

În conformitate cu prevederile art. 14 alin. (2) și ale art. 27 alin. (1) din Legea nr. 101/2016 privind remediile și căile de atac în materie de atribuire a contractelor de achiziție publică, a contractelor sectoriale și a contractelor de concesiune de lucrări și concesiune de servicii, precum și pentru organizarea și funcționarea Consiliului Național de Soluționare a Contestațiilor, Consiliul adoptă următoarea

DECIZIE

Nr.

Data:

Prin contestația nr. (...), transmisă prin mijloace electronice (e-mail), înregistrată la Consiliu sub nr. (...), (...), cu sediul în municipiul (...), înmatriculată în Registrul Comerțului sub nr. (...), având CUI (...), reprezentată legal prin administrator (...), formulată împotriva Răspunsului consolidat la clarificări nr. 1195/18.02.2025, publicat în SEAP la data de 19.02.2025, aferente procedurii de atribuire simplificată, organizată de (...), în calitate de autoritate contractantă, cu sediul în (...), în vederea atribuirii contractului având ca obiect „(...)”, inițiată prin anunțul de participare simplificat nr. (...), publicat în SEAP la data de 10.02.2025, s-au solicitat următoarele:

I. Suspendarea procedurii până la soluționarea contestației;

II. În principal, modificarea răspunsului la clarificări din data de 19.02.2025 și eliminarea cerințelor ilegale;

III. Obligarea autorității contractante la decalarea termenului de depunere a ofertelor și la continuarea procedurii în conformitate cu prevederile legale în vigoare aplicabile în materia achizițiilor publice, precum și cu respectarea principiilor consacrate de art. 2 al Legii nr. 98/2016;

IV. În subsidiar, în situația în care se va constata faptul că nu mai pot fi adoptate măsuri de remediere, anularea procedurii.

Prin Încheierea nr. (...) din data de 04.03.2025, Consiliul a respins ca rămasă fără obiect, cererea de suspendare a procedurii de atribuire, formulată de (...).

Procedura de soluționare în fața Consiliului s-a desfășurat în scris.

CONSILIUL NAȚIONAL DE SOLUȚIONARE A CONTESTAȚIILOR,
asupra cauzei de față, constată următoarele:

Consiliul a fost legal sesizat și este competent, potrivit dispozițiilor art. 12 alin. (1) din Legea nr. 101/2016, să soluționeze contestația formulată de (...).

I. Aspecte prealabile:

Contestatorul precizează că în calitate de ofertant de stații de încărcare electrică, înscris la procedura de achiziției în mod legal, este prejudiciat, fiind în imposibilitatea de a depune o ofertă, fiindu-i restricționat accesul din punct de vedere al cerințelor tehnice nou introduse prin răspunsul consolidat.

În acord cu prevederile Legii nr. 101 din 19 mai 2016, art. 8 alin. (1) „7 zile, începând cu ziua următoare luării la cunoștință despre actul autorității contractante considerat nelegal”, termenul de publicare în SICAP a răspunsului la clarificări fiind 19.02.2025, termenul limită de contestație este 24.02.2025, context în care (...) reiterează faptul că înțelege să conteste răspunsul consolidat la clarificările postat în SICAP în data de 19.02.2025.

II. Suspendarea procedurii – până la soluționarea contestației.

III. (...) susține că, contestația este întemeiată și trebuie admisă ca atare pentru următoarele argumente:

1. Nelegalitatea introducerii de noi cerințe tehnice în documentație fără prelungirea termenului de depunere a ofertelor.

Contestatorul menționează că prin răspunsul la clarificări postat în SICAP în data de 19.02.2025, autoritatea contractantă aduce modificări și adaugă în plus cerințe tehnice față de documentația de atribuire inițială.

Spre exemplu, contestatorul indică:

- Răspunsul 1 la clarificări, introduce noi cerințe tehnice minimale, care nu se regăseau în documentația inițial publicată în SICAP;

- Răspunsul 2 la clarificări, introduce noi cerințe tehnice minimale, care nu se regăseau în documentația inițial publicată în SICAP;

- Răspunsul 6 la clarificări introduce noi cerințe tehnice minimale, care nu se regăseau în documentația inițial publicată în SICAP;

- Răspunsul 9 la clarificări, introduce noi cerințe tehnice minimale, care nu se regăseau în documentația inițial publicată în SICAP.

Contestatorul precizează că modificarea prin clarificări a documentației inițiale este permisă de legislație, dar doar în măsură în care se iau și măsuri de remediere.

În acest sens, contestatorul invocă prevederile art. 153 alin. (1), (2), (3) și (4) din Legea nr. 98/2016 și arată că introducerea unor cerințe noi, cu doar 5 zile înaintea termenului de depunere a ofertelor, este o modalitate de eludare a obligațiilor legale cu privire la termenul minim de publicitate în SICAP a procedurii, o modalitate prin care regulile sunt schimbate în timpul jocului.

Contestatorul susține că autoritatea contractantă a introdus (în mod ilegal și părtinitor) obligativitatea respectării unor standarde ce nu se aplică sau sunt ale unor entități private, cu doar 5 zile înainte de termenul limită de depunere a ofertelor și fără a lua măsura obligatorie de prelungire.

2. Obligarea autorității contractante la schimbarea răspunsului dat la clarificarea/întrebarea 6 – referitor la „OCP 1.6 Security Certified emis de OCA (Open Charge Alliance)”

Contestatorul precizează că aceasta cerință este ilegală, neîntemeiată, restrictivă și vădit favorizează un unic operator economic ((...)SRL).

2.1. Ilegalitatea cerinței în sine, ea referindu-se la producător și nu la ofertant sau la produs.

Autoarea contestației susține că cerința „OCP 1.6 Security Certified emis de OCA (Open Charge Alliance)” se referă la „PRODUCĂTORUL

STAȚIEI” și nu la stația în sine. Astfel, cerința este impusă pentru producătorul stației și nu pentru produsul în sine.

Or, obiectul licitației nu este licitarea unui producător, ci licitarea unui produs care îndeplinește anumite cerințe tehnice. Impunerea unor standarde de calitate pentru producător este ilegală în viziunea Legii nr. 98/2016 care permite impunerea de standarde de calitate/conformitate doar pentru produsele supuse licitației și pentru operatorii economici/ofertanți, sub nici o formă nu permite impunerea unor standarde pentru fabricant/producător.

În acest context, contestatorul solicită eliminarea cerinței introduse prin clarificări, prin care producătorul trebuie să fie certificat „OCP 1.6 Security Certified emis de OCA (Open Charge Alliance).”

2.2. Nejustificarea cerinței raportat la obiectul contractului, în contextul în care cerința s-ar referi la stația de încărcare.

Contestatorul precizează că obiectul contractului este format din achiziția de stații de încărcare electrică fără software de exploatare/platformă/aplicație de exploatare.

Conform cerinței nou introduse prin clarificare din 19.02.2025, răspunsul nr. 6, contestatorul susține că autoritatea contractantă a introdus o cerință nouă, ce nu își are sensul în contextul de față, având în vedere următoarele:

i. În primul rând solicită CNSC să constate că autoritatea contractantă dorește ca pentru componenta hardware OCPP 1.6 - să existe certificare de securitate emisă de OCA;

ii. Subliniază din nou, că OCPP 1.6 (Open Charge Point Protocol 1.6) este un protocol de comunicație deschis utilizat în infrastructura stațiilor de încărcare pentru vehicule electrice (EV). Acesta permite comunicarea între stațiile de încărcare (Charge Points - CP) și sistemele centrale (Charge Point Operator - CPO sau Backend System), asigurând interoperabilitatea și gestionarea eficientă a rețelelor de încărcare;

iii. La bază este un element hardware care știe să comunice cu alte elemente hardware și software;

iv. La baza OCPP 1.6, este un element hardware, de sine stătător, este un element care funcționează doar exploatat/cu ajutorul unui element software;

v. Or, obiectul achiziției nu are nici un element software;

vi. Atunci când un alt hardware (ex. o mașină electrică) se conectează la stație nu se conectează direct (hardware la hardware), ci prin intermediul unui software. Prin urmare nu se poate aduce în discuție securitatea/certificarea securității elementului hardware decât în contextul unui instrument software;

vii. Impunerea unei cerințe de securitate, a unei certificări de securitate asupra unui element hardware este illogică în contextul în care nu se achiziționează acest instrument software, deoarece asupra unei componente hardware/cip/microcip/ se poate pune în discuție doar securitatea fizică (antivandalism) și nu securitatea informatică;

viii. Cu alte cuvinte, securitatea OCPP 1.6 nu este dată de partea hardware a stației, ci de aplicația software care exploatează stația, care

face ca stația să fie utilizată, care pune și învață stația să recunoască mașina electrică care i se adresează pentru încărcare;

ix. Acest lucru nu este făcut de către partea hardware care face obiectul contractului de față, ci de aplicația software, motiv pentru care cerința trebuie să se refere la aplicația softare și nicidecum la hardware;

x. Dovada este că inclusiv entitatea privată OCA (OCA este o organizație de tip ONG nesemnificativă și restrictivă) când atestă securitatea OCPP 1.6 de fapt atestă doar logarea la stație, adică tot pe baza unui soft.

