



Tallinna Linna Laste Tervekeskuse
Ehituse ja Arhitektuuri osakond

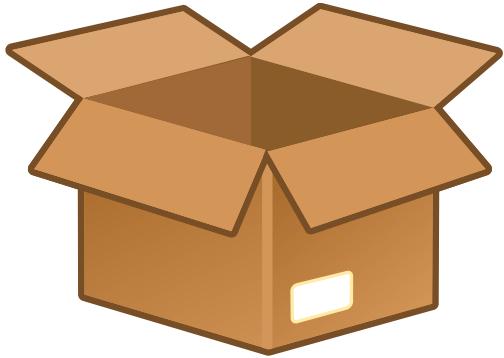
TEHNILINE ARHIIV

ETINE KACCH



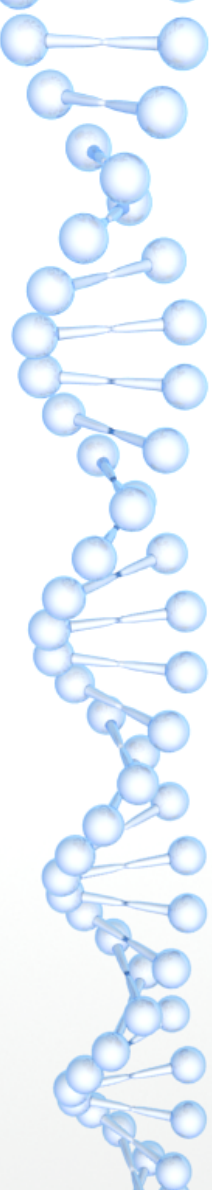
БЛАЕТИВЕ

2017-11-02



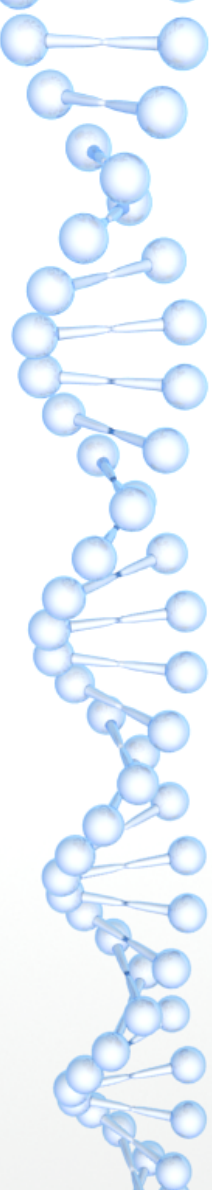
Infoturbe aastakokkuvõte blog.RIA.ee põhjal

Anto Veldre



blog.ria.ee [1]

2016-07-15 - Eurodigiajastu mõisteteselgitusi
2016-06-22 - Kaardiuuenduse teine laine
2016-06-14 - Kiri Aleixolt
2016-03-18 - Uuenda oma ID-kaarti
2016-02-22 - eID kasutusmallid
2016-01-28 - Tõus Vesuuvile
2016-01-12 - Kuningas on surnud, elagu kuningas! *
2016-01-06 - Riigiportaalist ei pea põgenema
2015-11-24 - Kolmas kivi päikesest
2015-10-22 - Räsist ja räsimisest
2015-10-01 - Probleem nr 532048
2015-08-28 - Sissejuhatus X-teele (osa 1)
2015-08-28 - Sissejuhatus X-teele (osa 2)
2015-08-28 - Sissejuhatus X-teele (osa 3)
2015-08-11 - Veel brauseriuudiseid: ka Mozilla Firefox'i turvalisus tõuseb
2015-07-29 - Põhjalikumalt Androidi turvaugust
2015-07-09 - FLASH'i tapmine
2015-07-01 - Suuremad sirviku-uuendused sel suvel
2015-04-09 - Veebilehitsejas Chrome läheb ID-kaardiga allkirjastamine (korra) katki
2014-05-14 - E-valimised on (liiga) turvalised
2014-04-30 - Windows XP on nüüd tööpoolest ja lõplikult surnud

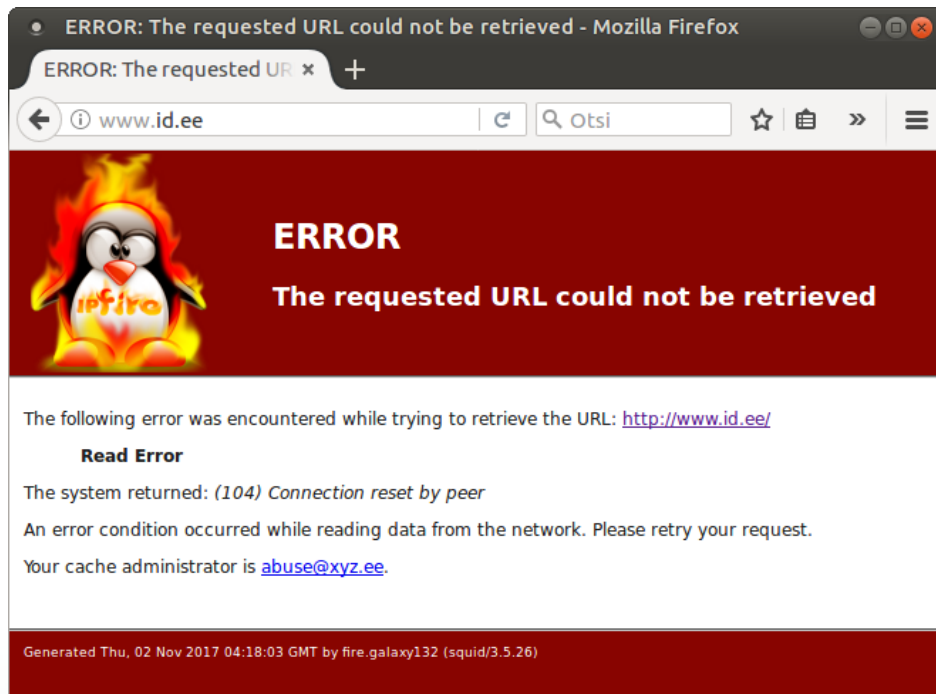


Blog.ria.ee [2]

2017-10-27 - ID-kaardi uuendamisest
2017-09-29 - Turvanõrkus, oht risk
2017-08-31 - Kroomitud teras
2017-06-21 - ID-kaardi tarkvara uueneb
2017-03-13 - Valimiste turvamudelitest
2017-03-06 - Küülikukasvatusest e-riigis
2017-03-02 - Kala jälg vees
2017-01-31 - Nimekirjade nimekiri
2017-01-27 - ID-kaardi tarkvara paigaldamine (eellugu)
2017-01-27 - ID-kaardi tarkvara paigaldamisest
2017-01-27 - ID-kaardi tarkvara paigaldamine Windowsile
2017-01-27 - ID-kaardi tarkvara paigaldamine macOSile
2017-01-27 - ID-kaardi tarkvara paigaldamine Linuxile
2016-12-21 - Kauguuendamise kolmas laine
2016-11-28 - Valimised võitsid robotid
(Elektroonilise demokraatia ragin)
2016-11-21 - Kuhu heidame usaldusankru?
2016-10-20 - sard-SIM tulekul

