Undersökning av underskriftslösningar- XBRL Sweden

Sammanställning enkätsvar

Om enkäten
XBRL Sweden genomförde en enkät i syfte att kunna lyfta upp väsentliga områden kopplat till eIDAS förordningen via frågor kopplade till hur de leverantörer som erbjuder signeringslösningar på den svenska marknaden har adresserat vissa av de förutsättningar förordningen innehåller. Svaren i enkäten ska kunna utgöra underlag för en vidare dialog kring hur kraven i förordning ska tolkas och vilka utmaningar och behov som finns och kommer att följas upp med ett seminarium där vi presenterar resultatet samt möjliggör för diskussion och frågor.

Sista svarsdatum var 28 augusti.

Svaren som redovisas nedan är anonymiserade och redovisade fritextsvar är förkortade, för att kunna jämföras utan att det framgår vem som skrivit vilket svar.

Vid frågor gällande enkäten och dess svar, kontakta gärna föreningens ordförande, Björn Rydberg – bjorn.rydberg@se.ey.com

1. Tjänstetyp

På marknaden förekommer en rad olika typer av signeringslösningar som här kategoriseras enligt följande:

Fristående underskriftstjänst enligt tekniskt ramverk från myndigheten för digital förvaltning (DIGG): Denna lösning innebär att användaren bekräftar underskrift genom legitimering av legitimeringstjänst enligt specificerad tillitsnivå. Protokoll för integration i e-tjänst följer DIGG:s tekniska ramverk.

Stämpeltjänst för intygande av underskrift: Denna lösning innebär att det är underskriftstjänstens avancerade underskrift som påförs underskriven handling. Annan information i den underskrivna handlingen intygar vilken eller vilka användare som legitimerats och godkänt underskrift, men dessa personers individuella avancerade underskrifter påförs inte dokumentet.

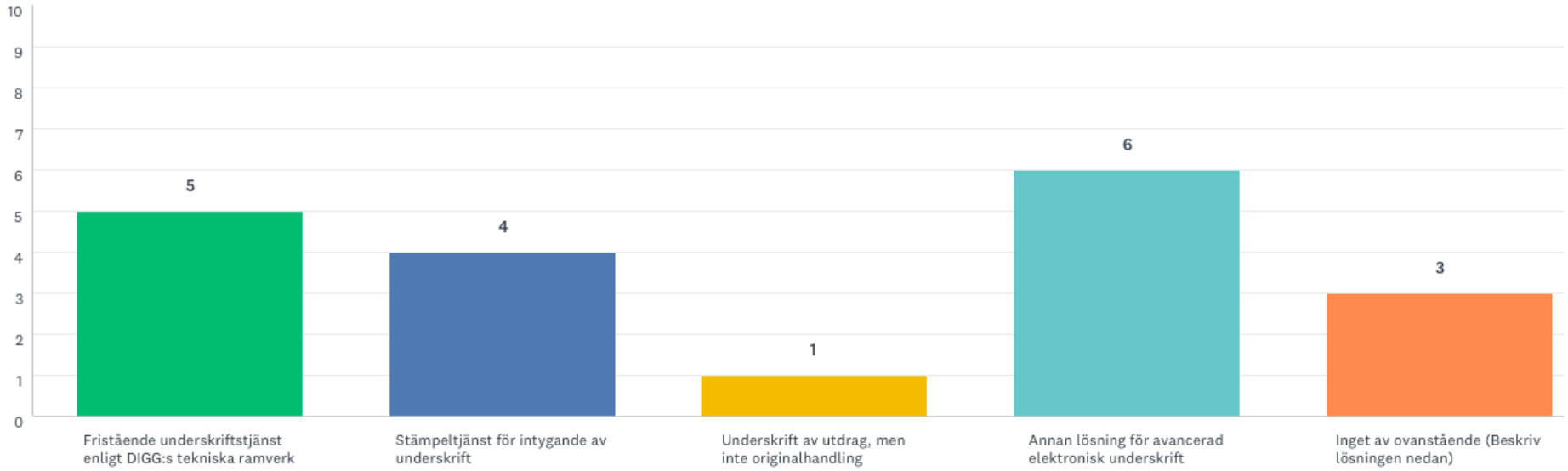
Underskrift av utdrag, men inte originalhandling: Denna lösning tillhandahåller inte möjlighet att skriva under godtycklig handling av formatet XML eller PDF men ger möjlighet att skriva under ett utdrag eller sammanfattning av originalhandlingen som godkänns av användaren vid underskrift.

Annan lösning för avancerad elektronisk underskrift: En lösning som inte är upprättad enligt alternativen ovan, men som ändå gör det möjligt för en användare att skriva under en elektronisk handling där den underskrivna handlingen påförs en avancerad elektronisk underskrift som verifierar användares identitet och som binder originalhandlingen till underskriften.

Vilken, eller vilka alternativ ovan beskriver hur er tjänst är utformad?

- Fristående underskriftstjänst enligt DIGG:s tekniska ramverk
- Stämpeltjänst för intygande av underskrift
- Underskrift av utdrag, men inte originalhandling
- Annan lösning för avancerad elektronisk underskrift
- Inget av ovanstående (Beskriv lösningen nedan)

Svar:



Analys:

En av tjänsterna som sägs uppfylla DIGG:s tekniska ramverk har svar på följdfrågor som inte är förenligt med DIGG:s tekniska ramverk. Rätta antalet här förmodas vara 4.

