SK aatakonverents 2014: mis juhtub 1. jaanuaril digidokumentidega?

12 aastat tagasi - 06.11.2014 Autor: AM

Sertifitseerimiskeskuse aastakonverentsil räägiti ka sellest, mis muutus meid 1. jaanuar 2015 ootab. Liisa Lukin räägib: "2014. aastal sai tehtud uus m-ID teenusplatvorm. m-ID kehtivusaja pikendamiseks ei saanud me aga riigiga veel kokkuleppele. Uus SIM-rakendus pidi tulema ja tuli ka. Operaatoripõhiselt lahenduselt SK kesksele lahendusele liikusime – platvorm on valmis, järgmisest nädalast esimene operaator hakkab seda kasutama. Seega ka see plaan on 2014. aastal, võiks öelda, täidetud."

Kuid 2015 on BDOC-ile ülemineku ja uue turvalisema m-ID aasta.

Digidokumendi formaadi muutus on normaalne areng, ütleb Lukin, sest krüptograafia aegub, oluline on ajaga kaasas käia ja krüptograafiat uuendada. BDOC-il on kaks põhiformaati, üks on rohkem Eesti-keskne, aga teine rahvusvaheline standard.

Kuid mis saab tulevikus?

Digidoc-idega on see probleem, et nõrgema räsiga digidocid tuleb igaks juhuks varsti näiteks digiarhiivipakkuja juures turvaliselt arhiveerida, et kindlustada nende tõesus. BDOC-iga peaks aga saama oma vana dokumendi, mis on allkirjastatud digidociga, tugevama digitempliga kindlustada. Sedagi võib teha kolmanda usaldusväärse osapoole abiga.

Üleminek BDOC-ile tehakse aastavahetusel. Kui on veebileht, kus saab allkirjastatud dokumente üles laadida, siis see võib esimesena mõneks ajaks katki minna.

Järgmisest aastast alates kehtivad aga välja antud m-ID kaardid alati kuni 31.12.2016 olenemata väljastamise ajast. Täna veel väljastatakse 1K RSA sertfikaate, uus standard on aga järgmisest aastast ECC (ja/või 2K RSA sertifikaat. ECC ehk elliptilised kurvid).

ECC sertifikaadiga ei saa digidocis paraku digiallkirja anda. BDOC-is saab. Kui allkirjastatakse digidoc-i, siis antakse 2K RSA sertifikaat juba teenuse poolel, BDOC-is aga kasutatakse ECC sertifikaati. Autentimisel aga tuleb alati kasutada

alati ECC formaati.

Kas mingi aeg peaks DDOC-i ümber allkirjastama BDOC-iga? Vastus Liisa Lukinilt: digiarhiivi võiks vana digidokumendi panna. Kasutada võib digiarhiivi pakkujat või lammuta ise dokument lahti ja panna peale turvalisem digitempel. Kolmas osapool võib uue templiga kinnitada, et vana DDOC on õige.

- Uudised
- Turvalisus