IIS VEEBISERVERILE ID-KAARDI TOE SEADISTAMINE

Juhend, kuidas autentida kasutajat IIS veebiserveril.

VERSIOONIINFO

Kuupäev	Versioon	Muudatused
04.2017	1704	Juhend uuendatud Windows Server 2016 tasemele, lisatud KLASS3-SK 2016 sertifikaadi tugi. Eemaldatud peatükk „IIS SERVERITEST JA KLIENDIPOOLSEST SERDIAHELAST“. Eemaldatud peatükk „ID-KAARDI SERTIFIKAADI KEHTIVUSE KONTROLL“. Lisatud märkus võimaluse kohta kasutada tasuta OCSP teenust. Listaud märkus alamsertifitseerija EID-SK 2016 seadistamise kohta. Muudetud versioniseerimise loogikat. Uue loogika puhul versiooninumber XXXX tuletatud aastast/kalendrikuust (yy:mm).
09.2016	6.3	Lisatud info 18. märtsil 2011 väljastatud alamsertifitseerija EID-SK 2011 seadistamise kohta.
08.2016	6.2	Eemaldatud paigalduse juhised Juur-SK, ESTEID-SK 2007 ja KLASS3-SK 2010 (Juur-SK) installeerimiseks 26. augustil 2016 aeguva juursertifikaadi Juur-SK tõttu.
01.2016	6.1	Lisatud info 17. detsembril 2015 väljastatud alamsertifitseerija ESTEID-SK 2015 seadistamise kohta.
11.2015	6.0	Lisatud juhisesse konfiguratsiooniinfo, mis puudutab SK kesktaseme sertifikaate ESTEID-SK 2007 ja ESTEID-SK 2011. Parandatud test-OCSPga seonduvad lingid.
01.2012	5.0	Eemaldatud juhisest alamsertifitseerija ESTEID-SK konfigureerimise õpetus, kuna ESTEID-SK CA aegus 13.01.2012
06.2011	1.0	Esimene avalikustatud versioon

SISSEJUHATUS

Käesolev juhend kirjeldab, kuidas realiseerida Sertifitseerimiskeskuse poolt väljastatud sertifikaatidega (ID-kaart, elamisloakaart, digi-ID ja e-residendi digi-ID) kasutaja autentimise tugi Microsoft IIS veebiteenustel. Juhendi loomisel on kasutatud Windows Server 2016 platvormi. Näidisjuhendis on toetatud Sertifitseerimiskeskuse „EE Certification Centre Root CA“ ahelast pärinevad sertifikaadid.

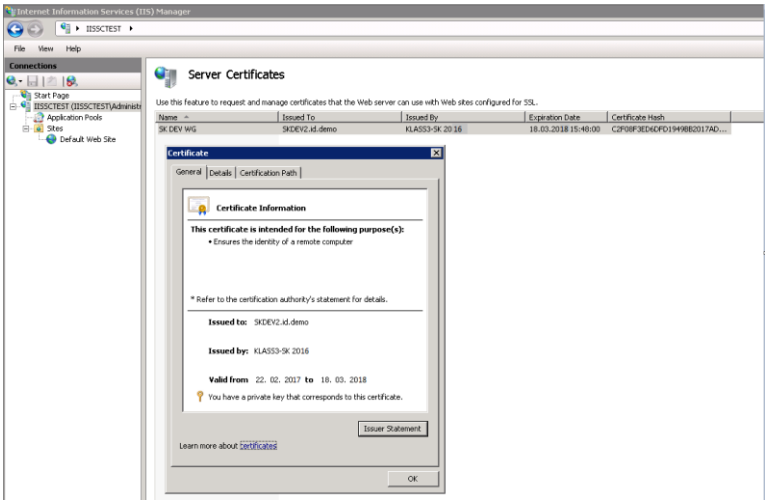
IIS kasutamisel on võimalik rakendada erinevaid autentimismeetodeid. Käesolev dokument vaatleb sertifikaadi nõude kehtestamist IIS anonüümse autentimise jaoks – st. et peale sertifikaadi kehtivuse kontrolli lastakse kasutaja eelnevalt määratud kasutaja (IUSR) õigustes veebisaidile ligi.