În acest sens, contestatorul redă o captură de ecran de pe site-ul OCA cu privire la ce anume certifică „*OCPP 1.6 Security Certified emis de OCA (Open Charge Alliance)*”

xi. Se face doar o certificate BASIC a autentificării (pe baza unui soft și nu strict pe elementul hardware).

De altfel, contestatorul precizează că este ușor de înțeles și de către orice persoană neavizată, cum că cerința unei certificări a securității unor elemente hardware (fără software) este illogică și de ce cerințele de securitate sunt de fapt pentru aplicațiile de exploatare a stațiilor:

- stațiile de încărcare nu stochează nici un fel de date personale sau de autentificare a utilizatorilor, acestea neavând o bază de date proprie. Stațiile de încărcare au doar un modul OCPP pe bază de hardware care permite comunicarea cu aplicații compatibile prin protocolul OCPP;

- utilizatorul final, împreună cu toate datele personale și nepersonale sunt stocate în baza de date a aplicației mobile (cum este în cazul (...)) aplicația Elvo). Aplicația criptează toate informațiile în tranzit precum și cele statice, și este protejată inclusiv prin autentificare prin 2 factori precum parola + SMS sau Email;

- astfel, stația știe doar cât se încarcă și la ce preț (acesta fiind setat la instalare). Nu știe cine încarcă sau orice altă informație despre utilizator.

În concluzie, (...) precizează că în condițiile în care autoritatea contractantă nu cumpără o aplicație de exploatare, impunerea unei astfel de cerințe este illogică, deoarece cerințele de securitate se referă la aplicațiile utilizate și nu la elemente hardware (la acestea sunt aplicabile elementele antivandalism).

2.3. Cerința este restrictivă.

Contestatorul menționează că „*OCA (Open Charge Alliance)*” este o organizație non-profit care dezvoltă și promovează protocoale deschise de comunicație pentru infrastructura stațiilor de încărcare a vehiculelor electrice (EV).

Contestatorul precizează că impunerea certificării doar de către o anumită entitate este restrictivă. Pentru a exemplifica este ca și cum într-o licitație s-ar solicita certificare CE, doar de către laboratorul X sau Y, doar de către firma X de certificare. Impunerea doar a unui anumit certificat -în cazul de față „*OCA (Open Charge Alliance)*” - este restrictiv. Scopul unei certificări este de a avea o opinie terță, imparțială, o probă imparțială care arată că o anumită cerință este îndeplinită. Or, impunerea ca această probă să fie furnizată exclusiv de un anumit ONG privat, este restrictivă.

Așadar, contestatorul subliniază că dacă autoritatea contractantă ar fi fost de bună credință, ar fi indicat ca cerința de asigurare a securității să fie la nivel de aplicație software, fără a indica un anumit organism de certificare.

În plus, contestatorul menționează că:

- OCA certifică OCPP, dar nu este un organism de securitate IT acreditat la nivel internațional pe nivel de software de utilizare stații;
- OCA Security nu oferă o protecție suplimentară garantată față de utilizarea standardelor consacrate (TLS 1.2/1.3, autentificare X.509, criptare avansată etc.);
- Există alternative echivalente de asigurare a securității, fără costurile suplimentare impuse de această certificare;
- Costurile obținerii certificării sunt ridicate și nejustificate, în condițiile în care nici legislația UE nu impune această certificare pentru stațiile de încărcare;
- În majoritatea statelor UE, stațiile de încărcare funcționează în siguranță, respectând standardele internaționale fără a fi nevoie de certificarea OCA Security (ONG privat) limitându-se la certificarea securității datelor la nivel de aplicație de exploatare.

2.4. Cerința este în scopul de a favoriza exclusiv un operator economic.

Contestatorul susține că această cerință este îndeplinită de un singur operator economic în România. Conform site-ului indicat în cerință (<https://openchargealliance.org/certified-companies/>) în România există doar 3 ofertanți de stații care îndeplinesc cerința:

- (...) – este un producător care „NU” mai produce stații de încărcare – este retras de pe piață din anul 2023;
- cu privire la (...)– este firmă de software – nu vinde și nu produce stații de încărcare electrică, este firma colaboratoare a (...), fiind o dovadă în plus că cerința se referă la software nu hardware;
- (...)– firmă favorizată de către autoritatea contractantă. Nu este prima dată când acest operator impune (prin metode ilicite) aceasta cerință care îl favorizează.

Practic, contestatorul susține că în România este un singur operator care îndeplinește această cerință restrictivă.

În plus, contestatorul solicită CNSC să observe că există o taxă prohibitivă impusă de către OCA pentru o certificare. Se poate vedea pe site-ul OCA - <https://openchargealliance.org/join-us/>

Or, impunerea unei certificări din partea unui anumit certicator, care are costuri astronomice și care în România are doar 2 operatori certificați – este o dovadă în sine, suficientă, pentru a demonstra că favorizează doar pe (...)și (...).

3. Obligarea autorității contractante la modificarea documentației de atribuire în urma răspunsului la clarificări unde a publicat ATR-ul.

Prin răspunsul la clarificări din data de 19.02.2025, contestatorul susține că autoritatea contractantă a publicat ATR-ul (avizul tehnic de racordare). Acest aviz „NU” a fost publicat odată cu documentația de atribuire inițială.

La publicitatea din 19.02.2025, contestatorul precizează că a luat la cunoștință că în ATR soluția de racordare este contrară celei din cadrul PTH.

Însă, contestatorul susține că în listele de cantități conform Proiectului Tehnic este prezentată o altă soluție în devizul „*Coloana electrică abonat (instalații electrice)*”, în pag 64-66, respectiv 72-74. Conform acesteia, se propune:

- anume înlocuirea cablului acyaby 3 x 240 + 70 mmp (din ATR) cu 2 cabluri acyaby 3 x 150 + 70 mmp;
- înlocuirea firidei E1+2 din ATR, cu o firida E2+2.

În consecință, contestatorul menționează că este în imposibilitatea de a elabora o ofertă în condițiile în care ATR-ul (avizul tehnic de racordare emis de operatorul de energie), impune o soluție diferită față de cea din PTH și listele de lucrări.

Având în vedere că, conform răspunsului la clarificările solicitate, instalația de racordare nu face obiectul prezentei proceduri, contestatorul solicită excluderea devizelor „*Coloana electrică abonat (instalații electrice)*” din cadrul documentației, având în vedere discrepanțele menționate.

Pe cale de consecință, contestatorul solicită CNSC admiterea contestației.

Prin adresa nr. (...), transmisă prin mijloace electronice (e-mail), înregistrată la Consiliu sub nr. (...), (...) **a transmis punctul său de vedere** cu privire la contestația formulată de (...), precizând următoarele:

Scurt istoric al procedurii:

Autoritatea contractantă susține că a transmis în SEAP răspunsul consolidat la solicitările de clarificări în data de 19.02.2025.

În data de 24.02.2025 a primit pe adresa de e-mail a primăriei contestația formulată de (...).

