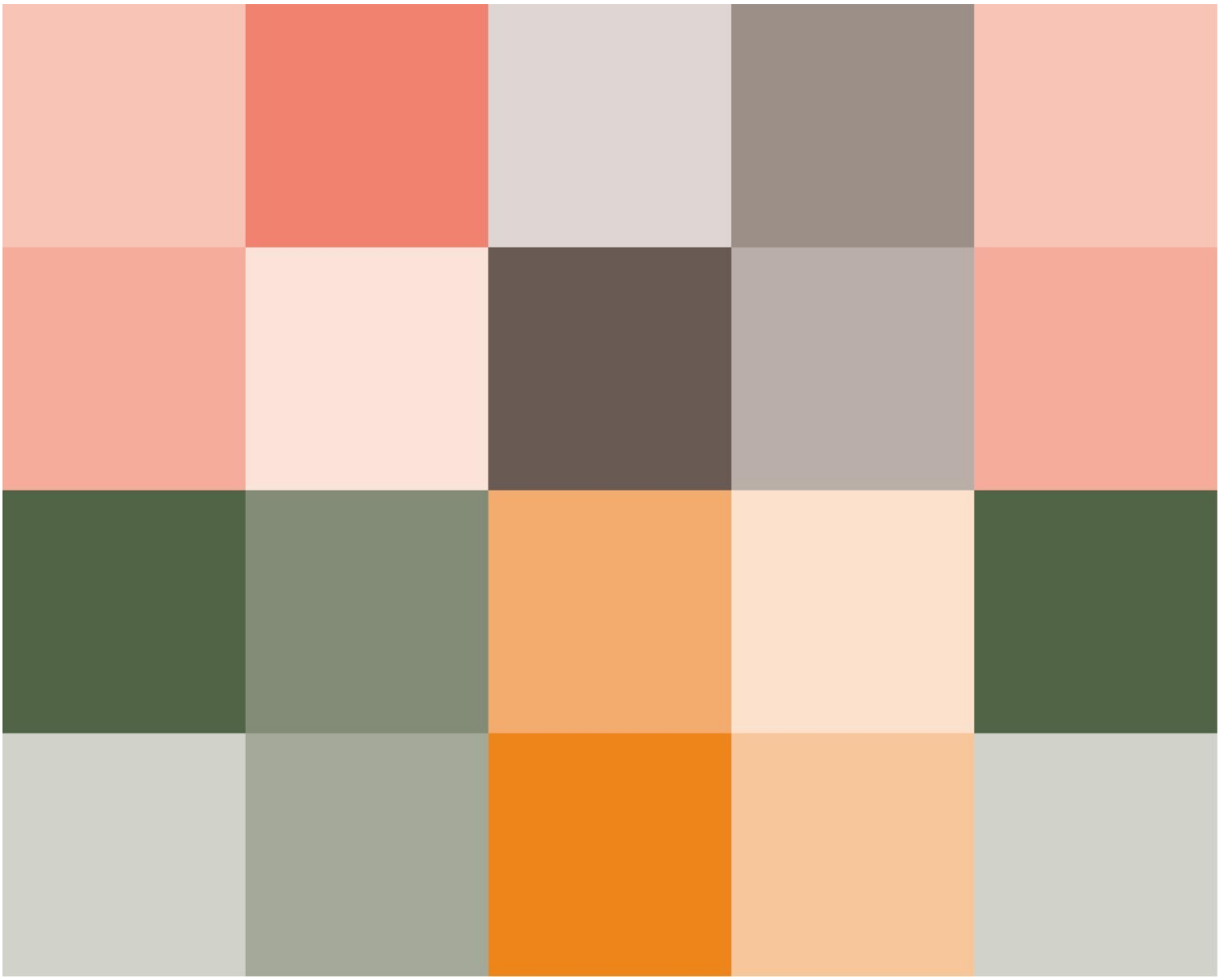

Normativ specifikation

Fristående Underskriftstjänst

Icke funktionella krav

Version 1.40

MYNDIGHETEN FÖR DIGITAL FÖRVALTNING
Agency for Digital Government

Innehållsförteckning

Versionshantering

Version	Datum	Beskrivning	Sign
1.00	2013-11-01	Första fastställda versionen av icke funktionella krav	SB
1.20	2015-09-15	Krav på kryptering i externa förbindelser avsnitt 4.2.1 korrigerat (TSL 1.1 ska gälla). Vissa mindre språkliga ändringar i avsnitt 2 och 2.1. Referens till avsnitt i Tjänstespecifikation för underskriftstjänst korrigerat.	SB
1.30	2018-08-01	Språkliga uppdateringar och förtydliganden. Knytningar till Svensk e-legitimation borttaget. Avsnitt 2 och 3 är nya. Avsnitt 4 är också nytt med förtydligande när det gäller ansvar för underleverantörer. I avsnitt 5 är totalt behov inom offentlig sektor borttaget och tillagt är förtydligande om att stöd för bråd tid ska finnas. Avsnitt 5.1, förtydligande avseende externa processer. Avsnitt 6.3 förtydligande om ansvar när det gäller rapportering av incidenter och statistik.	SB
1.40	2020-04-22	Dokumentet inlagt i DIGGs dokumentmall och E-legitimationsnämnden ändrat till DIGG. Underskriftstjänst ändrat till fristående underskriftstjänst. Förtydliganden har gjort i avsnitt 4 om underleverantörer, administrativ säkerhet avsnitt 6.1.1, 6.2,1 samt 6.2.2 samt avsnitt 7.1.2 om skydd i utvecklings- och testmiljö.	SB

1 Inledning

De krav som specificeras i detta dokument ska gälla för fristående underskriftstjänst (i det följande även benämnt underskriftstjänsten).

Icke funktionella krav avser krav på tillgänglighet, kapacitet, säkerhet och motsvarande. Funktionella krav på underskriftstjänsten framgår av tjänstespecifikationen för densamma.

2 Omfattning

Detta dokument är en del av den normativa specifikationen för fristående underskriftstjänst vilken sammantaget omfattar de krav som ställs på fristående underskriftstjänst.

Den normativa specifikationen för fristående underskriftstjänst omfattar följande dokument:

- Normativ specifikation fristående underskriftstjänst
- Policy fristående underskriftstjänst
- Tjänstespecifikation fristående underskriftstjänst
- Icke funktionella krav fristående underskriftstjänst (detta dokument)

3 Definitioner

De definitioner som framgår av dokumentet Normativ specifikation fristående underskriftstjänst gäller.

4 Underleverantör

Leverantören av underskriftstjänsten kan använda underleverantör för att tillhandahålla hela eller delar av tjänsten. Att använda underleverantör fråntar inte leverantören ansvar för tillhandahållande av tjänsten. Leverantören har ett helhetsansvar för tjänsten och ansvarar för underleverantörens arbete såsom sitt eget.