<https://blog.ria.ee/>

Täna varahommikul



03:50 – 07:50

Riigiametite veebe tabasid häired

Aivar Pau | 2. nov 2017 10:37

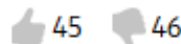


Post-Truth



Kristjan Vörno 3 tundi tagasi

See ei ole loogiline jutt, mida spetsialistid räägivad, sest, et kui inimene hakkab oma ID kaarti kasutama, kasutab ta tegelikult ID tarkvara ning neil on võimalik kohealt piirata selliste kaartide kasutamist, millel puudub sertifikaadi uuendus. Sellest jutust lähtub, et tegelikult püütakse mingit muud viga varjata või siis tekitada kaost meelega. Väidan seda seepärast, et ID kaarti kasutades inimene sisestab ID kaardi lugejasse ning pärast seda võtab ID kaardi tarkvara ühendust keskserveriga, mille kaudu toimub autentimine. Seda keskserverit haldab aga riik ise. Ja kui see moment aset leiab, võib inimese rahulikult suunata sertifikaatide uuendamisesse või siis ID kaardi vahetamisele. Kui häkkerid ID kaardi keskserverisse ei suuda sisse häkkida, siis ei ole võimalik ka kuidagi autentimist rünnata.



Teata sobimatust kommentaarist

Küsimus



Eesti eID ökosüsteem

- Mis on karul kõhus?
 - Arusaamine tehnoloogiast
 - Rahvavalgustus ...

Mälestusi aastast 2012

Postimees.ru

СРЕДА
« 27.06.2012 »

Обратная связь | Реклама | Новости
Калейдоскоп | Сделай стартовую

eesti keeles

Postimees

Эстония

Распечатать



ID-карта и считывающее устройство.
Фото: Elmo Riig / Sakala

Взломать ID-карту можно за 13 минут

26.06.2012 12:51

Комментировать | Распечатать

Ученые нашли способ, как за 13 минут взломать систему RSA SecurID 800. В числе прочих, эта система используется и для эстонских ID-карт.

SecurID 800 предназначена для максимально безопасного хранения данных пользователей; в теории, удалить эти данные из системы нельзя. Ученые же нашли способ, как с помощью слабых сторон шифра заполучить всю необходимую информацию, пишет E24 со ссылкой на Ars Technica.

По информации Ars Technica, RSA отказалась от подробных комментариев и активно приступила к устранению недочетов.

Редактировал Postimees.ru

Отправить в блог:         

Энциклопедия об Эстонии


Подать объявление
недвижимости
автомобили
для дома
электроника

НОВОЕ!

Отдых в Латвии
Limon
Wikileaks
Календарь на июнь
Сделать стартовой
Сudoku
Подать объявление

НОВОСТИ

Эстония
Таллинн
Мнение
Спорт
Криминал
Экономика
За рубежом

VIKING LOTTO
€0000000
теперь также
лотерейный
билет!

prognoz.ee
ТАРТУ
Сегодня 16 °C
Завтра 16 °C
ВВЕДИТЕ НАЗВАНИЕ

ЕВРО-2012

21:55 24.06 Сборная
Италии по пенальти
обыграла англичан и
вышла в полуфинал (23)

TALLINK

Mälestusi aastast 2012

RISK ASSESSMENT / SECURITY & HACKTIVISM

Scientists crack RSA SecurID 800 tokens, steal cryptographic keys

Scientists penetrate hardened security devices in under 15 minutes.

by **Dan Goodin** - June 25 2012, 6:20pm MSK

NATIONAL SECURITY WHITE HAT 61



RSA's SecurID 800 is one of at least five commercially available security devices susceptible to a new attack that extracts cryptographic keys used to log in to sensitive corporate and government networks.

EMC

Vox Populi



A...

November 1, 2017 at 6:59 pm

Tore!

Elliptköver! Miks? Kes otsustas?

Kuidas on võimalik nii keerulist tarkvara põhjalikult turvatestida loetud päevadega? Kas saan selle testiraportiga tutvuda? Testiraport ikka eksisteerib?



A...

November 1, 2017 at 7:08 pm

Kas vana võtmega dokumendid tuleb üle allkirjastada või krüpteerida? Mis on RIA soovitus? Vana võti on ju rünnatav aegade lõpuni.

Teadlikkus ja selle tõstmine [2]



DELFI

WWW

RUS

19.04.2017 19:15

Kui ID kaardi omanik ID kaardi sertifikaati uuendab, siis mis takistab riigil privaatvõtme koopiat endale salvestada. Ja edasi mõelge ise.

