SKLEP št. 2/2020 SKUPNEGA ODBORA, USTANOVLJENEGA S SPORAZUMOM MED EVROPSKO UNIJO IN ŠVICARSKO KONFEDERACIJO O POVEZAVI NJUNIH SISTEMOV TRGOVANJA Z EMISIJAMI TOPLOGREDNIH PLINOV

z dne 5. novembra 2020

o spremembi prilog I in II k Sporazumu in sprejetju tehničnih standardov za povezavo [2021/1034]

SKUPNI ODBOR JE –

ob upoštevanju Sporazuma med Evropsko unijo in Švicarsko konfederacijo o povezavi njunih sistemov trgovanja z emisijami toplogrednih plinov ([1]) (v nadaljnjem besedilu: Sporazum) ter zlasti člena 3(7) in člena 13(2) Sporazuma,

ob upoštevanju naslednjega:

(1) s Sklepom št. 2/2019 Skupnega odbora z dne 5. decembra 2019 ([2]) sta se spremenili prilogi I in II k Sporazumu, s čimer so bili izpolnjeni pogoji za povezavo iz Sporazuma.

(2) Po sprejetju Sklepa št. 2/2019 Skupnega odbora in v skladu s členom 21(3) Sporazuma sta pogodbenici izmenjali listini o ratifikaciji ali odobritvi, saj sta menili, da so vsi pogoji za povezavo iz tega sporazuma izpolnjeni.

(3) V skladu s členom 21(4) Sporazuma je Sporazum začel veljati 1. januarja 2020.

(4) Prilogo I k Sporazumu bi bilo treba spremeniti v skladu s členom 13(2) Sporazuma za zagotovitev nemotenega prehoda pri upravljanju operaterjev zrakoplovov, ki so bili dodeljeni Švici prvič ob upoštevanju napredka pri vzpostavitvi povezave med registroma.

(5) Zaradi upoštevanja najnovejšega razvoja dogodkov in zagotovitve večje ravni prožnosti za vzpostavitev povezave med registroma, kot zahteva Sporazum, bi bilo treba Prilogo II spremeniti v skladu s členom 13(2) Sporazuma, da bi se zagotovil širši, vendar enakovreden sklop tehnologij za vzpostavitev povezave med registroma.

(6) V skladu s členom 3(7) Sporazuma bi administrator švicarskega registra in centralni administrator Unije morala razviti tehnične standarde za povezavo na podlagi načel iz Priloge II k Sporazumu. Tehnični standardi za povezavo bi morali opisovati podrobne zahteve za vzpostavitev trdne in varne povezave med švicarsko dopolnilno evidenco transakcij (SSTL) in evidenco transakcij Evropske unije (EUTL). Tehnični standardi za povezavo bi morali začeti učinkovati, ko jih Skupni odbor sprejme s sklepom.

(7) V skladu s členom 13(1) Sporazuma bi moral Skupni odbor sprejeti tehnične smernice za zagotovitev ustreznega izvajanja Sporazuma, vključno z vzpostavitvijo trdne in varne povezave med SSTL in EUTL. Tehnične smernice lahko pripravi delovna skupina, ustanovljena v skladu s členom 12(5) Sporazuma. V delovno skupino bi morala biti vključena vsaj administrator švicarskega registra in centralni administrator Unije, pomagati pa bi morala Skupnemu odboru pri njegovih nalogah v skladu s členom 13 Sporazuma.

(8) Tehnične smernice, ki jih pripravita administrator švicarskega registra in centralni administrator Unije, bi bilo treba zaradi njihove tehnične narave in potrebe po njihovem prilagajanju nenehnemu razvoju predložiti Skupnemu odboru v vednost, ali kjer je to primerno, v odobritev –

([1]) UL L 322, 7.12.2017, str. 3.

([2]) Sklep št. 2/2019 Skupnega odbora, ustanovljenega s Sporazumom med Evropsko unijo in Švicarsko konfederacijo o povezavi njunih sistemov trgovanja z emisijami toplogrednih plinov z dne 5. decembra 2019 o spremembi prilog I in II k Sporazumu med Evropsko unijo in Švicarsko konfederacijo o povezavi njunih sistemov trgovanja z emisijami toplogrednih plinov (UL L 314, 29.9.2020, str. 68).

SPREJEL NASLEDNJI SKLEP:

Člen 1

Drugi odstavek točke 17 dela B Priloge I k Sporazumu se nadomesti z naslednjim besedilom:

„Švica operaterje zrakoplovov, ki so ji po začetku veljavnosti tega sporazuma prvič dodeljeni, upravlja po 30. aprilu leta, v katerem so ji dodeljeni, in ko začne delovati začasna povezava med registroma.“.

Člen 2

Četrti pododstavek Priloge II k Sporazumu se nadomesti z naslednjim besedilom:

„V tehničnih standardih za povezavo je določeno, da so komunikacije med SSTL in EUTL sestavljene iz varnih izmenjav spletnih storitev na podlagi naslednjih tehnologij (*) ali enakovrednih storitev:

— spletnih storitev, ki uporabljajo protokol SOAP (Simple Object Access Protocol),

— navideznega zasebnega omrežja (Virtual Private Network – VPN) na osnovi strojne opreme,

— XML (Extensible Markup Language – razširljivi označevalni jezik),

— digitalnega podpisa ter

— omrežnih časovnih protokolov.

_____

(*) Navedene tehnologije se trenutno uporabljajo za vzpostavitev povezave med registrom Unije in mednarodno evidenco transakcij ter med švicarskim registrom in mednarodno evidenco transakcij.“

Člen 3

Sprejmejo se tehnični standardi za povezavo, ki so priloženi temu sklepu.

Člen 4

S tem sklepom se v skladu s členom 12(5) Sporazuma ustanovi delovna skupina. Delovna skupina pomaga Skupnemu odboru pri zagotavljanju ustreznega izvajanja Sporazuma, vključno s pripravo tehničnih smernic za izvajanje tehničnih standardov za povezavo.

V delovno skupino sta vključena vsaj administrator švicarskega registra in centralni administrator Unije.

Člen 5

Ta sklep začne veljati na dan sprejetja.

V Bruslju, 5. novembra 2020.

