IT- og Telestyrelsen
Holsteinsgade 63
2100 København Ø

Kgs. Lyngby, den 1. august 2011

Vedr.: Høring om Person

OIO har entiteten og interface til Person i høring.

For god ordens skyld henleder jeg opmærksomheden på ITST's egen publikation.
”Nye Sikkerhedsmodeller” - http://digitaliser.dk/resource/781482

Det aktuelle udkast til Person er både sikkerhedsunderminerende, ikke-interoperabelt, innovationsbegrænsende og ineffektiviserende.

1. Hvis man skal kunne udnytte og samtidig sikre cloud og server-side services, så er det kritisk at Person-entiteten kan være en fuldt virtualiseret repræsentation af en person, dvs. at entiteten og interfacet ikke indeholder eller forudsætter nogen former for personidentificerende data.
2. Data skal kunne være semantisk definerede, så man kan dynamisk model-beskrive og udskyde oversættelsen til runtime frem for at hardkode strukturen.
3. Det er kritisk at man antager at borgeren selv altid er kilden til data, så man i stedet for at fastlåse processerne via systemkald på tværs kan flytte den afgørelse til den som ejer behovet og ved, hvor og i hvilken form data foreligger.

Ad 1. Virtuel person sikkerhed

Alle dele af person inkl. referencer, kommunikationskanaler, data og credentials skal kunne virtualiseres og erstattes af indirekte refererende data, jf. nedenfor.

Cprnummer skal kunne isoleres og erstattes af en ikke-informationsbærende identifier. CPR-nummer selv er en credentials som skal kunne både optionel og være formålsspecifikt krypteret, så det kan styres præcis hvem som kan identificere den pågældende borger.

F.eks. en stemme til et folketingsvalg er afgivet af en Person, som vi kender flere credentials på, f.eks. valgsted, statsborgerskab, men ingen (uden undtagelse inkl. borgeren selv) må kunne koble den afgivne stemme til en specifik borger.

En kontaktkanal (betaling, WWW, SMS, Email, fysisk post, mobil etc.) skal f.eks. kunne model-beskrives ved

- Kommunikationsprotokol,
- Virtualiseret modtager-adresse
- Krypteringsalgoritme
- Krypteringsnøgle

som alle skal kunne specificeres af modtageren formålsspecifikt.

Enhver person skal f.eks. kunne angive en email-adresse som IKKE er afledte af cpr-nummer (e.g. Dokumentboks), IKKE er fastlåst til et monopol (e.g. Nemkonto, Nemid), ikke skal låses i et afsendersystem (f.eks. ved at man antager at fysisk post-adresse kan ”oversættes” i et ”flytteregister”) etc.

Ad 2 – semantisk/modelbeskrevne data.

Det skaber ikke interoperabilitet, men det modsatte, når man specificerer data på lavt niveau. Konsekvensen er at man f.eks. låser it-strukturerne til gamle proprietære nationale ”standarder” uden at kunne håndtere cross-border strukturer eller andre kilder til de logisk samme data.

Ad 3 – behovsdrevne processer.

I stedet for at antage at man identificererer borgeren og derefter slår vedkommende op i allehånde databaser, så skal man i stedet anmode borgeren om de samme data og overlade det til runtimesystemerne (borgerens) at afgøre hvilke data som skal overføres hvorfra.

Afslutningsvist bør det påpeges, at Person er den mest kritiske af alle entiteter, idet det er her man begrænser den tekniske anskuelse og hardkoder en masse forældede antagelser og fastlåsende procedurer ind i stadigt mere ineffektive it-systemer.

Med venlig hilsen

Stephan Engberg
Priway ApS.
Stengårds Alle 33D,
2800 Kgs. Lyngby