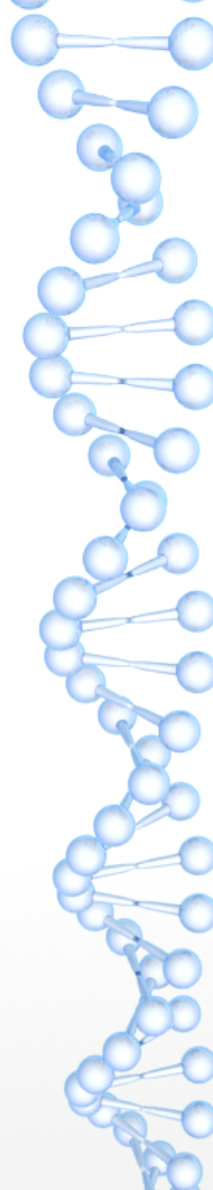


4



1

Sobimatu



Teadlikkus ja selle tõstmine

jamps

19.04.2017 14:06

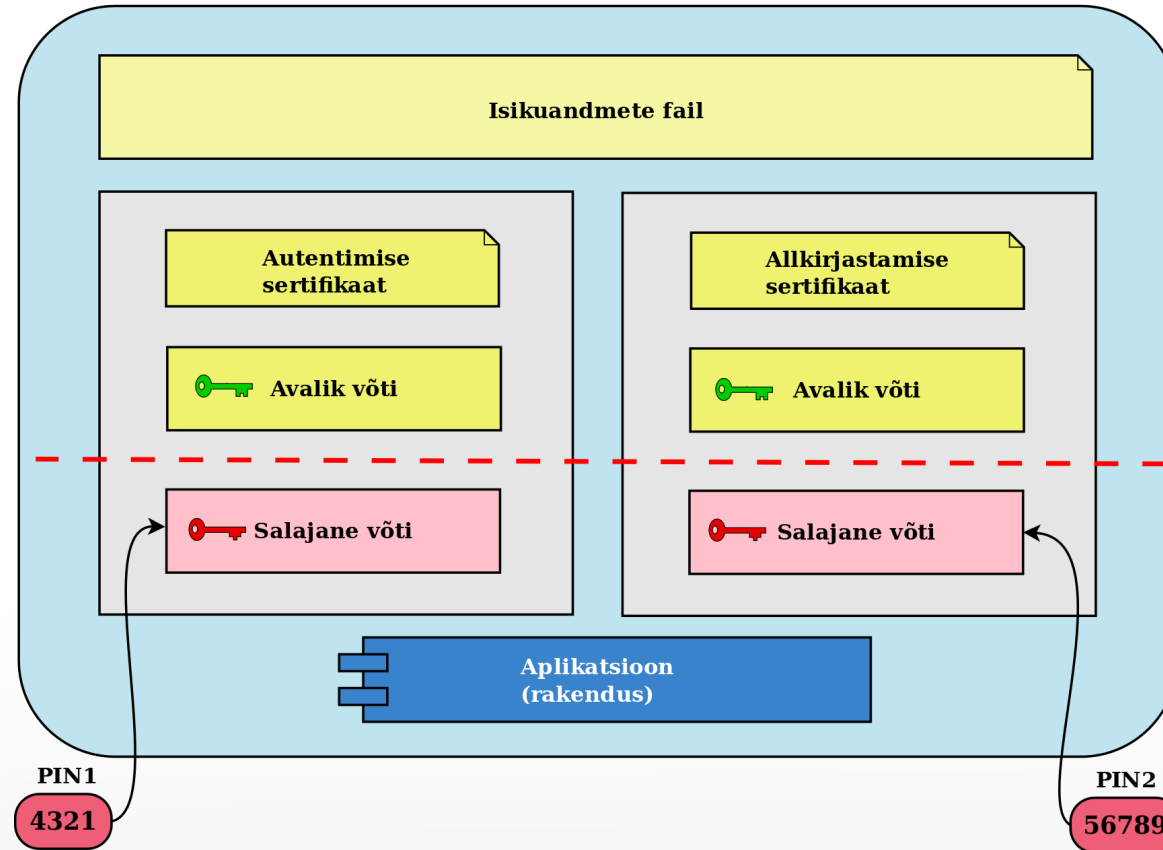
See on suitsukate. Tegelikuses liiguvad kõik need kokkuliidetud valimissedelite andmed enne avaldamist mõne üksiku inimese poolt kontrollitud keskkonnas ilma mingi krüpteeringuta. Lisaks veel võib AS Sertifitseerimiskeskus valimiste ajaks mõninga koguse valimisõiguslikke e-residente genereerida ja pärast valimisi ära kustutada. Keegi hakka mingit krüptot häkkima, kui piisab mõne inimese äraostmisest.

👍 15

👎 6

⚠️ Sobimatu

Igast vanaemast saagu kübermagister?

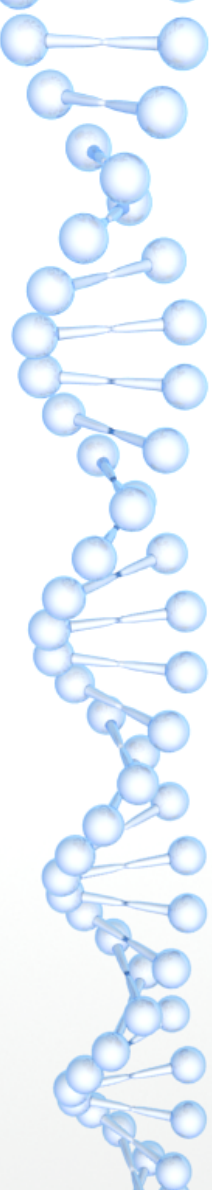


Küsimus



Küsimus PIN koodi kohta

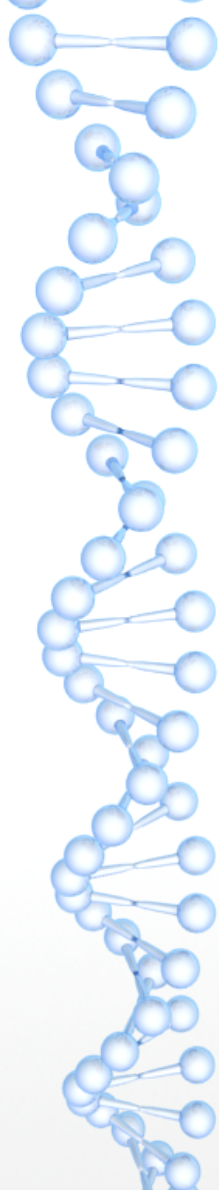
- Kuhu see pärast sisestamist satub?



Olulised küsimused

- Mis on räsi?
- Kuidas digiallkirju võltsida?
- Mis on kaardi sees?
- RSA krüptosüsteem – kuidas see töötab?
- Ei, nüüd jube elliptilised kõverikud ;)
- Kas e-hääletus / internetihääletus on turvaline?
- Mis *#€&%␣\$ jama nende sirvikutega on
- Halloo, tarbijakaitse, kas minu ID-kaart vahetatakse tasuta välja?
- Halloo, võrdse kohtlemise volinik, mul on Mac

Kas see kõik ongi nüüdsest turvalisus?



M

mul tuleb kaks teadet / 19:12, 1. nov 2017

mul tuleb kaks teadet, üks on, et ebaõnnestus, proovi uuest.
teine aga on seal all ja ütleb, et uuendamine käib.
jeerum. kuidas ma tean, mida ta siis teeb? kummat ma uskuma pean?
kas siis pean uuesti proovima või tõesti uuendab?
isegi sellist asja ei suudeta korda teha, et ütleks üheselt, mida ta siis teeb.

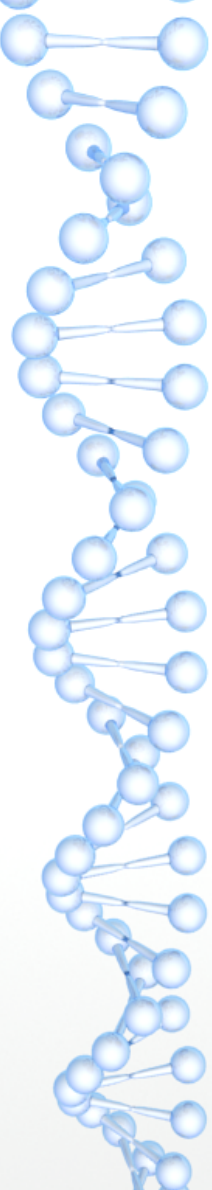
+44 · -1 · Vasta · Teata ebasobivast kommentaarist