În ceea ce privește conținutul contestației și motivele invocate de contestator, UAT (...) face următoarele precizări:

I. Suspendarea procedurii până la soluționarea contestației.

Contestația a fost publicată în SEAP în data de 24.02.2025 și procedura de atribuire a fost suspendată;

II. În principal, modificarea răspunsului la clarificări din data de 19.02.2025 și eliminarea cerințelor ilegale.

Contestatorul afirmă că se află „*în imposibilitatea de a depune o oferta, accesul fiind restricționat din punct de vedere al cerințelor tehnice nou introduse prin răspunsul consolidat.*”

Autoritatea contractantă precizează că prin răspunsul dat la solicitările de clarificări nu a urmărit restricționarea participării și nici favorizarea vreunui ofertant la procedura de atribuire, așa cum susține contestatorul.

De asemenea, autoritatea contractantă susține că nu au fost introduse cerințe tehnice suplimentare față de documentația de atribuire inițială, ci s-a urmărit ca prin răspunsul dat să fie corectate/clarificate cerințele tehnice definite inițial în fișele tehnice, în corelare cu normativele tehnice în vigoare.

Cu privire la susținerile contestatorului de la pct. 2, 2.1. și 2.2. din contestație, autoritatea contractantă face următoarele precizări:

Faptul că în listele OCA trebuie să apară numele producătorului și numele stației nu reprezintă o certificare a producătorului ca și companie, ci o certificare a produsului, numele producătorului fiind consemnat pentru identificarea clară a produsului.

Cerința la care face referire contestatorul nu este modificată, având în vedere că în caietul de sarcini s-a specificat necesitatea existenței certificărilor OCPP. Prin intermediul clarificărilor s-au specificat doar nivelul de certificare OCPP solicitat.

Sistemul hardware care asigură comunicație OCPP este integrat în stație și nu poate fi instalat ulterior. Scopul său este exact asigurarea intercomunicării cu softurile din rețelele de încărcare.

În acest sens, autoritatea contractantă redă extras din ghidul AFM articolul 6.

„Obligațiile Beneficiarului

23. să asigure instalarea unui acces deschis de management și operare care să permită identificarea locației, monitorizarea în timp real a funcționalității, disponibilității, cantității de energie transferate. De asemenea, acest acces trebuie să permită interconectarea și comunicarea cu alte instalații similare în timp real;

24. să se asigure că stațiile de reîncărcare comunică prin protocol de tip OCPP - Open Charge Point Protocol -minimum 1.5 și dispun de meniu în limba română și în limba engleză”

Așadar, autoritatea contractantă susține că în nici un caz cerința prin care „Beneficiarul” trebuie să se asigure că stația îndeplinește cerințele OCPP nu este abuzivă.

Nivelul de certificare pe care OCA îl vizează referitor la stațiile de încărcare este „SUBSET”, „FULL” și „SECURITY”.

Nivelul „SUBSET” și „FULL” se referă la parametrii și funcțiile ce trebuie transmise de stație către un soft de monitorizare, astfel încât să poată să se înțeleagă între ele, iar certificarea „SECURITY” este o măsură elementară pentru asigurarea și securizarea acestor conexiuni.

Autoritatea contractantă precizează că testele de certificare nu se referă doar la partea hardware a stației de încărcare care face legătură cu softul de monitorizare, ci și la componenta software instalată în componenta hardware a stației care să asigure această legătură.

Autoritatea contractantă subliniază că securitatea în OCPP (Open Charge Point Protocol) este crucială, deoarece infrastructura de încărcare a vehiculelor electrice (EV) poate fi o țintă pentru atacurile cibernetice. Fără măsuri de securitate adecvate, atacatorii pot perturba rețelele de încărcare, fura date sau manipula tranzacțiile.

Autoritatea contractantă prezintă de ce securitatea este esențială în OCPP:

1. Protejarea datelor utilizatorilor și a confidențialității.

Date personale (numere de card RFID, identificarea ID-ului mașinii, identități ale utilizatorilor, detalii de plată), istoricul de încărcare, locațiile și tiparele de utilizare. Atacatorii pot fura datele cardului RFID pentru a încărca fraudulos.

Risc de urmărire a utilizatorului—hackerii pot monitoriza unde și când se încarcă un EV.

Prin soluția impusă de standardul de certificare se impune criptarea TLS (wss://) și autentificarea, funcții ce previn scurgerile de date. Anonimizarea și stocarea securizată protejează identitatea utilizatorilor.

2. Prevenirea accesului neautorizat și a atacurilor.

Stațiile de încărcare (EVSE) pot fi hăckuite de la distanță. Atacatorii pot porni/opri sesiuni de încărcare fără permisiune. Dacă autentificarea este slabă, hackerii pot prelua controlul asupra stațiilor de încărcare și produce daune de genul:

- Încărcare gratuită pentru atacatori prin utilizarea unor date furate;
- Atacuri de tip Denial-of-Service (DoS), care pot face stațiile nefuncționale;
- Atacuri prin injectare de comenzi, permițând atacatorilor să modifice livrarea de energie. Soluția de combatere a acestora este autentificare puternică (mTLS, OAuth, chei API) pentru prevenirea accesului neautorizat și control bazat pe roluri (RBAC) pentru restricționarea privilegiilor.

3. Asigurarea unei comunicări securizate (Evitarea atacurilor MITM).

- Dacă de la stația de încărcare datele sunt transmise prin WebSockets nesecurizate (ws://), atacatorii pot modifica mesajele (de exemplu, pot schimba tarifele sau pot începe/opri tranzacțiile);
- Printr-un atac de tip Man-în-the-Middle (MITM)—hackerii interceptează mesajele și le modifică;
- Stații de încărcare false—atacatorii pot înregistra dispozitive fictive în rețea.

Soluția este utilizarea TLS (wss://) pentru criptarea comunicației prin WebSocket și autentificare bazată pe certificate pentru verificarea stațiilor de încărcare.

4. Prevenirea exploatării firmware-ului și software-ului.

- Atacatorii pot instala firmware malițios pe stațiile de încărcare;
- Infectare cu malware—hackerii preiau controlul asupra stațiilor de încărcare;
- Control de la distanță asupra EVSE—atacatorii pot dezactiva sau modifica funcționalitatea stațiilor.

Soluția este actualizări de firmware semnate digital pentru a preveni manipularea și restricționarea accesului la actualizări software.

5. Evitarea pierderilor financiare și operaționale

Atacatorii pot manipula tarifele de încărcare sau întreruperea serviciului din cauza atacurilor.

Autoritatea contractantă prezintă cum previne atacurile MITM în OCPP 1.6J:

- Utilizarea TLS (wss://) pentru criptarea comunicației. Activarea autentificării mutuale TLS (mTLS) cu certificate de client;
- Monitorizarea traficului de rețea pentru a detecta deconectări sau mesaje modificate suspecte.

Autoritatea contractantă susține că în gândirea contestatorului aceste cerințe de securitate nu au importanță și având în vedere că nu s-a cerut să fie achiziționat și un soft, nu pot fi solicitate.

Așadar, autoritatea contractantă susține că o platformă software care este securizată și certificată nu poate funcționa în regim securizat decât dacă toate componentele hardware și software a stației de încărcare dispun de aceleași caracteristici și standard de transmisie pentru a putea asigura securizarea comunicației.

În același timp, contrar alegațiilor contestatorului, autoritatea contractantă precizează că stațiile de încărcare dețin și local informații referitoare la cardurile ce pot porni în regim „OFF-LINE” stația, istoricul de evenimente, informații și date critice ce țin de plata locală prin POS integrat în stația de încărcare, etc. Așadar, securitatea stației și a datelor personale pot fi puse în pericol în nenumărate variante în cazul neimplementării soluțiilor prevăzute în certificarea de securitate a stațiilor de încărcare.

Autoritatea contractantă susține din nou că, contrar afirmațiilor contestatorului, atât stațiile de încărcare cât și platformele de monitorizare au nevoie de aceste certificări „SECURITY” pentru a asigura nivelul de securitate a informațiilor dintre cele două echipamente.

