

IIS VEEBISERVERILE ID-KAARDI TOE SEADISTAMINE

VERIOONIINFO	
Kuupäev	Muudatused
01.2012	Eemaldatud juhiseid alamsertifitseerija ESTEID-SK konfigureerimise õpetus, kuna ESTEID-SK CA aegus 13.01.2012
06.2011	Esimene avalikustatud versioon

SISSEJUHATUS

Käesolev juhend kirjeldab, kuidas kasutada ID-kaardi sertifikaate kasutaja autentimiseks Microsoft IIS veebiteenustel. Juhendi loomisel on kasutatud Windows Server 2008 R2 platvormi. Näidisjuhendis on toetatud nii Sertifitseerimiskeskuse „Juur-SK“ (ESTEID-SK 2007 alamsertifitseerija¹) kui „EE Certification Centre Root CA“ (ESTEID-SK 2011 alamsertifitseerija) ahelast väljaantud sertifikaadid.

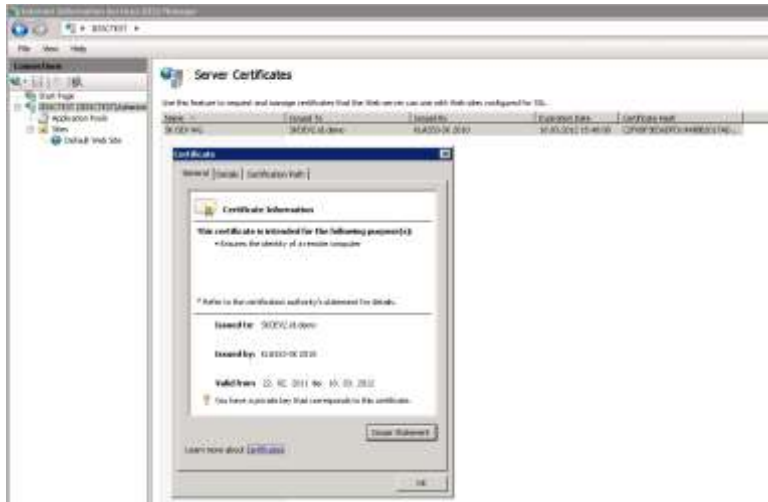
IIS kasutamisel on võimalik rakendada erinevaid autentimismeetodeid. Käesolev dokument vaatleb sertifikaadi nõude kehtestamist IIS anonüümse autentimise jaoks – st. et peale sertifikaadi kehtivuse kontrolli lastakse kasutaja eelnevalt määratud kasutaja (IUSR) õigustes veebisaidile ligi.

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. Sertifikaadinõude kehtestamiseks ja SK juurahelatest väljastatud sertifikaatide kasutuse lubamiseks:

¹ ESTEID-SK oli esimene alamsertifitseerija, mille alt hakati väljastama ID-kaardi sertifikaate. Kuna ESTEID-SK aegus 13.01.2012 siis vajadus selle toe konfigureerimiseks serverile puudub. Kui teil on ESTEID-SK tugi konfigureeritud, siis palun eemaldage see. Teenusepakujatel, kes kasutavad SK poolt väljastatud tühistusnimekirju (CRL-e), ei ole vajalik pärast 13.01.2012 ESTEID-SK tühistusnimekirja SK kodulehelt alla laadida. Palume teil oma teenustes üle kontrollida tühistusnimekirjade (CRL-ide) küsimise reeglid ning veenduda, et pärast 13.01.2012 ESTEID-SK tühistusnimekirja päringuid ei tehtaks.

- 1) Peavad vajalikud sertifikaadid olema korralikult imporditud/publitseeritud - SK sertifikaatide puhul Juur-SK ja „EE Certification Centre Root CA“ usaldusväärsete sertifikaatide konteinerisse ja „KLASS-SK 2010“ kesktaseme sertifikaatide konteinerisse².
- 2) IIS serveril olema määratud sertifikaat -meie näites on kasutatud SK poolt väljastatud sertifikaati, mis on välja antud „KLASS-SK 2010“ tasemelt³:



Joonis 1 - IIS serveri sertifikaat

- 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 protokoll ja kliendi sertifikaatide kasutamist:



Joonis 3 - SSL ja sertifikaadi nõue

Märkus: IIS serveri üldiseks häälestuseks mõeldud info asub aadressil <http://www.sk.ee/teenused/veebiserveri-sertifikaadid>.

² Muidugi sõltub juur- ja kesktaseme sertifikaatide versioon olemasolevast konkreetsest lahendusest.

³ Mis omakorda on välja antud Juur-SK poolt.

Loodud konfiguratsioon nõuab saidile ligipääsu 443 pordi kaudu ja kasutaja sertifikaati. Pöördudes saidi poole lubatakse meil valida soovitat serveri poolt aktsepteeritav sertifikaat:



Joonis 4 - sertifikaadi küsimine veebisaidile pöördudes

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.

Klient peab igal juhul kasutatavat sertifikaati lõpuni usaldama ja kõik ahela sertifikaadid peavad olema publitseeritud⁴.

AUTENTIMINE

Meie näites on lubatud ainult anonüümne autentimine:



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

ID-KAARDI CERTIFIKAADI KEHTIVUSE KONTROLL

Veebirakenduse külastaja ID-kaardi autentimissertifikaadi kehtivust tuleb kontrollida vastu kehtivuskinnitusteenust (SK OCSP teenus) veendumaks, et rakendust kasutab ikka kehtivate (OCSP staatus GOOD) sertifikaatidega ID-kaardi omanik. 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 rakendusse autentima.

⁴ Vaikimisi ID-kaardi tarkvara installatsiooni puhul on need tingimused täidetud.

Kehtivuskinnituspäringut võib teha veebirakenduse tasemel. PHP rakendustest OSCP päringu tegemise jaoks on näidisrakendus saadaval <http://www.id.ee>, .Net rakenduses tuleks kliendisertifikaat välja lugeda muutujast Request.ClientCertificate ning seejärel OSCP 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://www.openxades.org/cgi-bin/ocsp.cgi>, eelnevalt registreerida ID-kaardi autentimissertifikaat testkeskkonnas, et Test-OCSP oskaks sertifikaadi kehtivuse kohta midagi öelda: http://www.openxades.org/upload_cert.php

LIVE-OCSP teenus, mis annab ID-kaardi 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>