M

mari / 19:25, 1. nov 2017

sama siin, ei teagi kumb tekst õige on :D seni pole uuendamine õnnestunud

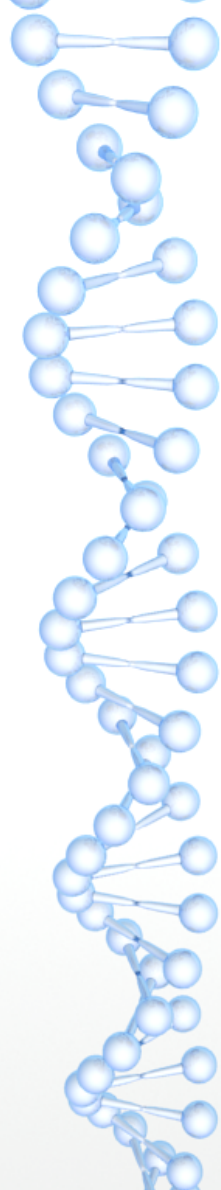
+23 · -1 · Vasta · Teata ebasobivast kommentaarist



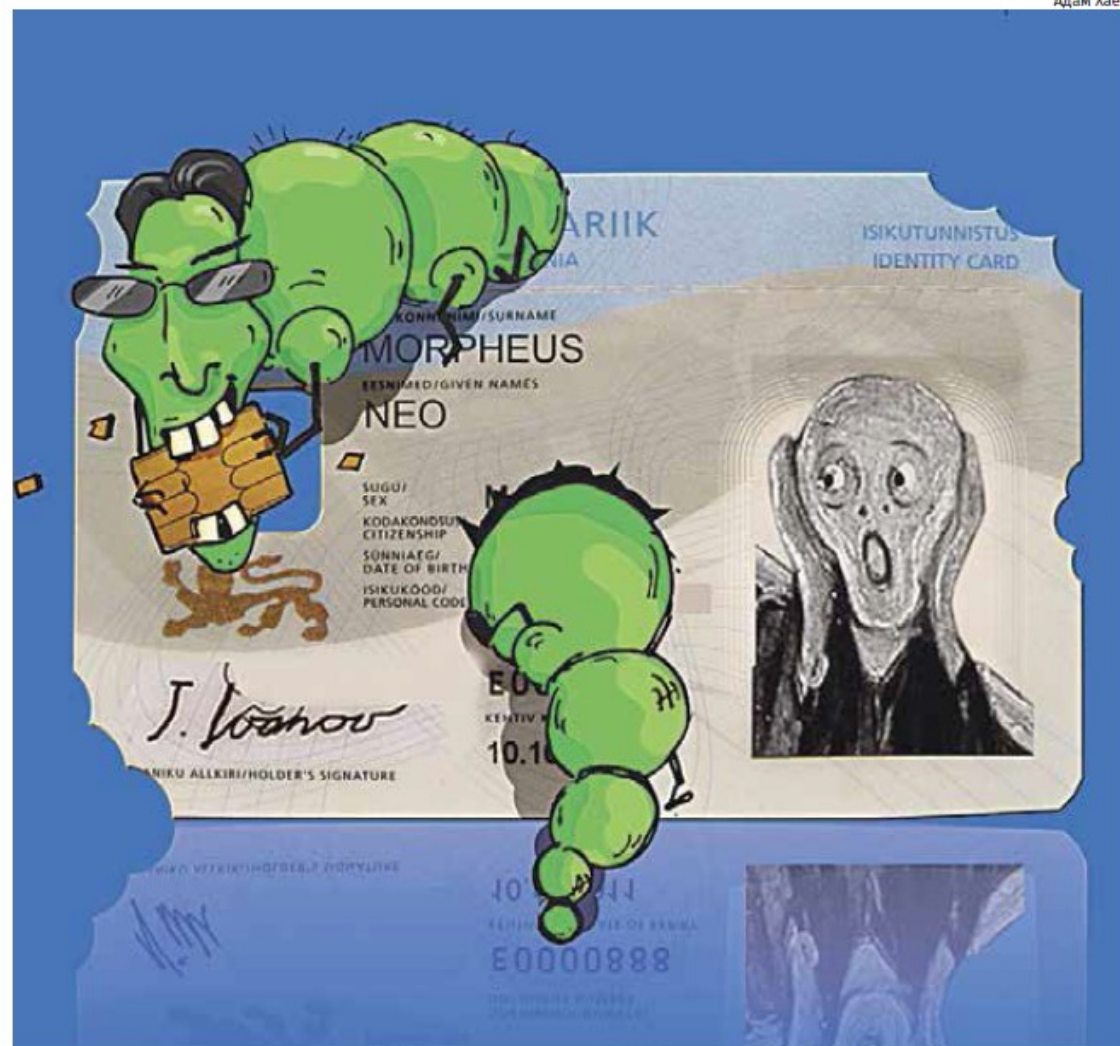
Olulised küsimused [2]

- Mis oli DDOC allkirjal viga, et me ta välja peame viskama?
- Nelja sorti allkirjad???? (eIDAS)
- Miks RIA ei suuda Edge sirvikut korda teha?
- Miks TEHIKusse saab puuhaluga sisse logida?
- Kes meie asutuse eelarvesse raha juurde lisab?

NB! Tehniline turvalisus pole enam probleemiks.



НЕДЕЛЯ В КВАДРАТЕ



MOPP

uudised

EV100

EESTI

ARVAMUS

MAJANDUS

VÄLISMAA

KULTUUR

RIA töötab välja oma alternatiivi mobiil-ID-le

MAJANDUS

Katrin Aarma

04.11.2016 19:00

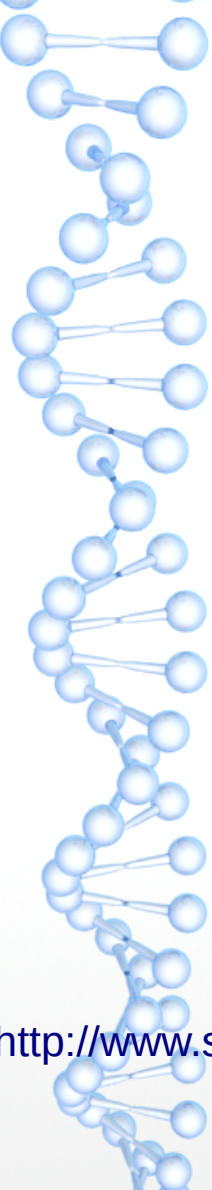


Küsimus



e-hääletamine

- nutiseadmega
 - Mida arvad?
 - (vt valikud)



n-hääletus

„E-valimised on lahutamatu osa Eesti demokraatiast,“ kinnitas SDE esimees Jevgeni Ossinovski. „Nende usaldusväärsus on sotsiaaldemokraatidele väljaspool kahtlust. Küll peame ka siin tehnoloogia arenguga sammu pidama. Nutiseadmete võidukäik tõukab vana hea lauarvuti peagi ajalukku, mistõttu on hädavajalik, et asuksime kohe looma turvalist tehnilist lahendust, mis võimaldab hiljemalt 2021. aastal ka n-hääletuse – hääle andmise nutitelefoni või tahvelarvutiga.”

