

Füüsilisest virtuaalsusse: SIMi ja eSIMi konvergennts

Jürgen Niinre
Arendusjuht
04/11/2016





POSTIMEES ARVAMUS MAJANDUS MAAILM KULTUUR KODU SPORT TERVIS TARBIJA NAINET

TEHNIKA

ILM



TÄNANE LEHT

TEADUS UNIVERSUM INIMENE LOODUS AJALUGU TEADUSELU TEHNOLOOGIA SEADMED TEENUSED IT ÄRI AUTO DIGITARK

TEADUS JA TEHNIKA » DIGITARK

VAATA SAADET!

Veekindel ja roostevaba: müügile jõudnud eSIM-iga Samsungi nutikell vastab ka kõnedele

[SISUTURUNDUS](#)

Raigo Neudorf, Digitarga kaasautor

9. juuni 2016 13:08



Otsi teemat või märksõna...



TELLI POSTIMEHE PAPERLEHT SIIT



KUULUTA POSTIMEHE PAPERLEHES



KALENDER

SUDOKU

RISTSÕNA

VIIMASED UUDISED

14:12 Google'i asutaja on investeerinud lendavate autode arendusse sadu miljoneid dollareid

13:52 Daimleri juht kahtleb Uberi üle 60 miljardi dollari suuruses väärtuses

13:08 Veekindel ja roostevaba: müügile jõudnud eSIM-iga Samsungi nutikell vastab ka kõnedele

11:59 USA liiklusohutusamet: peame inimjuhita autode seadustega kärmemalt tegelema

11:42 Tere tulemast, nihoonium, moskoovium, tennesiin ja oganesson! (2)

15:58 Uuring: kalad suudavad tuvastada inimeste nägusid

15:51 Eesti parim mobiilirakendus 2016 on Pipedrive

15:10 Ministeerium: petutarkvara eemaldamine on eelkõige edasimüüja huvides (1)

14:44 Eesti teadlased püüavad tõhustada vähiravi raku energiatarbimist mõõtes

SIM kaardi ajalugu I

Esimene NMT analoogmobiiltelefonivõrk lansseeriti 1981.a. (Eestis 1991)

SIM kaarti NMT telefonides ei olnud ning telefoninumber programmeeriti otse „kivisse“.

Juhtus see, et „kogemata“ hakkas tekkima telefone milledesse oli programmeeritud sama telefoninumber. Sellistele piraattelefonidele kes teiste arvelt helistasid ei õnnestunudki lõplikult piiri panna. Tekkisid abilahendused (SiS kood) mis ei olnud kasutajasõbralikud ning eriti turvalised.



SIM kaardi ajalugu II

Uue GSM standardi väljatöötamisel arvestati NMT puudujääkidega ning võeti kasutusele täiendav riistvaramoodul (*SIM – Subscriber Identity Module*) mis sisaldas võrku sissepääsemiseks vajalikke krüptovõtmeid ning PIN koodi



SIM kaardi ajalugu III

- Osutus, et SIM kaart oli turvaline lahendus, sest SIM kaarti oli palju raskem kloonida kui NMT mobiiltelefoni telefoninumbrit programmeerida
- SIM kaarte samas ikkagi klooniti, sest osutus, et algselt valitud krüpteerimisalgoritm COMP128-1 ei olnud eriti tugev, ning võimaldas krüpteerimisvõtme leida suhteliselt kiiresti
- Selleks, et ära hoida kloonimist on pidevalt uuendatud SIM krüpteerimisalgoritme ning ka autentimisprotsessi

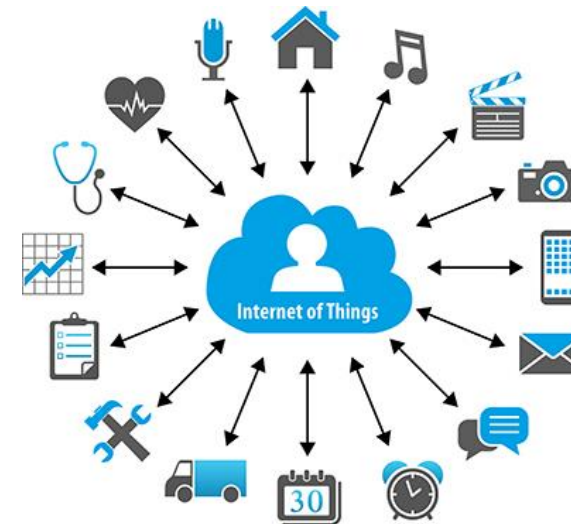
2G COMP128-2 -> 2G COMP128-3 -> 3G MILENAGE (AES) -> LTE TUAK (SHA-3)