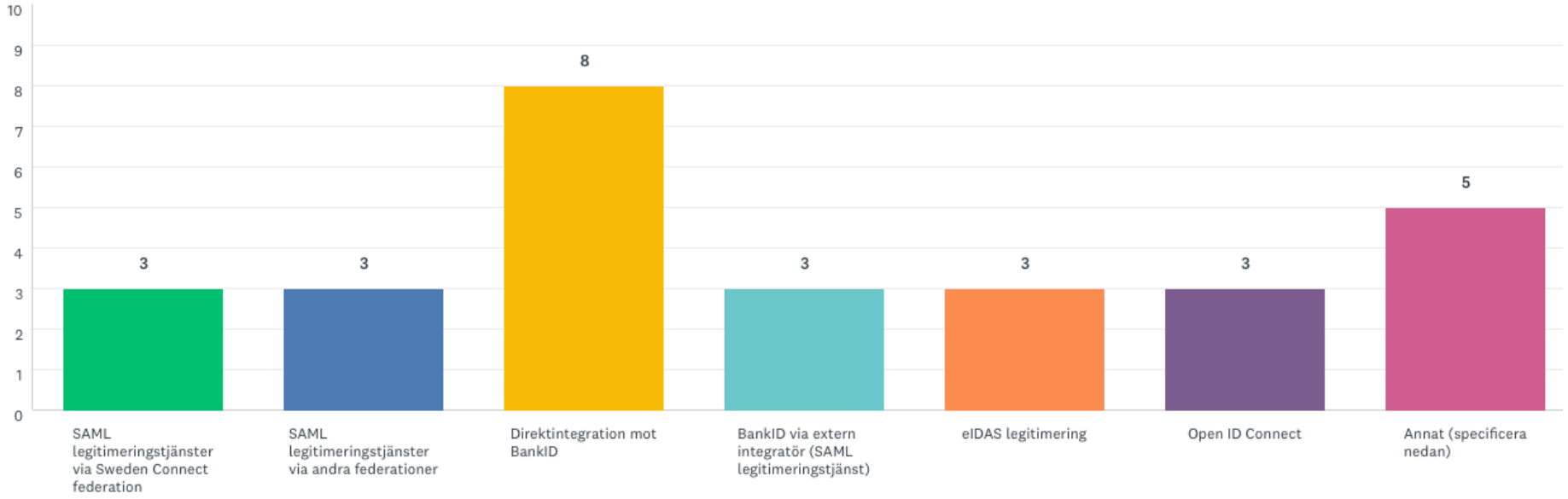
Av de som angivit annan lösning så hänvisar 2 svar till att man inte tillhandahåller en komplett tjänst, utan komponenter som kan användas för att bygga en lösning. Övriga lösningar är inte beskrivna i detalj.

2. Tillämpning av extern legitimeringstjänst

Om er underskriftstjänst tillämpar legitimering med extern legitimeringstjänst, vilka typer av legitimeringstjänster och integrationsmodeller har ni stöd för:

- SAML legitimeringstjänster via Sweden Connect federation
- SAML legitimeringstjänster via andra federationer
- Direktintegration mot BankID
- BankID via extern integratör (SAML legitimeringstjänst)
- eIDAS legitimering
- Open ID Connect
- Annat (specificera nedan)

Svar:



Analys:

Några har angett stöd för eIDAS legitimering utan att ange stöd för SAML legitimering via Sweden Connect, vilket är en förutsättning för eIDAS legitimering. Å andra sidan har en leverantör som genom sina svar demonstrerar stöd för eIDAS legitimering totts detta inte markerat stöd för eIDAS legitimering. Dessa två fel tar ut varandra och gör redovisade siffror korrekta i detta avseende.

Svaren här visar på att samtliga redovisade lösningar tillämpar underskrift med stöd av legitimering med extern legitimeringstjänst. Det visar intressant nog att det ”gamla” sättet att skriva under direkt med sin e-legitimation i lokal miljö i stort sett försvunnit om man skall tro resultatet av denna enkät.

