Leverantörsmöte och forum för betrodda tjänster

Program den 16 maj 2018

Alla hälsas välkomna och mötet inleds med en film från kommissionen om eIDAS och vad vi skulle vilja kunna åstadkomma med e-legitimation. Att äga sin egen vardag och göra vad jag vill när jag vill. Det ska vara snabbt och enkelt och gå att lita på. Ingen kan göra detta själv utan vi behöver alla varandra. Det ska bli bra för Sverige och vi spelar alla en viktig roll.

Dagens moderator tar över och informerar lite kort om att PTS och e-legitimationsnämnden ordnat ett sådant här forum där vi kan mötas under informella former en gång tidigare och det kommer ett nytt i höst. Kommer ni på några punkter/ämnen att ta upp på kommande forum hör av er. Efter genomgång av dagens agenda överlämnas till presentation av nästa punkt på agendan.

Andra betaltjänstdirektivet *(PTS)*

EU-direktiv trädde i kraft den 13 jan 2018. Finansinspektionen är tillsynsmyndighet. Tanken med direktivet är att utveckla marknaden för elektroniska betalningar och skapa förutsättningar för säkra och effektiva betalningar. Förändringar gentemot första betaltjänstdirektivet är att betaltjänstelagen utvidgas att även omfatta tredjeparts betaltjänsteleverantörer samt att det införs incidentrapporteringsplikt och detaljerade krav på att kunna hantera säkerhet och risker hos betaltjänstleverantörerna. Detta kommer att leda till att det vid online betalning behövs mellanhänder för att knyta samman din och butikens bank. Tjänsterna kan få en ren API-tillgång till informationen hos banken.

Nya rapporteringskrav träder i kraft från 1/5 2018. Se detaljer kring dessa samt kopplingen till eIDAS och betrodda tjänster i bifogad presentation. Mer info om PSD2 kommer att hållas i det forum som Finansinspektionens ordnar den 7/6.

ROCA-sårbarheten från ett eIDAS perspektiv *(PTS)*

En betrodd tjänst innebär att utfärdade certifikat kan användas för underskrifter, stämplar kan valideras, bevaras och tidsstämplas samt att webbplatser och meddelandetjänster kan autentiseras. Tillitsnivåerna är betrodd tjänst samt kvalificerad betrodd tjänst.

ROCA är en sårbarhet i mjukvaran hos en slumpvalsgenerator, som används för att skapa nycklar med RSAlib i produkter från tillverkaren Infineon, och drabbar vissa nyckellängder. ROCA blev publikt känd i oktober 2017. Dagen efter tillkännagivandet hade några forskare snabbat upp metoden med 25 %. Redan 1996 visade Dan Coppersmith att man kan återskapa ett krypterat meddelande under vissa förutsättningar. Hur attacken fungerar visas i bifogad presentation. Där finns även länkar att läsa vidare på om man är intresserad.

Chipen sitter i våra datorer, smarta kort m.m. det är alltså ganska allvarligt. De som drabbats är förlitande part för kvalificerade underskrifter och stämplar enligt EIDAS, TPM-chip samt vissa hårdvarumoduler som används för att skapa nycklar. Mer detaljer kring detta liksom historik från upptäckt till att vissa certifikat spärrats finns i bifogad presentation. Här finns

även en beskrivning av konsekvenser av ROCA för e-IDAS och slutsatser kring hur man ska agera.

En mötesdeltagare kommenterade att man mycket väl kan använda smarta kort med utsatta Infineonchip men göra nyckelgenerering utanför kortet.

Internet of Things och säkerheten *(Comfact och e-legitimationsnämnden)*

Standardisering – status

Comfact inledde.

Standardgrupp STF 539 (se bifogad presentation) visar standardiseringslandskapet för betrodda tjänster. Man arbetar med remote signature, hur man skapar en elektronisk underskrift. En skyddad miljö för att göra signaturer. Man jobbar mest med komponenter och följer DSS2 m.m. Något att lägga märke till är att det saknas saker i de befintliga så nya komponenter måste skapas.