Za Skupni odbor	Predsednica	Sekretarka za Švico
Sekretarka za Evropsko unijo	Beatriz YORDI	Caroline BAUMANN
Maja-Alexandra DITTEL		

PRILOGA

Tehnični standardi za povezavo v skladu s členom 3(7) Sporazuma med Evropsko unijo in Švicarsko konfederacijo o povezavi njunih sistemov trgovanja z emisijami toplogrednih plinov

STANDARDI ZA ZAČASNO REŠITEV

1. **Glosar**

Preglednica 1-1

Poslovne kratice in opredelitve pojmov

Kratica/pojem	Opredelitev
Pravica	Pravica do emisij ene tone ekvivalenta ogljikovega dioksida v določenem obdobju, ki velja samo za izpolnjevanje zahtev v okviru EU ETS ali švicarskega ETS.
CH	Švicarska konfederacija
CHU	Švicarske splošne pravice („CHU2“ se uporablja kot kratica za pravice CHU v drugem ciljnem obdobju)
CHUA	Švicarske pravice za letalstvo
COP	Skupni delovni postopki, ki jih skupaj razvijeta pogodbenici Sporazuma za operacionalizacijo povezave med EU ETS in švicarskim ETS.
ETR	Register za trgovanje z emisijami
ETS	Sistem za trgovanje z emisijami
EU	Evropska unija
EUA	Splošne pravice EU
EUAA	Pravice za letalstvo EU
EUCR	Konsolidirani register Evropske unije
EUTL	Evidenca transakcij Evropske unije
Register	Sistem obračunavanja za pravice, izdane v ETS, s katerim se vodi evidenca o lastništvu pravic na elektronskih računih.
SSTL	Švicarska dopolnilna evidenca transakcij
Transakcija	Postopek v registru, ki vključuje prenos pravice z enega računa na drugega.
Sistem evidence transakcij	Evidenca transakcij vsebuje zapis vsake predlagane transakcije, poslane iz enega registra v drugega.

Preglednica 1-2

Tehnične kratice in opredelitve pojmov

Kratica	Opredelitev
Asimetrična kriptografija	Uporablja javne in zasebne ključe za šifriranje in dešifriranje podatkov.
Overitelj potrdil	Subjekt, ki izdaja digitalna potrdila.

Kratica	Opredelitev
Kriptografski ključ	Del informacije, ki determinira funkcionalni izhod kriptografskega algoritma.
Dešifriranje	Postopek, ki poteka v obratni smeri od šifriranja.
Digitalni podpis	Matematična tehnika, ki se uporablja za potrditev avtentičnosti in celovitosti sporočila, programske opreme ali digitalnega dokumenta.
Šifriranje	Postopek pretvarjanja informacij ali podatkov v šifro, zlasti za preprečevanje nepooblaščenega dostopa.
Zajem datotek	Postopek branja datoteke.
Požarni zid	Izdelek s področja omrežne varnosti ali programska oprema, ki spremlja in nadzoruje vhodni in izhodni omrežni promet na podlagi vnaprej določenih pravil.
Spremljanje „utripa“	Periodičen signal, ki ga ustvari in spremlja strojna ali programska oprema, da označi normalno delovanje ali sinhronizira druge dele računalniškega sistema.
IPSec	Varnostni protokol za zaščito komunikacije. Nabor omrežnih protokolov za avtentikacijo in šifriranje podatkovnih paketov, ki zagotavlja varno šifrirano komunikacijo med dvema računalnikoma prek omrežja internetnega protokola.
Penetracijsko testiranje	Testiranje računalniškega sistema, omrežja ali spletne aplikacije, pri katerem se iščejo varnostne ranljivosti, ki bi jih napadalci lahko izkoristili.
Postopek usklajevanja	Zagotavljanje usklajenosti dveh sklopov zapisov.
VPN	Navidezno zasebno omrežje.
XML	Razširljivi označevalni jezik. Načrtovalcem omogoča, da ustvarijo svoje prilagojene značke, ki omogočajo opredelitev, prenos, potrditev in tolmačenje podatkov med aplikacijami in organizacijami.

2. **Uvod**

Sporazum med Evropsko unijo in Švicarsko konfederacijo o povezavi njunih sistemov trgovanja z emisijami toplogrednih plinov z dne 23. novembra 2017 (v nadaljnjem besedilu: Sporazum) določa medsebojno priznavanje pravic do emisije, ki se lahko uporabljajo za skladnost v okviru sistema Evropske unije za trgovanje z emisijami (v nadaljnjem besedilu: EU ETS) ali sistema Švice za trgovanje z emisijami (v nadaljnjem besedilu: švicarski ETS). Za operacionalizacijo povezave med EU ETS in švicarskim ETS bo vzpostavljena neposredna povezava med evidenco transakcij Evropske unije (EUTL) registra Unije in švicarsko dopolnilno evidenco transakcij (SSTL) švicarskega registra, s čimer bo omogočen prenos pravic do emisije, izdanih v katerem koli ETS, med registroma (člen 3(2) Sporazuma). Za operacionalizacijo povezave med EU ETS in švicarskim ETS bo maja 2020 ali čim prej po tem datumu vzpostavljena začasna rešitev. Pogodbenici sodelujeta, da začasno povezavo čim prej nadomestita s stalno povezavo med registroma (Priloga II k Sporazumu).

V skladu s členom 3(7) Sporazuma administrator švicarskega registra in centralni administrator Unije pripravita tehnične standarde za povezavo na podlagi načel iz Priloge II k Sporazumu, v kateri so navedene podrobne zahteve za vzpostavitev trdne in varne povezave med SSTL in EUTL. Tehnični standardi za povezavo, ki jih oblikujeta administratorja, začnejo učinkovati, ko jih Skupni odbor sprejme s sklepom.

Skupni odbor sprejme tehnične standarde za povezavo, navedene v tem dokumentu, s Sklepom št. 2/2020. Skupni odbor v skladu s tem sklepom zahteva od administratorja švicarskega registra in centralnega administratorja Unije, naj določita dodatne tehnične smernice za operacionalizacijo povezave in zagotovita, da se te smernice stalno prilagajajo tehničnemu napredku in novim zahtevam v zvezi z varnostjo in zaščito povezave ter njenim uspešnim in učinkovitim delovanjem.

2.1 *Področje uporabe*

Ta dokument predstavlja skupno stališče pogodbenic Sporazuma v zvezi z vzpostavitvijo tehnične podlage za povezavo med registroma EU ETS in švicarskega ETS. V njem je opisano izhodišče za tehnične specifikacije z vidika zahtev, povezanih z zgradbo, storitvami in varnostjo, za operacionalizacijo povezave pa bo treba pripraviti nekatere dodatne podrobne smernice.