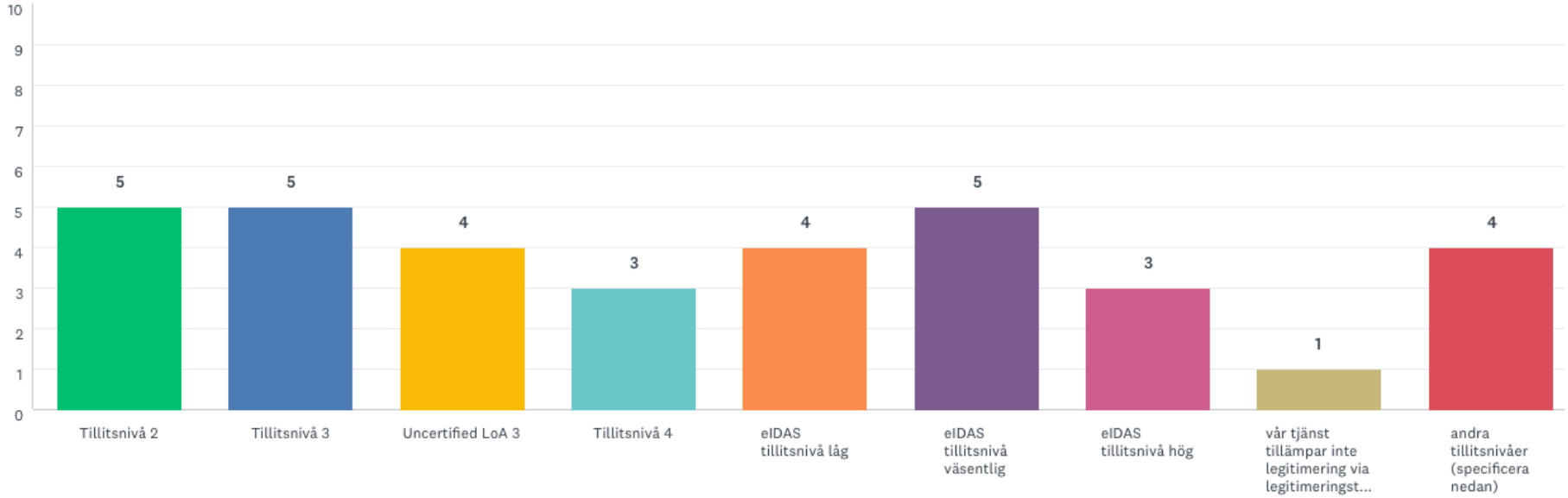
3. Tillitsnivåer

eIDAS-förordningens tillitsnivåer och det svenska Tillitsramverket bygger på samma internationella standard (ISO/IEC 29115). Inom eIDAS finns de tre olika tillitsnivåerna “låg”, “väsentlig” och “hög”. “Låg” ställer något lägre krav än den svenska tillitsnivån 2. “Väsentlig” motsvarar Sveriges tillitsnivå 3. ”Hög” kan likställas med den svenska tillitsnivån 4, med undantag för att ett personligt besök krävs vid förnyelse av en e-legitimation på den svenska tillitsnivån 4. Utöver detta har DIGG i sitt tekniska ramverk specificerat en identifierare för specialfallet ”Uncertified LoA 3” vilket kan tillämpas om en legitimeringstjänst åtnjuter ett allmänt förtroende på tillitsnivå 3, men där legitimeringstjänsten formellt inte är certifierad för denna nivå. Detta används idag av vissa legitimeringstjänster när legitimering sker via BankID.

Om er tjänst tillämpar legitimering av användare via legitimeringstjänst som metod när användaren bekräftar underskrift, vilka tillitsnivåer kan er tjänst hantera:

- Tillitsnivå 2
- Tillitsnivå 3
- Uncertified LoA 3
- Tillitsnivå 4
- eIDAS tillitsnivå låg
- eIDAS tillitsnivå väsentlig
- eIDAS tillitsnivå hög
- vår tjänst tillämpar inte legitimering via legitimeringstjänst
- andra tillitsnivåer (specificera nedan)

Svar:



Analys:

Här finns en stark korrelation mellan de tjänster som tillhandahåller fristående underskriftstjänst enligt DIGG:s tekniska ramverk och de tjänster som stödjer såväl DIGG:s tillitsnivåer såväl som eIDAS tillitsnivåer.

Några tjänster förefaller deklarerar stöd för tillitsnivå 3 trots att legitimering sker med BankID. Då BankID vid utskicket av denna enkät ännu ej var godkända för tillitsnivå 3 så borde dessa istället ha markerats som uncertified LoA 3.

Notera dock att BankID, strax efter det att svaren till denna enkätundersöknings inkommit, blev godkända enligt tillitsnivå 3 vilket gör att det inom en snar framtid kommer bli möjligt att skriva under med BankID enligt tillitsnivå 3. I en del fall kommer detta dock att kräva att även den mellanliggande legitimeringstjänst, som förmedlar legitimering med BankID, uppfyller kraven för tillitsnivå 3.

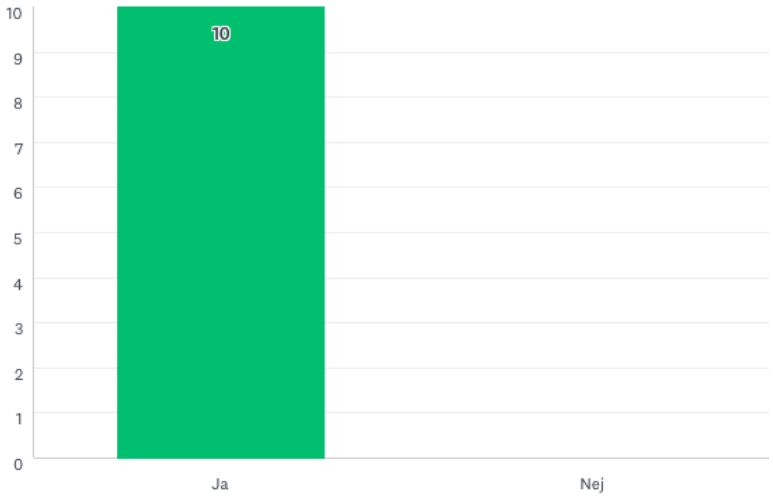
4. Avancerad elektronisk underskrift

En återkommande fråga kopplat till digital signering av specifikt årsredovisningar och revisionsberättelser har varit huruvida använd lösning uppfyller kravet på ”Avancerad Elektronisk Underskrift” (se 2 kap. 7 § ÅRL samt eIDAS-förordningen artikel 3 och artikel 26), dvs:

- Underskriften är unikt knuten den person som har undertecknat handlingen
- Undertecknaren skall kunna identifieras genom underskriften
- Underskriften har skapats med nyckel som med hög grad av tillförlitlighet endast kan användas för att skapa underskrifter koppat till undertecknaren
- Den binder innehållet i den underskrivna handlingen till underskriften på ett sådant sätt att efterföljande ändringar av den underskrivna handlingen kan upptäckas.

Anser ni att er lösning uppfyller de krav som ställs på avancerad elektronisk signatur?

