

Riigi infosüsteem, tugi meditsiinilistele registritele

Margus Püüa,
Riigi infosüsteemide osakond
Majandus- ja Kommunikatsiooniministeerium

Kava

- Riigi infosüsteemi arendamise põhimõtte
- Riigi infosüsteemi ülesehitus
- Kodeerimisteenus

Infoühiskond

- Infoühiskonnas hoitakse, teisendatakse ja edastatakse teavet universaalsel digitaalsel kujul
- Infoühiskonnas on kõigile ühiskonna liikmetele tagatud juurdepääs digitaalsel kujul teabele läbi andmeedastusvõrgu
- Infoühiskonnas on masinatele usaldatud rutiinne vaimne töö
- Infoühiskonnas on elukordalus ratsionaalne tuginedes eelnimetud eeldustele.

Olulised otsused

- Ei looda globaalseid integreeritud infosüsteeme, vaid järgitakse **hajusat ja teenusepõhist** arhitektuuri
- Ei ehitata eraldiseisvat turvalist andmesidevõrku riigi infosüsteemi jaoks, vaid kasutatakse avalikku internetti, kuid **turvatakse andmeid ja teenuseid**
- Avalike teenuste osutamiseks kasutame nii palju kui võimalik **e-teenuseid**
- e-teenused **ei tohi riivata inimeste privaatsust**. Igaüks peab saama teada milliseid andmeid korjatakse ja kes neid ning miks kasutab
- Personaalsete teenuste osutamisel kasutatakse **vaid tegevaid autentimisvahendeid**

