# SPECIFIKIMET TEKNIKE

## KORPORATA ELEKTROENERGJITIKE SHQIPTARE SH.A

## SISTEMI I SIGURISË KIBERNETIKE FAZA II

# 1 PËRMBAJTJA

# 2 Përfituesi /Autoriteti Kontraktues

Korporata Elektroenergjetike Shqiptare (KESH sh.a), është një shoqëri tregtare aksionere shtetërore dhe është prodhuesi kryesor dhe më i rëndësishëm i energjisë elektrike në Shqipëri, që administron dhe operon hidrocentralet e kaskadës së lumit Drin (HEC-Fierzë, HEC-Koman, HEC-Vau i Dejës).

## 2.1 Hyrje

Një nga detyrimet kryesore të Korporatës Elektroenergjitike Shqiptare, si kompani e rëndësisë së veçantë dhe që ofron shërbime unike në tregun shqiptar të energjise elektrike, është garantimi i zbatimit të proceseve dhe rregullave të përditshme të punës, me qëllim ofrimin cilësor dhe të pandërprerë të shërbimeve. Këto rregulla shtrihen në të gjitha proceset e punës së institucionit dhe një vëmendje e veçantë i kushtohet edhe aplikimit të tyre në infrastrukturën e kompanisë.

Në këtë kuadër KESH ka realizuar shërbimin e enkriptimit të komunikimit objektivi i të cilit është siguria e infrastrukturës së rrjetit dhe komunikimeve. Përmes këtij shërbimi, është adresuar zgjidhja e pikave të mëposhtme:

- Shmangia e problemeve të sigurisë së rrjetit aktual të infrastrukturës.
- Mbrojtja gjithëpërfshirëse e të dhënave të klasifikuara në nivele të ndryshme, si në nivel lokal ashtu edhe gjatë transferimit nëpërmjet rrjeteve të hapura.
- Sigurimi i të dhënave personale dhe parandalimi i çfarë do shkatërrimi të paqëllimshëm, ose të qëllimshëm të paautorizuar të tyre.

Për të optimizuar mënyrën e menaxhimit të shërbimit të enkriptimit për garantimin dhe ruajtjen e disponueshmërisë të tij, lind nevoja e ndërtimit të një sistemi automatik për backup dhe restore të dedikuar për shërbimin e enkriptimit sidhe zgjerimi i infrastrukturës së enkriptuar për të akomoduar zhvillimet e korporatës me adaptimet e TEC.

# 3 Përshkrimi i Përgjithshëm i kërkesave

Qëllimi i këtij proçesi është nevoja e implementimit të një zgjidhjeje sipas praktikave më të mira të menaxhimit të sistemeve për Backup/Restore/Monitoring të shërbimit menaxhues të sistemit të enkriptimit në platforma tërësisht të sigurta për ruajtjen e disponueshmërisë së shërbimeve dhe të të dhënave. Zgjidhje e dedikuar me platforma virtuale është një nga teknologjitë që ka aftësinë për të përmirësuar proçeset e kryerjes së punimeve dhe shërbimeve si dhe efikasitetin në rastet kur ka humbje të shërbimit në ambientet ku është instaluar platforma e menaxhimit e cila përmban të gjithë konfigurimet e paisjeve enkriptuese.
Me zhvillimet e fundit në korporatë, si pasojë e shtesave të infrastrukturës të klasifikuar si kritike, konkretisht TEC nevojitet adaptimit i rrjetit të enkriptuar duke shtuar diodat enkriptuese sipas nevojës për të akomoduar zgjerimin e njësive.

## 3.1 Situata aktuale

Infrastruktura e rrjetit në KESH është një infrastrukturë komplekse në të cilën përfshihet edhe sistemi i klasifikuar si infrastrukturë kritike. Sistemi i menaxhimi të prodhimit të instaluar në çdo njësi janë sisteme të tipit SCADA të cilat monitorojnë dhe komandojnë atribute tenkike për agregatët e prodhimit të energjisë elektrike. Për të siguruar sigurinë kibernetike mar shkasë nga veprimtaritë dashakeqe të vitit të fundit, KESH ka adaptuar shërbime enkriptimi në ndërlidhjen midis njësive të prodhimit dhe qëndrës së institucionit.
Paisjet enkriptuese (diodat) aktualisht janë të instaluara si pika ndërlidhjeje hyrëse dhe dalëse për të enkriptuar komunikimin në nivel IP (internet protokoll) dhë për të ndarë rrjetin kibernetik. Rrjeti aktualisht ndahet në nyjet BLACK (rrjet jo i sigurtë) dhe RED (rrjet i sigurtë i enkriptuar). Rrjeti i sigurtë RED përfshin shërbime të infrastrukturës kritike nga ku komuniki qëndron në një sistem të mbyllur të enkriptuar dhe të pa lexueshëm nga jashtë pa patur dioda enkriptimi së bashku me çelsat dhe kartat e enkriptimit. Për të realizuar mbylljen e komunikimit midis rrjeteve të sigurtë dhe atij normal midis datacenter në KESH qendër dhe pikave të prodhimit është bërë instalimi i pajisjeve enkriptuese dhe infrastrukturës së menaxhimit server – klient sipas specifikimeve teknike të mëposhtme:

| Nr. | Emertimi | Njesia | Sasia |
|---|---|---|---|
| 1 | Pajisje enkriptuese Diode (Siena Layer3) | copë | 4 |
| 2 | Server INSPUR | copë | 1 |
| 3 | Firewall Paloalto | copë | 1 |

| **FIREWALL** | |
|---|---|
| Porta GE RJ45 WAN / DMZ | 2/1 |
| Porta e brendshme GE RJ45 | 7 |
| Porta USB | 1 |
| Tastiere | (RJ45) |

| **SERVER** | |
|---|---|
| Form Factor | Të montueshëm në rack |
| Procesor: | Minimumi 1 CPU x 10 core minimum 2 GHz. |
| Chipset | Intel or AMD |
| Slote memorje RAM | Min 12 DIMMs of DDR4 memory |
| Memorja "RAM": | Minimum 32 GB Memory te perfshira. |
| Madhësia e Hard Diskut | 2 x 300GB 10k rpm SAS |
| "RAID Controller": | Hardware Raid Controller. |
| "Network" | Minimumi 1 kartë dual port 1GB Ethernet |
| "Management Network" | Portë menaxhimi e dedikuar e cila bën menaxhimin edhe nëse serveri është i fikur. Të japë mundësi për fikje/ndezje/logs etj. |
| Operating systems | vMware , RedHat Linux |
| | |

Pajisjet enkriptuese janë instaluar ne 4 pika kryesore: në KESH dhe në pikat e prodhimit aktualisht aktive Fierzë, Koman dhe Vau i Dejës. Ndërkohë paisjet shtesë për ndërtimin e rrjetit të sigurtë duhet të instalohen në KESH qendër dhe TEC Vlorë.

| Aspektet Teknike | *Shpjegim* | Zgjidhje e IP se Kriptimit |
|---|---|---|
| Pajisjet | *Suitë produktesh të instaluara*<br>*- Porta e kriptimit*<br>*- Klienti i kriptimit*<br>*- qendra e menaxhimit të sigurisë* | Porta e kriptimit:<br>- Kuti enkriptuese L3<br>Klienti i kriptimit:<br>- Departamenti (WS)<br>Qendra e menaxhimit të sigurisë:<br>- Server i menaxhimi (Mgmt) |
| Çertifikimi dhe vlerësimi | *Çertifikimi ndërkombetar / miratimi* | Çertifikimi ndërkombetar:<br>- Deri në EU SECRET<br>- Deri në NATO SECRET |

# 4 OBJEKTIVI DHE REZULTAT E PRITURA

## 4.1 Objektivi i Përgjithshëm

Objektivi i përgjithshëm i kësaj kontrate është zgjerimi i infrastrukturës së enkriptuar duke akomoduar ndryshimet në korporatë me futjen në infrastrukturën e sigurtë të TEC Vlorë. Kërkesa për shërbim të disponueshmërise dhe backup të konfigurimeve apo shërbim menaxhimi të enkriptimit me standartet më të larta të sigurisë sipas proçeseve si më poshtë:

- Furnizimi dhe instalimi i paisjeve hardware me liçensat, kartat e sigurisë dhe çelsat e sigurisë sipas specifikimeve teknike dhe kompatibël me sistemin e instaluar.
- Konfigurimet e nevojshme për të realizuar shërbimin.

## 4.2 Rezultat që duhet të arrihen nga Operatori Ekonomik

- Furnizimi dhe instalimi i paisjeve hardware me liçensat, kartat e sigurisë dhe çelsat e sigurisë sipas specifikimeve teknike dhe kompatibël me sistemin e instaluar.