10 företag är med i arbetsgruppen. Adobe är väldigt involverade via samarbetspartners. Intresset, speciellt för engångscertifikat, är väldigt stort i Europa. De har kämpat för att den svenska lösningen ska fungera i det nya.

13 juni under ETSI security week hålls en heldags workshop som redan är fulltecknad. I bifogad presentation eller på ETSI:s webbsida kan man läsa vad som kommer att behandlas.

Tidsplanen, som är väldigt tight, finns redovisad i bifogad presentation liksom mer detaljer kring ovanstående.

e-legitimationsnämndens representant fanns inte på plats utan deras punkt kring standardisering presenterades av en ersättare som inte är tillräckligt insatt i ämnet för att kunna svara på frågor som kan dyka upp vid genomgången av bifogad presentation. I denna visas hur arbetet bedrivs i CEN. De flesta länder i Europa har inte gått på det här spåret. Man är handfallna för att e-tjänsterna inte kommer att gå att signera och inga lösningar har tagits fram. Arbetar man enligt vårt tekniska ramverk är man i linje med hur utvecklingen går. Vad gäller signaturvalidering och bevarande – där är vi bara i början. Det är något man måste tröska sig igenom.

Vad upphandlas och på vilket sätt? *(e-legitimationsnämnden)*

Elektronisk identifiering, betrodda tjänster (i eIDAS mening) samt mina sidor, e-tjänster och olika stödtjänster upphandlas av upphandlande myndigheter (LOU), privata företag och organisationer samt leverantörer som behöver underleverantörer. En översikt av upphandling där staten har ett samlat ansvar, funktioner för identitetskontroll som täcks in av e-legitimationsnämndens valfrihetssystem och inriktningen för valfrihetssystemen förklaras närmare i bifogad presentation.

Den 15 maj 2018 fattades beslut om inriktning för valfrihetssystemen. Valfrihetssystem är enkelt för upphandlande myndigheterna men de måste gå med i flera. Det är inget måste att ha transaktionspris. Ni är välkomna att skicka in tips kring prissättning om ni har några.

Transaktioner enligt eIDAS upphandlas inte (se detaljer i bifogad presentation) Trafiken är gratis gentemot e-leg landet och utfärdaren. Myndigheterna kan ansluta sig och upphandlar hjälpen. E-legnämndens nod är en delmängd i Sweden Connect.

Allt kring upphandling ska vara klart under september i år.

Vad händer med förslagen i ”Reboot”? *(Finansdepartementet)*

Punkten inleds med en illustration av regeringens digitaliseringspolitik som rör sig inom flera sektorer. Digitalt ska vara förstahandsval i den offentliga förvaltningens verksamhet. Det måste fungera och vi måste ha regler och det finns många frågor att besvara.

Mer detaljer kring mål, inriktning, prioriterade områden och regeringens styrverktyg samt direktiv m.m. finns i bifogad presentation.

Idag saknas en effektiv styrning av de nationella digitala tjänsterna. Internationellt så är vi väldigt digitala i Sverige och har duktiga myndigheter som erbjuder digitala tjänster till medborgarna. Det vi ser nu är att vi ligger högt men långt bak det går inte så snabbt längre. Andra länder är duktigare på de horisontella frågorna. En utredning, som skulle titta mer på lag och förordning, startades då det behövs en effektiv styrning av anslutning till de nationella digitala tjänsterna samt att innovationskraften i näringslivet måste tas tillvara. Slutbetänkandet som består av tre övergripande delar kom i januari 2018 och finns att läsa på regeringens webbplats. Remisstiden gick ut den 23 april och inkomna svar finns att läsa på webben.

Ett stort antal förslag till åtgärder för elektronisk identifiering är framtagna då området är underreglerat. Förslag om uppgifter/uppdrag, både nya och gamla, till myndigheten för digital förvaltning har tagits fram. Se bifogad presentation för mer detaljer och tidplan.