Vajadus eSIM-i jaoks

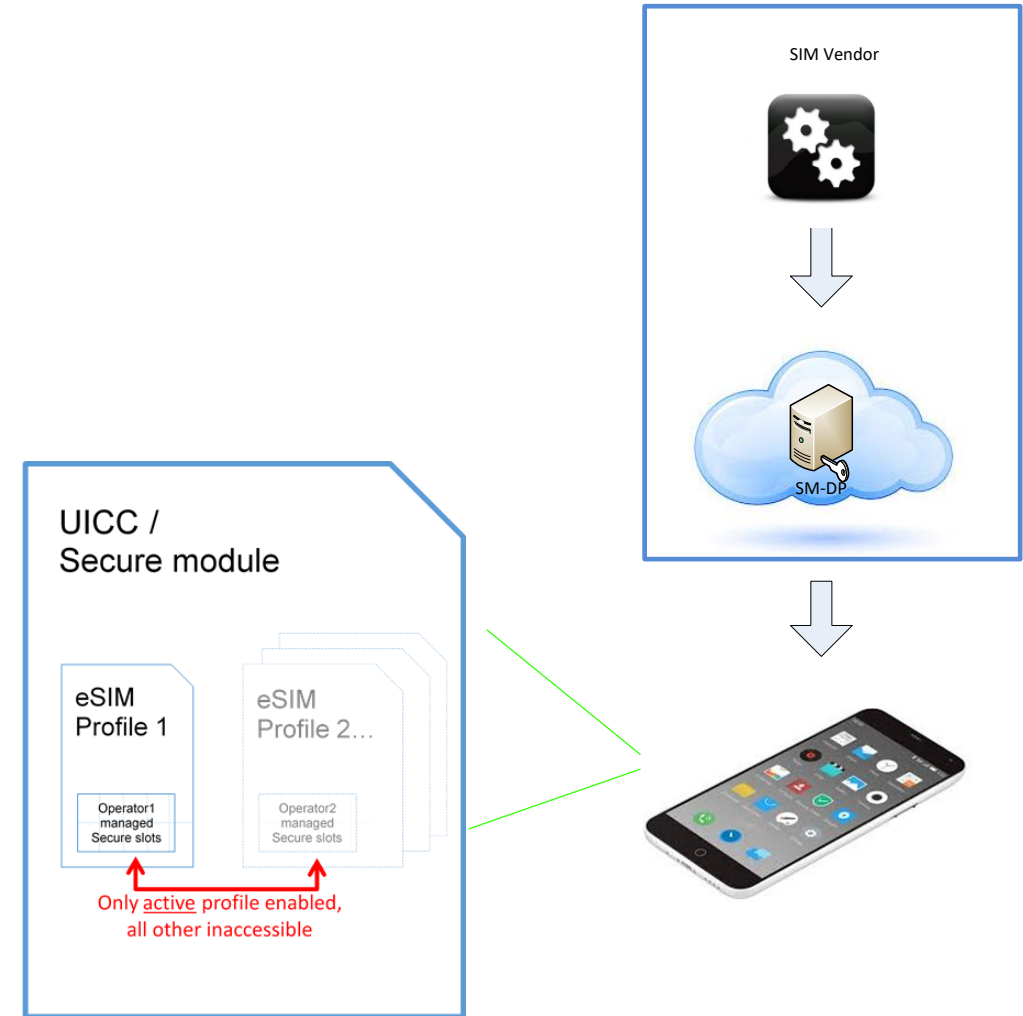
Füüsiliste SIM kaartidega tekkisid probleemid:

- Miniatuursed M2M seadmed, kuhu SIM ei mahu
- Veekindlust vajavad seadmed (nutikellad)
- Vähene kasutatavus erinevates (kodu)elektroonikaseadmetes, tänasel päeval kasutab mobiilset andmesidet vaid 15% võrku ühenduvatest seadmetest, sest seda on raske integreerida
- Keeruline logistika, SIM kaartide transport
- Vähene kasutajamugavus, SIM-de vahetamisel – surve telefonitootjate poolt