Svar:



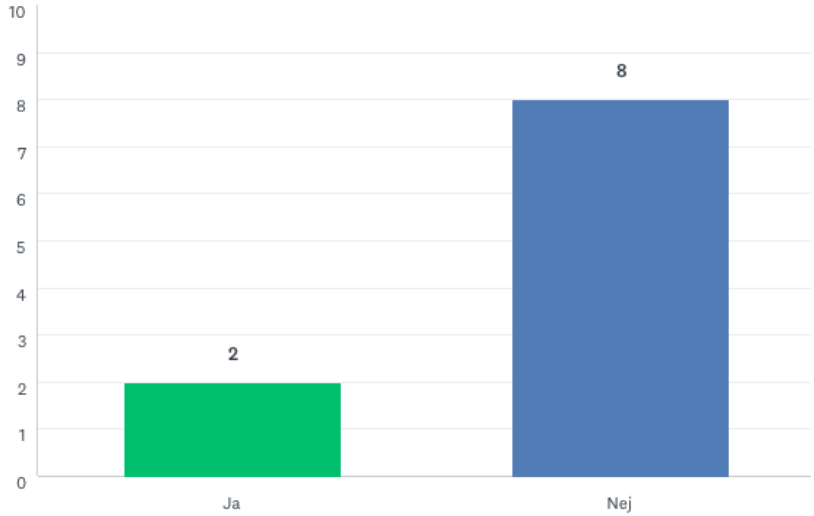
Analys:
Här svarar alla leverantörer utom 1 Ja på frågan även om stapeln ovan anger att alla svarat ja. En av dessa skriver i sin kommentar att man inte vet hur signaturen skall klassas då man inväntar svar från Bolagsverket.

Ett flertal tjänster anger att man har en tjänst som tillämpar en stämpeltjänst som intygar att handlingen skrivits under av en person. Här kan finnas ett logiskt dilemma eftersom en sådan tjänst kan anses tillhandahålla en avancerad underskrift. Problemet är bara att det är underskriftstjänstens avancerade underskrift/stämpel och inte användarens avancerade underskrift. Detta för att underskriftscertifikatet innehåller tjänstens identitet och inte användarens identitet. Så som frågan var avsedd så är inte detta att betrakta som användarens avancerade underskrift. Med detta taget i beaktande är det korrekta svaret på denna fråga förmodligen att 6 av 10 tjänster tillhandahåller avancerad underskrift på det sätt som frågan anger.

5. Kvalificerad elektroniska underskrift

Kan er underskriftstjänst användas för att skapa en kvalificerad elektronisk underskrift i enlighet med eIDAS regleringen?

Svar:



Analys:
Flera svar indikerar att det i dagsläget finns en obefintlig alternativt mycket begränsad marknad för kvalificerade underskrifter vilket i sin tur förmodligen beror på att vi inte har en tradition av att använda denna nivå. Flera aktörer säger att man skulle kunna tillhandahålla kvalificerade underskrifter om det bara fanns ett underlag. Den främsta anledningen till den magra efterfrågan förefaller vara att det är;

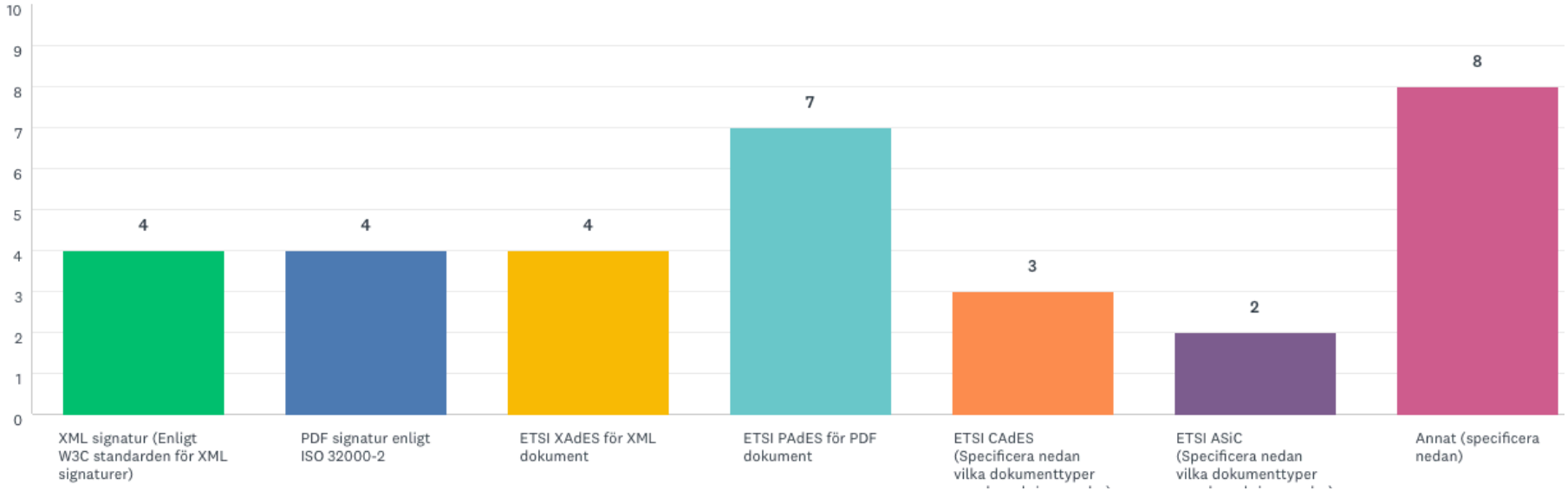
- kostnadsdrivande,
- det saknas relevanta formkrav som kräver elektroniska underskrifter, och;
- vi har lång och god erfarenhet av att använda avancerade underskrifter.

6. Underskriftsformat

Vilka underskriftsformat kan skapas med er underskriftstjänst?

