|  |
| --- |
| X-tee turvaserveri kasutajarollid |
| Analüüs  Redaktsioon: 0.9  12.11.2014  8 lk  Y-742-17 |

|  |  |  |  |
| --- | --- | --- | --- |
| Kuupäev | Nr | Kirjeldus | Autor |
| 14.08.2013 | 0.1 | Esialgne | Riin Saarmäe |
| 19.08.2013 | 0.2 | Kliendihaldur ümber nimetatud teenusehalduriks. Tegevuste tabel täiendatud ja korrigeeritud. | Riin Saarmäe |
| 30.08.2013 | 0.3 | Parandused | Riin Saarmäe |
| 27.09.2013 | 0.4 | Eliko. | Riin Saarmäe |
| 16.12.2013 | 0.5 | Süsteemiaudiitori ja kasutajakontode halduri rollid välja. | Riin Saarmäe |
| 16.12.2013 | 0.6 | Vaheversioon Eliko põhjal. | Riin Saarmäe |
| 01.07.2014 | 0.7 | Ajakohastatud. | Riin Saarmäe |
| 18.09.2014 | 0.8 | Süsteemiadministraator saab vaadata võtmeseadmete, võtmete ja sertifikaatide detailandmeid. | Riin Saarmäe |
| 12.11.2014 | 0.9 | Asünkroonsete teenuste privileegid välja, konfiguratsiooniankru privileegid juurde. | Riin Saarmäe |

Sisukord

[1 Sissejuhatus 4](#__RefHeading__1436_2115075793)

[2 Kasutajarollid 5](#__RefHeading__1450_2115075793)

[3 Privileegid 6](#__RefHeading__6294_160207474)

# Sissejuhatus

Töö eesmärgiks on kirjeldada X-tee turvaserverite kasutajarolle.

X-tee kasutajate ja õiguste haldus toetub operatsioonisüsteemi võimalustele.

See võimaldab:

- kasutada erinevaid kasutajahaldussüsteeme (lokaalsed, LDAP kasutajad vms),

- standardsete ja organisatsioonile sobivate vahenditega luua ja hallata õiguseid,

- läbipaistvus ja ühetaolisus tagab parema auditeeritavuse.

# Kasutajarollid

X-tee turvaserveris on toetatud järgmised rollid:

1. Turvahaldur – vastutab turvapoliitika ja turvanõuete rakendamise eest, sh haldab võtmeseadmeid, võtmeid ja sertifikaate.
2. Registreerimishaldur – vastutab turvaserverisse klientide registreerimise ja eemaldamise eest.
3. Teenusehaldur – haldab klientide poolt pakutavate teenuste andmeid ja pääsuõigusi.
4. Süsteemiadministraator – vastutab turvaserveri installeerimise, konfigureerimise ja tööshoidmise eest

Reeglid

1. Üks kasutaja võib esineda mitmes rollis.
2. Ühes rollis võib olla mitu kasutajat.
3. Kasuta privileegide hulga moodustab kasutaja rollide privileegide ühend.

# Privileegid

Rollidele omistatakse privileege kasutajaliidese tegevuse tasemel. Tegevuse käivitamiseks on kasutajaliideses reeglina nupp, mille funktsiooni võib dubleerida klahvikombinatsioon või hiiretoiming (näiteks saab erinevate nimekirjade objektide detailandmete vaatamise modaalakent avada vajutades nupule „Details“ või tehes hiirega topeltklõpsu objekti reale).

Juhul, kui kasutajaliidesesse sisse loginud kasutaja ei oma toimingu sooritamise privileegi, on tegevuse käivitamise nupp peidetud (ning tegevust ei ole võimalik käivitada ka dubleerivate klahvikombinatsioonide/hiiretoimingute abil) – kasutaja näeb vaid temale lubatud andmeid ja nuppe.

T - Turvahaldur

R - Registreerimishaldur

E - Teenusehaldur

S - Süsteemiadministraator

Täpploendi tasemed tabelis tähistavad modaalakende tasemeid kasutajaliideses. Madalama tasemega tegevustele õiguse andmiseks peab rollile olema antud õigus teostada eelneva taseme tegevust. Näiteks saab rollile anda õiguse kustutada kliendi andmeid vaid siis, kui eelnevalt on antud privileeg vaadata kliendi detailandmeid (st vajutada nupule, mis avab modaalakna, millel paikneb kliendi kustutamiseks vajalik nupp).