<http://www.sotsid.ee/sde-juhatuse-e-valimised-ka-valimispaeval-ja-nuti-valimised-hiljemalt-2021-aastal>

Oravast (jm loomadest) patsiga poisi seljataga



Vana mees maalt

15.10.2017 20:19

Kas keegi kahtles E valimiste tulemuses??

Patsiga poiss reformi palgal))

Ei usu mina neid E valimisi, iga it asi häkitav. Ja see, kes selle E valimiste programmi tegi, eks see ka jättis tagaukse, tulemuste muutmiseks...

Kindel 55000 vanurit, kes ka kõndida ei suuda, valisid reformierkaonna...



317



170



Sobimatu



Vasta

Ülemaks kui Riigikogu, tuleb Veldre/Martens tunnistada

Kriitik

27.07.2017 10:53

Ikka need veldred ja martensid hämavad. Kas tõesti ei suuda Riigikogu sätestada kontrolli kriteeriumid ja lõpetada logide hävitamine kahe nädala jooksul. Kui probleemi, kes kontrollib kontrollijat ei lahendata, siis jäävad ka e-valimiste kriitikud.



2



2



Sobimatu



Vasta



Kommenteerimise eest ju ei maksta?

Parimad töopakumised

[Менеджер отдела продаж](#)

[Tootmistööline / pingioperaato...](#)

[Sales representative \(one ethi...](#)

[Katlamajade hooldustehnikut](#)

[Kvaliteedijuht](#)

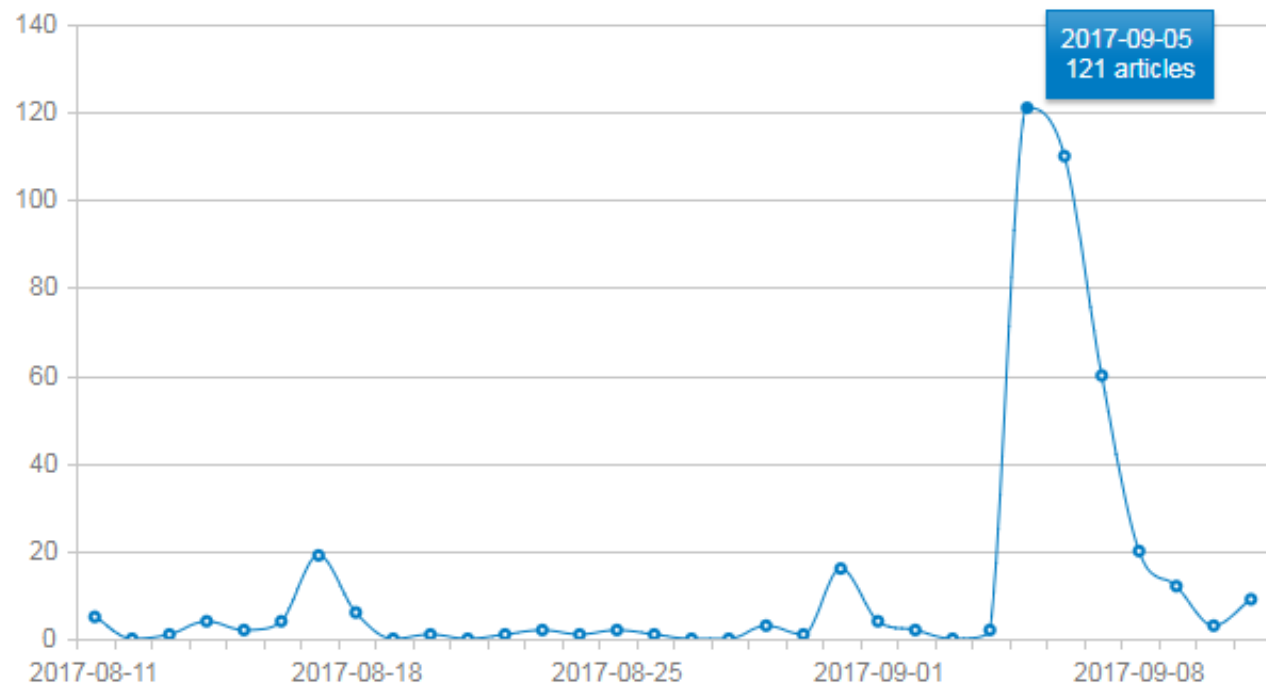
[Ms dynamics ax tarkvara arenda...](#)

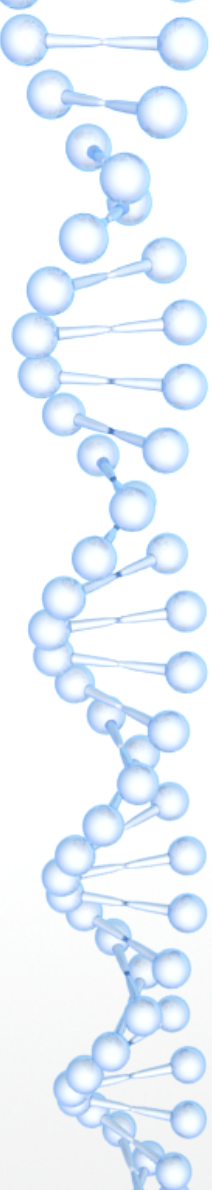
[C-kategooriga autojuhile](#)

[Müügiesindajat](#)

