-\_jmZ2B4rAyAGv\_ZtScom7JVtKNO6J2zl0cIWV5jskJTAkIZBJ7VY8m9Z0brPGyF0uwbuIhr**

Exista trei componente principale separate prin “.”:

1. **eyJhbGciOiJFUzUxMiIsInR5cCI6IkpXVCJ9** - reprezinta algoritmul si tipul de token, descris in format JSON si codificat in base64, denumit **json\_base64\_type**.

Decodificat contine:
**{**

 **"alg": "ES512",**

 **"typ": "JWT"**

**}**

1. **eyJhdXRoZW50aWNhdGlvbl9yZXF1ZXN0Ijp...** - reprezinta cererea in format JSON codificat in base64, denumit **json\_base64\_payload**.

Decodificat contine:
**{**

 **"authentication\_request": {**

 **"attribute\_list": [**

 **{**

 **"type": "requested\_attribute",**

 **"name": "FamilyName",**

 **"required": true**

 **},**

 **{**

 **"type": "requested\_attribute",**

 **"name": "FirstName",**

 **"required": true**

 **},**

 **{**

 **"type": "requested\_attribute",**

 **"name": "DateOfBirth",**

 **"required": true**

 **},**

 **{**

 **"type": "requested\_attribute",**

 **"name": "Gender",**

 **"required": false**

 **},**

 **{**

 **"type": "requested\_attribute",**

 **"name": "PersonIdentifier",**

 **"required": true**

 **}**

 **],**

 **"requested\_authentication\_context": {**

 **"comparison": "minimum",**

 **"context\_class": [**

 **"A"**

 **]**

 **},**

 **"citizen\_country": "IT",**

 **"created\_on": "2022-11-03T21:15:55.413+02:00",**

 **"force\_authentication": true,**

 **"id": "ab938797-805b-43e4-a61f-d8251a1ec1e3",**

 **"provider\_name": "SOME-SP-RO",**

 **"requester\_id": "http://eidas.eu/EidasNode/RequesterId\_RO",**

 **"serviceUrl": "https://your.sp.host/SP/ReturnPage",**

 **"sp\_type": "public",**

 **"version": "1"**

 **}**

**}**

1. **ALNwl5UNVKSqG7dTXKv1ihXPW7o6TDg82uD4maN9[...]**

reprezintă semnătura digitala folosind cheia privata a SP-ului asupra combinației **json\_base64\_type**.**json\_base64\_payload**;

rezultatul este un sir de octeți codificat in base64. Aceasta semnătură este critică, deoarece SITUE o va folosi pentru a verifica integritatea cererii. Verificarea se va realiza cu algoritmul criptografic, folosind cheia publica a SP-ului (menționat in secțiunea de înrolare).

*Atribute cerere*

1. attribute\_list - lista de atribute necesara SP-ului pentru identificarea unui cetățean străin al unui stat membru;
2. requested\_authentication\_context - precizează nivelul de încredere; valorile aferente context\_class vor conțin valori intre A si E; ordinea alfabetica crescătoare denota nivelul de încredere crescut.
3. citizen\_country - tara selectata de către cetățeanul străin pe pagina oferita de SP.
4. created\_on - timestamp aferent momentului creării cererii;
5. force\_authentication - se recomanda utilizarea valorii "true";
6. id - identificator unic generat de către SP; poate fi asociat ca o sesiune recunoscuta de catre SP.
7. provider\_name - identificator unic comunicat de către SP si înregistrat de către SITUE in procesul de înrolare;
8. requester\_id - va fi comunicat de către SITUE către SP conform procesului de înrolare
9. serviceUrl - URL-ul către o pagina oferita de SP care accepta o cerere de tip POST; va fi apelat pentru transmiterea răspunsului aferent cererii

Transmiterea cererii, după cum a fost descrisa anterior, va declanșa procesul de autentificare al cetățeanului străin de către SITUE, in colaborare cu nodul eIDAS al statului membru de origine al cetățeanului.