- Konfigurimi dhe lidhja në rrjetin ekzistues të enkriptuar (RED) të diodave paisjeve enkriptuese shtesë sipas kërkesave të stafit të KESH sh.a.

- Ngritja e një infrastrukture off-site (vendndodhje sekondare) sipas standarteve ISO27001 dhe rregullave në fuqi për vazhdueshmërinë e shërbimeve të sigurisë kibernetike.

- Konfigurimet përkatëse për ndërlidhjen midis vendodhjes kryesore të sistemeve të menaxhimit në KESH sh.a. dhe vendndodhjes së infrastrukturës backup.

- Sigurimin e ndërlidhjes midis site-eve me fibër optike të dedikuar duke kaluar në rrugë fizike të ndryshme për të ofruar disponueshmëri në raste avarie teknike.

- Konfigurimet për lidhjet nga jashtë kompanisë me rrjetin e sigurtë të enkriptuar (RED) nëpërmjet workstations të furnizuara.

- Dokumentimi i plotë i të gjithë instalimeve dhe konfigurimeve të realizuara.

# 5 SUPOZIMET DHE RISQET

## 5.1 Supozimet e projektit

Realizimi i këtij projekti do të bazohet në supozimet e mëposhtme:

- Pjesëmarrje aktive dhe disponibilitet i të gjithë palëve të interesuara në implementimin e këtij projekti
- Vënia në dispozicion e infrastrukturës së nevojshme për implementimin e zgjidhjes
- Alokimi i burimeve njerëzore të nevojshme për implementimin e këtij projekti

## 5.2 Risqet

Është i rëndësishëm impenjimi i plotë i grupeve të punës pjesëmarrëse në zhvillimin e projektit. Disa nga faktorët që do të mund të riskonin ecurinë e projektit:

- Mospërmbushja e plotë e kërkesave funksionale, teknike dhe kohore nga operatori ekonomik.
- Vlerësimi jo i saktë i situatës aktuale të sistemit dhe infrastrukturës.
- Mos përcaktimi i saktë i burimeve të nevojshëm për realizimin e projektit
- Rrezik me humbjen e konfidencialitetit te informacioneve mbi konfigurimet
- Dëmtim apo shpërndarje e pa autorizuar e çelsave, kartave të sigurisë.

# 6 PERSHKRIMI I DETYRAVE

## 6.1 Detyrat specifike

Në kuadër të qëllimit kryesor, i gjithë projekti duhet të realizojë detyrat e mëposhtme:

1. Analizimin e situatës aktuale dhe përcaktimin e planit të punës për ekzekutimin e projektit
2. Ngritja e grupeve të punës nga palët e interesuara
3. Aprovimin e planit të punës nga stafi i KESH IT dhe ndjekësit e kontratës
4. Furnizimi i pajisjeve hardware dhe liçensat e nevojshme në përputhje me specifikimet teknike të shprehura në këtë dokument.
5. Konfigurimet e nevojshme për adaptimin e infrastrukturës shtesë në rrjetin e sigurtë (RED)
6. Konfigurimet për aksesin e infrastrukturës së enkriptuar SCADA nga jashtë kompanisë duke përdorur worskstations të enkriptuar
7. Testimin e konfigurimeve
8. Dokumentimi i të gjithë instalimeve dhe konfigurimeve të realizuara.
9. Marrja në dorëzim e projektit
10. Transferimi i njohurive të stafit IT dhe atyre të mirëmbajtjes së sistemeve SCADA për adoptimet dhe konfigurimet.

# 7 Logjistika dhe Koha

## 7.1 Vendndodhja

- Zgjidhja backup duhet të instalohet në një infrastrukturë hardware të siguruar nga operatori ekonomik. Cdo liçense software e nevojshme në kuadër të shërbimit duhet të sigurohet nga operatori ekonomik.
- Operatori ekonomik do të jetë pergjegjës për vazhdueshmërinë e sistemit në 24x7 dhe të njoftojë paraprakisht për ndërhyrje mirëmbajtjeje apo raste difektesh.

## 7.2 Afati kohor për zbatimin e projektit

**Afati kohor-** për zbatimin e këtij projekti do të jetë 60 ditë, nisur nga data e nënshkrimit të kontratës.

**Mirembajtja -** do të përfshihet në shërbimet e mirëmbajtjes së kontratës që KESH disponon me objekt "Shërbimi i enkriptimit të komunikimit. Siguria kibernetike në infrastrukturën kritike". Shërbimet e mirëmbajtjes do të realizohen konform kërkesave bashkëlidhur këtyre specifikimeve teknike.