- XML signatur (Enligt W3C standarden för XML signaturer)
- PDF signatur enligt ISO 32000-2
- ETSI XAdES för XML dokument
- ETSI PAdES för PDF dokument
- ETSI CAdES (Specificera nedan vilka dokumenttyper som kan skrivas under)
- ETSI ASiC (Specificera nedan vilka dokumenttyper som kan skrivas under)
- Annat (specificera nedan)

Svar:



Analys:

PDF dominerar som format vilket troligen kan förklaras med att vi ser 2 olika sorters underskriftstjänster som dominerar, där den ena typen stödjer XML och PDF medan den andre endast hanterar PDF. Den första typen avser underskriftstjänster som integreras med e-tjänster för att signera deklarationer, ansökningar mm där detta inte först omvandlas till ett PDF dokument innan underskrift, medan den andra typen av tjänst innebär att man kan skriva under handlingar, avtal och deklarationer som först omvandlats till PDF innan underskrift.

I vissa fall tillhandahålls CAdES och ASiC. Dessa skiljer sig från XML och PDF signering på så vis att XML och PDF är dokumentformat medan CAdES och ASiC bara är dataformat för att signera data, vilken som helst. CAdES används dessutom som inre signaturformat vid signering av PDF och vi kan inte vara säkra på om den som signerar PDF även anser att man tillhandahåller CAdES även om det inte är som ett separat format.

7 av 10 stödjer någon form av ETSI format för XML eller PDF signering, och 4 av dessa stödjer endast ETSI formaten. Detta är en ganska intressant trend från tidigare väldigt blygsam användning av ETSI formaten. Främsta anledningen till detta förmodas vara en allmän kravbild från EU genom eIDAS förordningen samtidigt som flera tjänster använder EU kommissionens DSS bibliotek som endast stödjer ETSI signaturer.

7. Stöd för långtidsvalidering

ETSI signaturformat specificerar profiler (LT och LTA) som kan användas för att i efterhand utöka en befintlig underskrift med valideringsdata som kan användas för att validera underskriften i framtiden. Exempel på sådan valideringsdata är information om spärrstatus för certifikat, tidsstämplar mm.

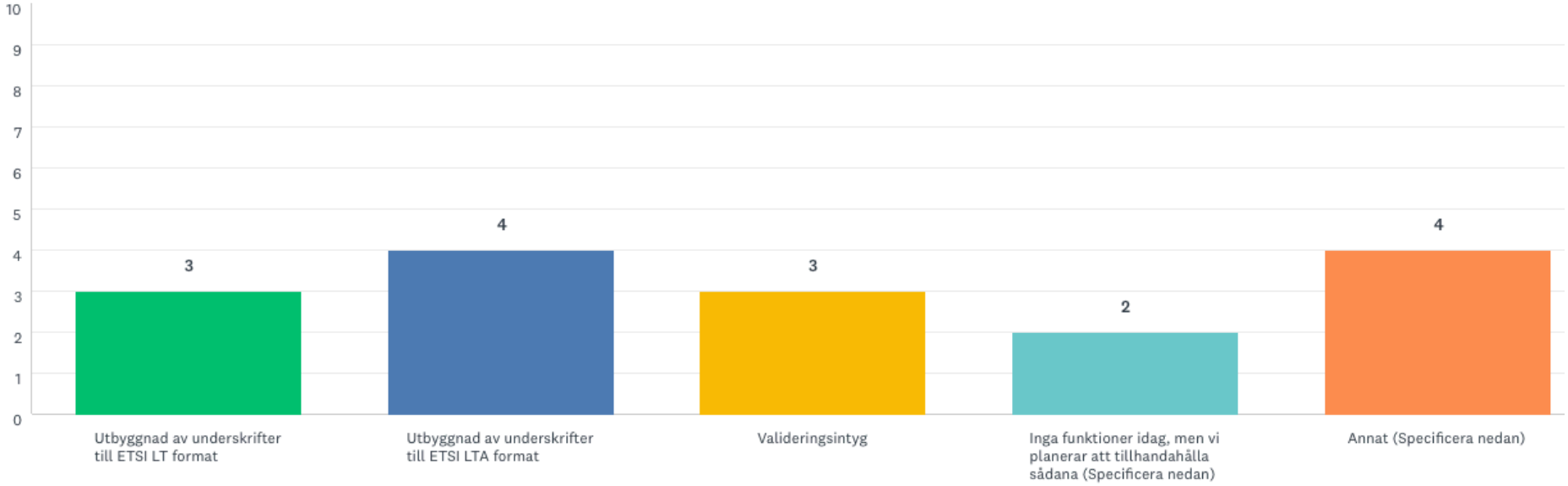
Andra vanliga lösningar för långtidslagring är extern loggning av det faktum att ett dokuments underskrift har kontrollerats.

DIGG har en pågående aktivitet för att utveckla och testa en lösning för valideringsintyg som kan förbättra möjligheten att skapa intyg om tidigare validering som alternativ till komplexa standarder för långtidsvalidering.

Tillhandahåller er tjänst några funktioner för att underlätta validering av elektroniska underskrifter i framtiden?

- Utbyggnad av underskrifter till ETSI LT format
- Utbyggnad av underskrifter till ETSI LTA format
- Valideringsintyg
- Inga funktioner idag, men vi planerar att tillhandahålla sådana (Specificera nedan)
- Annat (Specificera nedan)

Svar:



Analys:

4 tjänster anger att man kan bygga ut sina underskrifter till ETSI LTA där 3 av dessa även stödjer det enklare LT formatet. Dessa leverantörer är av naturliga skäl bland de som redan stödjer ETSI formaten. Och flera av dessa verkar använda EU kommissionens DSS bibliotek för att åstadkomma detta.

