17.07.2017

17. august 2017 15:50

17.08.2017
Küberneetika saal, Mäealuse 2/4
Algus kell 16.00, lõpp kell 17.50.

Osalesid: Juhan Kull, Mari Seeba, Janno Kase, Raul Ennus, Tarmo Oja, Tõnu Tomik, Toomas Viira, Teet Raidma, Aivo Kalu, Hillar Põldmaa, Epp Maaten, Ats Onemar, Mai Kraft, Andres Järv, Ingrid Mesilane, Vilmar Vahe, Jaanus Piirsalu, Rudolf Osman, Siret Schutting, Jaak Tepandi, Raul Rikk, Raini Mihkelson, Agu Kivimägi, Daniel Tikkerbär
Protokollis: Tõnu Tomik

Koosoleku päevakord:
1. Ettekanne eID tänastel aktuaalsetel teemadel
2. Kohapeal algatatud küsimused

1. eID täna aktuaalsetel teemad

Esineb Mark Erlich, RIA eID koosvõime ekspert-nõunik

Aeguvad algoritmid (SHA-1 ja ületembeldamine - TeRa)
SHA-1 algoritm ei loeta allkirjastamisel piisavalt turvaliseks, Google abiga teostati demonstratsioon SHA-1 algoritmi ebaturvalisuse osas 2016 aasta lõpus. SHA-1 algoritmi kasutavate Eesti digitaalsete allkirjade puhul on vajalik on tõestusväärtuse säilimiseks SHA-1algoritmi kasutavad dokumendid üle tembeldada tugevama (nt. SHA-2) algoritmiga. Selleks on tehtud RIA poolt TeRa tervikluse lahendus tavakasutajale (tädi Maali, väikeettevõtja). Eraisikutele ja väikeettevõtjatele kuni 31.08.2017 võimalik teha tasuta TeRa tarkvaraga SK digitempliga. Võimalik ka kasutada SK digitempli asemel alternatiivseid lahendusi (Guardtime jne.)

Usaldusteenused (eiDAS, juriidiline staatus, ETSI standardid, probleemid)
Kohustus EU liikmesriikidele avada usaldusteenuste turg september 2018.
Eestis antakse ca 7 miljonit digiallkirja kuus, muu EL ca 10 miljonit allkirja kokku.

Autentimine (tagatistasemed, vahendid, EE lahendus ja väljakutsed)
e-teenused mis ei nõua kodakontsust peab avama teiste EL riikide kodanikele. eID jagatakse kolme tasemesse, Madal (kasutajanimi ja parool), Märkimisväärne (2-faktoriline autentimine). Kõrge (2-faktorilne autentimine dubleerimise ja manipuleerimise kaitsega ja sõltumatu välise auditiga).
Käimas on Eesti riigi siseste eID vahendite tunnustamise protsess. Ei kata erasektori eID lahendusi (Smart-ID). Eesti riigi poolt tunnustatud siseriiklike eID vahenditega peavad teised EL riigid oma avalikes e-teenustes autentimist lubama. Samuti peab eesti oma avalikes e-teenustes lubama teiste EL riikide tunnustatud eID vahenditega autentimist. RIA poolt tulemas eIDAS lahendus, mille abil saab EL tunnustatud eID oma süsteemides ilma eraldi arendusteta kasutada.

eIDAS määrus rakendub 19.09.2018 ja selle täitma hakkamine eeldab avalike e-teenuste pakkujate RIA poolse või alternatiivse eIDAS lahenduse juurutamist.

Ülevaade muudest projektidest
Vt. täpsemalt presentatsioonist.

2. Kohapeal algatatud küsimused
Järgmine koosolek toimub 21. septembril 16.00