Med underleverantör avses en juridisk person som leverantören anlitar för att utföra hela eller delar av underskriftstjänsten. Underleverantören ska fullgöra sina delar av tjänsten enligt den normativa specifikationen för fristående underskriftstjänst.

Leverantören ska ha skriftligt avtal med underleverantör som utför väsentlig del av tjänsten. Med väsentlig del avses stor eller viktig del av tjänsten eller del som påverkar eller kan påverka informationssäkerheten i tjänsten. Exempel på väsentliga delar är drift av tjänsten, behandling av personuppgifter, viktig funktionell del eller säkerhetsrelaterad funktion i tjänsten.

Avtalet ska visa att leverantören har den kontroll som krävs för att säkerställa att de krav som finns på tjänsten uppfylls. Avtalet ska säkerställa att de krav som framgår av den normativa specifikationen för fristående underskriftstjänsten är väl kända och följs av underleverantören i relevanta delar. Varje

underleverantör ska ha god kunskap om och följa de krav som ställs på tjänsten genom de policyer, regler och processer som leverantören har för tjänsten.

Leverantören och dess underleverantörer bildar den organisation som tillhandahåller tjänsten, detta benämns också för den verksamhet som tillhandahåller tjänsten. De krav som framgår av avsnitt 6 gäller för den organisation som tillhandahåller tjänsten.

Det ska finnas en beskrivning över den organisation som tillhandahåller tjänsten inklusive de parter som ingår i organisationen och deras respektive ansvar.

Kund ska ha möjlighet att teckna avtal direkt med såväl leverantör som underleverantör avseende till exempel behandling av personuppgifter.

5 Tillgänglighet och kapacitet

Varje enskilt avrop/leverans ställer krav på underskriftstjänsten avseende tillgänglighet och kapacitet. Tjänsten ska kunna skala för att tillgodose de behov som kunden ställer krav på.

Tjänsten ska stödja tillämpning av bråd tid. Under bråd tid ska tjänsterna vara förbereda och bemanning vara på plats så att tjänsterna i princip kan upprätthållas utan avbrott med överenskommen kapacitet.

5.1 Svarstider

Följande krav på svarstider ska gälla som riktvärden för underskriftstjänsten.

Svarstider ska vara max 3 sekunder i 90 % av fallen.
Svarstid i lågt belastad tjänst ska vara max 0,3 sekunder.

Med lågt belastad avses här en transaktionstäthet på upp till två underskrifter per sekunden. Krav på svarstid avser tjänsten i sin helhet, inte per kund. Detta innebär att om det finns flera kunder som använder tjänsten och tjänsten belastas sammantaget mer än med två underskrifter per sekund, kan tjänsten inte betraktas som långt belastad av någon kund.