În concluzie, autoritatea contractantă menționează că securitatea comunicației „NU” este opțională, iar certificarea „SECURITY” asigură tocmai îndeplinirea de către stația de încărcare prin componenta hardware și software ce o deține a acestei cerințe.

OCPP este un protocol deschis și flexibil, dar securitatea trebuie implementată separat, mai ales în OCPP 1.6.

Fără măsuri de securitate, autoritatea contractantă susține că rețelele de încărcare sunt expuse atacurilor cibernetice, ceea ce poate duce la scurgeri de date, pierderi financiare și chiar riscuri fizice.

Autoritatea contractantă consideră că nivelul de securitate implementat pe stațiile de încărcare este o chestiune foarte serioasă care ține de implementarea ei atât la nivelul stației de încărcare, cât și la nivelul operatorului de rețea de încărcare.

De asemenea, autoritatea contractantă susține că obținerea acestui certificat este esențială în asigurarea funcționării corecte a stației. Implementarea într-o rețea de monitorizare și monetizare este obligatorie pentru operarea acestor stații. Stația din fabrică trebuie să fie dotată cu toate softurile necesare funcționării ei, atât în regim autonom cât și în regim OCPP, așa cum obligă însuși ghidul de finanțare.

Referitor la punctul 2.3 din contestație, autoritatea contractantă face următoarele precizări:

1. OCA (Open Charge Alliance) este o alianță industrială formată a furnizorilor de hardware și software de încărcare a vehiculelor electrice și a operatorilor de rețea de încărcare și a furnizorilor de servicii. Misiunea OCA este de a promova dezvoltarea globală, adoptarea și conformitatea cu Protocolul Open Charge Point (OCPP) și standardele aferente prin colaborare, educație și testare;

2. OCA este o asocierie a celor mai mari producători de stații de încărcare din lume și a producătorilor de software pentru monitorizarea lor, care are peste 400 de membrii, companiile cele mai importante din domeniu, companii ce participa activ la dezvoltarea acestui protocol,

companii care sunt prezentate în link-ul <https://openchargealliance.org/participants/>.

Autoritatea contractantă menționează că OCA se concentrează pe dezvoltarea „Open Charge Point Protocol (OCPP)” și „Open Charge Protocol (OSCP)”. De asemenea, OCA promovează și informează părțile interesate despre OCPP și OSCP la nivel mondial și dezvoltă servicii de membru al alianței și valoarea de piață/afacere.

OCA oferă doar specificația protocolului OCPP, și un instrument de testare pe care companiile pot să-l utilizeze pentru testarea implementării. Acest instrument (OCTT) este folosit și pentru programul de certificare.

OCTT nu generează un certificat ca dovadă că un producător a finalizat cu succes programul de certificare. Pentru certificarea unui produs a unui producător, un laborator de testare independent va folosi OCTT pentru a crea un raport de testare. După finalizarea cu succes a tuturor testelor necesare, OCA generează/emite certificatul de conformitate.

Autoritatea contractantă susține că acest protocol a luat naștere tocmai pentru a stabili un standard uniform, la care toți producătorii de stații de încărcare să adere, standard ce face că legătura între stație și softurile de monitorizare să poată avea loc.

„Impunerea doar a unui anumit certicator - în cazul de față OCA (Open Charge Alliance)) - este restrictiv. Scopul unei certificări este de a avea o opinie terță, imparțială, o probă imparțială care arată că o anumită cerință este îndeplinită. Ori, impunerea ca aceasta probă să fie furnizată exclusiv de un anumit ONG privat, este restrictivă”.

Autoritatea contractantă consideră că alegația prin care contestatorul dorește să inducă în eroare este și faptul că această companie OCA face teste și emite certificatele în mod unic și independent de alte organizații de testare.

Autoritatea contractantă susține că așa cum reiese din site-ul oficial la adresa [\(...\)](https://www.openchargealliance.org/), această organizație de profesioniști, singura care a pus la dispoziție fabricanților un standard de comunicație, nu face teste de conformitate. Aceasta a pus la dispoziție doar standardul și toolsurile de testare (OCTT). Testele de conformitate sunt efectuate de companii specializate acreditate de către OCA să testeze standardul OCPP, cum ar fi Dekra, Korea Testing Certification Institute, DNV, etc..

Companiile de testare sunt prezentate în site-ul OCA la adresa [https://\(...\)/](https://www.openchargealliance.org/). Așadar, activitatea OCA este de reglementare, supraveghere și dezvoltare a acestui sistem de comunicare OCPP, sistem care este singurul din lume recunoscut de producătorii de stații de încărcare și de producătorii de softuri de monitorizare a stațiilor de încărcare. Rolul ei este de a certifica testele făcute de laboratoare independente certificate în testarea conform standardului.

În același timp, autoritatea contractantă precizează că toate ghidurile de finanțare din România, atât AFM cât și PNRR prezintă foarte clar obligația autorității de a se asigura că aceste stații respectă acest tip de comunicare OCPP min 1.5

În acest sens, autoritatea contractantă redă extras din ghidul AFM Articolul 6

„Obligațiile Beneficiarului

24. să se asigure că stațiile de reîncărcare comunică prin protocol de tip OCPP - Open Charge Point

Protocol -minimum 1.5 și dispun de meniu în limba română și în limba engleză”.

Așadar, autoritatea contractantă consideră că în nici un caz cerința prin care „Beneficiarul” trebuie să se asigure că stația îndeplinește cerințele OCPP nu sunt abuzive.

Certificările OCPP sunt „SUBSET”, „FULL” și „Security”.

Prin cererile de clarificări, autoritatea contractantă menționează că s-au solicitat mai multe clarificări referitor la nivelul de certificare.

De asemenea, autoritatea contractantă susține că a transmis clarificări referitor la nivelul de certificare OCPP 1.6 și nu a introdus nici o cerință nouă.

Referitor la alegațiile contestatorului cu privire la faptul că această licitație este doar pentru producătorii din România, autoritatea contractantă precizează că această afirmație este total falsă, fiind mulți ofertanți și operatori care oferă produse în piața din România, fabricate în restul Europei sau din China.

De asemenea, autoritatea contractantă menționează că orice companie românească sau din străinătate poate participa la această licitație, această licitație nefiind una restrânsă la producători și în nici un caz la producătorii din România.

În același timp contestatorul afirmă că:

„În plus, aceasta cerință este îndeplinită de un singur operator economic în ROMÂNIA. Conform site-ului indicat în cerința (<https://openchargealliance.org/certified-companies/>) în România există doar 3 ofertanți de stații care îndeplinesc cerința.”

La o analiză a celor spuse de contestator, autoritatea contractantă constată că în România nu există nici un producător care să dețină aceste certificări, deoarece compania ELVO dezvoltă softuri de monitorizare așa cum a declarat și contestatorul și nu stații de încărcare, iar celelalte 2 companii nu dispun de certificări „FULL” și „Security” pentru stațiile de încărcare, lucru mascat de către contestator în poza pusă de pe site-ul oficial. Mai mult, certificările nu se referă la ofertanți sau alți operatori de stații de încărcare, ci se referă la producătorii de stații de încărcare și produsele în sine certificate.

Conform site-ului OCA există și pot fi vizualizate pe site-ul OCA peste 120 produse ce respectă certificările cerute, așadar autoritatea contractantă susține că nu este o cerință abuzivă, iar afirmațiile contestatorului sunt false.

Referitor la afirmația contestatorului:

„În plus, rugăm CNSC să vadă că există o taxă prohibitivă impusă de către OCA pentru o certificare. Se poate vedea pe site-ul OCA - <https://openchargealliance.org/join-us/>”

Autoritatea contractantă precizează că din nou, contestatorul face afirmații false. Aceste taxe sunt impuse firmelor producătoare care certifică calitatea și conformitatea sistemului de comunicație OCPP și nu

operatorilor economici ce participă la licitații în România. Producătorii trebuie să își certifice produsele pentru a face dovada calității produselor la fel ca și în cazul certificărilor CE. Costul certificărilor se împarte la numărul de stații vândute de către respectivul producător și nu este suportat de către ofertantul din România ce participa la licitațiile publice.