Za zagotovitev pravilnega delovanja bo treba za nadaljnjo operacionalizacijo povezave določiti procese in postopke. V skladu s členom 3(6) Sporazuma so navedene zadeve podrobno opredeljene v ločenem dokumentu s skupnimi delovnimi postopki, ki jih Skupni odbor ločeno sprejme s sklepom.

2.2 *Naslovniki*

Ta dokument je naslovljen na administratorja švicarskega registra in centralnega administratorja Unije.

3. **Splošne določbe**

3.1 *Zgradba komunikacijske vezi*

Namen tega oddelka je zagotoviti opis splošne zgradbe operacionalizacije povezave med EU ETS in švicarskim ETS ter različnih sestavnih delov, ki so vanjo vključeni.

Ker je varnost ključni del opredelitve zgradbe povezave med registroma, je bilo storjeno vse, da bi ta zgradba bila trdna. Čeprav bo predvidena stalna povezava med registroma temeljila na spletnih storitvah, se bo pri začasni rešitvi namesto tega uporabil mehanizem za izmenjavo datotek.

Tehnična rešitev uporablja:

— protokol za prenos za varno izmenjavo sporočil,

— sporočila XML,

— digitalni podpis in šifriranje XML,

— napravo VPN ali enakovredno varno omrežje za prenos podatkov.

3.1.1 Izmenjava sporočil

Komunikacija med registrom Unije in švicarskim registrom bo temeljila na mehanizmu za izmenjavo sporočil prek varnih kanalov. Na vsakem koncu bo na voljo ustrezen repozitorij prejetih sporočil.

Pogodbenici vodita evidenco prejetih sporočil, vključno s podrobnostmi o obdelavi.

Napake ali nepričakovano stanje je treba sporočiti v obliki opozoril, člani podpornih skupin pa bi morali vzpostaviti osebni stik.

Napake in nepričakovani dogodki se bodo obravnavali ob upoštevanju delovnih postopkov, določenih v postopku obvladovanja incidentov, ki je del skupnih delovnih postopkov.

3.1.2 Sporočilo XML – visokoravenski opis

Sporočilo XML vsebuje eno od naslednjega:

— enega ali več zahtevkov za transakcijo in/ali enega ali več odgovorov v zvezi s transakcijo,

— eno dejavnost/odgovor, povezan z usklajevanjem,

— eno testno sporočilo.

Vsako sporočilo vsebuje glavo, v kateri sta navedena:

— izvorni ETS,

— zaporedna številka.

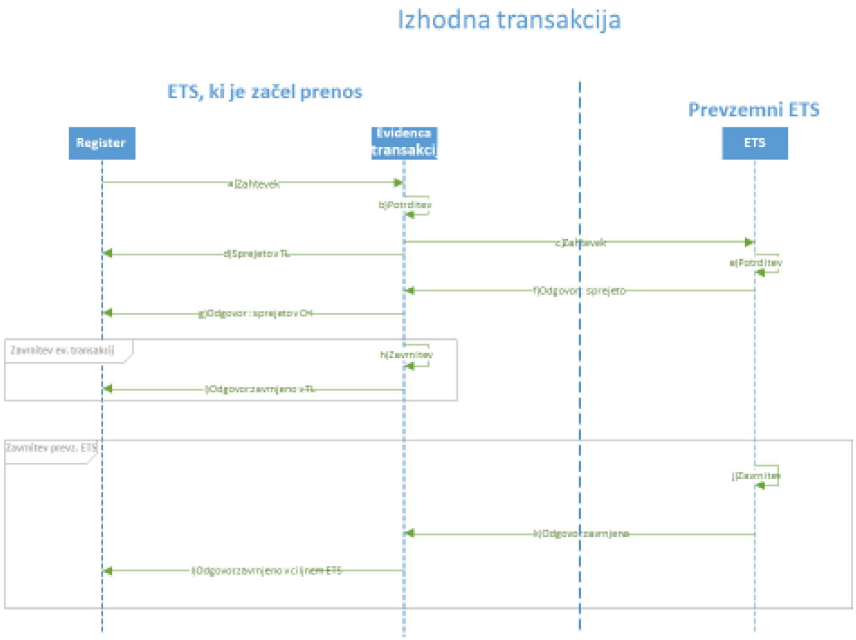
3.1.3 Zajemna okna

Začasna rešitev temelji na vnaprej določenih zajemnih oknih, ki jim sledi sklop poimenovanih dogodkov. Zahtevki za transakcije, prejeti prek povezave, se bodo zajeli samo v skladu z vnaprej določenimi intervali. Zajemna okna vključujejo tehnično potrjevanje izhodnih in vhodnih transakcij. Poleg tega se usklajevanja lahko izvajajo vsak dan in se lahko sprožijo ročno.

Spremembe pogostosti in/ali časovne razporeditve katerih koli od teh dogodkov se bodo obravnavale ob upoštevanju delovnih postopkov, določenih v postopku izpolnjevanja zahtevkov, ki je del skupnih delovnih postopkov.

3.1.4 Promet sporočil o transakcijah

Izhodne transakcije



Ta del obravnava vidik ETS, ki je začel prenos. Zgornji diagram zaporedja prikazuje ves promet določenih izhodnih transakcij.

Glavni promet „Običajna transakcija“ (s koraki, navedenimi na zgornji sliki):

(a) pri ETS, ki je začel prenos, se zahtevek za transakcijo pošlje iz registra v evidenco transakcij, ko pretečejo vsi poslovni roki (24-urni rok, kjer je primerno);

(b) evidenca transakcij potrdi zahtevek za transakcijo;

(c) zahtevek za transakcijo se pošlje v ciljni ETS;

(d) odgovor o sprejetju se pošlje v register izvornega ETS;

(e) ciljni ETS potrdi zahtevek za transakcijo;

(f) ciljni ETS pošlje odgovor o sprejetju nazaj v evidenco transakcij izvornega ETS;

(g) evidenca transakcij pošlje odgovor o sprejetju v register.

Alternativni promet „Zavrnitev evidence transakcij“ (s koraki, navedenimi na zgornji sliki, ki se prav tako začnejo s točko (a)):

(a) v izvornem ETS se zahtevek za transakcijo pošlje iz registra v evidenco transakcij, ko pretečejo vsi poslovni roki (24-urni rok, kjer je primerno).

