Remiss – Kammarkollegiets studie om Organisationslegitimering, DNR 93-33-09

SNUS anser att en lösning först och främst måste skilja på de tre olika typerna av identifiering som behövs, och i varje fall försöka etablera en standard för hur certifikat ska utfärdas, hur betrodda tredje parter skall etableras (potentiellt genom ett ackrediteringsförfarande), och mindre genom att även i fortsättningen försöka utveckla standarder och lösningar som är unika för Sverige och svensk förvaltning. För övrigt vill vi referera till SNUS Remissvar på Vervas slutrapport om säkert elektroniskt informationsutbyte och säker hantering av elektroniska handlingar (Fi2006/6773 (delvis), Fi2006/967)[1].

Studien är en gedigen genomgång av en syn på hur elektronisk verifiering och identifiering av såväl personer som juridiska enheter. Den beskriver det motstånd som finns för viss typ av användning av legitimering på ett korrekt sätt, men, den beskriver enligt föreningen SNUS fortfarande ett föråldrat tänkande på hur e-ID fungerar. En syn som baserar sig på hur dagens e-ID är designade.

Vi vill speciellt påpeka följande:

Att använda termen "*e-legitimation*" för t.ex. servercertifikat anser vi vara förvirrande. Just termen "legitimation" bör enligt föreningen SNUS enbart användas för det certifikat som direkt identifierar en person eller juridisk person. Certifikat som indirekt kan härledas till en sådan bör inte kallas "e-legitimation".

Servercertifikat

Servercertifikat identifierar inte en "*server*", utan en tjänst. T.ex. "e-posttjänst som används av kammarkollegiet". Det kan mycket väl inträffa att samma server används även för t.ex. "webserver för kammarkollegiet". Dessa två tjänster kan (tekniskt) i vissa fall använda samma certifikat, men så behöver inte vara fallet. Speciellt i fallet e-post är det ofta tjänsteleverantören (som Kammarkollegiet köper upp mailtjänsten av) som innehar certifikatet för den mailtjänst Kammarkollegiet använder, och inte Kammarkollegiet. Att därför dels kalla detta certifikat e-Legitimation eller servercertifikat är inte optimalt.

Vad gäller certifikat som används av sådana tjänster finns det i världen en etablerad marknad av certifikatutgivare, och att skapa en ny sådan enbart för Sverige går i praktiken inte. Därför bör denna del separeras från övrig certifikathanterig och begränsa sig till en upphandling där krav finns på bl.a. interoperabilitet med dominerande produkter på marknaden (som de webbläsare som distribueras från t.ex. Apple och Microsoft).

[1] http://www.snus.se/media/utkast/SnusRemissvarVervaEid.pdf

Stämpelcertifikat

Föreningen SNUS ser inte idag internationellt någon utpräglad standard som används, utan det är de facto certifikat för juridiska personer för kommunikation som även används för signering av dokument etc. inför lagring. Dock finns det för lite erfarenhet av hur sådana tjänster skall utformas varför SNUS föreslår ytterligare utredning och tester för detta. Vi ser alltså inget omedelbart behov för denna typ av tjänster som inte kan lösas med certifikat för juridiska personer (tjänstelegitimation för en juridisk person).

Tjänstelegitimation

Föreningen SNUS är oroad över att Kammarkollegiet fortfarande tittar på de lösningar som provats i Sverige och i andra länder under många år, utan att de visat sig vara fungerande. Speciellt oroad är vi över att t.ex. genomlysningen av vad som används i Danmark inte visar att man i Danmark 2008 övergav det e-ID system som finns beskrivet och istället slog fast att ett federationsbaserat system (baserat på SAML 2.0) skall användas[2]. Vi föreslår att Sverige tar motsvarande beslut, vilket skulle vara enkelt då IT- og Telestyrelsen i Danmark redan har gjort det mesta av arbetet.

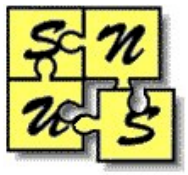
Vi anser att studien har fel då den påstår att det inte finns någon generell metod för att säkra e-post. Det finns i praktiken två som används: PGP (specificerat in RFC 4880[3]) och S-MIME (specificerat i RFC 3851[4]), vilka båda använder multipart/signed som är definierat i RFC 1847[5]. Dessa mekanismer fungerar, och används, både av juridiska och fysiska personer över hela världen redan idag. Det som saknas är en gemensam överenskommelse av hur certifikaten skall utfärdas, men det är det som SAML-arbetet med olika federationer bygger på.

Föreningen SNUS är av dessa, och andra motsvarande, skäl mycket oroad över att rapporten inte bygger vidare på de öppna och använda standarder som redan finns.

Lövestad 27 juni 2009

Styrelsen för SNUS genom Patrik Fältström, vice ordförande

[2] OIO Web SSO Profile V2.0.5 - http://www.itst.dk/arkitektur-og-standarder/Standardisering/standarder-for-serviceorienteret-infrastruktur/standarder-for-brugerstyring/filer-til-standarder-for-brugerstyring/saml.pdf
[3] http://www.ietf.org/rfc/rfc4880
[4] http://www.ietf.org/rfc/rfc3851
[5] http://www.ietf.org/rfc/rfc1847



Om SNUS
SNUS är en ideell förening för svenska nätverksanvändare. Vårt syfte är att höja nätverkskunskapen i Sverige och därmed vår nationella konkurrenskraft.

SNUS är föreningen för dig som är nätverkstekniker och arbetar med IP-nätverk. Föreningen har funnits i många år och är ett forum för tekniskt intresserade personer inom nätverksområdet. Vi ska verka för att medlemmarna får del av varandras kunskaper inom ramen för våra olika aktiviteter, främst genom arbetsgrupper, seminarier, testrapporter och medlemstidning. Genom dessa aktivitet är SNUS ett forum med verksamhet inriktad på att

- öka förståelsen för nätverksteknik och -användande i Sverige.
- driva på utvecklingen vad gäller samtrafik och samverkan.
- testa vad som fungerar i verkligheten sprida kunskap och erfarenheter.

Under SNUS historia sedan 1991 har fokus varit att sprida kunskap om leverantörsoberoende kommunikation (TCP/IP). SNUS har starkt bidragit till den tekniska utvecklingen av Internet vi har bl.a. initierat Swipnet (Det första kommersiella IP-nätet i Sverige) och medverkat till en överenskommelse om samtrafik för elektronisk post (mellan X.400- och Internet-världarna). SNUS har genomfört seminarier där intressanta ämnen inom TCP/IP-området tagits upp. SNUS är mest känt för att anordna Interoperabilitets-tester. Som bäst kan beskrivas som en avancerad provplats inför öppen ridå. Där de deltagande företagen genom hårt arbete och samarbete fått insikter och testat utlovade funktioner i praktiken. Testresultaten har presenterats dels direkt på plats, dels i detalj i testrapporter som publiceras här i vår Web. Vi har även arbetat med politiker, operatörer och övriga intressenter om vikten av fungerande interoperabilitet och samtrafik mellan de olika näten. SNUS har medverkat som sakkunniga i regeringens Internetutredning. Varit delaktiga i skapandet av den svenska delen av ISOC, Internet Society, som är det internationella värdorganet för IETF, Internet Engineering Task Force. SNUS har även varit värdorganisation för de svenska internetoperatörernas forum; SOF-gruppen.