Nodul eIDAS al statului membru de origine va redirecționa cetățeanul, in cadrul procesului de autentificare către pagina de login aparținând furnizorului de identități al statului membru:



#### Procesarea răspunsului de autentificare de catre SP

Răspunsul aferent cererii de autentificare se trimite prin POST către serviceUrl-ul din cerere.

Exemplu răspuns:
***HTTP POST:*** [***https://your.sp.host/SP/ReturnPage***](https://your.sp.host/SP/ReturnPage) ***Content-Type: application/x-www-form-urlencoded***
***SMSSPResponse=*eyJhbGciOiJFUzUxMiIsInR5cCI6IkpXVCJ9.eyJyZXNwb25zZSI6eyJhdHRyaWJ1dGVfbGlzdCI6W3sidHlwZSI6InN0cmluZ19saXN0IiwibmFtZSI6IkZhbWlseU5hbWUiLCJ2YWx1ZXMiOlt7InZhbHVlIjoiTWFyY28ifV19LHsidHlwZSI6InN0cmluZ19saXN0IiwibmFtZSI6IkZpcnN0TmFtZSIsInZhbHVlcyI6W3sidmFsdWUiOiJHaXVzZXBwZSJ9XX0seyJ0eXBlIjoiZGF0ZSIsIm5hbWUiOiJEYXRlT2ZCaXJ0aCIsInZhbHVlIjoiMTk2NC0xMi0zMSJ9LHsidHlwZSI6InN0cmluZ19saXN0IiwibmFtZSI6IlBlcnNvbklkZW50aWZpZXIiLCJ2YWx1ZXMiOlt7InZhbHVlIjoiMjM0OTg3NTYyMzk1NjIzOTQ1In1dfV0sImF1dGhlbnRpY2F0aW9uX2NvbnRleHRfY2xhc3MiOiJCIiwiY3JlYXRlZF9vbiI6IjIwMjItMTEtMDNUMjE6MTU6NTUuNDEzKzAyOjAwIiwiaWQiOiIxMGY0NmE5ZC0yYTYwLTRmODUtOGY0Ni1hNGZmMGVmOTlmNDEiLCJpbnJlc3BvbnNlX3RvIjoiYWI5Mzg3OTctODA1Yi00M2U0LWE2MWYtZDgyNTFhMWVjMWUzIiwiaXNzdWVyIjoic3BlY2lmaWNDb25uZWN0b3JSTyIsIm5hbWVfaWQiOiJ1bnNwZWNpZmllZCIsInN0YXR1cyI6eyJzdGF0dXNfY29kZSI6InN1Y2Nlc3MifSwic3ViamVjdCI6IjAxMjM0NTYiLCJ2ZXJzaW9uIjoiMSJ9fQ.AdyLBbK\_ma-svZZ2LtZA5QsDN4ELG-BrnXgkU-6NvSisbybBi6y\_b8t4S6b4dGMxm7OcVG3OCDbxKPWM-gqOWVkfAHZX0QoPtBY8HgWcY4KcA9JRQTzIlZCndzVIuOh7qbn1LIJivta8GeVnom7caw91RQSIfWgcqDaPBBHkB9q14YTB**

Similar cu cererea transmisa, SP-ul primește un răspuns in format JWT.

Informațiile primite se afla in a doua secțiune (separate prin "."), in format JSON codificat in base64: **eyJyZXNwb25zZSI6eyJhdHRyaWJ1dGVf[...]**