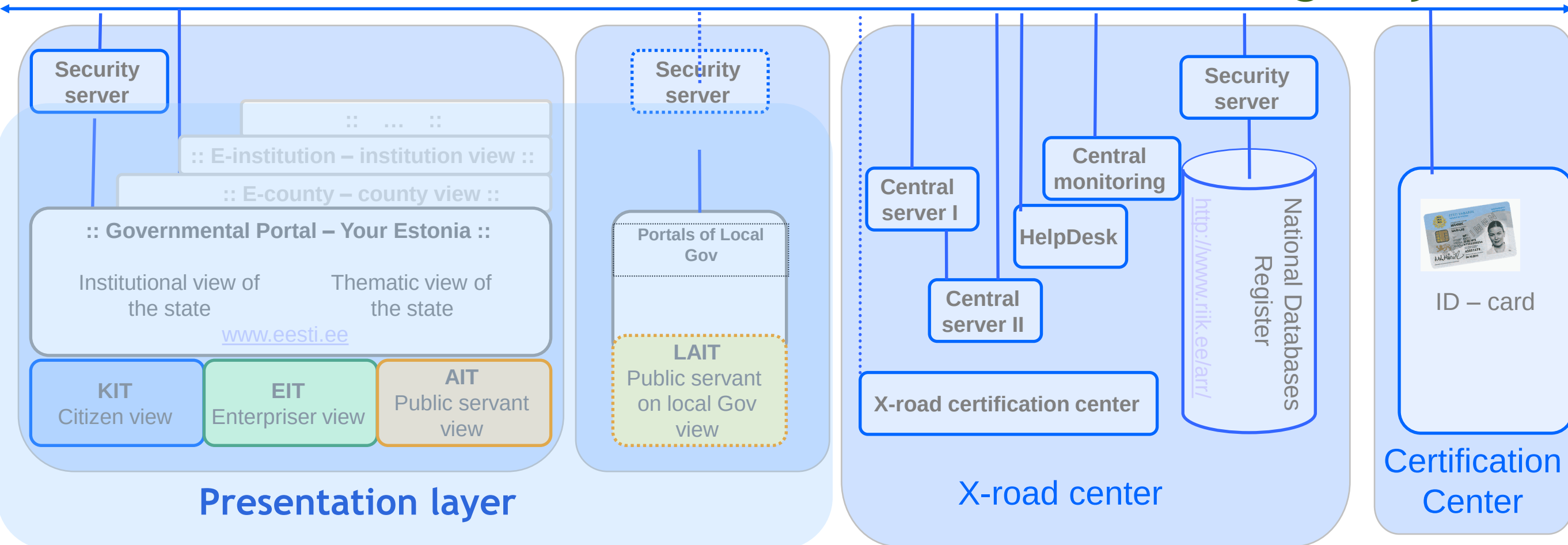
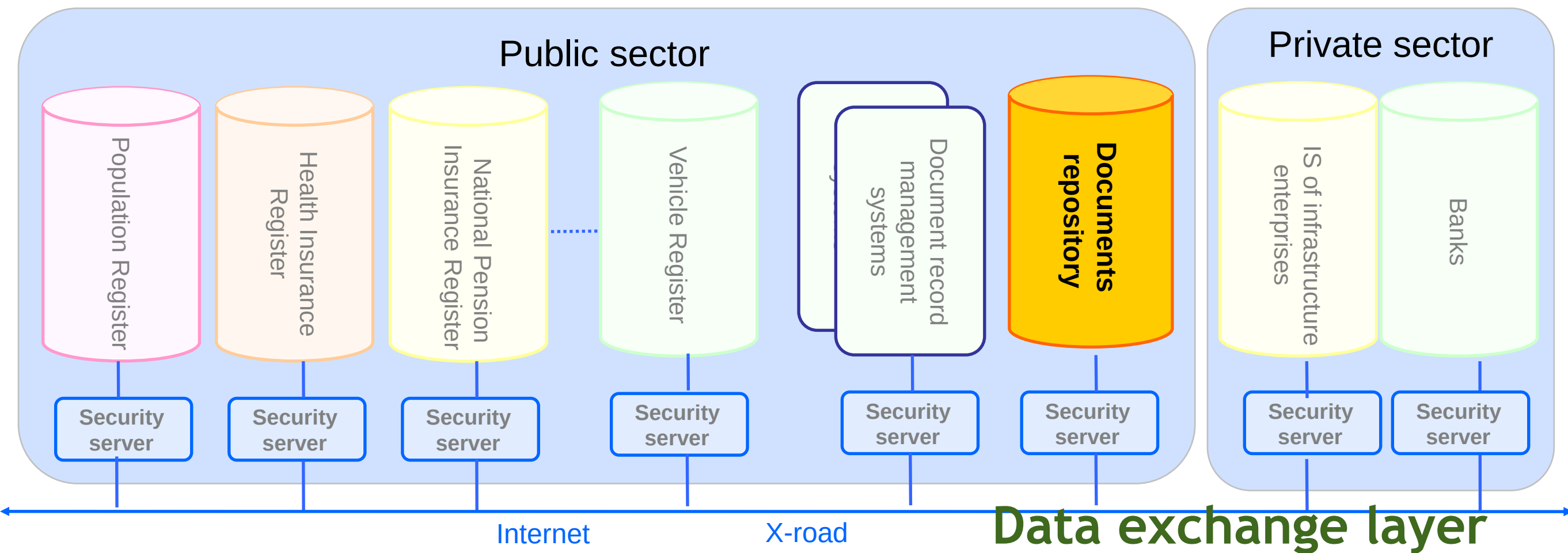
IKT'_{ga} seotud põhilised õigusaktid

- Isikuandmete kaitse seadus (1996)
- Andmekogude seadus (1997-2008) *(2008 liideti avaliku teabe seadusega)*
- Avaliku teabe seadus (2001)
- Isikut tõendavate dokumentide seadus (1999)
- Digitaallalkirja seadus (2000) *(2010 täiendatud definitsiooni ja regulatsiooniga digitaaltempli osas)*

Mis on Eestis teisiti?