Temu sledijo naslednji koraki:

(b) evidenca transakcij ne potrdi zahtevka;

(c) sporočilo o zavrnitvi se pošlje v izvorni register.

Alternativni promet „Zavrnitev ETS“ (s koraki, navedenimi na zgornji sliki, ki se prav tako začnejo s točko (a)):

(a) v izvornem ETS se zahtevek za transakcijo pošlje iz registra v evidenco transakcij, ko pretečejo vsi poslovni roki (24-urni rok, kjer je primerno);

(b) evidenca transakcij potrdi transakcijo;

(c) zahtevek za transakcijo se pošlje v ciljni ETS;

(d) sporočilo o sprejetju se pošlje v register izvornega ETS.

Temu sledijo naslednji koraki:

(e) evidenca transakcij prevzemnega ETS ne potrdi transakcije;

(f) prevzemni ETS pošlje odgovor o zavrnitvi v evidenco transakcij ETS, ki je začel prenos;

(g) evidenca transakcij pošlje zavrnitev v register.

Vhodne transakcije

Ta del obravnava vidik prevzemnega ETS. Zadevni promet je prikazan na naslednjem diagramu zaporedja:

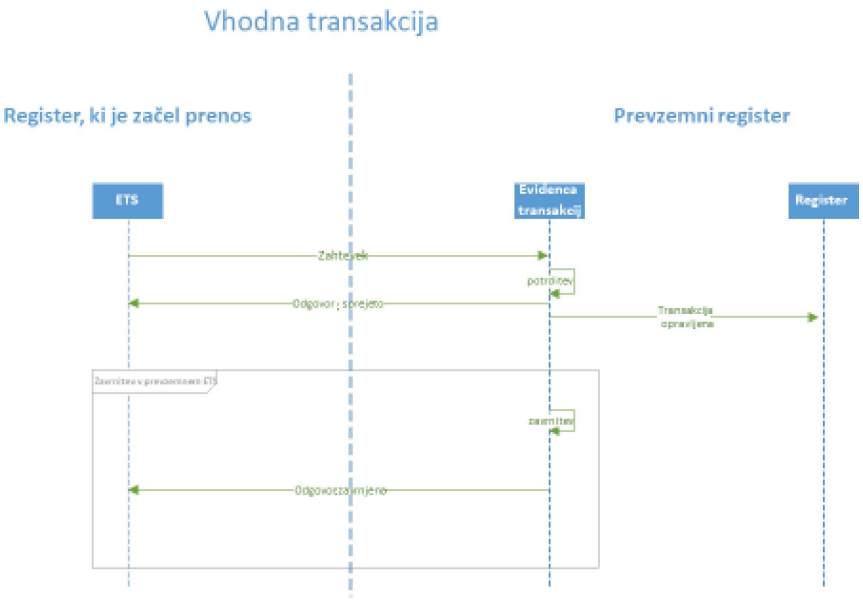


Diagram prikazuje naslednje:

1. kadar evidenca transakcij prevzemnega ETS potrdi zahtevek, pošlje sporočilo o sprejetju v ETS, ki je začel prenos, in sporočilo o „opravljeni transakciji“ v register prevzemnega ETS;

2. kadar prevzemna evidenca transakcij zavrne vhodni zahtevek za transakcijo, se ta ne pošlje v register prevzemnega ETS.

Protokol

Ciklus sporočil o transakciji vključuje samo dve sporočili:

— predlog za transakcijo – ETS, ki je začel prenos prevzemni ETS;

— odgovor za transakcijo – prevzemni ETS ETS, ki je začel prenos: sprejeta ali zavrnjena (vključno z razlogi za zavrnitev).

  — Sprejeta: transakcija je opravljena.

  — Zavrnjena: transakcija je prekinjena.

Stanje transakcije

— Stanje transakcije v ETS, ki izvaja prenos, se nastavi na „predlagana“, ko se zahtevek pošlje.

— Stanje transakcije v prevzemnem ETS se nastavi na „predlagana“, ko je zahtevek prejet in ko poteka njegova obdelava.

— Stanje transakcije v prevzemnem ETS se nastavi na „opravljena“/„prekinjena“, ko se predlog obdela. Prevzemni ETS nato pošlje ustrezno sporočilo o sprejetju/zavrnitvi.

— Stanje transakcije v ETS, ki je začel prenos, se nastavi na „opravljena“/„prekinjena“, ko je sporočilo o sprejetju/zavrnitvi prejeto in obdelano.

— Če ni bil prejet noben odgovor, se stanje transakcije v ETS, ki je začel prenos, ohrani v obliki predloga.

— Če se stanje katere koli predlagane transakcije ohrani v obliki „predloga“ več kot 30 minut, se v prevzemnem ETS stanje transakcije nastavi na „prekinjena“.

Incidenti, povezani s transakcijami, se bodo obravnavali ob upoštevanju delovnih postopkov, določenih v postopku obvladovanja incidentov, ki je del skupnih delovnih postopkov.

3.2 *Varnost prenosa podatkov*

Varnost podatkov, ki se prenašajo, se zagotovi na štirih ravneh:

(1) nadzor nad dostopom do omrežja: požarni zid in plast medomrežne povezave;

(2) šifriranje na ravni prenosa: VPN ali enakovredno varno omrežje za prenos podatkov;

(3) šifriranje na ravni seje: varen protokol za prenos za izmenjavo sporočil;

(4) šifriranje na ravni aplikacije: šifriranje in podpis vsebine XML.

3.2.1 Požarni zid in medomrežna povezava

Vzpostavi se povezava v omrežju, zaščitenem s strojnim požarnim zidom. Požarni zid je konfiguriran na podlagi pravil tako, da se v strežnik VPN lahko povežejo samo „registrirani“ odjemalci.

3.2.2 Navidezno zasebno omrežje (VPN)

Vse komunikacije med pogodbenicama so zaščitene s tehnologijo varnega prenosa podatkov. V primeru navideznega zasebnega omrežja (VPN) bi morala infrastruktura temeljiti na strojni opremi ali navideznih napravah. Tehnologije VPN zagotavljajo možnost „tuneliranja“ skozi omrežje, kot je internet, ki pelje od ene točke do druge, pri čemer so zaščitene vse komunikacije. Pred vzpostavljanjem tunela VPN se izda digitalno potrdilo potencialni končni točki odjemalca, s katerim odjemalec lahko zagotovi dokazilo o identiteti med pogajanjem o povezavi. Vsaka pogodbenica je odgovorna za namestitev potrdila v svojo končno točko VPN. Strežnik VPN na vsakem koncu bo imel z digitalnim potrdilom dostop do centralnega overitelja zaradi pogajanja o avtentikacijskih poverilnicah. Med vzpostavljanjem tunela poteka pogajanje o šifriranju, s čimer se zagotovi zaščita vseh komunikacij, ki potekajo po tunelu.