Așadar, autoritatea contractantă menționează că autoarea contestației face afirmații neadevărate pentru inducerea în eroare a CNSC-ului.

3. În ceea ce privește cerința de a modifica documentația de atribuire, pct. 3 din contestație, autoritatea contractantă specifică faptul că în listele de cantități se face referire în cadrul obiectului „*Coloana electrică abonat*” la instalația de utilizare, aceasta neavând nicio legătură cu instalația de racordare a cărei soluție este prezentată în ATR-ul pus la dispoziție.

Ca urmare, autoritatea contractantă menționează că documentația de atribuire, respectiv proiectul tehnic nu necesită nicio modificare.

Având în vedere că procedura de atribuire este suspendată, autoritatea contractantă precizează că în cazul în care Consiliul decide continuarea procedurii cu adoptarea măsurilor de remediere, va fi stabilit un nou termen de depunere a ofertelor, cu respectarea legislației în vigoare.

În cazul în care Consiliul decide că se impune anularea procedurii, autoritatea contractantă susține că va proceda la anularea acesteia și inițierea unei noi proceduri de atribuire după revizuirea documentației de atribuire.

Documentele necesare soluționării cauzei au fost transmise Consiliului de către autoritatea contractantă, fiind înregistrate la CNSC sub nr. (...)și, respectiv sub nr. (...).

Din documentele depuse de părți și din susținerile acestora, Consiliul constată următoarele:

(...), în calitate de autoritate contractantă, a inițiat procedura de atribuire simplificată a contractului de achiziție publică de furnizare având ca obiect „(...)”, cod CPV (...) (Rev.2), prin publicarea în SEAP a anunțului de participare simplificat nr. (...) / 10.02.2025, stabilind data limită de depunere a ofertelor la 24.02.2025 ora 15:00, criteriul de atribuire fiind „prețul cel mai scăzut” și valoarea estimată de 294.100 lei, fără TVA.

Fiind nemulțumită de conținutul Răspunsului consolidat la clarificări nr. 1195/18.02.2025, publicat în SEAP la data de 19.02.2025, societatea (...) a depus contestația care formează obiectul prezentului dosar solicitând următoarele:

I. Suspendarea procedurii până la soluționarea contestației.

II. În principal, modificarea răspunsului la clarificări din data de 19.02.2025 și eliminarea cerințelor ilegale.

III. Obligarea Autorității contractante la decalarea termenului de depunere a ofertelor și la continuarea procedurii în conformitate cu prevederile legale în vigoare aplicabile în materia achizițiilor publice, precum și cu respectarea principiilor consacrate de art. 2 al Legii nr. 98/2016.

IV. În subsidiar, în situația în care se va constata faptul că nu mai pot fi adoptate măsuri de remediere, anularea procedurii.

Cererea de suspendare a procedurii de atribuire a fost soluționată de Consiliu prin Încheierea nr. (...)din data de 04.03.2025, fiind respinsă ca rămasă fără obiect.

Autoarea contestației a prezentat Consiliului dovada respectării dispozițiilor art. 61¹ alin. (1) lit. a) din Legea nr. 101/2016, cu modificările și completările ulterioare, respectiv Recipisa de consemnare a cauțiunii nr. (...)din data de 27.02.2025, eliberată de CEC BANK – Sucursala Iași, în sumă de 5.882 lei.

Recipisa de consemnare se va restitui în condițiile stipulate de art. 1064 din Codul de procedură civilă, coroborate cu dispozițiile art. 61¹ alin. (5), (6) și (7) din Legea nr. 101/2016, cu modificările și completările ulterioare.

În continuare, Consiliul procedează la analiza punctuală a criticilor formulate de contestatoare.

Prima critică a contestatoarei vizează *„Nelegalitatea introducerii de noi cerințe tehnice în documentație, fără prelungirea termenului de depunere a ofertelor”*, sens în care se exemplifică după cum urmează:

„- Răspunsul 1 la clarificări introduce noi cerințe tehnice minimale, care nu se regaseau în documentatia initial publicata in SICAP

- Răspunsul 2 la clarificari introduce noi cerinte tehnice minimale, care nu se regaseau in documentatia initial publicata in SICAP

- Răspunsul 6 la clarificari introduce noi cerinte tehnice minimale, care nu se regaseau in documentatia initial publicata in SICAP

- Răspunsul 9 la clarificari introduce noi cerinte tehnice minimale, care nu se regaseau in documentatia initial publicata in SICAP”.

Procedând la analiza Răspunsului consolidat la solicitări de clarificări, înregistrat la autoritatea contractantă sub nr.1195/18.02.2025 – **Solicitare clarificare 1, dată postare 14.02.2025**, Consiliul reține următoarele solicitări de clarificări și răspunsuri aferente, invocate de contestatoare:

Întrebare 1:

În Formularul F5 – fișa 1 și 2 tehnică se specifica următoarele:

La punctul 1.2 se specifica «Alimentare trifazată 400V+-20%»

Normativele ANRE din Romania prevăd ca tensiunea de alimentare trifazica este de 400+-10%.

Inserarea unor tensiuni ce nu aparțin rețelelor si a normativelor din Romania reprezintă o cerința abuziva.

Vă rugăm să respectați cerințele si sa corectati tensiunile de alimentare conform normativelor in vigoare.

Răspuns 1:

Se va modifica fisa tehnica F5 fisa 1 astfel: 1.2 «Alimentare trifazată 304V – 456 V» în 1.2 «Alimentare trifazata 400V+-10%»

Se va elimina cerința 1.15 «Tensiune de alimentare maxim admisă: 600V»

Se va elimina cerința 1.3 «Voltaj maxim admis 600V»

Se va modifica fisa tehnica F5 fisa 2 astfel: 1.2 «Alimentare trifazată 304V – 456 V» în 1.2 «Alimentare trifazata 400V+-10%»

Se va elimina cerința 1.14 «Tensiune de alimentare maxim admisă: 600V»

Se va elimina cerința 1.3 «Voltaj maxim admis 600V»

Întrebare 2:

La pct 1.4 se solicita «Frecvență curent: 50/60Hz»

Normativul național este de 50Hz +-5%.

Va rugam sa respectati normativele naționale si sa corectati specificațiile.

Răspuns 2:

În Fișa tehnică 1 și 2 se modifică cerința «Frecvență curent: 50/60Hz» cu «Frecvență curent 50Hz +-5%».

Întrebare nr. 6

Statiile sunt solicitate sa detina versiune de comunicație «Versiune OCPP: minim OCPP 1.6 cu upgrade gratuit la 2.0». La punctul 2.7 se solicita «Producătorul statiei de incarcare va fi certificat OCA (Open Charge Alliance), denumirea producătorului se va regasi pe site-ul oficial www.openchargealliance.org la secțiunea «Producători certificați, împreună cu tipurile de certificări dobândite»

Având in vedere exodul de produse chinezești care declara ca dețin comunicație OCPP 1.6 dar care in realitate nu dețin asa ceva, este binevenita o astfel de cerința.

Va rugam sa confirmați ca statiile de incarcare trebuie sa detina certificare «OCPP 1.6 Fully Certified» si «OCPP 1.6 Security Certified» pentru îndeplinirea tuturor cerințelor OCPP 1.6. Doar aceste certificări fac dovada ca statiile intr-adevar dețin acest protocol de comunicație si asigura securitatea comunicației cu serverul de monitorizare. Va rugam sa confirmați necesitatea prezentării celor doua certificate.

Răspuns nr. 6:

Cerința se modifica astfel la ambele fise tehnice: Ofertantul va prezenta certificatele «OCPP 1.6 Fully Certified» si «OCPP 1.6 Security Certified emis de OCA (Open Charge Alliance) in numele producătorului.

Denumirea producătorului si certificatele se vor regăsi pe site-ul oficial www.openchargealliance.org la secțiunea «Producători certificați, împreună cu tipurile de certificări dobândite mai sus mentionate».

