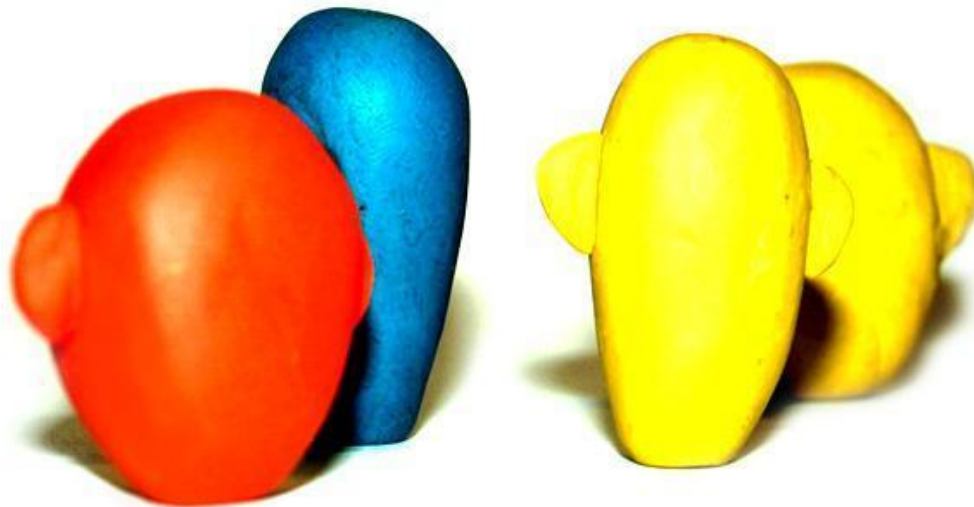


SK aastakonverents 2013

07.11.2013

Jaan Murumets

AS Sertifitseerimiskeskus





- Tagasivaade aastale
- Uus leping
- Kaardid ja krüptograafia
- Formaadid
- Teegid
- GUI
- Tulevik organisatoorselt





- **Driverid**
 - Minidraiver, Tokend, PKCS#11 (OpenSC ja Esteid)
- **Teegid**
 - Allkirjastamiseks ja krüpteermiseks
 - Java, C/C++ ja ülejäänud
- **GUI**
 - Brauseri integratsioon
 - PIN haldus
 - Allkirjastamine ja verifitseerimine
 - Krüpteerimine ja dekrüpteerimine



Tagasivaade

- 3.7.0, 3.7.1, 3.7.2
- Uus leping!
- Arhitektuurinõukogu
- Kevad-suvine 2013 reliis jäi ära uue lepingu tõttu
- Valimiste tsükkel algas
- 1K RSA ja SHA-1 lõpu algus



- ID-kaardi platvormid
 - Spetsifikatsioon väljas veebis
 - RSA 1024 ja 2048, SHA1 kuni SHA512, tulevikus SHA3
 - Kurvid ECC M-ID 2014, kaartidel 2016-2017
 - 3.5 kaart 2014
 - Digi-ID kaardi põhi 3.5 peale 2014



Formaadid

- DDOC
- BDOC 2.1
 - TM
 - TS
- X-tee BDOC hash-linkimine
- PDF Pades
- Guardtime ajatempliga



- **Põhiteegid**

- **Jdigidoc (DDOC, BDOC, CDOC)**
 - Jdigidoc rewrite 2014
- **C teek (ainult DDOC, CDOC)**
 - Asendub CPP teegiga 2014-2016
- **CPP teek (ainult BDOC)**
 - DDOC tugi läbi C teegi wrap

- **Abiteegid**

- **COM teek (ainult DDOC)**
 - Asendub CPP teegiga 2014-2016
- **.NET ndigidoc (ainult CDOC)**



Baastarkvara GUI jt

- **Mooduli kaupa reliisid 2014**
 - Siis kui vaja tuleb sisuline muutus
- **OSX appstore + brauseri integratsioon**
- **XP ja Vista tugi kaob**
- **Linuxite tugi kogukonna abil**
- **Lähiriikide tugi Soome ja Baltikum**
 - Azerbaidzan jt kaugemad
- **TSL**



Organisatoorne

- Infokirjad ja infohommikud
- Dokumentatsioon fookuses
 - Beeta ja RC perioodid
 - Avalik veahaldus





Aitähh!

Küsimused?