Konfigurirajo se končne točke odjemalcev v VPN, da tunel VPN ohrani za stalno, s tem pa omogoči, da med pogodbenicama ves čas poteka zanesljiva, dvosmerna komunikacija v realnem času.

Vse druge enakovredne rešitve so skladne z zgoraj navedenimi načeli.

3.2.3 Izvajanje IPSec

Pri uporabi rešitve z VPN bo uporaba protokola IPSec za vzpostavitev infrastrukture VPN od spletnega mesta do spletnega mesta omogočila avtentikacijo od spletne strani do spletne strani, celovitost podatkov in šifriranje podatkov. Konfiguracije VPN IPSec omogočajo pravilno avtentikacijo med dvema končnima točkama v povezavi VPN. Pogodbenici ugotovita istovetnost in opravita avtentikacijo oddaljenega odjemalca prek povezave IPSec z digitalnimi potrdili overitelja potrdil, ki ga priznava nasprotna končna točka.

IPSec zagotavlja tudi celovitost vseh komunikacij, ki potekajo skozi tunel VPN. Podatkovni paketi so razpršeni in podpisani z avtentikacijsko informacijo, ki jo določi VPN. Zaupnost podatkov se prav tako zagotovi z omogočanjem šifriranja z IPSec.

3.2.4 Protokol za prenos za varno izmenjavo sporočil

Začasna rešitev je odvisna od več plasti šifriranja za varno izmenjavo podatkov med pogodbenicama. Oba sistema in njuni različni okolji so medsebojno povezani na ravni omrežja s tuneli VPN ali enakovrednimi omrežji za varen prenos podatkov. Na ravni aplikacije se datoteke prenašajo s pomočjo protokola za prenos za varno izmenjavo sporočil na ravni seje.

3.2.5 Šifriranje in podpis XML

Podpisovanje in šifriranje v datotekah XML poteka na dveh ravneh. Vsak zahtevek za transakcijo, odgovor v zvezi s transakcijo in sporočilo o usklajevanju se digitalno podpiše.

V drugem koraku se šifrira vsak podrejeni element elementa „sporočila“.

Poleg tega se v tretjem koraku za zagotovitev celovitosti in preprečevanja izpodbijanja celotnega sporočila digitalno podpiše korenski element sporočila. S tem se zagotovi visoka raven zaščite vgrajenih podatkov XML. Pri tehničnem izvajanju se upoštevajo standardi Konzorcija za svetovni splet.

Da bi se sporočilo dešifriralo in preverilo, se izvede postopek, ki poteka v obratni smeri.

3.2.6 Kriptografski ključi

Za šifriranje in podpisovanje se uporablja kriptografija javnih ključev.

V posebnem primeru IPSec se uporabi digitalno potrdilo, ki ga izda overitelj potrdil, ki mu zaupata obe pogodbenici. Ta overitelj potrdil preveri identiteto imetnika potrdila in izda potrdila, ki se uporabljajo za pozitivno identifikacijo organizacije in vzpostavitev varnih kanalov za podatkovne komunikacije med pogodbenicama.

Za podpisovanje in šifriranje komunikacijskih kanalov in podatkovnih datotek se uporabljajo kriptografski ključi. Pogodbenici digitalno izmenjujeta javna potrdila prek varnih kanalov in jih preverjata po drugi poti. Ta postopek je sestavni del postopka upravljanja informacijske varnosti, ki je del skupnih delovnih postopkov.

3.3 *Seznam funkcij znotraj povezave*

Povezava določa sistem prenosa za niz funkcij, s katerimi se izvajajo poslovni postopki, ki izhajajo iz Sporazuma. Vključuje tudi specifikacijo za postopek usklajevanja in testna sporočila, ki bodo omogočili izvajanje spremljanja „utripa“.

3.3.1 Poslovne transakcije

Povezava s poslovnega vidika predvideva štiri (4) vrste zahtevkov za transakcije:

— zunanji prenos:

  — po začetku veljavnosti povezave med ETS so pravice EU in CH med pogodbenicama zamenljive in s tem tudi v celoti prenosljive,

— v prenos prek povezave sta vključena račun, ki je začel prenos, v enem ETS in prevzemni račun v drugem ETS,

— prenos lahko vključuje kakršno koli količino štirih (4) vrst pravic:

— švicarskih splošnih pravic (CHU),

— švicarskih pravic za letalstvo (CHUA),

— splošnih pravic EU (EUA),

— pravic za letalstvo EU (EUAA);

— mednarodna dodelitev:

operaterji zrakoplovov, ki jih upravlja en ETS z obveznostmi do drugega ETS in ki so upravičeni do brezplačnih pravic iz navedenega drugega ETS, prejmejo od drugega ETS brezplačne pravice za letalstvo v okviru transakcije za mednarodno dodelitev;

— razveljavitev mednarodne dodelitve:

ta transakcija se izvede, če je treba brezplačne pravice, ki jih je drug ETS dodelil imetniškemu računu operaterja zrakoplova, v celoti razveljaviti;

— vračilo prevelikega števila dodeljenih pravic:

podobno razveljavitvi, vendar če dodelitve ni treba v celoti zavrniti, temveč le vrniti odvečno število dodeljenih pravic v ETS, iz katerega se opravi dodelitev.

3.3.2 Protokol usklajevanja

Usklajevanja se izvajajo po zaprtju oken za zajemanje, potrjevanje in obdelavo sporočil.

Usklajevanja so sestavni del ukrepov za zagotavljanje varnosti in skladnosti znotraj povezave. Pogodbenici sprejmeta točno časovno razporeditev usklajevanja, preden pripravita kakršen koli časovni načrt. Dnevno načrtovano usklajevanje se lahko izvede, če se tako dogovorita obe pogodbenici. Po vsakem postopku zajemanja se opravi najmanj eno načrtovano usklajevanje.

V vsakem primeru pa lahko katera koli od pogodbenic kadar koli sproži postopek ročnega usklajevanja.