Întrebare 9:

9. La pct 4.2 se solicita «Stația se va putea integra în sisteme ulterioare de încărcare de 100KW».

Va rugam sa ne precizați despre ce sisteme este vorba. Daca autoritatea se gândește la extinderea acestora cu module de putere de inca 100kW, adica o statie de 150kW, structura ei trebuie de la început proiectata sa permită aceasta extindere, modificând structura de forța si siguranța a statiei. Acest lucru ridica foarte mult costurile statiei iar daca autoritatea nu dispune de puterea disponibila in locație de 50DC + 100DC extindere + 22AC adica 172kW, atunci aceasta cerința nu va putea fi implementata niciodata.

Va rugam sa specificați clar despre ce este vorba.

Răspuns 9:

Se elimină această cerință din fișa tehnică.

Răspunsul consolidat la solicitări de clarificări, înregistrat la autoritatea contractantă sub nr. 1195/18.02.2025 a fost publicat în SEAP la data de 19.02.2025 (miercuri) ora 10:27, iar termenul limită pentru depunerea ofertelor era stabilit la data de 24.02.2025 (luni) ora 15:00.

La data de 23.02.2025 (duminică), contestatoarea a transmis Consiliului și autorității contractante contestația care formează obiectul prezentului dosar, iar la data de 24.02.2025 ora 09:38, (...) a suspendat procedura de atribuire, context în care urmează a se stabili un nou termen pentru depunerea ofertelor, motiv pentru care solicitarea contestatoarei de prelungire a termenului limită pentru depunerea ofertelor apare ca rămasă fără obiect.

A doua critică a contestatoarei vizează obligarea autorității contractante la schimbarea răspunsului dat la clarificarea/întrebarea 6 – referitor la „OCP 1.6 Security Certified emis de OCA (Open Charge Alliance)”.

Analizând prevederile documentației de atribuire, Consiliul reține că în cadrul Proiectului Tehnic, autoritatea contractantă a introdus următoarele documente:

- **Formular F5 – Fișa tehnică Stație de reîncărcare multistandard** în cadrul căreia se regăsesc următoarele specificații tehnice:

„1. Stație de reîncărcare: (...)

*1.25 - **Versiune OCPP** : minim OCPP 1.6 cu upgrade gratuit la 2.0*

2. Condiții privind conformitatea cu standardele relevante: (...)

*2.7 Producătorul stației de încărcare **va fi certificat OCA (Open Charge Alliance)**, denumirea producătorului și modelul stației se vor regăsi pe site-ul oficial www.openchargealliance.org la secțiunea «Producători certificați, împreună cu tipurile de certificări dobândite»;*

- **Formularul F5 – Stație de reîncărcare**, în cadrul căreia se regăsesc următoarele specificații tehnice:

„1. Stație de reîncărcare: (...)

*1.24 - **Versiune OCPP** : minim OCPP 1.6 cu upgrade gratuit la 2.0*

2. Condiții privind conformitatea cu standardele relevante: (...)

*2.7 Producătorul stației de încărcare **va fi certificat OCA (Open Charge Alliance)**, denumirea producătorului și modelul stației se vor regăsi pe site-ul oficial www.openchargealliance.org la secțiunea «Producători certificați, împreună cu tipurile de certificări dobândite».*

Se vor atașa certificatele de conformitate **OCA** tip «**Fully Certified**» pentru versiunea OCPP 1.6”.

De asemenea, Consiliul reține că în Fișa de date a achiziției, la punctul IV.4.1 Modul de prezentare al propunerii tehnice, autoritatea contractantă a menționat următoarele: „Propunerea tehnica va fi elaborata astfel incat sa rezulte ca sunt indeplinite si asumate in totalitate cerintele tehnice din documentatia de atribuire. Propunerea tehnica trebuie sa corespunda cerintelor minime prevazute în caietul de sarcini, conform art.133 alin. (2) din HG 395/2016, cu modificarile si completarile ulterioare **și informațiilor cuprinse în Proiectul tehnic, pus la dispoziție de achizitor**”.

În soluționarea prezentei critici, Consiliul reține că răspunzând următoarei solicitări de clarificări adresată de un operator economic interesat: „Întrebare nr. 6: Statiile sunt solicitate sa detina versiune de comunicație «Versiune OCPP : minim OCPP 1.6 cu upgrade gratuit la 2.0». La punctul 2.7 se solicita «Producătorul stației de incarcare va fi certificat OCA (Open Charge Alliance), denumirea producătorului se va regăsi pe site-ul oficial www.openchargealliance.org la secțiunea «Producători certificați, împreună cu tipurile de certificări dobândite». Având în vedere exodul de produse chinezești care declara ca dețin comunicație OCPP 1.6 dar care in realitate nu dețin așa ceva, este binevenita o astfel de cerință. Va rugam sa confirmați ca statiile de incarcare trebuie sa detina certificare «OCPP 1.6 Fully Certified» si OCPP 1.6 Security Certified» pentru îndeplinirea tuturor cerințelor OCPP 1.6. Doar aceste certificări fac dovada ca statiile intr-adevar dețin acest protocol de comunicație si asigura securitatea comunicației cu serverul de monitorizare. Va rugam sa confirmați necesitatea prezentării celor doua certificate”, autoritatea contractantă a menționat următoarele: „Răspuns nr. 6: Cerința se modifica astfel la ambele fise tehnice: Ofertantul va prezenta certificatele «OCPP 1.6 Fully Certified» și «OCPP 1.6 Security Certified emis de OCA (Open Charge Alliance) in numele producătorului. Denumirea producătorului si certificatele se vor regăsi pe site-ul oficial www.openchargealliance.org la secțiunea «Producători certificați, împreună cu tipurile de certificări dobândite mai sus mentionate».

Analizând prevederile Fișelor tehnice incluse în cadrul Proiectului Tehnic, Consiliul constată că încă de la publicarea în SEAP a prevederilor documentației de atribuire (**10.02.2025**), operatorii economici interesați au luat cunoștință de faptul că **producătorul stației de reîncărcare trebuie să fie certificat OCA (Open Charge Alliance)**, iar denumirea producătorului și modelul stației trebuie să se regăsească pe site-ul oficial www.openchargealliance.org la secțiunea „Producători certificați, împreună cu tipurile de certificări dobândite”. De asemenea, în cadrul ambelor fișe este menționată specificația tehnică: „**Versiune OCPP: minim OCPP 1.6 cu upgrade gratuit la 2.0**”.

Față de această situație, Consiliul apreciază că în situația în care contestatoarea aprecia că solicitarea ca **producătorul stației de reîncărcare să fie certificat OCA (Open Charge Alliance)**, este ilegală, restrictivă (OCA fiind organizație non profit, în România există doar trei organizații certificate de OCA), împovărătoare (taxă prohibitivă impusă de OCA) și favorizează un anumit operator economic din România ((...)SRL) trebuia să conteste prevederile documentației de atribuire în cadrul termenului prevăzut de art. 8 alin. (1) lit. b) și alin. (2) din Legea nr. 101/2016, aplicabil în condițiile în care valoarea estimată a prezentei proceduri de atribuire este mai mică decât pragul valoric menționat la art. 7 alin. (1) lit. b) din Legea nr. 98/2016: „(1) Persoana care se consideră vătămată de un act al autorității contractante poate sesiza Consiliul în vederea anulării actului autorității contractante, obligării acesteia la emiterea unui act sau la adoptarea de măsuri de remediere, precum și pentru recunoașterea dreptului pretins sau a interesului legitim, în termen

de: (...) b) **7 zile, începând cu ziua următoare luării la cunoștință despre actul autorității contractante considerat nelegal**, în cazul în care valoarea estimată a procedurii de achiziție publică/sectorială sau de concesiune este mai mică decât pragurile valorice în raport cu care este obligatorie transmiterea spre publicare către Jurnalul Oficial al Uniunii Europene a anunțurilor de participare, potrivit legislației privind achizițiile publice, legislației privind achizițiile sectoriale sau legislației privind concesiunile de lucrări și concesiunile de servicii. (2) În cazul în care contestația privește conținutul documentației de atribuire, publicată în Sistemul electronic de achiziții publice, denumit în continuare SEAP, data luării la cunoștință este data publicării documentației de atribuire”.