Myndigheten för digital förvaltning

Tidplan över arbetet i organisationskommittén som ska bygga upp den nya myndigheten presenterades. Verksamheten startar den 1 september i Sundsvall och kommer till slut att ha ca 70 medarbetare men vid starten räknar man med ca 25-30 st. Regeringen har sagt att myndigheten ska samordna och stödja digitaliseringen av statliga myndigheter samt kommuner och landsting. Hela den offentliga sektorn är myndighetens målgrupp. GD rekryteras av regeringen. Efter 1 april har det varit fokus på rekrytering, lokaler, IT, bygga upp styrdokument etc. samt vilka verksamheter från nuvarande myndigheter som ska in i/över till den nya. Man vill skapa en organisation som möjliggör synergier.

Ett förslag till instruktion för myndigheten är inlämnat och beslut kommer kanske att fattas av regeringen under sommaren.

Se mer detaljer i bifogad presentation kring myndighetens vision och mission, uppgifter, utmaningar som är viktiga att hantera, prioriterade uppdrag, vad som ska tas över från andra myndigheter samt vad myndigheten inte ska göra.

Hur blir man en kvalificerad tillhandahållare av en betrodd tjänst? *(PTS)*

Talaren inleder kort med att berätta om PTS roll. PTS är tillsynsmyndighet för betrodda tjänster och tillhandahåller förteckning över kvalificerade tillhandahållare och betrodda tjänster. Därefter följde en genomgång av regler och skillnader kring anmälan, säkerhetskrav, skadestånd, incidentrapportering, tillsyn och juridisk verkan för betrodd respektive kvalificerad betrodd tjänst samt hur man blir en kvalificerad tillhandahållare. En kvalificerad betrodd tjänst har högre tillförlitlighet och erkännande över landgränser. Den som vill bli kvalificerad tillhandahållare gör enligt den Europeiska tillitsmodellen för kvalificerade betrodda tjänster.

När man anmäler sig till PTS lämnar man en beskrivning av verksamheten, redovisning av ekonomiska medel, utdrag ur bolagsregistret m.m. PTS granskar, fattar beslut och för upp på trusted list. Alla medlemsländer i EU har skyldighet att tillhandahålla en trusted list med kvalificerade tillhandahållare. Numera finns en tjänst - trusted list browser.

Mer detaljer kring ovanstående finns i bifogad presentation.

Volymen på det PTS tar emot är väldigt låg och det finns inga utgivare av certifikat.

Rapport från andra eIDAS-myndigheter

FMV/CSEC

CSEC är Sveriges Certifieringsorgan för it-säkerhet. CSEC intygar att kontroller, via de två privata företag som granskar produkter åt dem, har visat att it-produkter motsvarar definierade krav på IT-säkerhet.

Det finns tre olika typer av certifikat – identitetscertifikat (digitala) som visar vem du är, verksamhetscertifikat som de som utfärdar id-certifikat måste ha samt produktcertifikat som visar att produkterna håller måttet. Vad gäller eIDAS ska CSEC ansvara för certifiering av anordningar för skapande av kvalificerade elektroniska underskrifter och anordningar för kvalificerade elektroniska stämplar. Inget sådant certifikat är gjort ännu då ingen efterfrågat.

Standardisering är viktigt för kravställning vid lagstiftning som reglerar EU:s eller medlemsstats marknad. Det främjar god marknadsutveckling, kan användas vid kravställning vid myndighets upphandling och för att undvika snedvridning av konkurrensen.

Certifiering är viktigt då det är ett intyg att någon tittat på och kontrollerat produkten så den motsvarar kraven. Samma krav ställs och det blir lika villkor för alla. Det finns fyra viktiga organisationer i arbetet med certifiering av säkerhet i it-produkter EU, ISO/IEC, CCRA och SOG-IS MRA. Status i de olika organisationerna gällande förhandlingar, frågor som diskuteras, analyser som görs m.m. finns i bifogade presentation.