| **Tegevused** | **T** | **R** | **E** | **S** |
| --- | --- | --- | --- | --- |
| * Klientide nimekirja vaatamine | **x** | **x** | **x** |  |
| * + Uue kliendi andmete lisamine |  | **x** |  |  |
| * + Kliendi detailandmete vaatamine |  | **x** | **x** |  |
| * + - Kliendi registreerimise taotluse saatmine keskserverisse (register) |  | **x** |  |  |
| * + - Kliendi kustutamise taotluse saatmine keskserverisse (unregister) |  | **x** |  |  |
| * + - Kliendi andmete kustutamine |  | **x** |  |  |
| * + Kliendi teenuste vaatamine |  |  | **x** |  |
| * + - WSDL lisamine |  |  | **x** |  |
| * + - WSDL URL muutmine |  |  | **x** |  |
| * + - WSDL aktiveerimine/inaktiveerimine |  |  | **x** |  |
| * + - WSDL värskendamine |  |  | **x** |  |
| * + - WSDL kustutamine |  |  | **x** |  |
| * + - Teenuse parameetrite muutmine |  |  | **x** |  |
| * + - Teenuse pääsuõiguste vaatamine |  |  | **x** |  |
| * + - * Teenuse pääsuõiguste subjektide lisamine ja eemaldamine |  |  | **x** |  |
| * + Kliendi lokaalsete gruppide nimekirja vaatamine |  |  | **x** |  |
| * + - Uue lokaalse grupi loomine |  |  | **x** |  |
| * + - Lokaalse grupi kirjelduse muutmine |  |  | **x** |  |
| * + - Lokaalse grupi koosseise muutmine |  |  | **x** |  |
| * + - Lokaalse grupi kustutamine |  |  | **x** |  |
| * + Kliendi sisevõrgu serverite andmete vaatamine |  | **x** | **x** |  |
| * + - Teenuste kliendi rollis olevate sisevõrgu serverite ühendusviisi muutmine |  | **x** | **x** |  |
| * + - Sisevõrgu serveri sertifikaadi lisamine/kustutamine |  | **x** | **x** |  |
| * + - Sisevõrgu serveri sertifikaadi vaatamine |  | **x** | **x** |  |
| * + - Turvaserveri sertifikaadi eksportimine |  | **x** | **x** |  |
| * + Kliendi teenuste klientide (pääsuõiguste subjektide) nimekirja vaatamine |  |  | **x** |  |
| * + - Teenuste kliendi lisamine |  |  | **x** |  |
| * + - Teenuste kliendile avatud teenuste nimekirja vaatamine |  |  | **x** |  |
| * + - Teenuste kliendile avatud teenuste lisamine/eemaldamine |  |  | **x** |  |
| * Turvaserveri süsteemsete parameetrite vaatamine | **x** |  |  | **x** |
| * + Konfiguratsiooniankru üleslaadimine | **x** |  |  |  |
| * + Konfiguratsiooniankru allalaadimine | **x** |  |  | **x** |
| * + Ajatempliteenuste lisamine/kustutamine | **x** |  |  |  |
| * + Sisemise SSL ühenduse sertifikaadi vaatamine | **x** |  |  | **x** |
| * + Sisemise SSL ühenduse sertifikaadi eksportimine | **x** |  |  | **x** |
| * + Sisemise SSL ühenduse võtme loomine/muutmine | **x** |  |  | **x** |
| * Võtmete ja sertifikaatide nimekirja vaatamine | **x** | **x** |  | **x** |
| * + Võtmeseadmetesse sisse-välja logimine | **x** |  |  | **x** |
| * + Võtmeseadme detailandmete vaatamine | **x** | **x** |  | **x** |
| * + Võtme genereerimine | **x** | **x** |  |  |
| * + Võtme detailandmete vaatamine | **x** | **x** |  | **x** |
| * + Ilma rollita võtme kustutamine (sign/auth määramata) | **x** | **x** |  |  |
| * + Sertifikaadi detailandmete vaatamine | **x** | **x** |  | **x** |
| * + Autentimissertifikaadi päringu genereerimine | **x** |  |  |  |
| * + Autentimissertifikaadi importimine | **x** |  |  |  |
| * + Autentimissertifikaadi desaktiveerimine ja aktiveerimine | **x** |  |  |  |
| * + Autentimissertifikaadi registreerimistaotluse loomine & keskserverisse saatmine | **x** |  |  |  |
| * + Autentimissertifikaadi kustutamistaotluse loomine ja keskserverisse saatmine | **x** |  |  |  |
| * + Autentimissertifikaadi kustutamine | **x** |  |  |  |
| * + Autentimisvõtme kustutamine | **x** |  |  |  |
| * + Allkirjastamissertifikaadi päringu genereerimine | **x** | **x** |  |  |
| * + Allkirjastamissertifikaadi importimine | **x** | **x** |  |  |
| * + Allkirjastamissertifikaadi desaktiveerimine ja aktiveerimine | **x** | **x** |  |  |
| * + Allkirjastamissertifikaadi kustutamine | **x** | **x** |  |  |
| * + Allkirjastamisvõtme kustutamine | **x** | **x** |  |  |
| * Turvaserveri konfiguratsiooni varundusfailide nimekirja vaatamine |  |  |  | **x** |
| * + Varundusfaili genereerimine |  |  |  | **x** |
| * + Varundusfaili allalaadimine |  |  |  | **x** |
| * + Varundusfaili üleslaadimine |  |  |  | **x** |
| * + Varundusfaili kustutamine |  |  |  | **x** |
| * + Konfiguratsiooni taastamine varundusfailist |  |  |  | **x** |