IIS SERVERI ÜLDINE NÕUTAV KONFIGURATSIOON

IIS server peab olema häälestatud nõudmaks kasutajalt sertifikaati. IIS server lubab enda poole pöördumisel kasutada kõiki sertifikaate, mis on välja antud samadest juursertifikaatide ahelatest, mida ta ise usaldab. Samas peab IIS server suutma luua kogu sertifikaadiahela alates kasutajasertifikaadist kuni juursertifikaadini – see tähendab, et IIS lisaks juurtaseme sertifikaatide olemasolule IIS serveris on vajalik ka kesktaseme (*intermediate*) sertifikaatide olemasolu. Sertifikaadinõude kehtestamiseks ja SK ahelatest väljastatud sertifikaatide kasutuse lubamiseks:

1) Peavad vajalikud sertifikaadid olema korralikult imporditud/publitseeritud:
    a. Usaldusväärsete sertifikaatide konteinerisse:
        i. „EE Certification Centre Root CA“ (https://www.sk.ee/upload/files/EE_Certification_Centre_Root_CA.der.crt)
    b. Kesktaseme sertifikaatide konteinerisse[1]:
        i. ESTEID-SK 2011 (https://www.sk.ee/upload/files/ESTEID-SK_2011.der.crt)
        ii. ESTEID-SK 2015 (https://www.sk.ee/upload/files/ESTEID-SK_2015.der.crt)
        iii. juhul, kui IIS serveri SSL sertifikaadiks on SK veebiserveri sertifikaat mis välja antud tasemest „KLASS3-SK 2016“[2], siis ka sertifikaat „KLASS3-SK 2016“ (https://www.sk.ee/upload/files/KLASS3-SK_2016_EECCRCA_SHA384.der.crt).

2) Peab IIS serveril olema määratud SSL sertifikaat - meie näites on kasutatud SK poolt väljastatud sertifikaati, mis on välja antud „KLASS-SK 2016“ tasemelt[3], ent see võib vabalt olla ka mõnest teisest ahelast väljastatud veebiserveri sertifikaat:



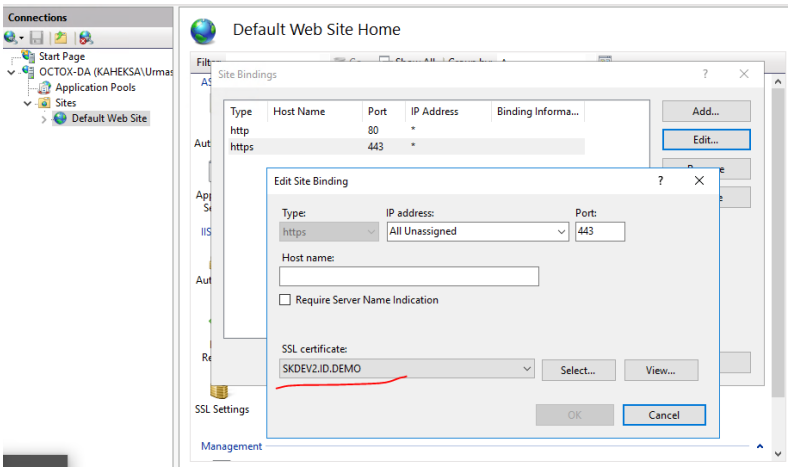
Joonis 1 - IIS serveri sertifikaadi näidis

[1] SK poolt väljastatud organisatsioonide kaartide kasutuse puhul peavad kesktaseme sertifikaatide hulka olema häälestatud ka EID-SK 2011 (https://sk.ee/upload/files/EID-SK_2011.der.crt) EID-SK 2016 (https://www.sk.ee/upload/files/EID-SK_2016.der.crt) sertifikaadid!

2 „Klass3-SK 2016“ sertifikaat kehtib alates 01.06.2017. Selle ajani väljastatakse veebiserverite sertifikaate „Klass3-SK 2010“ tasemelt https://www.sk.ee/upload/files/KLASS3-SK_2010_EECCRCA_SHA384.der.crt).

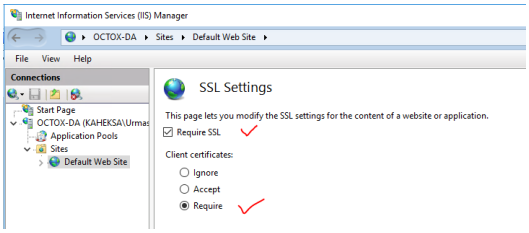
[3] Mis omakorda on välja antud „EE Certification Centre ROOT CA“ poolt.