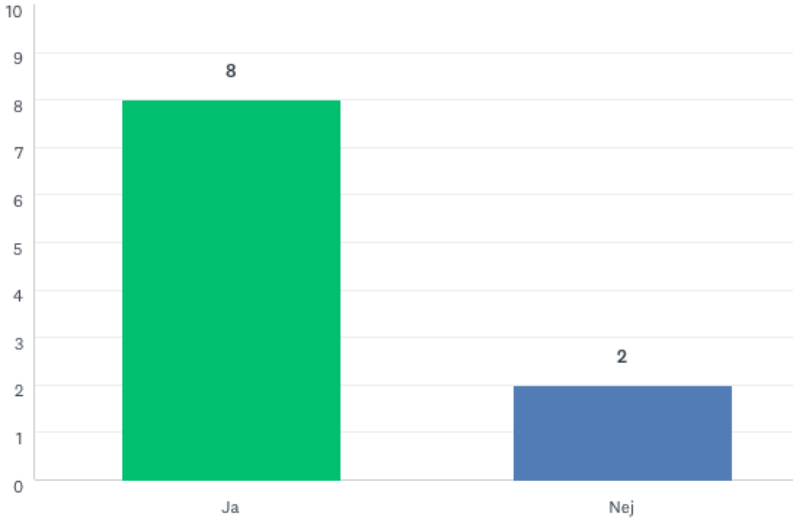
Hälften av alla svar anger att man inte har långtidsvalidering av själva underskriften, men några av dessa anger trots detta alternativa lösningar så som blockkedja eller andra leverantörsspecifika lösningar.

3 leverantörer anger att man antingen stödjer eller planerar att stödja validering med stöd av valideringsintyg enligt de normer som DIGG för närvarande utvecklar och testar.

8. Validering av underskrifter

Tillhandahåller ni även funktioner för att kunna validera elektroniskt underskrivna handlingar?

Svar:



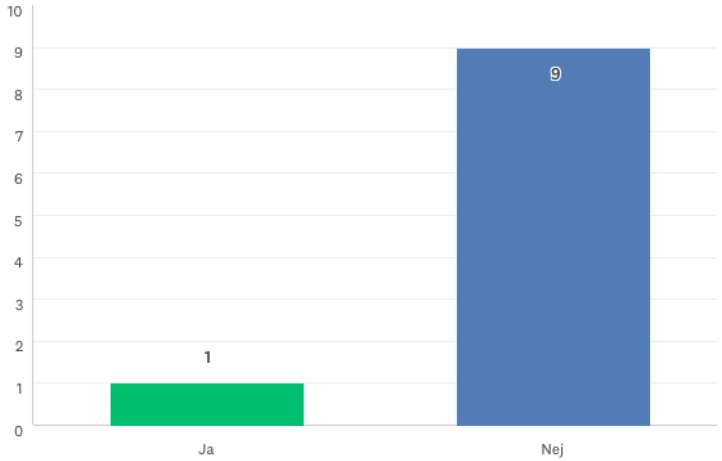
Analys:

Av de två som svarat nej så anger den ena att valideringstjänst bör ligga hos oberoende part medan den andre har planer som ännu ej konkretiserats. Flera leverantörer har integrerat validering i det allmänna API:et mot hantering av underskrift så att både processen att skriva under handlingar och att validera dessa sker genom ett och samma API för e-tjänsten. En av de som svarat ja anger att man har en manuell process för validering/verifiering av underskrift via sin support, vilket bör räknas som ett nej i denna fråga.

9. Beroende av valideringstjänst

Om ja, är kunden beroende av er portal/server för att kunna validera att avancerad elektronisk underskrift har gjorts och säkerställa att signerat dokument inte har förändrats efter signering?

Svar:



Analys:

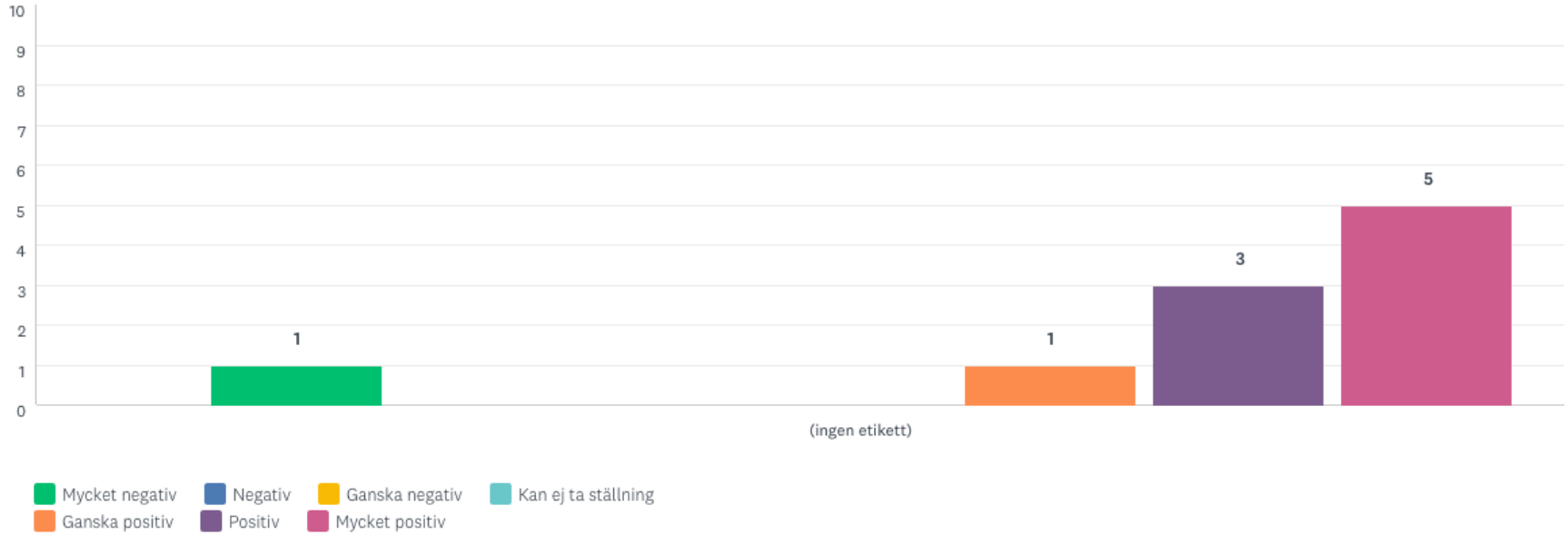
Den typ av underskrifter som enkäten främst handlar om är standardiserade och kan valideras av vem som helst som har tillit till utfärdaren av underskriftscertifikat. Det är därför som förväntat att en övervägande majoritet av alla tjänster inte kräver att den egna valideringstjänsten används, utan att validering kan göras av var och envar med lämpliga verktyg.

