Uus Eesti ID kaart ja Chrome-IIS probleem

Dokumendi info	
Loomise aeg	21.08.2019
Tellija	RIA
Autor	Urmas Vanem, OctoX
Versioon	19.11/2

Versiooni info		
Kuupäev	**Versioon**	**Muutused/märkused**
21.08.2019	19.08/1	Avalik versioon
01.10.2019	19.10/1	Lisatud info paranduste staatuse osas serverite versioonide lõikes, vt. sissejuhatus, lõik 3. Muutja: Urmas Vanem
18.10.2019	19.10/2	Kirjeldatud Windows Server 2016 parandus KB4516061, mis lahendab Chrome-IIS probleemi. Muutja: Urmas Vanem
08.11.2019	19.11/1	Kirjeldatud Windows Server 2019 parandus KB4520062, mis lahendab Chrome-IIS probleemi. Lisatud Windows Server (SAC) info. Muutja: Urmas Vanem
14.11.2019	19.11/2	Kirjeldatud Windows Server (1903, SAC) parandus KB4524570, mis lahendab Chrome-IIS probleemi. Muutja: Urmas Vanem

Sissejuhatavalt

2018 aasta lõpus selgus üllatav tõsiasi, et kasutades Google Chrome veebibrauseri viimaseid versioone, ei olnud kasutajal võimalik end autentida Microsoft/IIS platvormil töötavate teenuste vastu uue ID kaardiga. Probleemi selgitamine oli küllaltki keeruline, kuna IIS teiste brauseritega toimis ja samuti toimis Chrome vastu teisi veebiservereid. Ja siis oli meil veel kolmas uus komponent – uus ID kaart.

Kuna iseseisvad tegevused ja erinevate konfiguratsioonide testimised tulemust ei andnud, võtsime ühendust nii Microsoft'i kui Google tugiteenustega. Loomulikult väitsid mõlemad pooled, et viga on teises poole teenustes :) Pika väitluse tulemusena jõudsime märtsi lõpuks niikaugele, et Microsoft lõpuks tunnistas endapoolset RFC 5246 mitte päris korrektset implementatsiooni.

Täna (14.11.2019) oleme jõudnud tulemusteni, kus kõik Windows Server versioonid on toimivad peale järgmiste uuenduste installatsiooni!:

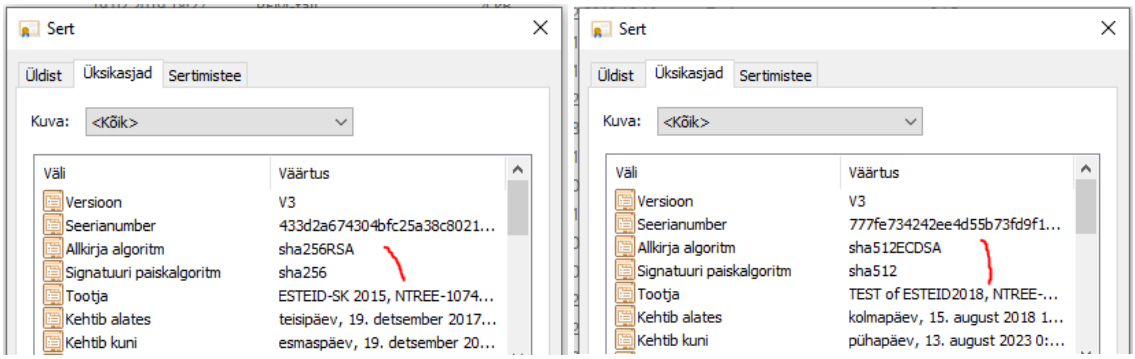
1) **Windows Server 2016 (LTSC) osas lahendab probleemi uuendus KB4516061!**
2) **Windows Server 2019 (LTSC) osas lahendab probleemi uuendus KB4520062!**
3) **Windows Server 1903 (SAC) osas lahendab probleemi uuendus KB4524570!**[1]

Teame, et serveri Windows serveri versioonidele 2012 ja 2012R2 parandusi ei tehta, kuna need versioonid ei kuulu peavoolu tugitoodete hulka[2].

Viga klassifitseeriti Microsofti poolt kui *issue as „by design"*.