Timeline

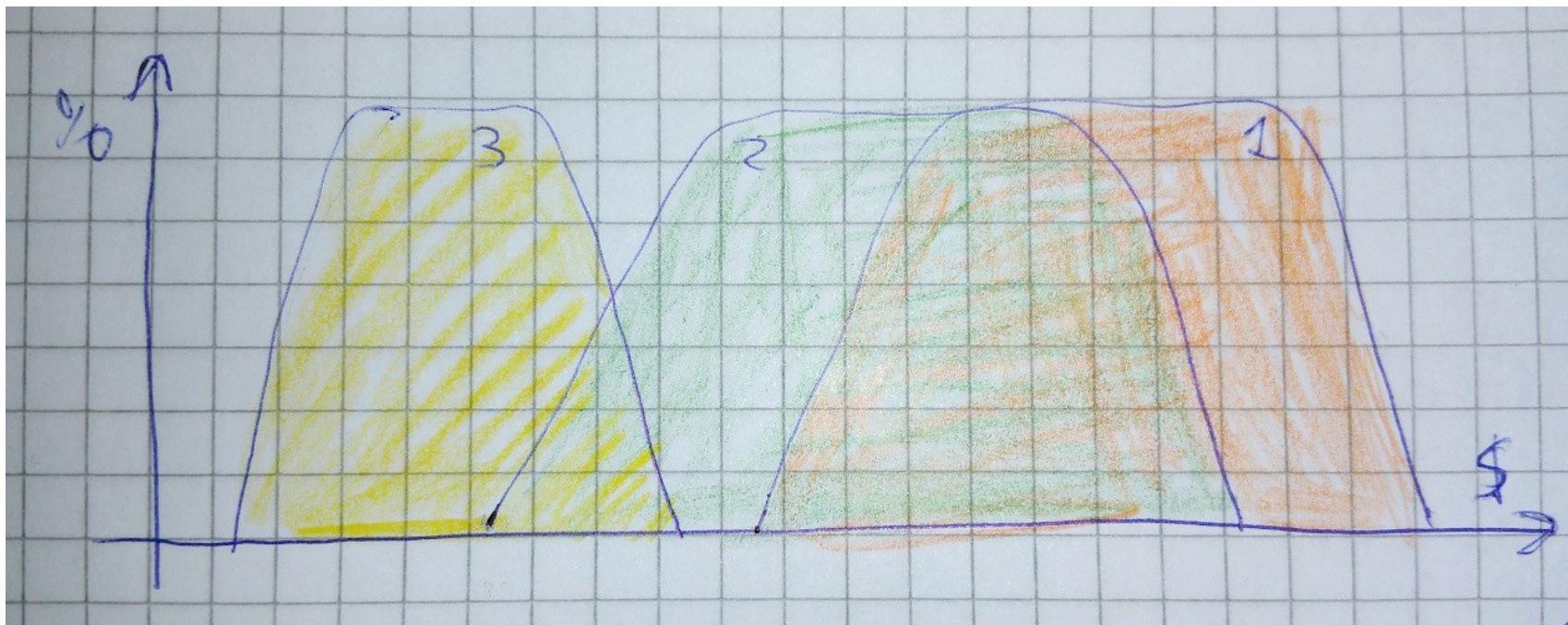
Articles count



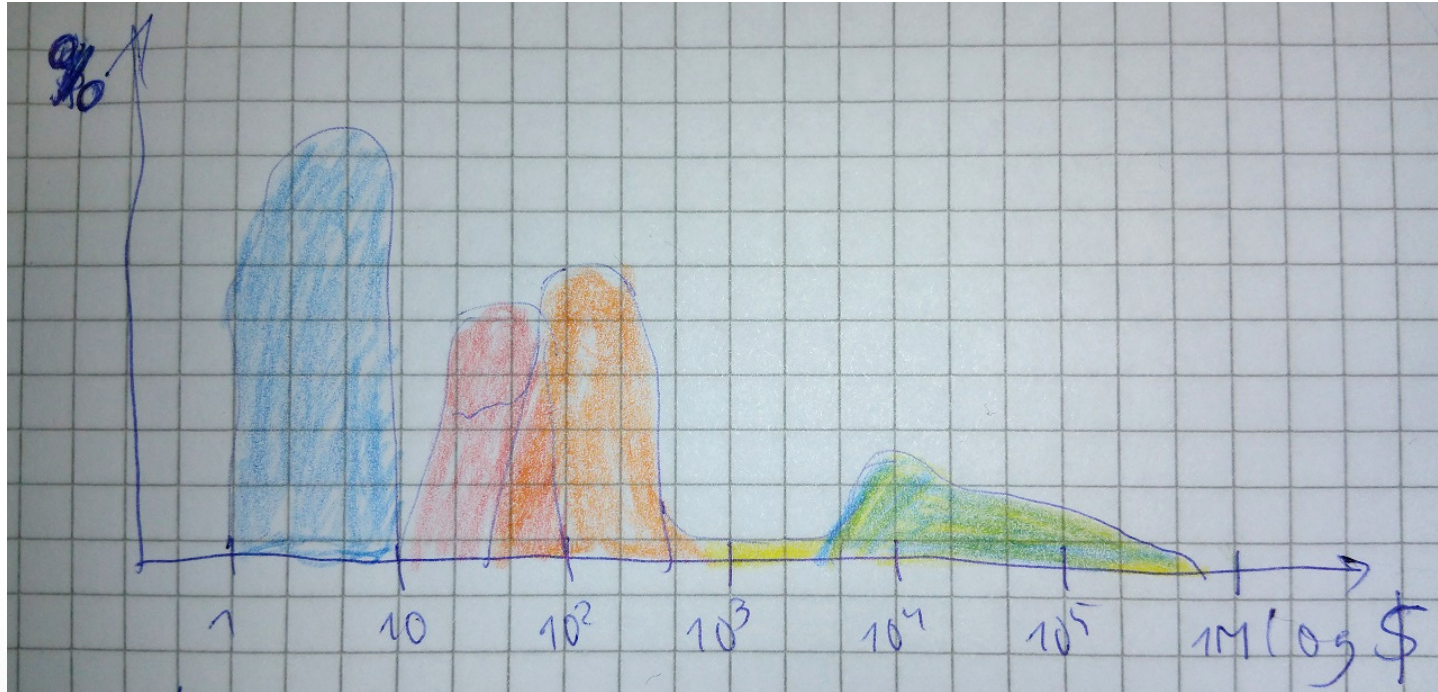


Mustanditest

Autentimis- (jms) vahendid



Eraisiku poolt sooritatavad maksed



Küsimus



Eesti isikukood

- Kas see vajab reformi?
 - Millist täpselt?
 - Vt vastusevalikud!

E-põrgu?

≡ EestiPäevaleht DELFI RUS ÄRILEHT SPORT PUBLIK FORTE NAISTEKAS EPL EKSPRESS MAALEHT

05.04.2017, 00:05

e-põrgu kadalipp: kuidas tõestada, et sa pole skisofreeniahaige (120)



Laura Mallene
laura.mallene@epl.ee

72 f

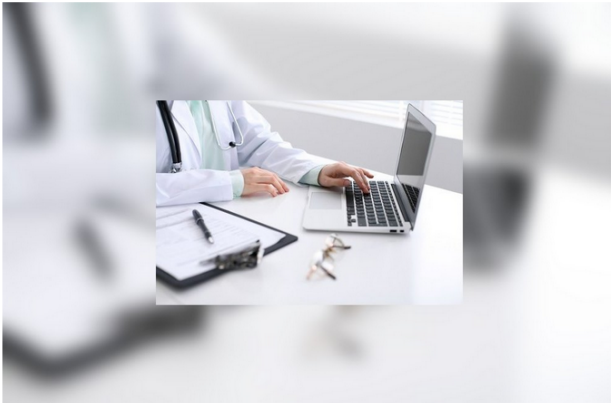
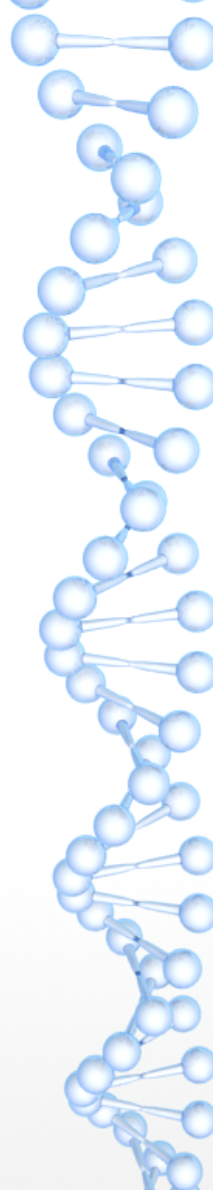


Foto: Shutterstock

Logopeedina töötav naine avastas perearsti juures käies juhuslikult oma haigusloost ehmatava diagnoosi: F20 skisofreenia. Peaaegu poolteist kuud on ta pidanud lakkamatut võitlust, et ekslikult pandud haigumäärangust vabaneda, ja otsinud abi eri ametitest – helistanud, saatnud kirju, käinud kohapeal, kuid haiguse nimi ei taha tema terviseandmetest kaduda.