În condițiile în care, documentația de atribuire a fost publicată în SEAP la data de 10.02.2025, operatorii economici interesați puteau contesta solicitarea ca **producătorul stației de reîncărcare să fie certificat OCA (Open Charge Alliance), precum și specificația tehnică: „Versiune OCPP: minim OCPP 1.6 (...)”**, până la data de **17.02.2025 (inclusiv)**, motiv pentru care criticarea acestui aspect la data de **23.02.2025** apare ca fiind tardivă.

Analizând site-ul OCA (<https://openchargealliance.org/about-us/>), Consiliul constată că OCA (Open Charge Alliance) este o organizație care are misiunea de a promova dezvoltarea globală, adoptarea și conformitatea protocoalelor de comunicare în infrastructura de încărcare a vehiculelor electrice și standardele aferente prin colaborare, educație, testare și certificare.

OCA are multiple activități, printre care guvernarea protocoalelor **OCPP (Open Charge Point Protocol)** și OSCP (Open Smart Charging Protocol).

În soluționare, Consiliul reține ca relevante susținerile autorității contractante referitoare la faptul că **„OCA oferă doar specificația protocolului OCPP și un instrument de testare pe care companiile pot să-l utilizeze pentru testarea implementării. Acest instrument (OCTT) este folosit și pentru programul de certificare.**

OCTT nu generează un certificat ca dovadă că un producător a finalizat cu succes programul de certificare. Pentru certificarea unui produs a unui producător, un laborator de testare independent va folosi OCTT pentru a crea un raport de testare. După finalizarea cu succes a tuturor testelor necesare, OCA generează/emite certificatul de conformitate.

Acest protocol a luat naștere tocmai pentru a stabili un standard uniform, la care toți producătorii de stații de încărcare să adere, standard ce face ca legătura între stație și softurile de monitorizare să poată avea loc. (...) aceasta organizație de profesioniști, singura care a pus la dispoziție fabricanților un standard de comunicație, nu face teste de conformitate. Aceasta a pus la dispoziție doar standardul și toolurile de testare (OCTT). Testele de conformitate sunt efectuate de companii specializate acreditate de către OCA să testeze standardul OCPP, (...) **Certificările OCPP sunt SUBSET, FULL și Security”.**

Analizând informațiile care sunt pe site-ul OCA, Consiliul reține existența următoarelor **tipuri de certificate:**

- Subset;
- Security;
- Core & Advanced Security;
- Full;
- Full & Security;
- Subset & Security;
- Core,
- Core + S + L + C + D + R;
- Core + C + D + I.

Pentru lămurirea acestei situații în cadrul punctului de vedere, autoritatea contractantă menționează următoarele aspecte: „**Nivelul SUBSET si FULL se refera la parametrii si funcțiile ce trebuie transmise de stație către un soft de monitorizare astfel incat sa poata sa se inteleaga intre ele, iar certificarea SECURITY este o masura elementara pentru asigurarea si securizarea acestor conexiuni (...)**”.

Față de cele mai sus menționate, în condițiile în care în Proiectul Tehnic s-a menționat necesitatea ca **producătorul stației de reîncărcare să fie certificat OCA (Open Charge Alliance), precum și specificația tehnică**

„Versiune OCPP : minim OCPP 1.6 cu upgrade gratuit la 2.0”, aspecte care nu mai pot face obiectul analizei CNSC în contextul tardivității acestora așa cum s-a arătat anterior, Consiliul constată că prin Răspunsul consolidat la solicitări de clarificări, înregistrat la autoritatea contractantă sub nr.1195/18.02.2025, respectiv răspunsul 6, **s-a specificat doar nivelul de certificare OCPP solicitat**, respectiv „Ofertantul va prezenta certificatele «OCPP 1.6 **Fully Certified**» și «OCPP 1.6 **Security Certified** emis de OCA (Open Charge Alliance)”, neputându-se reține modificarea documentației de atribuire ci doar explicitare tipurilor de certificări OCPP solicitate, în condițiile în care prevederile documentației de atribuire nu erau clare/explicite, din acest punct de vedere, pentru considerentele ce urmează:

La punctul 2.7 din **Formular F5 - Fișa tehnică Stație de reîncărcare multistandard**, se menționa că: „**Producătorul stației de încărcare va fi certificat OCA (Open Charge Alliance)**, denumirea producătorului și modelul stației se vor regăsi pe site-ul oficial www.openchargealliance.org la secțiunea «Producători certificați, împreună cu tipurile de certificări dobândite»”, **fără a fi menționat tipul certificatului de conformitate OCA**, în timp ce în Formularul F5 - **Stație de reîncărcare**, la punctul 2.7 se menționa „**Producătorul stației de încărcare va fi certificat OCA (Open Charge Alliance)**, denumirea producătorului și modelul stației se vor regăsi pe site-ul oficial www.openchargealliance.org la secțiunea «Producători certificați, împreună cu tipurile de certificări dobândite»”. **Se vor atașa certificatele de conformitate OCA tip «Fully Certified» pentru versiunea OCPP 1.6**”, pentru această stație fiind solicitat tipul de certificare „Full”. ,

În cadrul punctului de vedere, autoritatea contractantă menționează următoarele informații apreciate de Consiliu ca fiind relevante în justificarea solicitării nivelului de certificare **Security**, în contextul în care

contestatoarea susține că această cerință nu își are sensul în contextul de față, **afirmații necombătute de către contestatoare deși la dosarul cauzei s-a făcut dovada comunicării punctului de vedere către aceasta** (la data de 27.02.2025 confirmând primirea punctului de vedere, conform dovezii înregistrată la CNSC sub nr. 25014/16.04.2025):

„In primul rand testele de certificare nu se refera doar la partea hardware a statiei de incarcare care face legătură cu softul de monitorizare, ci si la componenta software instalata in componenta hardware a statiei care sa asigure aceasta legătură.

Securitatea în OCPP (Open Charge Point Protocol) este crucială deoarece infrastructura de încărcare a vehiculelor electrice (EV) poate fi o țintă pentru atacurile cibernetice. Fără măsuri de securitate adecvate, atacatorii pot perturba rețelele de încărcare, fura date sau manipula tranzacțiile.

Iată de ce securitatea este esențială în OCPP:

1. Protejarea datelor utilizatorilor și a confidențialității.

Date personale (numere de card RFID, identificarea ID-ului mașinii, identități ale utilizatorilor, detalii de plată), istoricul de încărcare, locațiile și tiparele de utilizare. Atacatorii pot fura datele cardului RFID pentru a încărca fraudulos.

Risc de urmărire a utilizatorului—hackerii pot monitoriza unde și când se încarcă un EV.

Prin soluția impusa de standardul de certificare se impune criptarea TLS (wss://) și autentificarea, funcții ce previn scurgerile de date. Anonimizarea și stocarea securizată protejează identitatea utilizatorilor.

2. Prevenirea accesului neautorizat și a atacurilor

Stațiile de încărcare (EVSE) pot fi hăckuite de la distanță. Atacatorii pot porni/opri sesiuni de încărcare fără permisiune. Dacă autentificarea este slabă, hackerii pot prelua controlul asupra stațiilor de încărcare si produce daune de genul

- Incarcare gratuita pentru atacatori prin utilizarea unor date furate.*
- Atacuri de tip Denial-of-Service (DoS), care pot face stațiile nefuncționale.*

• Atacuri prin injectare de comenzi, permițând atacatorilor sa modifice livrarea de energie. Soluția de combatere a acestora este autentificare puternica (mTLS, OAuth, chei API) pentru prevenirea accesului neautorizat si control bazat pe roluri (RBAC) pentru restricționarea privilegiilor.

3. Asigurarea unei comunicări securizate (Evitarea atacurilor MITM)

- Daca de la statia de incarcare datele sunt transmise prin WebSockets nesecurizate (ws://) atacatorii pot modifica mesajele (de exemplu, pot schimba tarifele sau pot incepe/opri tranzacțiile).*

- Printr-un atac de tip Man-in-the-Middle (MITM)—hackerii interceptează mesajele și le modifica.*

- Stații de încărcare false—atacatorii pot înregistra dispozitive fictive în rețea.*

Soluția este utilizarea TLS (wss://) pentru criptarea comunicației prin WebSocket și autentificare bazată pe certificate pentru verificarea stațiilor de încărcare.