# 8 PLANIFIKIMI I BUXHETIT

| Nr. | Emërtimi | Sasia | Njësia | Çmimi |
|---|---|---|---|---|
| **1** | Shërbim i instalimit dhe kofigurimit të Sistemit Backup | 1 | Copë | |
| **2** | Infrastruktura e ruajtjes së të dhënave | 1 | Copë | |
| **3** | Pajisje rrjeti enkriptuese (diodë) | 4 | Copë | |
| **4** | Konfigurim i paisjeve të enkriptimit (dioda) | 1 | Copë | |
| **5** | Worskstation i enkriptuar (Laptop) | 3 | Copë | |
| | **TOTALI ME TVSH (LEKË)** | | | |

# 9 Zbatimi i projektit dhe shërbimet

## 9.1 Menaxhimi i Projektit

1. Operatori ekonomik duhet të jetë përgjegjës për furnizimin e hardware dhe software sipas sasisë së specifikuar.

2. Instalimi, setup-i, konfigurimi i hardware-ve dhe software-ve.

3. Projekti duhet të përfundojë plotësisht brenda 60 ditëve, nga data e firmosjes së kontratës.

| Nr | Përshkrimi | Afati |
|---|---|---|
| **1** | Levrim, instalim, setup, testim dhe venie në punë të paisjeve shtesë të enkriptimit (diode) | 60 ditë |
| **2** | Ngritja e infrastrukturës backup sipas kërkesave teknike | 60 ditë |
| **3** | Levrim, konfigurim, testim dhe vënie në punë të stacioneve (laptop) të enkriptuar | 60 ditë |
| **4** | Sherbime implementimi | 60 ditë |
| **5** | Trajnim i stafit | 5 ditë |

### 9.2 Trajnimi

Trajnimi i përdoruesve duhet të jetë për të gjithë përdoruesit e rrjetit të enkriptuar si dhe për ndryshimet që do të realizohen në infrastrukturë.

## 10 PËRGJIGJA DHE SHKALLËZIMI I SHËRBIMIT

Në tabelën e mëposhtme përcaktohet kategorizimi i seriozitetit të problemeve te lindura dhe koha e përgjigjes për zgjidhjen e tyre.

| **Kategoria A ( Kritik/ I Larte)** | **Kategoria A (I Mesem)** | **Kategoria C (I Ulet)** |
|---|---|---|
| Mos funksionimi i aplikacionit krijon apo rrezikon shumë aktivitetin normal | Mos funksionimi i aplikacionit krijon vonesa në aktivitetin normal | Mos funksionimi i aplikacionit pengon në mënyrë minimal aktivitetin |
| ***Numri i përdoruesve të ndikuar*** | | |
| Mos funksionimi i sistemit ndikon një numër ***shumë të madh*** të përdoruesve | Mos funksionimi i sistemit ndikon një numër ***të vogël*** të përdoruesve | Mos funksionimi i sistemit ndikon pjesërisht në disa përdorues |
| ***Pezullimi i punës*** | | |
| Mos funksionimi i sistemit pengon përdoruesit ***të realizojnë pjesën më të madhe të punës së tyre.*** | Mos funksionimi i sistemit pengon përdoruesit ***të realizojnë pjesë te punës së tyre*** | Mos funksionimi i sistemit pengon përdoruesit ***të realizojnë disa pjesë të vogla të punës së tyre***, |
| ***Zgjidhje alternative e përkohshme*** | | |

| | | |
|---|---|---|
| ***Nuk ka një mënyre alternative*** të përkohshme dhe të pranueshme për zgjidhjen e problemit | ***Ka pjesërisht një mënyre alternative*** të përkohshme dhe të pranueshme për zgjidhjen e problemit. | ***Ka një mënyrë alternative*** të përkohshme dhe të pranueshme për zgjidhjen e problemit.. |
| ***Koha e përgjigjes*** | | |
| ○ *1 orë për të kthyer përgjigje*<br>○ *Në vend brenda 4 orëve* | ○ *2 orë për të kthyer përgjigje*<br>○ *Në vend brenda 8 orëve* | ○ *4 orë për të kthyer përgjigje*<br>○ *Në vend brenda 24 orëve* |
| ***Koha e zgjidhjes*** | | |
| Maksimumi i pranimit Kjo zgjidhjes është 1 dite pas kërkesës. | Maksimumi i pranimit Kjo zgjidhjes është brenda 5 ditëve të punës. | Maksimumi i pranimit Kjo zgjidhjes është 10 ditë kalendarike. |

### 10.1 Raportimi

Shërbimi duhet të përfshije kontrollet periodike të sistemeve, si dhe përpilimin e raporteve periodike mujore të cilat do të japin një pershkrim të përgjithshëm të performancës dhe gjëndjes së backup.