X XXXXXX XXX X
| | | |
sünni- kontroll-
aeg number
soo ja järje-
sajandi number
tunnus



Isikukood ja selle kontrollnumber

Eesti isikukoodiga on veel kolmaski probleem - nimelt kontrollsumma algoritm on välja mõeldud üsna käpardlikult. Üldiselt, näiteks pankade kontonumbrites, on viimane number valitud niisugune, et juhul kui ükskõik milline eelnev number valesti sisestada, muutub alati ka kontrollnumber. Eesti isikukoodiga see nii ei ole - on täiesti võimalik olukord, kus muutub üks number, kuid ei muutu kontrollkood (näide: 61107121760 ja 51107121760). Siit ka küsimus - milleks siis selline mõttetu kontrollsumma üldse isikukoodile lisada?

Isikukoodi kontroll

ISIKUKOODI TEST (KONTROLL, VALIDEERIMENE). ISIKUKOODI
INFO (SÜNNIAEG, SUGU, VANUS)

TÄNA: NELJAPÄEV, 02. NOVEMBER 2017, 07:17

TÄHELEPANU! SIIN SAAB KONTROLLIDA VAID SISESTATUD
ISIKUKOODI VASTAVUST EV STANDARDILE: [EVS 585:2007](#)
"ISIKUKOOD. STRUKTUUR"

TÜHISTA

KONTROLLI

SUGU: Mees

SÜNNIAEG

AASTA: 2011

KUU: 7 (juuli)

PÄEV: 12, teisipäev

VANUS

AASTAID: 6

KUID: 3

PÄEVI: 21

ISIKUKOODI TEST (KONTROLL, VALIDEERIMENE). ISIKUKOODI
INFO (SÜNNIAEG, SUGU, VANUS)

TÄNA: NELJAPÄEV, 02. NOVEMBER 2017, 07:17

TÄHELEPANU! SIIN SAAB KONTROLLIDA VAID SISESTATUD
ISIKUKOODI VASTAVUST EV STANDARDILE: [EVS 585:2007](#)
"ISIKUKOOD. STRUKTUUR"

TÜHISTA

KONTROLLI

SUGU: Naine

SÜNNIAEG

AASTA: 2011

KUU: 7 (juuli)

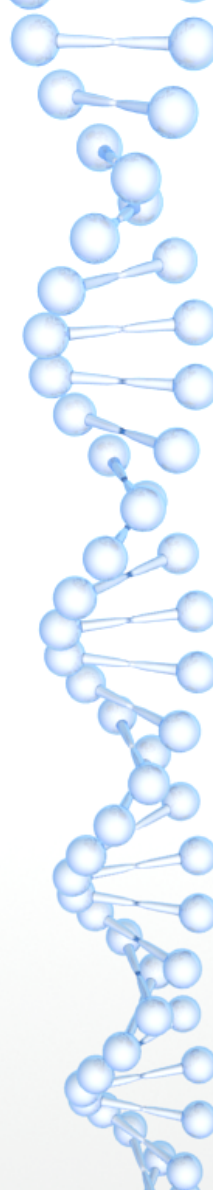
PÄEV: 12, teisipäev

VANUS

AASTAID: 6

KUID: 3

PÄEVI: 21



Isikukoodi kontrollnumber

Kontrollnumber [[muuda](#) | [muuda lähteteksti](#)]

Isikukoodi kontrollnumber formeeritakse "Moodul 11" meetodil, kasutades I või II astme kaalu:

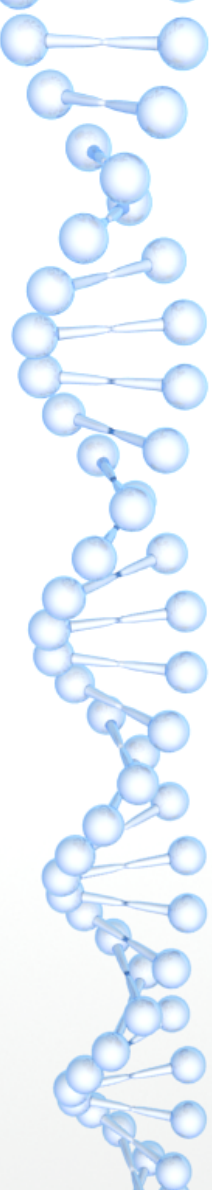
I astme kaal: 1 2 3 4 5 6 7 8 9 1

II astme kaal: 3 4 5 6 7 8 9 1 2 3

See tähendab, et isikukoodi kümme esimest numbrit korrutatakse igaüks omaette I astme kaaluga, korrutised liidetakse. Saadud summa jagatakse 11ga. Kui jagatise jääk ei võrdu 10ga, on jääk kontrollnumbriks.

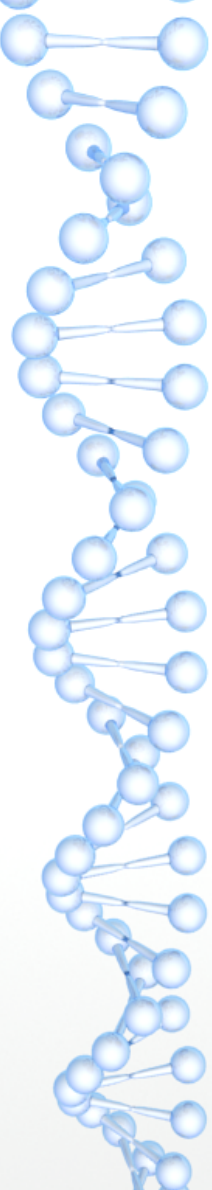
Kui jääk võrdub 10ga, siis korrutatakse koodi kümme esimest numbrit igaüks omaette II astme kaaluga. Korrutised liidetakse. Saadud summa jagatakse 11ga. Kui jääk ei võrdu 10ga, on saadud jääk kontrollnumbriks. Kui jääk võrdub 10ga, siis on kontrollnumber 0.