3) Soovitud veebisaidil peab olema lubatud SSL port (vaikimisi 443) ja see peab olema seotud soovitava sertifikaadiga:



Joonis 2 - veebisaidil on lubatud 443 port ja kasutatavaks sertifikaadiks on SKDEV2.id.demo

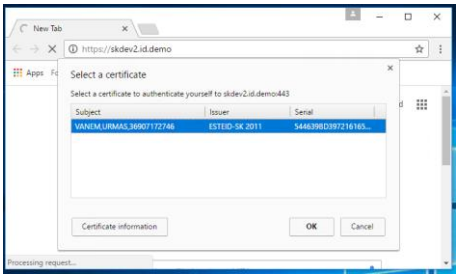
4) Veebisaidi SSL omaduste alt tuleb nõuda SSL protokolli ja kliendi sertifikaatide kasutamist:



Joonis 3 - SSL ja sertifikaadi nõue

Märkus: Veebisertifikaate puudutav lisainfo asub aadressil http://www.sk.ee/teenused/veebiserveri-sertifikaadid.

Loodud konfiguratsioon nõuab veebisaidile ligipääsu 443 pordi kaudu ja kasutaja sertifikaati. Pöördudes veebisaidi poole lubatakse valida soovitav serveri poolt aktsepteeritav sertifikaat:



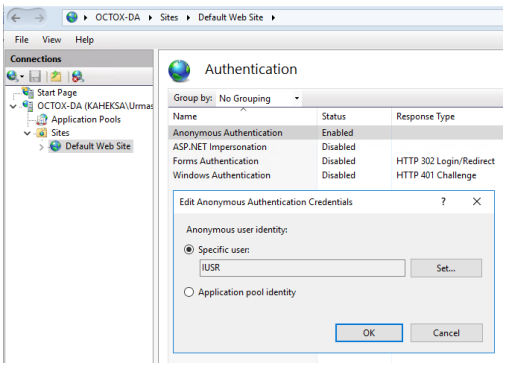
Joonis 4 - sertifikaadi küsimine veebisaidile pöördudes, Google Chrome

Peale PIN-i sisestamist kontrollitakse sertifikaadi kehtivust veebiserveri poolt ja kui kõik on korras, lastakse kasutaja veebisaidile ligi.

Alternatiivina võib IIS-i poolse sertifikaadinõude (*Require*) asemel kasutada ka lihtsat sertifikaadi aktsepteerimist (*Accept*) IIS serveri poolt – see võimaldab lisaks sertifikaadile saada serverile ligi ka kasutajanime ja parooliga.

AUTENTIMINE

Meie näites on lubatud ainult anonüümne autentimine:



Joonis 5 - anonüümne autentimine, kasutaja saab saidile ligi kasutaja IUSR õigustes

KASUTAJA SERTIFIKAADI KEHTIVUSE KONTROLL

Veebirakenduse külastaja autentimissertifikaadi kehtivust tuleb kontrollida vastu OCSP teenust (kehtivuskinnitusteenus) veendumaks, et veebisaiti üritab siseneda ikka kehtivate (OCSP staatus GOOD) sertifikaatidega kasutaja.

Näiteks varastatud ID-kaardi ja PIN-ide puhul peaks ID-kaardi omaniku initsiatiivil olema sertifikaadid peatatud ning üldisemalt mis tahes põhjusel mittekehtivate (OCSP staatus REVOKED või UNKNOWN) sertifikaatidega ID-kaardi puhul ei peaks kasutajat veebisaiti autentima.

OCSP võib teha veebirakenduse tasemel. PHP rakendustest OCSP päringu tegemise jaoks on näidisrakendus saadaval http://www.id.ee/index.php?id=30368, .Net rakenduses tuleks kliendisertifikaat välja lugeda muutujast Request.ClientCertificate ning seejärel OCSP päringu tegemiseks võib kasutada mõnda netist kättesaadavat teeki, näiteks http://www.bouncycastle.org/csharp/

Rakenduse testimise ajal soovitame kasutada SK Test-OCSP teenust aadressil http://demo.sk.ee/ocsp , eelnevalt tuleb registreerida autentimissertifikaat testkeskkonnas, et Test-OCSP oskaks sertifikaadi kehtivuse kohta midagi öelda: https://demo.sk.ee/upload_cert/

Live-OCSP teenus, mis annab SK poolt väljastatud sertifikaatide kohta reaalajas kehtivusinfot, asub aadressil http://ocsp.sk.ee, aga selle kasutamiseks tuleb SK'ga sõlmida leping, lisainfo teenuse kirjelduse ja tellimise kohta on lehel http://www.sk.ee/teenused/kehtivuskinnituse-teenus

Kasutaja sertifikaadi kehtivust saab kontrollida ka CRL-ide abil või vastu vabalt kasutatavat OCSP-d, ent soovitus on teha seda vastu tasulist OCSP teenust, mis tagab pakutava teenuse kõrgkäideldavuse.