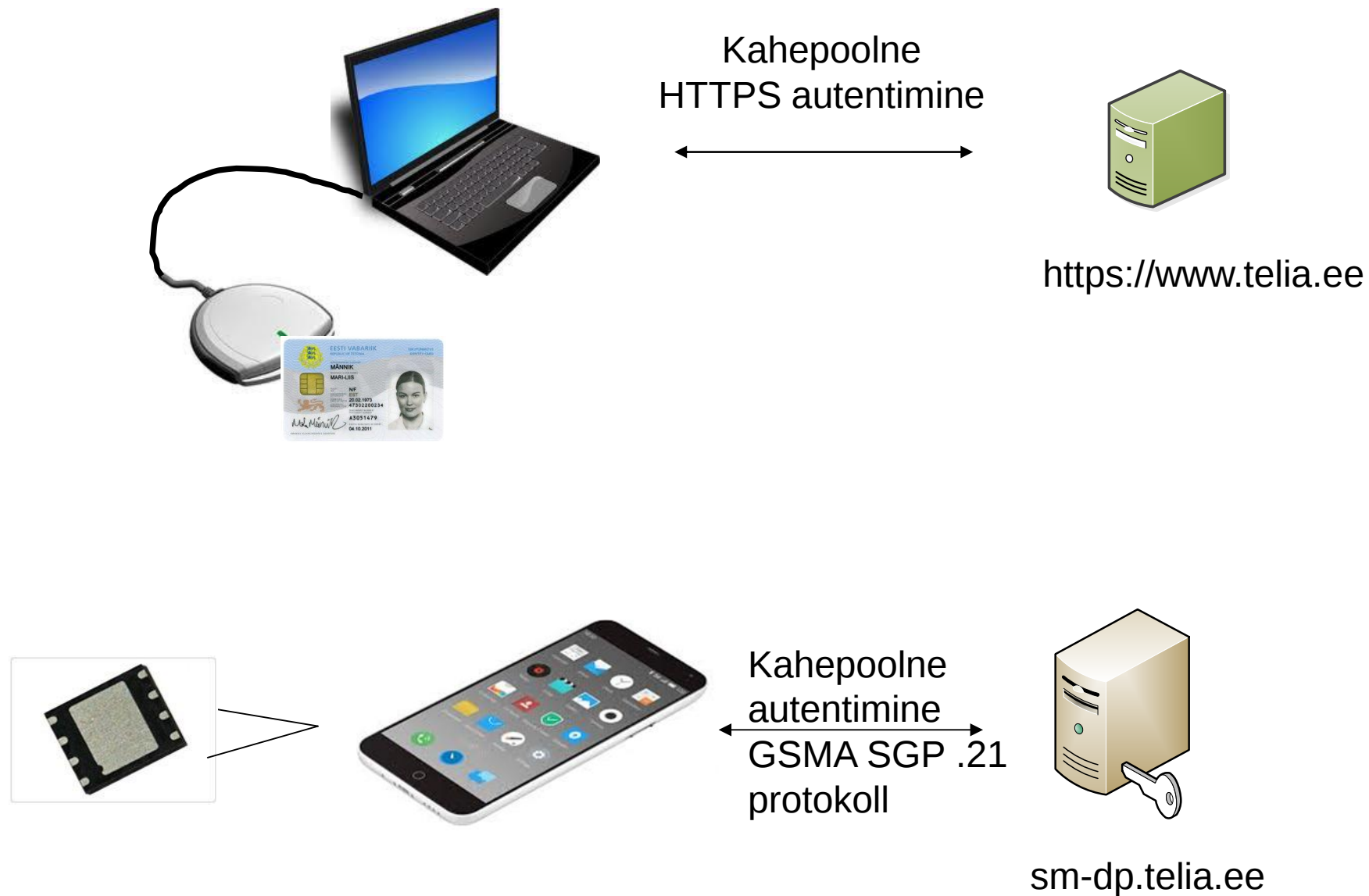


eSIM tuleb pilvest

- eSIM puhul tarnija valmistab ette eSIM profiili ning laeb selle pilvesse.
- Klient laeb pilvest eSIM-i turvaliselt oma seadmesse. Seadmes võib olla korraga mitu eSiM-i
- Kasutaja saab oma eSim-e hallata (lisada, kustutada, aktiveerida jne telefonis oleva haldusrakenduse kaudu)



eSIMi allalaadimise idee



eSIM allalaadimise „token“

- eSIM allalaadimiseks on vaja aktiveerimiskoodi (sisaldab serveri aadressi), ning mida esitatakse QR koodi kujul
- Voucherit saab pakkuda ka online keskkonnas
- eSIM-i alla laadida (s.t. QR koodi kasutada) saab vaid üks kord
- Voucheril esitatakse koos QR koodiga ka PIN koodid (enam ei ole 0000)
- Võimalus ka lisaturvalisuse jaoks (lisa kood mida küsitakse allalaadimisel)