Decodificat:
**{**

 **"response": {**

 **"attribute\_list": [**

 **{**

 **"type": "string\_list",**

 **"name": "FamilyName",**

 **"values": [**

 **{**

 **"value": "Marco"**

 **}**

 **]**

 **},**

 **{**

 **"type": "string\_list",**

 **"name": "FirstName",**

 **"values": [**

 **{**

 **"value": "Giuseppe"**

 **}**

 **]**

 **},**

 **{**

 **"type": "date",**

 **"name": "DateOfBirth",**

 **"value": "1964-12-31"**

 **},**

 **{**

 **"type": "string\_list",**

 **"name": "PersonIdentifier",**

 **"values": [**

 **{**

 **"value": "234987562395623945"**

 **}**

 **]**

 **}**

 **],**

 **"authentication\_context\_class": "B",**

 **"created\_on": "2022-11-03T21:15:55.413+02:00",**

 **"id": "10f46a9d-2a60-4f85-8f46-a4ff0ef99f41",**

 **"inresponse\_to": "ab938797-805b-43e4-a61f-d8251a1ec1e3",**

 **"issuer": "specificConnectorRO",**

 **"name\_id": "unspecified",**

 **"status": {**

 **"status\_code": "success"**

 **},**

 **"subject": "0123456",**

 **"version": "1"**

 **}**

1. **}**

SP-ul va valida semnătura folosind cheia publica oferita de către SITUE:
**AdyLBbK\_ma-svZZ2LtZA5QsDN4ELG-BrnXgkU-[…]**

SP-ul poate interpreta câmpurilor astfel:

1. status
	1. comunica daca autentificarea a fost realizata cu success sau nu
	2. posibile valori:
		1. success
		2. responder failure.
	3. alte informatii pot fi aprovizionate in campurile status\_message si sub\_status\_code
2. attribute\_list
	1. lista de atribute initiate din cerere, dar de data aceasta aprovizionate cu informatiile cerute.
	2. "Gender" nu a fost trecut deoarece in momentul in care a fost creata cererea, s-a mentionat required=false ceea ce oferă libertate SITUE de a alege daca oferă sau nu aceasta informație; in cazul de fata se poate interpreta ca a refuzat sa trimită aceasta informație, asadar nu este completata in răspuns;
3. authentication\_context\_class
	1. nivelul de incredere oferit de catre nodul eIDAS al statului membru din care face parte cetateanul
	2. se observa ca in cerere s-a precizat un minim de clasa A dar s-a raspuns cu un alt nivel, clasa B; SP-ul va decide daca ii este suficient acest nivel de incredere
4. created\_on
	1. timestamp aferent momentului in care a fost creat raspunsul;
5. id
	1. identificator unic al raspunsului;
6. inresponse\_to
	1. identic cu id-ul din cerere.
	2. va fi folosit de catre SP pentru a identifica originea cererii si a o corela cu acest raspuns;
7. issuer,name,id,subject,version
	1. informatii metadata din SITUE
	2. pot fi pot fi folosite (optional) de catre SP pentru a verifica un potential de inconsistenta;

## Furnizori de identitati (IdP)

### Descriere generală

OpenID Connect este un modul simplu de identitate simplu dezvoltat pe protocolul OAuth 2.0, care permite clienților să verifice identitatea unui utilizator pe baza autentificării efectuate de un server de autorizare sau furnizor de identitate (IdP), dar și să obțină informații despre utilizatorul final într-o manieră interoperabilă și similară serviciilor REST.

*Beneficiile openid:*

1. Token-uri usor de consumat. Aplicațiile client primesc identitatea utilizatorului codificată într-un JSON Web Token (JWT) securizat numit id\_token. JWT-urile sunt simple, usor de procesat și portabile și acceptă o gamă largă de algoritmi de semnătură și criptare.
2. Protocolul OAuth 2.0. Clienții folosesc fluxuri OAuth 2.0 pentru a obține token-uri de identificare, care funcționează cu aplicații web, precum și cu aplicații mobile native. OAuth 2.0 înseamnă, de asemenea, că exista un singur protocol pentru autentificare și autorizare (obținerea token-urilor de acces).
3. Simplu, dar capabil. Simplitate cu capacitate. OpenID este suficient de simplu pentru a fi integrat cu aplicațiile de bază, oferind în același timp funcții și opțiuni de securitate care pot satisface cerințele exigente ale întreprinderii.

