SWEDISH STANDARDS INSTITUTE

Datum
2018-04-23

Er referens
Fi2018/00106/DF

Fredrik Göthe, tfn: 08-555 522 68
fredrik.gothe@sis.se

Till Finansdepartementet

SIS yttrande över Finansdepartementets remiss ”Reboot – omstart för den digitala förvaltningen” (SOU 2017:114)

Swedish Standards Institute (SIS) önskar härmed inkomma med kommentarer till slutbetänkandet ”Reboot – omstart för den digitala förvaltningen” SOU 2017:114.

Dagens samhälle kräver säkra metoder för kommunikation, identifikation och integritet. Den elektroniska kommunikationen har blivit etablerad och fortsätter att utvecklas. Det övergripande målet med SIS standardiseringsarbete inom informationssäkerhetsområdet är att skapa förutsättningar för rätt säkerhet i samhället och näringslivet genom att informationssäkerhetsstandarder är det naturliga valet för styrt informationssäkerhetsarbete.

SIS har inga invändningar mot slutbetänkandet i sak men vill kommentera att när man refererar till en standard är det viktigt att referensbeteckningen är korrekt, vilket i slutbetänkandet innebär att ISO 15408 bör betecknas med ISO/IEC 15408 och samma sak gäller ISO 29115 som har beteckning ISO/IEC 29115.

På sidan 89 i slutbetänkandet föreslås att ett rådgivande organ ska bistå digitaliseringsmyndighetschefen i strategiska frågor förande myndighetens verksamhet och vid framtagning av föreskrifter. I rådet ska representanter för statliga myndigheter, kommuner och landsting, SKL samt Sveriges standardiseringsförbund ingå. Standardiseringsförbundet består i huvudsak av SIS och vi stödjer förslaget och bistår gärna i diskussioner om hur standarder och utveckling av standarder kan hjälpa och utveckla myndigheten till att bli en mer användardriven verksamhet.

SIS vill vidare även betona att nedanstående paragrafer i slutbetänkandet är viktiga och särskilt sid. 516, §72).

Sid 516:
§72) När kommissionen antar delegerade akter eller genomförande akter bör den ta vederbörlig hänsyn till de standarder och tekniska specifikationer som utarbetats av europeiska och internationella standardiseringsorgan, särskilt Europeiska standardiseringskommittén (CEN), Europeiska institutet för telekommunikationsstandarder (ETSI), Internationella standardiseringsorganisationen (ISO) och Internationella teleunionen (ITU), i syfte att säkerställa en hög nivå av säkerhet och interoperabilitet när det gäller elektronisk identifiering och betrodda tjänster.

Sid 164:
9.2) Varje myndighet ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av ett ledningssystem för informationssäkerhet. I detta arbete ska standarderna ISO/IEC 27001:2014 och ISO/IEC 27002:2014 beaktas. Tillräckliga resurser ska tilldelas för

informationssäkerhetsarbetet samt löpande och regelbunden information lämnas till myndighetsledningen.

Sid 509:
§16) Tillitsnivåerna bör återge graden av tillit till ett medel för elektronisk identifiering vid fastställande av en persons identitet och skapa visshet om att den person som gör anspråk på en viss identitet faktiskt är den person som har tilldelats denna identitet. Tillitsnivån beror på den grad av tillit detta medel för elektronisk identifiering ger i fråga om en persons påstådda eller styrkta identitet med beaktande av olika processer (t.ex. styrkande och kontroll av identitet, och autentisering), förvaltningsverksamhet (t.ex. den enhet som utfärdar medel för elektronisk identifiering och förfaranden för att utfärda sådana medel) och de tekniska kontroller som tillämpas. Det finns olika tekniska definitioner och beskrivningar av tillitsnivåer tack vare unionsfinansierade storskaliga pilotprojekt, standardiseringsarbete och internationell verksamhet. Det storskaliga pilotprojektet Stork och ISO 29115 avser, bland annat, nivåerna 2, 3 och 4, som bör tas under noggrant övervägande vid fastställandet av minsta tekniska krav, standarder och förfaranden för tillitsnivåerna låg, väsentlig och hög enligt denna förordning, samtidigt som en konsekvent tillämpning av denna förordning säkerställs med särskilt hänseende på tillitsnivån hög i samband med styrkande av identitet för utfärdande av kvalificerade certifikat. De fastställda kraven ska vara teknikneutrala. Det ska vara möjligt att uppnå de nödvändiga tekniska kraven med hjälp av olika tekniklösningar.

Sid 514:
§55) IT-säkerhetscertifiering som bygger på internationella standarder, såsom ISO 15408 och besläktade utvärderingsmetoder och arrangemang för ömsesidigt erkännande, utgör ett viktigt verktyg för att kontrollera säkerheten hos kvalificerade anordningar för skapande av elektroniska underskrifter och bör främjas. Innovativa lösningar och tjänster, såsom undertecknande via mobil och datamoln, förlitar sig emellertid på tekniska och organisatoriska lösningar för kvalificerade anordningar för skapande av elektroniska underskrifter, för vilka det eventuellt ännu inte finns tillgängliga säkerhetsstandarder eller för vilka den första it-säkerhetscertifieringen pågår. Säkerhetsnivån för sådana kvalificerade anordningar för skapande av elektroniska underskrifter skulle kunna utvärderas genom alternativa processer endast om sådana säkerhetsstandarder inte finns tillgängliga eller om den första it-säkerhetscertifieringen pågår. De processerna bör vara jämförbara med standarderna för IT-säkerhetscertifiering i den mån deras säkerhetsnivåer är likvärdiga. Förfarandena skulle dessutom kunna underlättas av en sakkunnighetsbedömning.

SIS finns tillgängliga för att förtydliga eller svara på följdfrågor om så önskas.

Med vänlig hälsning,

SIS, Swedish Standards Institute

Thomas Idermark
VD