**Raportet** duhet të pergatiten mbi të dhenat e menaxhimit të problemeve dhe duhet të permbajnë minimalisht:

a. Raportimin e problemeve të identifikuara (nëse ka)
b. Propozimin e masave organizativo-teknike që duhen marrë me qëllim minimizimin e përsëritjes së tyre.

## 11 KËRKESAT TEKNIKO FUNKSIONALE

### 11.1 Strategjia e Backup

- Operatori ekonomik, me qëllim garantimin e vazhdimësisë së biznesit, si dhe mbrojtjen e të dhënave personale në përputhje me legjislacionin kombëtar, siguron nëpërmjet një vendndodhje sekondare (off site) kryerjen e back up automatik të serverave të menaxhimit dhe konfigurimeve të paisjeve të enkriptimit të KESH sh.a.

- Komunikimi midis serverit in site dhe off site realizohet nëpërmjet teknologjisë VPN (Virtual Private Network), me qëllim garantimin e një komunikimi të sigurt informacioni. Ndërlidhja fizike nëpërmjet vendndodhjeve primar dhe off site duhet të sigurohet nga operatori ekonomik me anë të fibrës optike e cila kalon në rrugë fizike të ndryshme për të garantuar vazhdueshmëri.

- Operatori ekonomik përdor sisteme backup të automatizuara që sigurojnë sinkronizim të dhënash në një periudhë çdo 24 orë.

## 11.2 Kërkesat teknike

| Workstation i enkriptuar (Laptop) | |
|---|---|
| Pikët Min. për Procesorin sipas: cpubenchmark.net Min Proc. Rating According to: cpubenchmark.net: | 4500 pikë |
| “Chipset”: | Intel ose Ekuivalent |
| “RAM”: | 32 GB DDR4 2666 MHz |
| Madhësia e Hard Diskut “HDD Size”: | 1 TB Solid State Drive |
| “Graphics”: | Integrated HD Graphics |
| Ekrani “Display”: | TFT 14.0" FHD IPS (1920x1080) Backlit Anti-Glare Display |
| Bateria “Battery”: | Min. 45 Wh |
| Sistemi i Operimit “Preinstalled Licensed O.S.”: | OEM Windows 10 64-bit Professional |
| Portat e Komunikimit “Ports”: | Min. (3) USB; (1/1)Headphone/Microphone; (1) Integrated Web Camera; (1) DisplayPort/HDMI |
| Garancia | 48 muaj |

| Porta e Kriptimit | | |
|---|---|---|
| Karakteristikat e portës së kriptimit | *Hapi i 3 i portës së kriptim*<br>*- pajisjet duhet të ftohen vetevetiu në mënyrë pasive (pa freskuese)*<br>*- minimumi 3 porta USB*<br>*- minimumi 4 konfigurime*<br>*- rrjeti RJ45* | Kuti enkriptuese (2 Gbit/s) |
| Përdorimi i Kartës Inteligjente | Funksionimi i kripto portës së ofruar kërkon një kartë inteligjente të parakonfiguruar dhe të lidhu gjatë gjithë kohës të krijuar në sistemin e menaxhimit.<br>Sistemet funksionale të pranuara të kartave inteligjente:<br>- CardOS<br>- STARCOS | Kutitë enkriptuese duhet të kërkojnë kartë inteligjente të parakonfiguruar dhe<br>të lidhur gjatë gjithë kohës (pajisja e vogël ka nevojë për një USB token përfshirë kartën inteligjente).<br>Sistemet operative të përshtashme të kartave inteligjente:<br>CardOS 4.01 a / CardOS 4.03 b<br>STARCOS<br>Kartat Inteligjente përmbajnë çertikatat dixhitale të sistemit të menaxhimit |
| Sistemet Operativ | Përshtatja e sistemit operativ të pajisjes kripto-portë | Sistem operativ i veçantë i minimizuar dhe më i përforcuar me siguri bazuar në burimet e LINUX.<br>Përfshirë këtu ndarja e proçeseve dhe mekanizmat e komunikimit ndër-procesor (IPC).<br>Kufizimet e aksesit për menaxhimin<br>Dhe të drejtat e aksesit për përdoruesit<br>Lidhjet kryesore/bazë (IP, PPP, Ethernet)<br>Drejtuesi i pajisjes (serial, USB, parallel, rrjeti)<br>Mbrojtja e rrjetit USB<br>Kriptografiket fillestare :<br>Kriptimi/vërtetimi simetrik/hash<br>Algoritme asimetrike<br>Gjenerator i numrave të rastit<br>Funksionet e kartës inteligjente<br>Siguria e rrjetit<br>IPsec (i avancuar për funksione shtesë të sigurisë)<br>IKE dhe funksione të tjera të marra<br>Nga menaxhimi i kriptimit (menaxhimi çertifikatës)<br>Filtrimi i paketave (tabelat IP)<br>Shënuesi specifik i paketave (gjurmon paketat brënda përbrenda) |