Probleemi kirjeldus

Analüüsisime esmalt vana ja uue kaardi erinevusi ja mis meile esmalt silma hakkas, oli allkirja algoritm. Vanal kaardil on selleks sha256/RSA ja uuel sha512/ECDSA.



Pilt 1 - uus ja vana kaart

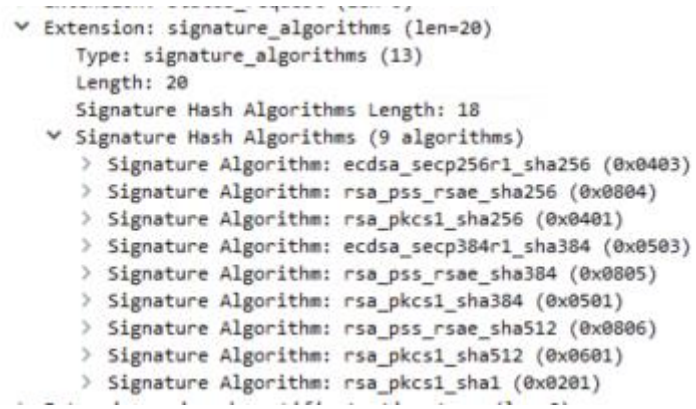
Probleemi mõistmiseks on oluline aru saada, kuidas TLS 1.2 töötab – selle kohta saavad kõik lugeda aadressilt https://tools.ietf.org/html/rfc5246.

[1] Serveri 1909 (SAC) versioonile on kättesaadav sama uuendus juhuks, kui meie probleem seal vaikimisi pole parandatud!

[2] Vt. https://support.microsoft.com/en-us/help/14085/fixed-lifecycle-policy

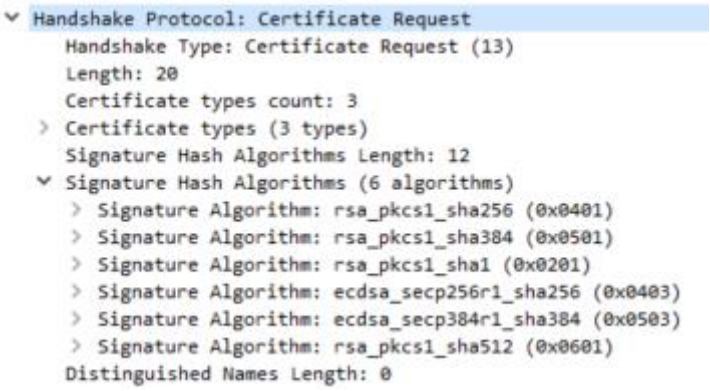
Kirjeldan nüüd järgnevalt lühidalt, kuidas tekib probleem kasutades Chrome-IIS kombinatsiooni uue ID kaardiga TLS kontekstis.

1. Klient saadab serverile *Client Hello*, mis muuhulgas sisaldab toetatud allkirja algoritme:



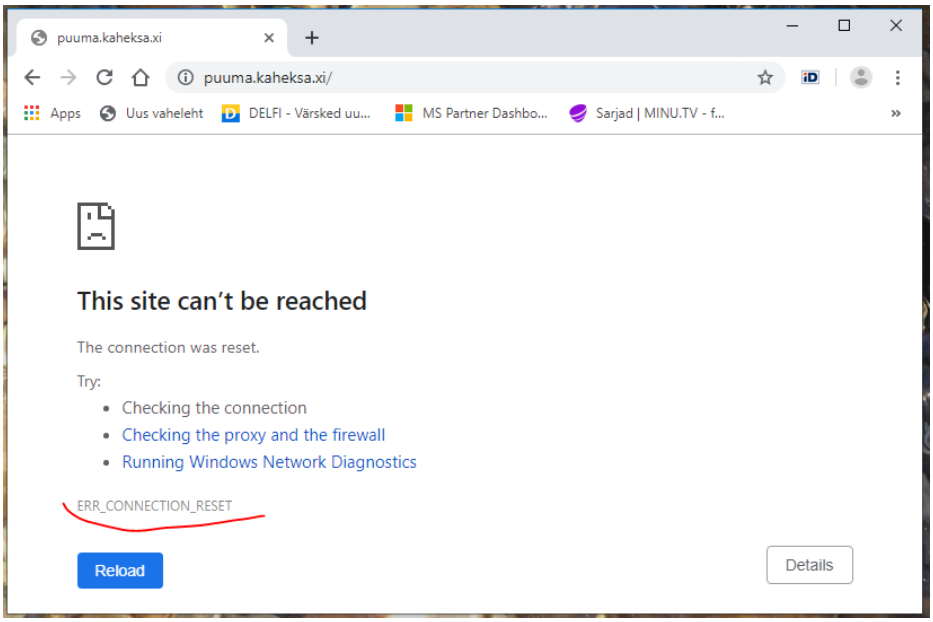
Pilt 2 - Google Chrome viimaste versioonide poolt toetatud allkirja algoritmid