De kort som drabbades av ROCA var certifierade. En analys av vad som gick fel är gjord och bl.a. konstaterades att kravbilden hur korten måste vara gjorda angav inte en rimlig algoritm hur RSA – nycklarna skulle genereras. Samhället bör aldrig göra sig beroende av hemmasnickrade kryptolösningar. Det blir fel färre gånger om man använder standard granskad av flera experter. Vi upprepar misstag som egentligen är gamla sanningar. När vi bygger nationell infrastruktur måste vi jobba igenom så varenda detalj blir rätt. Vissa länder och organ visste om sårbarheten tidigare än andra. Det är inte bra med ojämlikhet. Många produkter vi gör oss beroende av innehåller så otroligt mycket kod att det inte går att hitta felen och det fungerar inte att ha det så. De åtgärder CSEC gör i fallet ROCA finns listade i bifogad presentation.

Summering – cybersäkerhetsakten kommer reglera vilka länder vi litar på. Vi måste gå över till att se till att leverantörerna gör rätt istället för att hitta felen.

Frågor/kommentarer:

När det gäller HSM:er – nu kommer Common Criteria med stormsteg. Det kommer FIPS som gör i princip samma sak.

FIPS-systemet är regler och granskning som leds av USA och Kanada. Euroepiska leverantörer tvingas granska en gång och USA en gång. Talaren anser att det är en politisk fråga. Det finns inget formellt granskningsprogram i Europa. Enskilda myndigheter kan bestämma att de litar på FIPS. Borde vi inte då kräva att amerikanarna litar på vårt.

Är det bara gemensamma kriterier mellan Europa och USA som gäller?
Nej, det är lättare att förstå om man talar om relationen mellan Europa och USA men det gäller även Europa- Indien, Europa – Kanada m.fl. alltså alla 28 medlemsstaterna i CCRA.

Inte ens i Europa är vi överens om vi ska dra tillbaka ROCA-certifikatet. CCRA brottas med den här frågan om att dra tillbaka. Ett förslag är att inget certifikat ska ses som giltigt i längre än 5 år, inte som idag då man aktivt måste dra tillbaka.

Kommer det bli en europeisk lista om kryptoalgoritmer?

SOG-IS- gruppen har tagit fram en lista över kryptoalgoritmer vi litar på. Vi ska alltid ha möjlighet att bestämma vilka kryptoalgoritmer vi litar på. Ingen svensk myndighet har ett uppdrag att granska denna lista.

Övriga myndigheter som skulle redogjort under denna punkt – SWEDAC, ESV och MSB hade tyvärr inte möjlighet att medverka idag.

Vad händer internationellt?

En representant från PTS rapporterade från möte i Tallinn och hur de där hanterat sårbarheten ROCA. Estland är en digitaliserad nation som anser det viktigt att bygga upp den nationella it-infrastrukturen. Man har många giltiga e-legitimationer, e-tjänster m.m. ROCA – sårbarheten, påverkade ca 800 000 kort.

Sårbarheten innebär i korthet att den privata nyckeln kan beräknas givet den publika nyckeln och gör att man i en annan persons namn t.ex. kan använda e-tjänster, signera dokument eller stjäla en elektronisk identitet. De åtgärder som vidtagits är bl.a. att åtkomsten till databasen med publika nycklar har strypts, säkra alternativ som mobilt-ID har lyfts fram, samtliga berörda certifikat deaktiverades varefter de så småningom spärrades. Vad man vet har sårbarheten inte nyttjats. Estland blev inte informerade av sin leverantör av ID-kort utan fick endast kännedom om sårbarheten genom informella kanaler. Se mer detaljer i bifogad presentation.

Detta är inte sista sårbarheten utan vi måste lära oss hantera den här typen av risker och våga ”dra i snöret” när något sånt här händer säger Björn.