| | | |
|---|---|---|
| Mbrojta ndaj ndezjes së pa-autorizuar | | Administratori ka mundesi<br>të përcaktojë një hyrje të kërkuar të një, dy ose zero numrave PIN, për të mbrojtur proçesin e nisjes, të inicializuar nga një person i paautorizuar. |
| Algoritmi i kriptimit | *Algoritme mbështetëse të kriptimit*<br>*(Kërkohet AES 256bit)* | Kutia enkriptuese të mbështetet<br>në algoritmet e mëposhtme të kriptimit<br>- AES 192 / 256 |
| Funsionet HASH | *Funksionet mbështetëse HASH*<br>*(Janë të nevojshme RIPEMD 160 and SHA1)* | Kutia enkriptuese të mbështetet<br>në funksionet e mëposhtme HASH:<br>- RIPEMD 160<br>- SHA1/2/256 |
| Vlefshmëria e çelësit konfirmues (çelësi IKE) | *-Koha e vlefshmërisë nga 10 minuta deri në 24 orë* | Përkufizimi i IKE dikton vlefshmërinë çelësit të konfirmimit midis kutive enkriptuese. |
| Vlefshmeria e çelësit të sesionit (çelësi IPSec) | *-Koha e vlefshmërisë nga 2 minuta deri në 24 orë* | Përkufizimi i IPSec dikton Vlefshmërinë<br>kryesore të sesionit midis kutive enkriptuese. |
| Veçoritë NAT-T | *Të mbështesë teknologji NAT* | NAT-T e konfigurueshme dhe ka veçori përkrahëse/mbështetëse (përkthimi i adresave të rrjetit) |
| Karakteristikat QoS | *Të mbështesë QoS* | |
| Menaxhimi i kapacitetit të transmetimit | | Kutia enkriptuese të suportojë<br>në menaxhimin e kapacitetit të transmetimit bazuar në përkufizimet DSCP (Pika e Kodit të Shërbimit të Diferencuar). Një administrator krijon vlera DSCP për të përcaktuar klasa të ndryshme trafiku sipas udhëzimeve të operatorëve të rrjetit të përfshire. Për çdo klasë trafiku mund të caktohet një vlerë fikse e kapacitetit trasmetues. |
| Filtrimi i paketave | | Kutia enkriptuese të mbështesë<br>filtrimin e paketave në të dy sitet (të koduara dhe të pa koduara) |
| Protokolli i kriptimit | *IPSec / IKE me çertifikata dixhitale* | Protokolli i zbatuar i kriptimit të produkteve duhet të jetë IPSec me IKE përfshirë çertifikatat dixhitale |
| Portat e komunikimit | | IPSec → protokolli 50 i TCP/IP<br>Pa veçorinë e funksionit "Grup privat përdoruesish", porta UPD 500 përdoret për mesazhin e parë IKE. |

| | | |
|---|---|---|
| Çelësat e sesionit | | Çelësat e sesionit duhet të krijohen nga një gjenerator i numrave të rastit Shkëmbimi i çelësit të sesionit të gjeneruar duhet të bëhet duke përdorur mekanizmin e shkëmbimit të çelësave |
| Portë lokale për log-e | *Porta kripto duhet të ofrojë Mundësi lokale për mesazhet log* | Kutia enkriptuese të lidhet me një monitor dhe tastierë të jashtme për mesazhet log |
| Grup privat përdoruesish | | Kutia enkriptuese të mbështetet në veçorinë "grup privat/i mbyllur i përdoruesve". Vetem kutitë me të njëjtin çelës mund të komunikojnë me njëri-tjetrin. |