- Me kaitseme andmeid, mitte andmeedastuskanalit;
- Kasutame tugevaid autentimisvahendeid (tugev e-ID kõikjal);
- Andmete tõendatus;
- Kõrge käideldavus;
- Konfidentsiaalsus;
- Veebi põhiste teenuste jälgitavus;

Data layer



ID-kaardi kasutamine

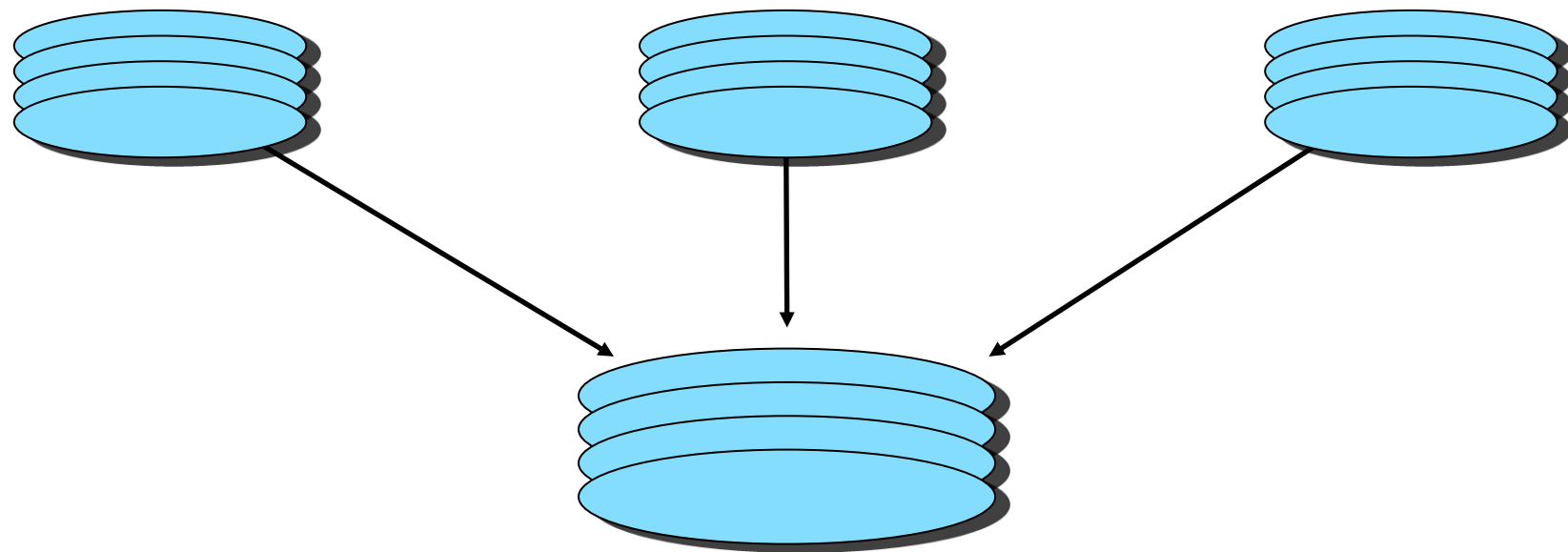
- Unique usage of ID card
- Unique usage of digital signature



Kodeerimisteenus

Probleem

- Andmekogusse või registrisse kuuluvad andmed võivad olla nii delikaatsed, et andmetöötaja ei tohi neisse kantud isikuid identifitseerida
- Samas on erinevaid allikbaase/ allikregistreid vaja isikuti linkida



Kodeerimisteenus

Lahendus

- Pseudonümiseerimisteenus, mis võimaldab agregaatanalüüside läbiviimiseks isikut üheselt identifitseeriva informatsiooni (isikukoodi) pseudonümiseerida
- Isikukoodi või muude delikaatsete andmete pseudonümiseerimiseks kasutatakse krüptimist sümmeetrilise krüptosüsteemi abil, sel juhul on isiku pseudonüümiks tema isiku krüptogramm.
- Pseudonümiseerimist realiseeritakse hajutatud kujul, tsentraalset kodeerimiskeskust ei ehitata
- Andmekogu turvaserveris realiseeritakse pseudonümiseerimisteenus, mis tegeleb delikaatsete andmete krüptimisega

Kokkuvõtteks

Tönan