Näst på tur att informera var e-legitimationsnämnden. Än så länge är det bara Tyskland som anmält eID-system vilket innebär att från 29 sept 2018 måste alla länder inom EU ta emot e-legitimation från Tyskland. I Italien, Spanien, Luxemburg, Ungern och Estland pågår peer-review och den 11 juli tas frågan upp till beslut och med största sannolikhet blir länderna godkända. Utöver dessa länder finns ett antal som säger att de ska anmäla sig. Ganska snart kommer vi ha internationella e-leg som kan gå i systemet. Sverige har inte anmält någo eID-system ännu men det finns minst en intresserad leverantör. Det är mycket dokumentation som ska plockas fram vilket tar tid. Vi hoppas på att man gjort det mesta av jobbet när man blivit godkänd i svenska e-legitimation. eIDAS har legitimering av juridiska personer men vi ser inte att det är tillämpbart mot svensk lagstiftning. I Sverige ser vi det som att en fysisk person alltid företräder en juridisk person.

Frågor/kommentarer:

Hur många eIDAS system kan ett land verifiera ?

Det finns ingen gräns.

Om en svensk myndighet tar emot ett ROCA-kort vem vänder man sig till då?

Vi ser inte att det är ett ROCA-kort. Loggar du in med bank-id kommer en demo sen hur data flödar. Om regress mot t.ex. Spanien får e-legitimationsnämnden vända sig till polisen i Spanien. I art. 6-12 framgår saker kring dessa frågeställningar.

Anslut till den svenska eIDAS-noden!

Talaren började med att fråga hur många av mötesdeltagarna som stöder någon kommun eller myndighet i arbetet med att ansluta till den svenska eIDAS-noden. Det visade sig vara ganska få. Att ansluta till noden är det som är mest bråttom nu då myndigheter och kommuner är skyldiga att kunna ta emot trafik från den 29 september i år. Det är alltså flera hundra organisationer som måste förbereda och anpassa e-tjänsten genom analyser, hantering och val av olika slag samt teckna avtal med e-legitimationsnämnden om anslutning till Sweden Connect och därefter ska metadata anmälas. Nästa steg är sedan att test. Det har funnits en testmiljö under ett års tid. Innan man går in i skarp produktion ska man ha testat i QA-miljö. Det kommer även erbjudas möjlighet för eID-utfärdare och privata parter att ansluta sig till aktörsregistret. Se mer detaljer kring detta i den bifogade presentationen.

En demo i eIDAS webb, som ska ersättas av Sweden Connect, av metadata och hur en inloggning går till följde.

Digital överlåtelse av fastigheter *(Lantmäteriet)*

Digital överlåtelse av fastigheter är inte möjligt i dagens Sverige men vi tittar på det. Lantmäteriet skapar fastigheter. Varje dag beviljas och registreras lagfarter till över 1000 nya ägare till fastigheter. Geodata är information om fastigheter och geografi. Tekniken för att etablera och offentliggöra rätten till land och egendom har tagit stora utvecklingssteg under alla hundratals år det hållit på. Vi går nu från papper till en digital värld och behöver digitala rättshandlingar.

Hur en fastighetstransaktion går till beskrivs. Det krävs inte så mycket identifiering i processerna sälja, köpa och äga och framförallt vid få tillfällen. Lagfartskapningar kan uppstå men talaren har inte hört om sådana på flera år och de som varit tidigare var få. Pappersmässigt är det möjligt att förfalska en lagfart. Lantmäteriet har idag e-ansökan om lagfart. Identifiering sker med bank-ID.

Lantmäteriet har en digital agenda och har jobbat med blockkedjeteknik. Blockkedja erbjuder säkra original. 11 juni är det tänkt att det första köpet med hjälp av blockkedja ska levereras. Det kommer att ske live i Stockholm. Man kommer dock inte att implementera i verksamheten ännu då det fortfarande saknas saker. Vad man vill är att få till stånd en statlig utredning om att göra det möjligt med digitala fastighetsöverlåtelser i Sverige inom rimlig tid.