Den enda leverantör som svarat ja på denna frågan representerar en tjänst som deklarerar att man inte tillämpar traditionella signaturformat och att man istället tillämpar en annan lösning.

10. Certifiering

Hittills sker certifiering av lösningar endast av kvalificerade betrodda tjänster (PTS). Hur ser ni som leverantör på att en oberoende part (myndighet) får i uppdrag att även certifiera lösningar på nationell nivå så som lösningar för avancerad elektronisk underskrift?

Svar:



Analys:

Alla utom en leverantör är positiv till en nationell certifiering av lösningar för elektronisk underskrift. Den som anser att detta skulle vara mycket negativt anför att den är typen av certifieringar inte får vara en svensk angelägenhet som driver kostnader för svenska leverantörer som sedan inte kan användas inom resten av EU.

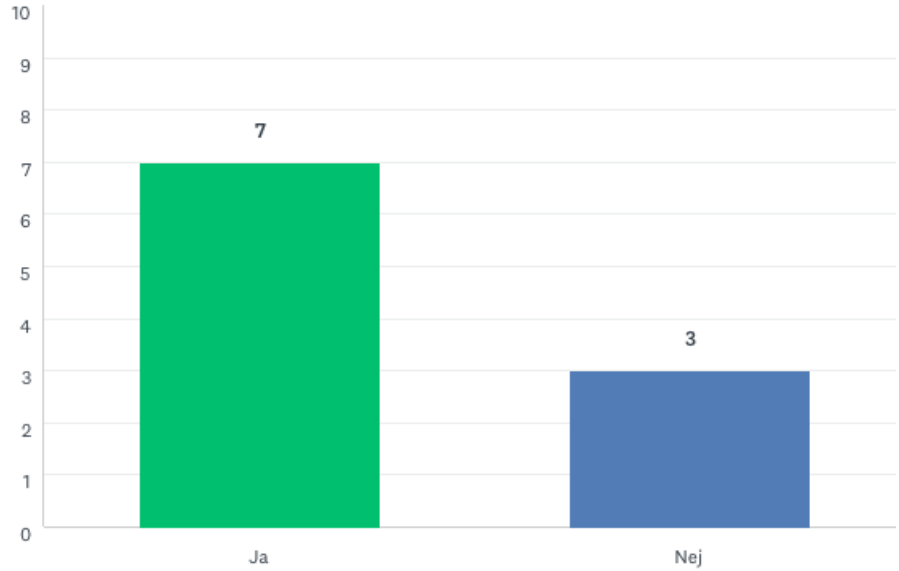
Ett av grundproblemen här är att det saknas EU gemensamma standardiserade normer för certifiering eller kvalitetsmärkning av icke kvalificerade underskriftstjänster och betrodda tjänster i allmänhet.

De flesta är positiva eftersom det trots allt skulle göra det lättare att möta svenska kunder om man har gemensamma riktlinjer att förhålla sig mot som man dessutom kan demonstrera att man följer. Många har upplevt en svårighet att tolka kraven som ställs av myndigheter som ex Bolagsverket vad gäller vad som anses vara eller inta vara en godkänd avancerad underskrift på inskickad elektronisk handling.

11. Dokumentation

Tillhandahåller ni dokumentation som, utöver funktionalitet i er lösning, även beskriver hur denna hanterar uppfyllnad av deklarerad säkerhetsnivå, certifikatpolicy samt relevanta krav från eIDAS regleringen?

Svar:



Analys:

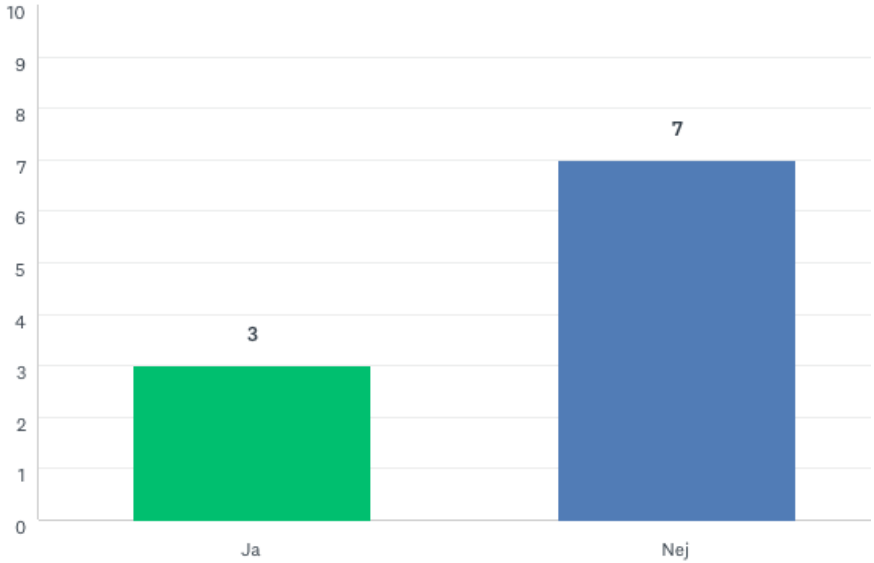
De som svarat nej på denna fråga tillhör en av följande kategorier:

- Man tillhandahåller inte en traditionell underskriftslösning med standardiserade underskriftsformat
- Man har en lösning som är så djupt integrerad med BankID att man hänvisar till BankID:s dokumentation
- Man tillhandahåller en programvara som kan användas för att bygga en tjänst, men tillhandahåller ingen tjänst själva

12. Garanti

Kopplat till fråga 11, utfärdar ni någon garanti eller motsvarande till era kunder kopplat till uppfyllnad av deklarerade säkerhetskrav.

Svar:



Analys:

De flesta som svarat nej anser att detta är en fråga som hanteras genom de avtal/ramavtal som upprättas med kunden och därför har man inga separata garantier av något slag, men att detta inte innebär att man inte lämnar några garantier eller tar något ansvar för sin tjänst.

En fri tolkning av dessa svar är att vi i Sverige inte har en tradition av att lämna garantier gentemot en tredje förlitande part för att täcka eventuella förluster förorsakat av felaktighet i en underskrift eller en legitimering. Däremot lämnar man i stort sett alltid garantier i bilaterala avtal mot kund.

13. Behov för en fortsatt positiv utveckling i Sverige

Allmänt, och för möjlig kommunikation till pågående utredning ”Utredningen om betrodda tjänster - I 2020:01 Ökad och standardiserad användning av betrodda tjänster i den offentliga förvaltningen”, vilka behov ser ni i form av samverkan myndigheter-näringsliv, riktlinjer, ansvar m m.

Svar:

- Behov av standarder, certifieringar och tydliga krav tillhandahållna av oberoende part.
- Vi är generellt positiva till att det upprättas standarder, certifieringar och förtydligande av kravbilder. Marknaden skulle nog må bra av en oberoende part som håller i detta.
- DIGGs arbete med godkända underskriftstjänster måste tas bort. Det förhindrar digitalisering.
- Det är av stor vikt att Offentlig förvaltning etablerar lösningar som det privata näringslivet också kan nyttja. Det är av stor vikt att det inte utvecklas egna nationella lösningar utan att det är de internationella standarderna som följs.
- Vi ser generellt sett ett stort behov av att bygga end-to-end-digitala flöden inklusive korrekt underskrivna digitala beslut.
- För att olika organisationer skall kunna validera och lita på andras information är det extremt viktigt att standarder följs och att man inför tillitssystem som är dokumentorienterade (EJ systemorienterade). Vi ser många verksamheter inför system där man kommer få ha kvar databaser och system på datorer "i källaren" LÅNGT efter att man bytt systemleverantör och LÅNGT efter att support och uppgraderingar tillhandahålls.
- Ett självbärande dokument som innehåller all information inklusive det som behövs för att validera dess äkthet kan skickas,
- arkiveras och överleva systemskiften.
- Tydlig kravställning för olika tillitsnivåer.
- Det finns ett antal områden där det råder gråzoner, så som tex validerings policy, brist på trustlist på utfärdare i Sverige med mera med mera. Därför är samverkan inom Sverige mycket viktig.
- Vi måste förhålla oss till det som standardiseras inom EU och det som specificeras inom ramen för eIDAS förordningen så att de lösningar och tjänster som vi tar fram är gångbara även utanför Sveriges gränser. Att definiera en egen svensk certifiering för att ersätta eIDAS certifiering som kvalificerad tjänst medför onödigt dubbelarbete.

14. Allmänna kommentarer

Har ni några allmänna kommentarer till andra områden/frågor som borde aktualiseras och som kan vara relevanta att fokusera vid ett kommande seminarium för att gå igenom resultatet av enkäten? Samt, hur ser ni på initiativet från Föreningen XBRL Sweden till att ta fram denna enkät?

Svar:

- Denna enkät är bra då den får till följd att kunskapen ökar. Den borde egentligen ha utförts av DIGG för länge sedan.
- Ett arbetsområde som vi saknar initiativ inom är en lösning för att rendera/visa och koppla XML till en eller flera elektroniska underskrifter. Dagens lösning (för t.ex. Årsredovisning) att separera det som bearbetas (XML) från det som undertecknas (PDF/papper) är inte den ultimata då det kan uppstå avvikelser, inte är kostnadseffektiv och ger brister i tillförlitlighet.
- Jättebra att ni gör detta arbete, men det är viktigt att det görs på rätt sätt. Det är tyvärr väldigt snårigt i denna bransch med begrepp och tillvägagångssätt.
- Vi har nått långt med Digital inlämning årsredovisning och XBRL som format för dessa. Och nu digital signering som en följd av det. Nästa stora är SBR - att plocka ner den, så vi ser vad i kan göra för den enskilda lilla företagaren, idag är den fortfarande på en väldigt hög nivå, och ej synkad med NSG initiativet. Hitta nya fokusområdet för XBRL gruppen 2021.
- Mycket bra initiativ då marknaden i Sverige är något obalanserad avseende vilka lösningar som faktiskt uppfyller kraven för avancerade underskrifter.
- Ett bra initiativ, vi ser att det varierar ganska mycket mellan länder i Europa så om vi har en samsyn i Sverige är det värdefullt.