4. Prevenirea exploatarei firmware-ului și software-ului

- Atacatorii pot instala firmware malițios pe stațiile de încărcare.*
- Infectare cu malware—hackerii preiau controlul asupra stațiilor de încărcare.*

- Control de la distanță asupra EVSE- atacatorii pot dezactiva sau modifica funcționalitatea stațiilor.*

Soluția este actualizări de firmware semnate digital pentru a preveni manipularea și restricționarea accesului la actualizări software.

5. Evitarea pierderilor financiare și operaționale

Atacatorii pot manipula tarifele de încărcare sau întreruperea serviciului din cauza atacurilor.

Cum prevenim atacurile MITM în OCPP 1.6?

Utilizarea TLS (wss://) pentru criptarea comunicației. Activarea autentificării mutuale TLS (mTLS) cu certificate de client.

Monitorizarea traficului de rețea pentru a detecta deconectări sau mesaje modificate suspecte.

În gândirea contestatarului aceste cerințe de Securitate nu au importanță și având în vedere că nu s-a cerut să fie achiziționat și un soft, nu pot fi solicitate. Amintim contestatarului că o platformă software care este securizată și certificată nu poate funcționa în regim securizat decât dacă toate componentele hardware și software a stației de încărcare dispun de aceleași caracteristici și standard de transmisie pentru a putea asigura securizarea comunicației.

În același timp, contrar legărilor contestatarului, stațiile de încărcare dețin și local informații referitoare la cardurile ce pot porni în regim OFF-LINE stația, istoricul de evenimente, informații și date critice ce tin de plată locală prin POS integrat în stația de încărcare, etc. deci securitatea stației și a datelor personale pot fi puse în pericol în nenumarate variante în cazul neimplementării soluțiilor prevăzute în certificarea de Securitate a stațiilor de încărcare.

Specificăm din nou că, contrar afirmațiilor contestatarului, atât stațiile de încărcare cât și platformele de monitorizare au nevoie de aceste certificări SECURITY pentru a asigura nivelul de Securitate a informațiilor dintre cele două echipamente.

În concluzie securitatea comunicației NU este opțională iar certificarea "SECURITY" asigura tocmai îndeplinirea de către stația de încărcare prin componenta hardware și software ce o deține a acestei cerințe.

OCPP este un protocol deschis și flexibil, dar securitatea trebuie implementată separat, mai ales în OCPP 1.6.

Fără măsuri de securitate, rețelele de încărcare sunt expuse atacurilor cibernetice, ceea ce poate duce la scurgeri de date, pierderi financiare și chiar riscuri fizice.

După cum se vede mai sus, nivelul de securitate implementat pe stațiile de încărcare este o chestiune foarte serioasă care tine de

implementarea ei atat la nivelul statiei de incarcare cat si la nivelul operatorului de rețea de incarcare.

Obținerea acestui certificat este esențială în asigurarea funcționării corecte a statiei. Implementarea într-o rețea de monitorizare si monetizare este obligatorie pentru operarea acestor statii. Statia din fabrica trebuie sa fie dotata cu toate softurile necesare funcționării ei atat in regim autonom cat si in regim OCPP asa cum obliga insusi ghidul de finantare”.

În condițiile în care autoritatea contractantă a justificat temeinic și pertinent solicitarea nivelului de certificare **Security**, Consiliul reține nevoia acesteia de certificare „Security” motiv pentru care va respinge solicitarea contestatoarei de eliminare a cerinței prin care producătorul trebuie să fie certificat „OCPP 1.6 **Security Certified emis de OCA** (Open Charge Alliance)”, „Security” fiind un tip de certificare OCA, solicitată prin documentația de atribuire publicată în SEAP la data de 10.02.2025, aspect care nu poate face obiectul analizei CNSC în actualul stadiu al procedurii de atribuire, critica fiind tardivă.

Analizând site-ul OCA (<https://openchargealliance.org/certified-companies/>) în care pot fi vizualizate produse, producători și tipuri de certificate/ niveluri de certificare a produselor, se constată că în România niciun produs din cele trei care figurează pe site nu deține „Security Certified” (nici chiar producătorul indicat de contestatoare ca fiind favorizat – (...)SRL), însă la nivel mondial există foarte mulți producători care dețin o astfel de certificare pentru produsele lor din țări precum Bulgaria, Coreea, China, USA, Taiwan, Germania, India etc., pentru versiune **OCPP 1.6**, cerință minimă impusă prin documentația de atribuire publicată în SEAP la data de 10.02.2025, aspect care, de asemenea, nu poate face obiectul analizei CNSC în actualul stadiu al procedurii de atribuire, critica fiind tardivă.

A treia solicitare a contestatoarei vizează obligarea autorității contractante la modificarea documentației de atribuire în urma răspunsului la clarificări unde a publicat ATR-ul.

În susținerea acestei critici, contestatoarea arată că prin răspunsul la clarificări din data de 19.02.2025, achizitorul a publicat ATR-ul (avizul tehnic de racordare). Acest aviz nu a fost publicat odată, cu documentația de atribuire inițială iar în data de 19.02.2025 a luat la cunoștință că în ATR soluția de racordare este contrară celei din cadrul PTH.

În listele de cantități conform Proiectului Tehnic este prezentată o altă soluție în devizul „Coloana electrica abonat (instalații electrice)”, în pag 64-66, respectiv 72-74. Conform acesteia, se propune:

- anume înlocuirea cablului acyaby 3x240+70mmp (din ATR) cu 2 cabluri acyaby 3x150+70mmp :

- înlocuirea firidei E1+2 din ATR cu o firidă E2+2.

În consecință, contestatoarea arată că este în imposibilitatea de a elabora o ofertă în condițiile în care ATR-ul (avizul tehnic de racordare emis de operatorul de energie) impune o soluție diferită față de cea din PTH și listele de lucrări și având în vedere că, conform răspunsului la clarificările solicitate, instalația de racordare nu face obiectul prezentei proceduri,

solicită excluderea devizelor „Coloana electrică abonat (instalații electrice)” din cadrul documentației, având în vedere discrepanțele menționate.

În cadrul punctului de vedere, autoritatea contractantă arată că „în listele de cantități se face referire în cadrul obiectului «Coloana electrică abonat» **la instalația de utilizare**, aceasta neavând nicio legătură cu instalația de racordare a cărei soluție este prezentată în ATR-ul pus la dispoziție”.

Față de explicația lămuritoare a autorității contracte și având în vedere că așa cum rezultă din Răspunsul consolidat la solicitări de clarificări, înregistrat la autoritatea contractantă sub nr.1195/18.02.2025 – **Solicitare clarificare 2, dată postare 18.02.2025**, „Răspuns solicitare de clarificare nr. 2 : 1. *realizarea instalațiilor de racordare nu face obiectul prezentei proceduri. Se va oferta și realiza doar instalația de utilizare*”, Consiliul apreciază că nu se impune „excluderea devizelor «Coloana electrică abonat (instalații electrice)» din cadrul documentației”, motiv pentru care Consiliul va respinge și această critică a contestatoarei.

În consecință, luând în considerare cele mai sus menționate, în temeiul dispozițiilor art. 26 alin. (6) din Legea nr. 101/2016, va respinge, ca nefondată, contestația formulată de (...), în contradictoriu cu autoritatea contractantă (...).

Pentru aceste motive,
în baza legii și a mijloacelor de probă aflate la dosar,

CONSILIUL DECIDE:

Respinge, ca nefondată, contestația formulată de (...), în contradictoriu cu autoritatea contractantă (...).

Prezenta decizie este obligatorie pentru părți, în conformitate cu dispozițiile art. 28 alin. (1) din Legea nr. 101/2016.

Împotriva prezentei decizii se poate formula plângere, în termen de 10 zile de la comunicare pentru părțile cauzei, respectiv de la data luării la cunoștință de către alte persoane vătămate.

PREȘEDINTE,

Redactat în 4 exemplare originale, conține 22 pagini.