Vad juridiken ställer för krav och lite om den formelutredning som gjordes 2003 och vad lantmäteriet säger om det digitala alternativet finns formulerat i bifogad presentation.I det digitala alternativet håller sig Lantmäteriet fortfarande till ett dokumentformat som påminner om pdf/word och man kommer nog inte kunna hantera genom blockkedja. Vi får vänta ett tag till innan vi ser de slutliga digitala alternativen. E-ID spelar en stor roll i sammanhanget.

Frågor/kommentarer:

Digitala överlåtelser med blockchain. Någon skillnad gentemot vanligt e-id?

Det finns en identifieringsdel i blockkedjan

För 30 år sedan blev det inget av digitala underskrifter

Skillnaden nu att det kan bli något är att vi fått möjligheten att utreda. Projektet med blockkedjetekniken har visat på att det kan vara möjligt.

Kommer e-underskrifterna att behöva vara kvalificerade eller inte?

Finns svar i utredningen som publiceras sista maj.

Skatteverket gav sig in i detta – kan det vara bouppteckningar?

Kvitton och redovisningar är intressant för skatteverket men inget nämnt om bouppteckningar.

Incidentrapportering *(PTS och e-legitimationsnämnden)*

Incidentrapporteringen är en stor del av tilliten bakom betrodda tjänster. Rapport ska ske till PTS eller annan myndighet om relevant. En incident kan t.ex. vara svagheter i nyckelhantering eller avslöjande av personuppgifter. Det kommer inte in så många incidentrapporter för detta område. I bifogad presentation finns angivet vad det är som ska rapporteras, när och vad rapporten ska innehålla. Det finns även länkar till vägledning för incidentrapportering utfärdade av PTS och ENISA. I dagsläget finns ingen e-tjänst för incidentrapportering men det kan komma om volymen ökar.

Frågor/kommentarer:

Är incidentrapporten offentlig?

Ja, men PTS gör sekretessbedömning om begäran om utlämning inkommer. PTS vill bara ha in den info vi behöver, inget extra. PTS får inte in så många rapporter idag och vill ha fler.

Om incidenten är gränsöverskridande – skicka till den myndighet där du har säte så får myndigheten distribuera vidare. Gäller det ad hoc rapportering av kvalificerad tjänst ska det spridas till de länder som kan vara drabbade. En kvalificerad betrodd tjänst drabbar alltid annat land.

eIDAS innebär en ny del av incidentrapportering. e-leg ska rapporteras till e-legnämnden som har till uppgift att rapportera till andra länder. Vi ska stänga noden så det inte sprids till andra länder därför måste det ske en snabb rapportering.

Frågor/kommentarer

Om det är en falsk underskrift vems är då felet om attributen är fel?

Det finns ingen skyldighet att rapportera men det är ni som först upptäcker att något är fel så en tidig varning som säger att något är fel kan göras. Rutinerna kring rapportering enl. art. 10 är inte klara. Det kommer att komma bättre instruktioner så småningom.

Vem har ansvaret att rapportera till PTS?

E-legitimationsnämnden för incidenter som de kan konstatera. E-legitimationsnämnden jobbar på att samordna incidentrapporteringen med PTS.

Vi vill kunna rapportera till e-legitimationsnämnden när vi mottagit en rapport eller till myndigheterna. Vi vill ha en ansvarig utpekad för incidenthantering på myndigheten att rapportera till och som sedan får ta ansvar för eventuell vidaredistribution.

Avslutning och diskussion

Inga utestående frågor eller förslag på ämnen att ta upp i kommande forum framfördes. Presentationsmaterialet kommer läggas upp på både e-legitimationsnämndens och PTS hemsidor.

Tack till alla deltagare och vi hör av oss till höstens forum.