*Tipuri de autentificare (Grant Types):*

1. Openid suporta 4 tipuri de autentificare, in functie de tipul de aplicatie
2. Fluxul implicit (implicit flow) este necesar pentru aplicațiile care nu au o logică „back-end” pe serverul web, cum ar fi o aplicație Javascript.
3. Fluxul de baza (authentication flow) este conceput pentru aplicațiile care au un back-end care poate comunica cu IdP
4. Acordare parola proprietarului resurselor (Resource Owner Password Grant) este folosita când nu exista o interfață de conectare si utilizatorul nu interacționează direct cu sistemele
5. Atribuirea acreditărilor client (client credential grant) este utilă pentru autorizarea de la o mașină la alta, fără intervenția utilizatorului.

*Flux implicit*

Fluxul implicit este necesar pentru aplicațiile și site-urile web care nu au o logică back-end pe serverul web și tot ceea ce este transmis între aplicație sau site și IdP poate fi vizualizat folosind instrumente de dezvoltare a browserului.

În fluxul implicit, o schemă de cheie publică/privată (Cheie Web JSON sau JWK) este utilizată pentru a cripta sau semna detaliile utilizatorului. Când se înregistrează o aplicație client cu IdP se primește un un ID de client și un secret de client. Într-un flux implicit, secretul clientului nu ar trebui să fie niciodată expus.



1. Pasul1. Utilizatorul încearcă să înceapă o sesiune cu aplicația dvs. client și este redirecționat către IDP, transmițând ID-ul clientului, care este unic pentru aplicația respectivă.
2. Pasul 2. IDP-ul autentifică și autorizează utilizatorul pentru o anumită instanță de aplicație.
3. Pasul 3. Detaliile utilizatorului sunt codificate de către IDP într-un id\_token (JWT) care conține informații despre utilizator și semnătura (folosind RS256), care este transmisă unei pagini de redirecționare preconfigurate de pe serverul web.
4. Pasul 4. Aplicația client confirmă JWT id\_token și confirmă semnătura folosind cheia publică. Dacă totul este în regulă, se stabilește o sesiune pentru utilizator.

În fluxul implicit, tranzacția este sigură, în ciuda faptului că totul este trecut în „front end” și aplicația client nu poate fi autentificată, deoarece IdP-ul trimite token-uri criptate folosind o schemă de chei publice/private și va trimite doar tokenuri către URI de redirecționare preconfigurat. Cu alte cuvinte, cineva ar putea fura cheia publică și id-ul clientului, dar asta nu contează, deoarece numai IdP-ul are informațiile adecvate (URI-ul de redirecționare pentru aplicația client dorită și cheia privată) pentru a utiliza cheia publică și clientul ID corect.

*Fluxul de baza (autentificare)*

Fluxul de autentificare (sau de bază) este o opțiune pentru aplicațiile care au o logică de server web care permite comunicarea back-end cu IdP. Funcționează ca un flux OAuth tradițional cu trei noduri și are ca rezultat returnarea în secret a unui token de acces OAuth tradițional aplicației web prin apeluri efectuate în back-end. În acest flux, mai degrabă decât să transmită detaliile utilizatorului, furnizorul trimite un cod special, de unică folosință, care poate fi schimbat de serviciul web back-end cu un token de acces OAuth. Acest schimb trebuie să includă ID-ul clientului și secretul clientului pe lângă cod, la fel ca un flux tradițional OAuth 2.0. Este mai sigur decât fluxul implicit, deoarece token-urile nu sunt vizibile prin browser și aplicația client poate fi, de asemenea, autentificată.