Spremembe časovne razporeditve in pogostosti načrtovanega usklajevanja se bodo obravnavale ob upoštevanju delovnih postopkov, določenih v postopku izpolnjevanja zahtevkov, ki je del skupnih delovnih postopkov.

3.3.3 Testno sporočilo

Za testiranje komunikacije med koncema je na voljo testno sporočilo. Sporočilo vsebuje podatke, ki ga opredeljujejo kot testno sporočilo, nanj pa se odgovori, ko je prejeto na drugem koncu.

3.4 *Standardi za spletne storitve*

Spletne storitve se v začasni rešitvi ne uporabljajo. Vendar je treba opozoriti, da bosta oblika in format sporočil XML večinoma ostala nespremenjena. Spletne storitve bi z uvedbo stalne povezave med registroma v prihodnosti morale omogočiti izmenjavo sporočil XML v realnem času.

3.5 *Posebna opredelitev spletnih storitev*

Ta oddelek se ne uporablja za začasno rešitev. Kot je navedeno v prejšnjem oddelku, se bodo spletne storitve uporabljale samo v prihodnji stalni povezavi med registroma.

3.6 *Zahteve glede zapisovanja podatkov*

V podporo potrebi obeh pogodbenic po ohranitvi točnih in doslednih informacij ter za zagotovitev orodij, ki se uporabljajo v postopku usklajevanja za odpravo neskladnosti, pogodbenici vodita štiri (4) vrste evidenc podatkov:

— evidence transakcij,

— evidence usklajevanja,

— arhiv sporočil,

— evidence notranjih revizij.

Vsi podatki v teh evidencah se hranijo najmanj tri (3) mesece za odpravljanje težav, njihova nadaljnja hramba na vsakem koncu za revizijo pa je odvisna od veljavne zakonodaje. Zapisi, starejši od treh (3) mesecev, se lahko arhivirajo na varni lokaciji v neodvisnem sistemu IT, dokler jih je mogoče pridobiti ali do njih dostopati v razumnem obdobju.

Evidence transakcij

Podrejeni sistemi EUTL in SSTL vsebujejo izvajanja evidenc transakcij.

Natančneje, v evidencah transakcij se hranijo zapisi o vsaki predlagani transakciji, poslani v drugi ETS. Vsak zapis vsebuje vsa polja vsebine transakcije in poznejši rezultat transakcije (odgovor prevzemnega ETS). V evidencah transakcij se hranijo tudi zapisi v zvezi z vhodnimi transakcijami in odgovor, poslan izvornemu ETS.

Evidence usklajevanja

Evidenca usklajevanja vsebuje zapis o vseh sporočilih o usklajevanju, ki sta si jih izmenjali pogodbenici, vključno z identifikacijsko oznako usklajevanja, časovnim žigom in rezultatom usklajevanja: stanjem usklajevanja „Uspešno“ ali „Neskladnosti“. Pri začasni rešitvi so sporočila o usklajevanju sestavni del izmenjanih sporočil.

Pogodbenici v evidenco usklajevanja shranita vsak zahtevek in odgovor nanj. Čeprav se informacije iz evidence usklajevanja ne posredujejo neposredno kot del samega usklajevanja, bo za odpravo neskladnosti morda potreben dostop do teh informacij.

Arhiv sporočil

Pogodbenici morata arhivirati kopijo izmenjanih podatkov (datoteke XML), tj. poslanih in prejetih, ter navesti, ali je bil format navedenih podatkov ali sporočil XML pravilen ali ne.

Arhiv je predvsem namenjen za revizijo, tj. da se zagotovijo dokazi o tem, kaj je druga pogodbenica poslala in prejela. V tem smislu je treba poleg datotek arhivirati tudi z njimi povezana potrdila.

Te datoteke vsebujejo tudi dodatne informacije za odpravljanje težav.

Evidenca notranje revizije

Te evidence opredeli in uporablja vsaka pogodbenica zase.

3.7 *Operativne zahteve*

Izmenjava podatkov med sistemoma pri začasni rešitvi ni v celoti avtonomna, kar pomeni, da so za operacionalizacijo povezave potrebni upravljavci in postopki.

4. **Določbe glede razpoložljivosti**

4.1 *Načrt razpoložljivosti komunikacij*

Zgradba za začasno rešitev je v osnovi infrastruktura IKT in programska oprema, ki omogoča komunikacijo med švicarskim ETS in EU ETS. Zagotavljanje visokih ravni razpoložljivosti, celovitosti in zaupnosti tega pretoka podatkov zato postane bistven vidik, ki ga je treba upoštevati pri načrtovanju začasne rešitve in stalne povezave med registroma. Ker gre za projekt, v katerem imajo ključno vlogo infrastruktura IKT, prilagojena programska oprema in postopki, je treba upoštevati vse tri elemente, da bi se lahko oblikoval odporen sistem.

Odpornost infrastrukture IKT

V poglavju o splošnih določbah v tem dokumentu so podrobno opisani gradniki zgradbe. Na področju infrastrukture IKT začasna povezava vzpostavlja odporno omrežje VPN (ali enakovredno omrežje), ki vzpostavlja varne komunikacijske tunele, skozi katere lahko poteka varna izmenjava sporočil. Drugi infrastrukturni elementi so konfigurirani kot visoko razpoložljivi in/ali se zanašajo na nadomestne mehanizme.

Odpornost prilagojene programske opreme

Moduli prilagojene programske opreme povečujejo odpornost z večkratnim poskušanjem vzpostavitve komunikacije v določenem času z drugim koncem, če ta iz katerega koli razloga ni na voljo.

Odpornost storitve

Pri začasni rešitvi izmenjave podatkov med pogodbenicama potekajo vse leto v vnaprej določenih časovnih okvirih. V nekaterih korakih je bilo pri vnaprej načrtovanih izmenjavah podatkov potrebno ročno posredovanje upravljavcev sistemov in/ali administratorjev registrov. Ob upoštevanju tega vidika ter zaradi povečanja razpoložljivosti in uspešnosti izmenjav:

— so v delovnih postopkih predvidena velika časovna okna za izvajanje vsakega koraka,

— moduli programske opreme za začasno rešitev izvajajo asinhrono komunikacijo,

— samodejni postopek usklajevanja odkrije morebitne težave pri zajemu podatkovnih datotek na katerem koli koncu,

— postopek spremljanja (infrastrukture IKT in modulov prilagojene programske opreme) velja za enega od postopkov upravljanja incidentov, ki jih tudi sproži (kot je opredeljeno v dokumentu o skupnih delovnih postopkih). Navedeni postopki, katerih cilj je skrajšati čas za obnovitev normalnega delovanja po incidentih, so bistveni za zagotovitev visokih ravni razpoložljivosti.