The image shows a Telia eSIM activation card. At the top left is the Telia logo. To its right is a standard 1D barcode with the number 8163363634000500010 below it. Below the Telia logo is the text 'eSIM'. To the right of this text are two stylized, colorful, rounded shapes. Below the 'eSIM' text is a paragraph in Estonian: 'Puhu oma nutiseadmele elu sisse! Selleks vali uus innovatiivne sisse ehitatud SIM-kaart ehk eSIM.' Below this is the instruction 'Aktiveeri eSIM järgnevalt:' followed by a numbered list of five steps in Estonian. To the right of the list is a square QR code. Below the list is the text 'Rohkem infot telia.ee Meeldivat kasutamist!'. At the bottom left, under the heading 'eSIM turvakoodid:', there is a table with two columns: the code type and the code itself. The codes are: PIN 1 (1234), PIN 2 (4321), PUK 1 (12345678), and PUK 2 (87654321). At the bottom left of the card is the website 'telia.ee'.

Telia

8163363634000500010

eSIM

Puhu oma nutiseadmele elu sisse!
Selleks vali uus innovatiivne sisse
ehitatud SIM-kaart ehk eSIM.

Aktiveeri eSIM järgnevalt:

1. Veendu, et Sinu seadmel oleks olemas internetiühendus ning ava seadmes olev QR-koodi lugemise toega eSIM-i haldamise äpp.
2. Lisaseadme puhul (nt nutikell) järgi oma lisaseadmes juhiseid, kuidas seadme haldamise äppi kasutama asuda.
3. Ava oma põhiseadme äpis eSIM-i menüü ja vali sealt eSIM i profiili aktiveerimine.
4. Skaneeri juuresolev QR-kood, kui seade seda teha palub ning järgi nutiseadme äpis kuvatavaid juhiseid.
5. Sinu eSIM-i andmed laetakse hetke pärast seadmesse.

Rohkem infot telia.ee
Meeldivat kasutamist!

eSIM turvakoodid:	PIN 1	1234
	PIN 2	4321
	PUK 1	12345678
	PUK 2	87654321

telia.ee

Embedded SIM, Soft SIM, *****SIM,

Tüüp	Tehniline vaade	Ärivaade	Kasutaja vaade
1 Embedded SIM (eSIM) GSMA	• Turvaline riistvara, mis on joodetud telefoni trükkplaadile • Võimalus operaatoreid lisada/kustutada	• GSMA poolt väljatöötatud standard loob aluspinna rahvusvaheliseks kasutuselevõtuks kõikide mobiiloperaatorite poolt	• Mobiiliteenuste mugav kasutamine ilma SIM kaardita
2 Telefonitootja spetsifiline *****SIM	• Turvaline riistvara mis on joodetud telefoni trükkplaadile või sarnane tänasele füüsilisele SIM-le • Võimalus operaatoreid lisada/kustutada	• Kuvatavat operaatorite nimekirja kontrollib telefonitootja	
3 Soft SIM	• Riistvara võtmete hoidmiseks puudub ning see on asendatud tarkvaraga	• Suurendatud võrguidentiteedi kloonimise oht • „Metsik Lääs“ – kasutus reguleerimatu	



GSMA eSIM-i operaatori valiku teesid

- Klient peab sama valida ise operaatorit, ilma telefoni „abita“
- Telefonitootja poolseid operaatorite eel- või järelvalikuid ei tohi olla
- Kõik operatsioonid eSIM-ga – aktiveerimine, kustutamine, installeerimine peab olema kinnitatud kasutaja poolt (s.t ei saa olla automaatvalikuid)