<https://et.wikipedia.org/wiki/Isikukood>



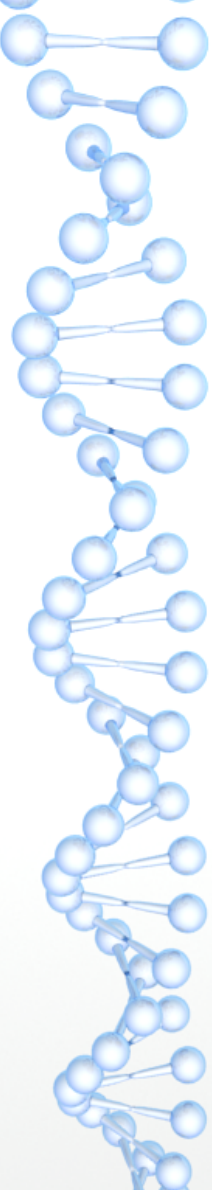
Isikukoodi ajalugu

- **Isikukood Eestis juurutati 12. oktoobri 1989 ENSV Plaanikomitee määrusega nr 121.**
- Ülejäänud dokumendid on juba loogiline tagajärg. (ENSV VST 585-89, EV ST 585-90 ja EVS 585:2007)
- Eesti oli isikukoodi juurutamisel pilootprojektiks
- Arvutusvalem tuli Ungarist (SKV lähetus -> .HU)
 - Thnx to Oleg Lissenko
- **Mis sellest järeldeb?**
- **Tegelikult mitte midagi. Kas täna ongi kontrollnumbrit vaja?**



Aga tegelikult?

<https://github.com/ToomasMolder/isikukood>



Против исикукоода нет приёма кроме другого исикукоода.

Тратка 09.06.2017 20:26

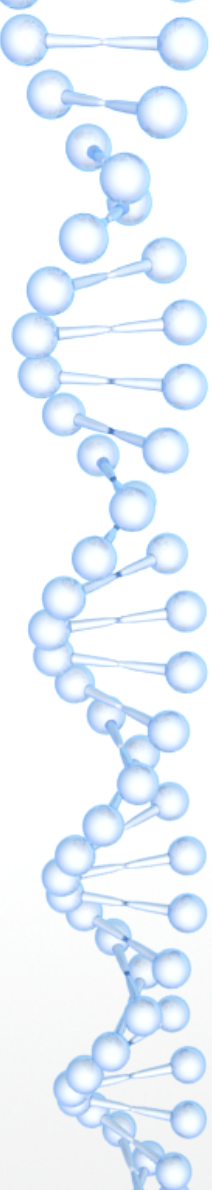
А как отказаться от исикукоода? Я не хочу число. У меня есть имя. Я не хочу как при немцах номер.

👍 17

👎 2

⚠️ Сообщить о неуместном комментарии!

↩️ Ответить



Sertifitseerimisteenus tõejärgsel ajastul?

- Asjad ja esemed läksid vahepeal oluliselt keerulisemaks
- Kasutajate emotsioonid muutusid palavamaks
- Turvavigu muudkui saeveskist tuleb
- Räägivad, et tatt ja teip enam ei pea...
- Paroolid ei pea enam no kohe kindlasti mitte.
 - Kasutajal on endiselt vaja seadet, mis teda identifitseerib.
- Eesti otsib oma kohta maailmas.
- Võimalik, et tuleb fööniksina tuhest tõusta.

Room Time	Dallas Ballroom A1
07:30-09:00	
09:00-10:30	1H: Crypto Attacks
	Session chair: Daniel Genkin
	The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli★ <i>Matus Nemec (Masaryk University/Ca' Foscari University of Venice); Marek Sys and Petr Svenda (Masaryk University); Dusan Klinec (Masaryk University/EnigmaBridge); Vashek Matyas (Masaryk University)</i>

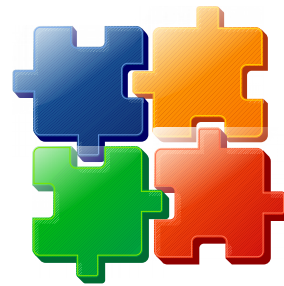
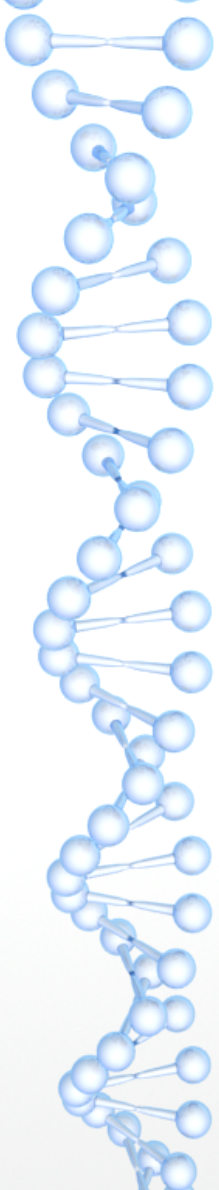
Järgmine ettekanne ... Dallases


[Home](#)
[Call for...](#)
[Agenda](#)
[Workshops](#)
[Registration](#)
[Travel & Venue](#)
[Organization](#)
[Sponsorship](#)
[Accepted](#)
[Proceedings](#)

CCS Main Conference on Thursday, November 2nd, 2017

Room Time	Dallas Ballroom A1	Dallas Ballroom A2	Dallas Ballroom A3	Dallas Ballroom D1	Dallas Ballroom D2	Dallas Ballroom D3
07:30-09:00	Breakfast & Registration					
09:00-10:30	1H: Crypto Attacks Session chair: Daniel Genkin The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli★ <i>Matus Nemec (Masaryk University/Ca' Foscari University of Venice); Marek Sys and Petr Svenda (Masaryk University); Dusan Klinec (Masaryk University/EnigmaBridge); Vashek Matyas (Masaryk University)</i>	2H: Code Reuse Attacks Session chair: Suman Jana The Dynamics of Innocent Flesh on the Bone: Code Reuse Ten Years Later <i>Victor van der Veen, Dennis Andriess, Manolis Stamatogiannakis (Vrije Universiteit Amsterdam); Xi Chen (Vrije Universiteit Amsterdam/Microsoft); Herbert Bos, and Cristiano Giffurda (Vrije Universiteit Amsterdam) [Paper] [Artifact]</i>	3H: Web Security Session chair: Suman Jana Rewriting History: Changing the Archived Web from the Present <i>Ada Lerner (Wellesley College); Tadayoshi Kohno, and Franziska Roesner (University of Washington)</i>	4H: Formal Verification Session chair: Dinghao Wu A Comprehensive Symbolic Analysis of TLS 1.3 <i>Cas Cremers (University of Oxford); Marko Horvat (The Max Planck Institute For Software Systems); Jonathan Hoyland, Sam Scott, and Thyla van der Merwe (Royal Holloway, University of London) [Paper] [Artifact]</i>		Tutorial [9:00–12:30] SGX Security and Privacy <i>Taesoo Kim (Georgia Tech), Zhiqiang Lin (UT Dallas), Chia-Che Tsai (UC Berkeley/Texas A&M University)</i>

<https://www.sigsac.org/ccs/CCS2017/agenda.html>



Küsimused?