4.2 *Načrt inicializacije, komunikacije, ponovne aktivacije in testiranja*

Vsi različni elementi, vključeni v zgradbo začasne rešitve, opravijo niz posameznih in skupinskih testov za potrditev pripravljenosti platforme na ravni infrastrukture IKT in informacijskega sistema. Ti operativni testi so obvezen predpogoj pri vsakem prehodu začasne rešitve na platformi iz stanja prekinitve v stanje delovanja.

Za aktivacijo stanja delovanja povezave se nato zahteva uspešna izvedba vnaprej določenega načrta testiranja. S tem se potrdi, da je bil v vsakem registru najprej opravljen niz notranjih testov, čemur je sledila potrditev povezljivosti med koncema pred začetkom pošiljanja produkcijskih transakcij med pogodbenicama.

Načrt testiranja bi moral vključevati celotno strategijo za testiranje in podrobnosti o testni infrastrukturi. Za vsak posamezen element v vsakem testnem bloku bi moral predvsem vključevati:

— testna merila in orodja,

— dodeljene vloge za izvajanje testa,

— pričakovane rezultate (pozitivne in negativne),

— časovni načrt testiranja,

— zahteve glede zapisovanja rezultatov testa,

— dokumentacijo o odpravljanju težav,

— določbe o prenosu reševanja.

Testi za aktivacijo stanja delovanja bi se kot postopek lahko razdelili na štiri (4) konceptualne bloke ali faze:

4.2.1 Interni testi infrastrukture IKT

Te teste naj bi izvajali in/ali preverjali pogodbenici na vsakem koncu.

Posebej se testira vsak element infrastrukture IKT na vsakem koncu. To vključuje vsak posamezen sestavni del infrastrukture. Ti testi se lahko izvajajo samodejno ali ročno, v obeh primerih pa preverjajo, ali deluje vsak element infrastrukture.

4.2.2 Testi komunikacije

Te teste sproži katera koli od pogodbenic posamično, za zaključek teh testov pa je potrebno sodelovanje z drugim koncem.

Ko posamezni elementi začnejo delovati, je treba testirati komunikacijske kanale med obema registroma. V ta namen vsaka pogodbenica preveri, ali internetni dostop deluje, ali so vzpostavljeni tuneli VPN (ali enakovredno varno omrežje za prenos) in ali obstaja IP-povezljivost od spletnega mesta do spletnega mesta. Nato je treba na drugem koncu potrditi dosegljivost elementov lokalne in oddaljene infrastrukture ter IP-povezljivost.

4.2.3 Testi celotnega sistema (med koncema)

Ti testi naj bi se izvajali na vsakem koncu, rezultati pa bi se delili z drugo pogodbenico.

Ko se opravi testiranje komunikacijskih kanalov in vsakega posameznega sestavnega dela obeh registrov, vsak konec pripravi niz simuliranih transakcij in usklajevanj, ki predstavljajo vse funkcije, ki naj bi se izvajale v okviru povezave.

4.2.4 Testi varnosti

Te teste naj bi izvajali in/ali sprožili na vsakem koncu v skladu s podrobnimi navodili v oddelkih 5.4 „Smernice za testiranje varnosti“ in 5.5 „Določbe o oceni tveganja“.

Šele ko se vsaka od štirih faz/blokov konča s predvidljivim rezultatom, se lahko šteje, da je začasna povezava v stanju delovanja.

Viri testiranja

Vsaka pogodbenica ima na voljo določene vire testiranja (določeno programsko in strojno opremo infrastrukture IKT) ter v svojih sistemih razvije testne funkcije, ki zagotavljajo podporo ročni in neprekinjeni potrditvi platforme. Administratorji registrov lahko te postopke sami ali v sodelovanju z drugimi administratorji kadar koli izvajajo ročno. Aktivacija stanja delovanja je sama po sebi postopek, ki se izvaja ročno.

Prav tako je zagotovljeno, da platforma izvaja redna samodejna preverjanja. Namen navedenih preverjanj je povečati dostopnost platforme z zgodnjim odkrivanjem potencialnih težav pri infrastrukturi ali programski opremi. Ta načrt spremljanja platforme sestavljata dva elementa:

— spremljanje infrastrukture IKT: infrastrukturo na obeh koncih spremljajo ponudniki storitev infrastrukture IKT. Samodejni testi zajemajo različne elemente infrastrukture in razpoložljivost komunikacijskih kanalov;

— spremljanje aplikacije: moduli programske opreme začasne povezave izvajajo sistem spremljanja komunikacije na ravni aplikacije (ročno in/ali redno), s čimer se testira razpoložljivost povezave na obeh koncih s simulacijo nekaterih transakcij prek povezave.

4.3 *Okolja sprejemanja/testiranja*

Zgradba registra Unije in švicarskega registra vsebuje naslednja tri okolja:

— produkcija (PROD): to okolje vsebuje realne podatke in obdeluje realne transakcije,

— sprejemanje (ACC): to okolje vsebuje nerealne ali anonimizirane, reprezentativne podatke. V tem okolju upravljavci sistemov obeh pogodbenic potrjujejo nove izdaje,

— test (TEST): to okolje vsebuje nerealne ali anonimizirane, reprezentativne podatke. To okolje je omejeno na administratorje registrov in je namenjeno izvajanju integracijskih testov pri obeh pogodbenicah.

Razen v primeru VPN (ali enakovrednega omrežja) so tri okolja povsem neodvisna drugo od drugega, kar pomeni, da se strojna in programska oprema, podatkovne zbirke, navidezna okolja, IP-naslovi in vhodi vzpostavljajo in delujejo neodvisno drug od drugega.

Postavitev VPN je vzpostavljena v dveh različnih okoljih, tj. ena za PROD, druga, neodvisna pa za ACC in TEST.

5. **Določbe o zaupnosti in celovitosti**

Varnostni mehanizmi in postopki vsebujejo metodo dveh oseb (načelo štirih oči) za delovanje v povezavi med registrom Unije in švicarskim registrom. Metoda dveh oseb se uporabi, kadar koli je to potrebno. Vendar se morda ne bo uporabila za vse korake, ki jih izvajajo administratorji registrov.