2. Server vastab seepeale oma paketiga, kus *Certificate Request* osas teavitatakse klienti sertifikaadinõudest. Kliendile saadetakse selle päringu osana loend toetatud allkirja algoritmidest:



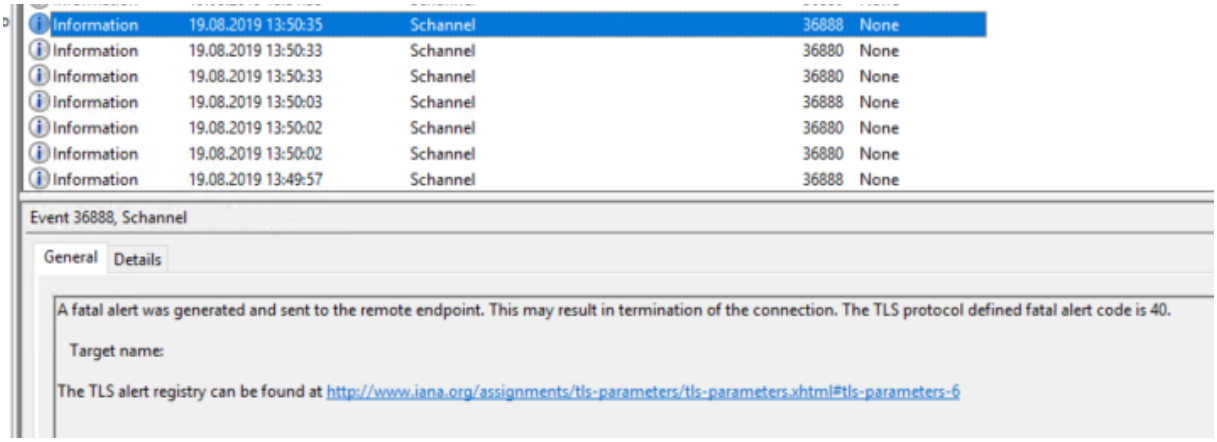
Pilt 3 - IIS serveri *Certificate Request* - puudu on SHA512/ECDSA, mida server tegelikult toetab

Ja nüüd see juhtub - server katkestab ühenduse:



Pilt 4 - Err_Connection_Reset

IIS serveri süsteemilogisse kirjutatakse üsnagi abstraktne veateada:



Pilt 5 - viga süsteemi logis

Põhjus! Alates Google Chrome versioonist 56 (tuli välja 2017.02) ei kuulutata kliendi poolt *Client Hello's* enam tuge signatuuri algoritmile SHA512/ECDSA[3], Google Chrome ei toeta P-521 sertifikaate. Erinevalt teistest veebiserveritest ei saada IIS *Certificate Request* päringus kliendile mitte kõiki serveri poolt toetatud allkirja algoritme, vaid filtreeritakse välja need, mis ei ole loetletud *Client Hello's*. Selline käitumine ei ole RFC vaates õige, tegemist on üle-konfigureerimisega! Igatahes sellise käitumise tulemusena ei toeta IIS server täna SHA512/ECDSA allkirjadega sertifikaate juhul, kui kliendiks on Google Chrome[4].

[3] https://bugs.chromium.org/p/chromium/issues/detail?id=655318

[4] Teised teada brauserid kuulutavad *Client Hello's* SHA512/ECDSA signatuuri algoritmi.

Märkusena mainin siin, et ka Google Chrome ei käitu päris RFC põhiselt, kuna vastavalt RFC-le ei tohiks see saata serverile SHA512/ECDSA signatuuri algoritmiga sertifikaati. Google seisukoht aga on, et kõik kliendisertifikaadid saadetakse serverile edasi ja nende aktsepteerimise otsuse peab tegema server! Mis tundub mõistlik.