Uppgjord	Dok.id		
Fredrik Ljunggren	KIREI-2008-87		
Godkänd	Datum	Rev	Referens
	2008-11-29	A	Fi2006/6773 (delvis), Fi2006/967

Framtidens svenska e-legitimation. Vervas slutrapport om säkert elektroniskt informationsutbyte och säker hantering av elektroniska handlingar.

Personerna bakom Kirei AB har arbetat praktiskt i näringslivet under drygt 10 år med frågor som rör elektronisk identifiering och underskrifter. Vi har valt att prioritera dessa frågor och endast lämna yttrande om elektronisk identifiering i Vervas slutrapport.

Det är med glädje vi noterat att Verva under arbetets gång i sitt arbetsmaterial tagit visst intryck av de praktiska erfarenheter från verkligheten som omvärlden bidragit med i form av det som näringsliv, utbildningsväsen och andra intressen tillfört, men det är också tydligt att det inom verket finns olika krafter med olika förmåga att ta till sig utvecklingen på området.

Intrycken man tagit till sig av har dock inte satts i sina sammanhang, och flera av tankarna har fallit bort. Det har medfört att slutrapporten är motsägelsefull och innehåller en rad sakfel och missuppfattningar.

I den inledande behovsanalysen och i målbilden lyfts värdet fram av att ha en *tillräckligt säker* och *teknikoberoende* lösning som ger *fullgott skydd av innehavarnas personliga integritet*. Man konstaterar också att dagens upphandlade modell fungerar dåligt, och att en fungerande lösning utgör en förutsättning för säker elektronisk kommunikation i samhället generellt. En uppfattning vi delar.

Därför finner vi det särskilt olyckligt att man redan i rubriken till förslaget överger samtliga av dessa mål. Avsnittet "Förslag till svensk e-legitimation och certifikat" innehåller en rad missförstånd som tyvärr visar att myndigheten till stor del misslyckats med det uppdrag som den givits av regeringen.

Förslaget till utformning av en svensk e-legitimation är identiskt med tankesätten som rådde 1999. Det finns genomgående i slutrapporten en inlåsning i tankesätten kring användande av certifikat respektive kvalificerade- och avancerade elektroniska signaturer. Det är vår bedömning att endast formerna för utgivning har förändrats.

Denna inställning har medfört en blockering i utvecklingen av e-legitimationen. Många företag och affärsidéer har inte blivit verklighet, då infrastrukturen för identifiering fortfarande inte finns på plats.

Det är i sammanhanget viktigt att framhäva att det inte finns någon som helst efterfrågan på kvalificerade certifikat, vare sig från myndighetshåll eller näringsliv. Kostnaderna för kvalificerade certifikat har inte gått att motivera; de möjliggör inga ytterligare tjänster, de ger en inlåsning i en föråldrad teknik, tekniken är dyr och komplex att integrera och svår att skapa interoperabilitet med, den saknar helt möjlighet till skydd av personuppgifter och ger en

Kirei AB
Box 53204
400 16 Göteborg

031 - 787 80 00
info@kirei.se
http://www.kirei.se

synnerligen dålig upplevelse för användarna.

Vervas målbild beskriver en bred användning av e-legitimation, där nyttan av e-legitimationen upplevs vara så stor att innehavaren själv är villig att betala för den. Bara utgivning av en identitet baserad på kvalificerade elektroniska certifikat med erforderlig utrustning kostar idag över 2000:- per identitet. Till detta kommer rörliga kostnader för underhåll, utbildning och användarstöd. Målbilden är en utopi om man står fast vid kvalificerade certifikat baserade på ETSI-standarder, aktiva kort och säkra anordningar för signaturframställning. Baserat på vår erfaraenhet är det vår starka uppfattning att kostnaderna för en sådan lösning vida överstiger nyttan.

En certifikatbaserad lösning är av ovan nämnda skäl endast möjlig att införa i myndighetssammanhang, då kostnaderna kan påtvingas/abstraheras innehavarna via skattsedeln. Näringslivet kan heller inte använda en sådan lösning, inte minst på grund av dess brister i skydd av innehavarnas personliga integritet då personuppgifter sprids på ett okontrollerat sätt.