Varnostne zahteve so upoštevane in obravnavane v načrtu upravljanja varnosti, ki vključuje tudi postopke, povezane z obravnavo varnostnih incidentov, ki sledi morebitni kršitvi varnosti. Del teh postopkov, ki se nanaša na delovanje, je opisan v dokumentu o skupnih delovnih postopkih.

5.1 *Infrastruktura za testiranje varnosti*

Vsaka pogodbenica se zaveže, da bo vzpostavila infrastrukturo za testiranje varnosti (z uporabo skupnega sklopa programske in strojne opreme, ki se uporablja pri odkrivanju ranljivosti v fazi razvoja in delovanja):

— ločeno od produkcijskega okolja,

— kadar varnost analizira skupina, in sicer neodvisno od razvoja in delovanja sistema.

Vsaka pogodbenica se zaveže, da bo opravila statično in dinamično analizo.

Pri dinamični analizi (kot je penetracijsko testiranje) se obe pogodbenici zavežeta, da bosta omejili ocene večinoma na okolja testiranja in sprejemanja (kot je opredeljeno v oddelku 4.3 „Okolja sprejemanja/testiranja“). Izjeme pri tej politiki morata odobriti obe pogodbenici.

Pred postavitvijo v produkcijsko okolje se testira varnost pri vsakem modulu programske opreme v povezavi (kot je opredeljeno v oddelku 3.1 „Zgradba komunikacijske vezi“).

Infrastruktura za testiranje mora biti na ravni omrežja in na ravni infrastrukture ločena od produkcijske infrastrukture. Testi varnosti, potrebni za preverjanje skladnosti z varnostnimi zahtevami, se izvajajo znotraj infrastrukture za testiranje.

5.2 *Določbe o prekinitvi povezave in ponovni aktivaciji*

Če obstaja sum, da je varnost švicarskega registra, SSTL, registra Unije ali EUTL ogrožena, se pogodbenici takoj medsebojno obvestita o tem ter prekineta povezavo med SSTL in EUTL.

Postopki izmenjave informacij ter postopki za odločitev o prekinitvi in odločitev o ponovni aktivaciji so del postopka izpolnjevanja zahtevkov, ki je del skupnih delovnih postopkov.

Prekinitve

Prekinitev povezave med registroma v skladu s Prilogo II k Sporazumu se lahko zgodi zaradi:

— razlogov, povezanih z upravljanjem (npr. vzdrževanje), ki so načrtovani,

— varnostnih razlogov (ali okvar infrastrukture IT), ki niso načrtovani.

V nujnih primerih pogodbenica o tem obvesti drugo pogodbenico in enostransko prekine povezavo med registroma.

Če je sprejeta odločitev o prekinitvi povezave med registroma, vsaka pogodbenica zagotovi, da se povezava prekine na ravni omrežja (z delnim ali celotnim blokiranjem vhodnih in izhodnih povezav).

Odločitev o prekinitvi povezave med registroma, bodisi načrtovani bodisi nenačrtovani, bo sprejeta v skladu s postopkom upravljanja sprememb ali postopkom obvladovanja varnostnih incidentov, ki sta del skupnih delovnih postopkov.

Ponovna aktivacija komunikacije

Odločitev o ponovni aktivaciji povezave med registroma se sprejme na način, ki je podrobno opisan v skupnih delovnih postopkih, nikakor pa ne pred uspešnim dokončanjem postopkov testiranja varnosti, kot je navedeno v oddelkih 5.4 „Smernice za testiranje varnosti“ in 4.2 „Načrt inicializacije, komunikacije, ponovne aktivacije in testiranja“.

5.3 *Določbe o kršitvah varnosti*

Kršitev varnosti velja za varnostni incident, ki vpliva na zaupnost in celovitost vseh občutljivih informacij in/ali razpoložljivost sistema, ki jih obdeluje.

Občutljive informacije so opredeljene na seznamu občutljivih informacij in se lahko obdelujejo v sistemu ali katerem koli povezanem delu sistema.

Informacije, neposredno povezane s kršitvijo varnosti, štejejo za občutljive, označene so z oznako „ETS KRITIČNA“ in se obdelujejo v skladu z navodili za obdelavo, če ni določeno drugače.

Vsaka kršitev varnosti se obdela v skladu s poglavjem o obvladovanju varnostnih incidentov v dokumentu o skupnih delovnih postopkih.

5.4 *Smernice za testiranje varnosti*

5.4.1 Programska oprema

Pri vseh večjih novih izdajah programske opreme se v skladu z varnostnimi zahtevami, ki jih določajo tehnični standardi za povezavo, opravi testiranje varnosti, po potrebi vključno s penetracijskim testiranjem, da bi se ocenili varnost povezave in povezana tveganja.

Če v zadnjih 12 mesecih ni bila pripravljena nobena večja izdaja, se testiranje varnosti izvede v trenutnem sistemu ob upoštevanju razvoja kibernetskih groženj v zadnjih 12 mesecih.

Testiranje varnosti povezave med registroma se izvede v okolju sprejemanja in po potrebi v produkcijskem okolju ter z usklajevanjem in na podlagi medsebojnega dogovora obeh pogodbenic.

Pri testiranju spletne aplikacije se upoštevajo mednarodni odprti standardi, kot so standardi, razviti v okviru projekta o varnosti odprtih spletnih aplikacij (Open Web Application Security Project – OWASP).

5.4.2 Infrastruktura

Infrastruktura, ki podpira produkcijski sistem, se redno pregleduje zaradi morebitnih ranljivosti (vsaj enkrat na mesec), odkrite ranljivosti pa se popravijo. Testiranje se izvede v skladu z metodo iz oddelka 5.4.1 z uporabo posodobljene zbirke podatkov o ranljivosti.

5.5 *Določbe o oceni tveganja*

Če je penetracijsko testiranje mogoče uporabiti, ga je treba vključiti v testiranje varnosti.

Vsaka pogodbenica mora skleniti pogodbo s specializiranim podjetjem za izvajanje testiranja varnosti, če to podjetje:

— ima znanje in izkušnje v zvezi s takim testiranjem varnosti,

— ne poroča neposredno razvijalcu in/ali svojemu izvajalcu in če ni vključeno v razvoj programske opreme za povezavo ali če ni podizvajalec razvijalca,

— podpiše sporazum o zaupnosti, da bi ohranilo zaupnost rezultatov in jih obdelovalo na ravni „ETS KRITIČNA“ v skladu z navodili za obdelavo.