1. Pasul 1. Utilizatorul încearcă să înceapă o sesiune cu aplicația client și este redirecționat către IDP, transmițând ID-ul clientului, care este unic pentru aplicația respectivă.
2. Pasul 2. IDP-ul autentifică și autorizează utilizatorul pentru o anumită instanță de aplicație. Până acum, arată ca fluxul implicit.
3. Pasul 3. Un cod de o singură utilizare este transmis înapoi serverului web folosind un URI de redirecționare predefinit.
4. Pasul 4. Serverul web transmite codul, ID-ul clientului și secretul clientului punctului final de token al IDP-ului, iar acesta validează codul și returnează un jeton de acces de o oră.
5. Pasul 5. Serverul web folosește jetonul de acces pentru a obține mai multe detalii despre utilizator (dacă este necesar) și stabilește o sesiune pentru utilizator.

*Configurare SITUE pentru autentificare si autorizare prin openid PSCID*

Autentificarea si autorizarea prin PSCID si Openid se realizează prin fluxul de baza.

De aceea pentru configurarea SITUE se vor face mai multe operații:

1. In IDP se va crea un client dedicat aplicatiei. CLIENT\_ID si CLIENT\_SECRET trebuie trimise către dezvoltatorii SITUE, impreuna cu url-urile pentru
	1. Emitere ( de ex sso.beta.roeid.ro/CASSO/oidc/pscid)
	2. Autorizare (sso.beta.roeid.ro /CASSO/oidc/pscid/authorize)
	3. Token (sso.beta.roeid.ro /CASSO/oidc/pscid/token)
	4. Userinfo (sso.beta.roeid.ro/CASSO/oidc/pscid/userinfo)
	5. Introspectie (sso.beta.roeid.ro /CASSO/oidc/pscid/introspect)
	6. Revocare (sso.beta.roeid.ro /CASSO/oidc/pscid/revoke)
	7. JWT Set (sso.beta.roeid.ro /CASSO/oidc/pscid/jwks)
	8. Metadata (sso.beta.roeid.ro/CASSO/oidc/pscid/.well-known/openid-configuration)
2. Nota. Autorizare, Token si Userinfo sunt obligatorii

Acțiuni programate:

1. Dezvoltarea unui conector in SITUE care sa proceseze pasii a)-e) din procesul de autentificare openid
2. Trimiterea URL-ului către IDP pentru a-l seta ca REDIRECT\_URI in proprietățile clientului.
3. Adăugarea in conectorul din cadrul SITUE a opțiunii de a se autentifica cu PSCID/ROEID si cu link către pagina mai sus menționată.

### Scenariu de implementare

Un utilizator roman dorește sa se autentifice pentru a putea folosi un serviciu public străin (oferit de către Franța sau Germania).

1. Utilizatorul accesează pagina unui serviciu public străin, apoi selectează tara de origine RO (Romania) - "Login with EIDAS".

2. Dupa o serie de redirectari (EIDAS FR/DE -> EIDAS RO) precum cele de mai jos,

977999





Utilizatorul este redirectat pe URL-ul https://dev.eidas.gov.ro/IdP unde cererea de mai jos este analizata:

{

 "authentication\_request": {

 "attribute\_list": [

 {

 "type": "requested\_attribute",

 "name": "FamilyName",

 "required": true

 },

 {

 "type": "requested\_attribute",

 "name": "FirstName",

 "required": true

 },

 {

 "type": "requested\_attribute",

 "name": "DateOfBirth",

 "required": true

 },

 {

 "type": "requested\_attribute",

 "name": "PersonIdentifier",

 "required": true

 }

 ],

 "requested\_authentication\_context": {

 "comparison": "minimum",

 "context\_class": [

 "A"

 ]

 },

 "citizen\_country": "FR",

 "created\_on": "2023-02-08T07:29:29.390752-05:00",

 "force\_authentication": true,

 "id": "3185c703-c41a-4068-b6e4-e7395fa9326e",

 "provider\_name": "DEMO-SP-RO",

 "requester\_id": "http://eidas.eu/EidasNode/RequesterId\_RO",

 "serviceUrl": "https://dev.eidas.gov.ro/SP/ReturnPage",

 "sp\_type": "public",

 "version": "1"

 }

}

După analiza cererii, se accesează link-ul de redirectare către ROEID, iar pagina finala unde utilizatorul se autentifica este de forma:

[https://sso.beta.roeid.ro/affwebservices/CASSO/oidc/eidas/authorize?client\_id=<client\_id>&response\_type=code&redirect\_uri=https%3A%2F%2Fdev.eidas.gov.ro%2FIdP%2FCallback&state=3a22d4a4-21ad-4885-ad2f-37320f4467f9&scope=openid+eidas&code\_challenge\_method=S256&code\_challenge=<challange](https://sso.beta.roeid.ro/affwebservices/CASSO/oidc/eidas/authorize?client_id=%3cclient_id%3e&response_type=code&redirect_uri=https%3A%2F%2Fdev.eidas.gov.ro%2FIdP%2FCallback&state=3a22d4a4-21ad-4885-ad2f-37320f4467f9&scope=openid+eidas&code_challenge_method=S256&code_challenge=%3cchallange)>



Începe astfel procesul de autentificare folosind Oauth2 OpenID-Connect.

După autentificarea cu succes, un cod de autorizare este aprovizionat către https://dev.eidas.gov.ro/IdP/Callback.

Codul de autorizare este folosit pentru a obține un token de access (access\_token) prin apelarea https://sso.beta.roeid.ro/affwebservices/CASSO/oidc/eidas/token.

După obținerea token-ului de acces (access\_token) se pot solicita informațiile despre utilizator prin trimiterea token-ului de acces, ca header de autorizare către <https://sso.beta.roeid.ro/affwebservices/CASSO/oidc/eidas/userinfo>. Se oferă răspunsul:

{

 "FamilyName": "Garcia",

 "FirstName": "Javier",

 "PersonIdentifier": "1233345123453",

 "BirthName": "Garcia",

 "DateOfBirth": "1964-12-31"

 "sub": "javier.garcia@some-email.com",

 "cnp": "1233345123453",

 "SessionToken": "u5QF7MlTvyHs/KMx2I15...",

 "prenume": "Javier",

 "iss": "https://sso.beta.roeid.ro/affwebservices/CASSO/oidc/eidas",

 "nume": "Garcia",

 "nonce": "83q0zZTW6gwJn7WQC8kG9rQMVhBm-kvjC5RWRUI9KmE",

 "aud": "000440fe-290b-1345-9981-04140a000000",

 "telefon": "123456789",

 "auth\_time": 1675858099,

 "name": "Javier Garcia",

 "exp": 1675859019,

 "iat": 1675858719,

 "email": "javier.garcia@some-email.com"

}

Folosind informațiile acestea se poate forma răspunsul:

{

 "response": {

 "attribute\_list": [

 {

 "type": "string\_list",

 "name": "FamilyName",

 "values": [

 {

 "value": "Garcia"

 }

 ]

 },

 {

 "type": "string\_list",

 "name": "FirstName",

 "values": [

 {

 "value": "Javier"

 }

 ]

 },

 {

 "type": "date",

 "name": "DateOfBirth",

 "value": "1964-12-31"

 },

 {

 "type": "string\_list",

 "name": "PersonIdentifier",

 "values": [

 {

 "value": "1233345123453"

 }

 ]

 }

 ],

 "authentication\_context\_class": "D",

 "created\_on": "2023-02-08T07:53:38.621-05:00",

 "id": "0bc24a01-3c69-4456-887b-2a287bb1cc1a",

 "inresponse\_to": "3185c703-c41a-4068-b6e4-e7395fa9326e",

 "issuer": "specificConnectorRO",

 "name\_id": "unspecified",

 "status": {

 "status\_code": "success"

 },

 "subject": "0123456",

 "version": "1"

 }

}

Acest răspuns se trimite înapoi către nodul romanesc, care îl transmite către nodul străin (EIDAS RO -> EIDAS FR/DE). Nodul străin trimite informațiile cerute către serviciul public străin.

3. Utilizatorul roman este considerat autentificat in cadrul serviciului public străin accesat după ce acesta verifică răspunsul primit de la nodul eIDAS.