Föreställningen av behovet av signering är också kraftigt överdriven. Det är ytterst få sammanhang då ett viljeyttring inte kan ersättas med en metod baserad på säker identifiering. Fokuseringen kring signaturer kan möjligen förklaras då de flesta av dessa situationer uppträder i samband med förvaltningsrätt, en situation som skapats genom samma missbedömning av tekniska egenskaper som Verva gör i sin rapport.

Att rapporten har ett tydligt myndighetsperspektiv är måhända inte så konstigt. Men om en e-legitimation utformas så att den endast kan användas gentemot myndigheter kommer kostnaderna aldrig kunna motivera nyttan.

Det är vår uppfattning, att en lösning endast avsedd för myndigheter aldrig kommer kunna få den spridning som beskrivs i målbilden. Därmed är det inte heller sannolikt att den enskilde upplever nyttan till den grad att denne själv är villig att betala för identifieringslösningen.

Vervas slutrapport nämner även tjänstecertifikat. Vi delar uppfattningen att det finns ett behov av att på nationell nivå säkerställa tillgången av denna typen av certifikat. Frågan bör dock hanteras separat.

Förslag

Ansträngningarna bör inriktas på ett etablera en infrastruktur för identifiering som uppfyller de grundläggande kraven att vara *tillräckligt säker*, *teknikoberoende* och ge ett *fullgott skydd av innehavarnas personliga integritet*.

Den kan därmed får den spridning som krävs för att kostnaderna skall kunna fördelas över fler intressenter och i förlängningen självfinansieras.

För att nå dit föreslår vi en variant av den statliga samordningsfunktion som

nämns i slutrapporten (alternativ 3). Vi föreslår att infrastrukturen baseras på federationsteknik som ger den distribuerade struktur som krävs för att möta kraven på tillgänglighet, säkerhet och integritetsskydd.

Staten bör genom myndighets försorg ta den rent administrativa rollen som federationsoperatör. Denne etablerar förutsättningarna för elektronisk identifiering enligt kraven för **svensk e-legitimation**.

Myndigheten etablerar policy, ramverk, ackrediteringsprocess och metod för informationsutbyte för identitetsleverantörerna.

Alla ackrediterade utgivare kan genom federationen erbjuda sin identifiering till alla anslutna tjänster, både inom den offentliga förvaltningen och näringslivet. Därigenom skapas ett incitament för marknaden att erbjuda innovativa och kostnadseffektiva identifieringslösningar till allmänheten.

Staten behöver inte heller driva centraliserade och därmed kritiska och sårbara IT-system. Statens roll blir minimerad men styrande, och ansvaret för drift distribueras mellan identitetsleverantörerna i förhållande till deras storlek.

Genom att standardisera metoder för datautbyte snarare än hela identifieringkedjan (som föreslaget) kan flera oberoende identitetsleverantörer samverka inom federationen. Det gör det enkelt för tjänsteleverantörerna att integrera mot federationen, och det blir också möjligt att skapa långsiktig interoperabilitet över t.ex. landsgränserna. Det finns redan idag redan etablerade öppna standarder för denna typ av informationutbyte. Ett exempel på ett sådan standard är SAML version 2.

Mekanismerna för identifiering blir helt transparenta för tjänsteleverantörerna, vilket ger sann teknikneutralitet. Olika situationer kräver olika lösningar, och användaren tillåts använda den lösning som bäst passar dennes behov vid det givna tillfället. Kvalificerade certifikat kan användas i de sällsynta fall de faktiskt existerar. Det möjliggör att alla nuvarande och framtida tekniska metoder för identifiering kan användas.

I en modern identifieringslösning bär själva e-legitimationen heller ingen information om individen. Identifieringsprocessen baseras på utfärdande av temporära elektroniska intyg som bärare av relevant information. Denna information hämtas från externa register vid lyckad identifiering, och är specifik för den aktuella relationen. Därför behövs heller ingen separat tjänstelegitimation. I vissa relationer bifogas ingen information alls vilket ger egenskapen *pseudonymitet*, där innehavaren tillåts vara anonym men ändå kan utkrävas ansvar för de handlingar denne utför. Härigenom kan ett kraftfullt skydd av innehavarnas personlig integritet uppnås.

Staten bör också arbeta för att ändra lagstiftningen på området till att utelämna metoder för signaturframställning, och istället framhäva målsättningen för att därigenom kunna möjliggöra nya moderna metoder.