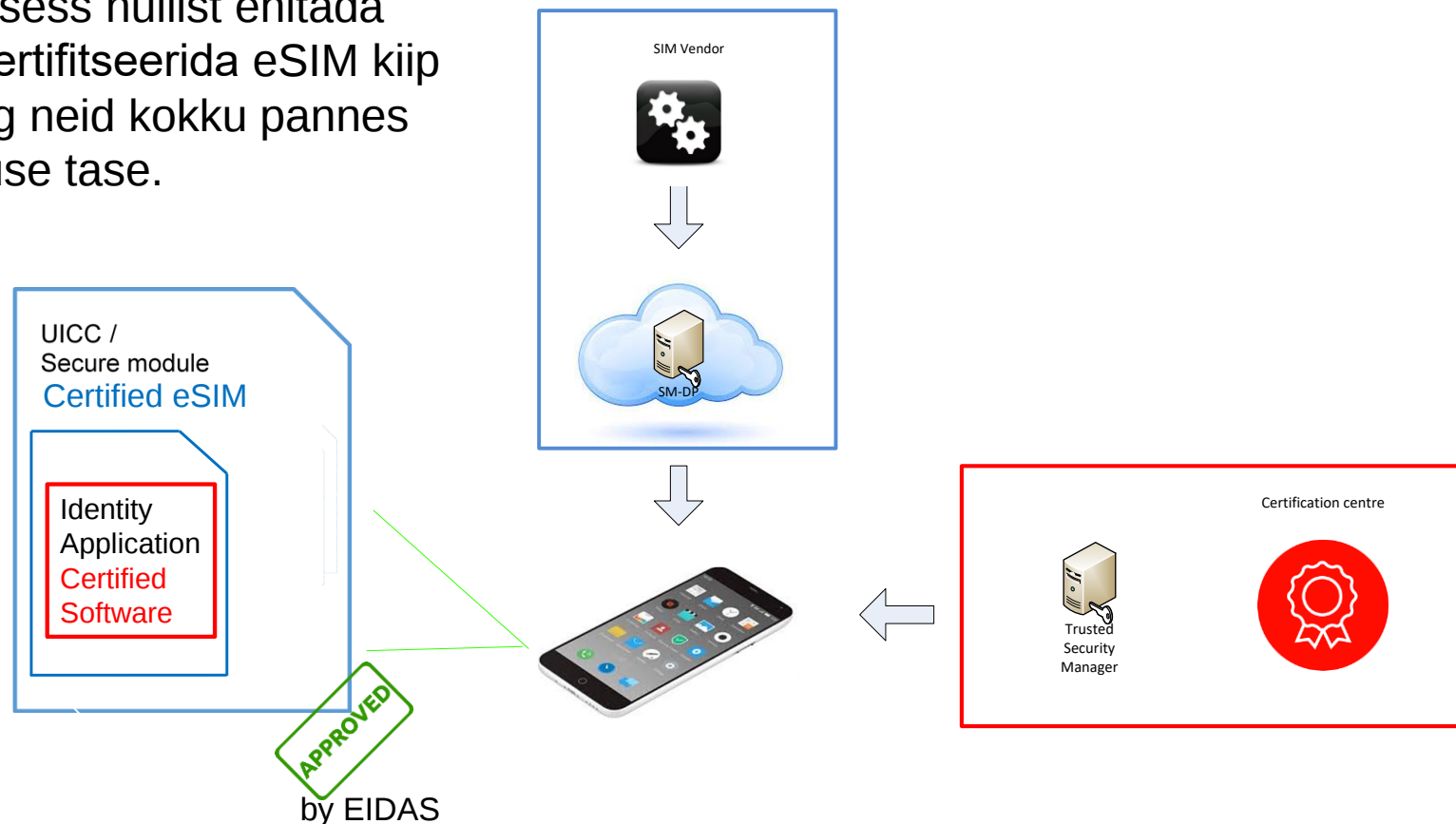
Mida eSIM tähendab kasutaja jaoks?

- eSIM on saadaval interneti kaudu
 - Mugavam eSIM-i laadida, teha liitumisi, ei pea tellima füüsilist SIM-i
 - Turistidel mugav tellida sihtkohamaa eSIM.
 - eSIM bussipeatusest/reklaamiplakatilt
- Mugavam hoida mitut eSIM-i telefonis
 - Laadida saab eSIM-e niipalju kui kiibil ruumi jätkub (tänapäevaste võimaluste juures ~10)
 - Saab hõlpsasti eSIM-e aktiveerida/deaktiveerida/kustutada



Mobiil-ID võimalikkusest eSIM-i

- eSIM-i on võimalik laadida tänane Mobiil-ID rakendus, plaanis on läbi viia Mobiil-ID eSIM tehnilised testid 1 kvartal 2017
- Lahendus on vaja EIDAS-e järgi sertifitseerida, kuna tegemist on väga uue tehnilise lahendusega siis tuleb sertifitseerimisprotsess nullist ehitada
- Üks võimalik lahendus on sertifitseerida eSIM kiip ja eSIM rakendus eraldi ning neid kokku pannes saavutatakse vajalik turvalisuse tase.



Tänu!

Jürgen Niinre
Arendusjuht
jyrgen.niinre@telia.ee

TUAK SHA3