Krav på svarstid avser den sammanlagda tiden som åtgår i de processer som Leverantören av underskriftstjänsten ansvarar för. Det vill säga tid för externa processer ingår inte i den svarstiden som avses här. Med externa processer avses här sådan funktion som ligger utanför den funktion som framgår av den normativa specifikationen för fristående underskriftstjänst, till exempel utställande av identitetsintyg som ska användas vid underskrift.

Fördröjningar i de förbindelser som Leverantören använder för att ansluta underskriftstjänsten till internet ska inkluderas i den svarstid som Leverantören ansvarar för.

6 Administrativ säkerhet

6.1 Policy och regelverk

6.1.1 Policy och processer

Leverantören av underskriftstjänsten ska ha ett dokumenterat och infört ledningssystem för informationssäkerhet som omfattar den verksamhet som tillhandahåller tjänsten. Det ska finnas säkerhetspolicy, dokumenterade processer och rutiner som omfattar informationssäkerhetsarbetet, hantering av risker, uppföljning och förbättring av informationssäkerheten. Ledningssystemet ska vara baserade på ISO-27001 eller likvärdigt.

Säkerhetsarbetet ska omfatta samtliga förebyggande skyddsåtgärder inom säkerhet, riskhantering, krishantering och beredskap.

Leverantören ska dokumentera mål och riktlinjer för säkerheten i IT-miljöer från anskaffning till avveckling.

6.1.2 Säkerhetsorganisation

Det ska finnas en säkerhetschef eller motsvarande hos Leverantören med ansvar för informationssäkerhet och teknisk säkerhet för den verksamhet som omfattar att tillhandahålla underskriftstjänsten.

6.1.3 Roller och ansvar

Det ska finnas en tydlig beskrivning av roller och ansvar gällande skydd av all information som ingår i den verksamhet som omfattar att tillhandahålla underskriftstjänsten.

6.2 Rutiner

6.2.1 Riskanalys

Det ska upprättas en riskanalys gällande hot mot verksamheten som omfattar att tillhandahålla underskriftstjänsten som ska ligga till grund för säkerhetsarbetet. Riskanalyser ska genomföras med återkommande intervall. Som underlag för riskanalysen ska finnas en krav- och intressentanalys och uppföljning av riskanalysen ska innefatta en värdering av vidtagna åtgärder och ett formellt utverkande av riskägarens acceptans av kvarvarande risk.

Sker förändringar i verksamheten som omfattar att tillhandahålla underskrifts-tjänsten som är eller kan vara av betydelse för säkerheten ska en förnyad riskanalys genomföras.

6.2.2 Uppföljning/revision

Leverantörens styrning och ledning av informationssäkerhetsarbetet och den egna internkontrollen är centrala delar för att säkerställa leverantörens efterlevnad gentemot ställda krav över tid. Revision av ledningssystemet och säkerheten i tjänsterna ska genomföras med kontinuerliga intervaller enligt plan. Den som utför revision ska har relevant kompetens samt vara oberoende till den verksamhet som hanterar underskriftstjänsten.

6.2.3 Åtkomstskontroll

Innan personal ges åtkomst till systemet ska denne vara registrerad som behörig administratör och ha fått utbildning i de regler och säkerhetsinstruktioner som gäller för systemet.

Allokering och användning av rättigheter ska begränsas och kontrolleras. Administratör ska ges en behörighetsprofil som endast medger åtkomst till de resurser i systemet som krävs för att lösa dennes arbetsuppgifter.

Alla administratörer ska ha en unik identifierare för personlig användning så att aktiviteter kan spåras tillbaka till ansvarig administratör. Autentisering av administratör ska vara utformad så att det med säkerhet går att koppla ihop en genomförd aktivitet med den unika administratören.

Det ska finnas en förteckning över vilka administratörer som har behörighet att använda systemet. Denna förteckning ska sparas för att spårbarhet ska kunna uppnås i efterhand.

6.3 Övervakning och kontroll

Leverantören av underskriftstjänst ska ha en process för informationsspridning i samband med driftavbrott och incidenter.

Säkerhetsincidenter som påverkar eller kan påverka verksamheten som omfattar att tillhandahålla underskriftstjänsten ska rapporteras utan oskälig fördröjning till part och i format som DIGG bestämmer.

Incidenter som uppstår i anslutning till underskriftstjänsten, som är eller kan vara av den art att incidenten uppstår hos eller påverkar annan aktör inom eID-systemet, ska rapporteras utan oskälig fördröjning till part som DIGG bestämmer och i anvisat format.

Leverantören ska månadsvis leverera statistik över transaktioner i underskrifts-tjänsten till part som DIGG bestämmer och i anvisat format.

Om inte annat överenskommes ska incidenter och statistik också rapporteras till kund.

7 Teknisk säkerhet

7.1 Fysisk säkerhet

7.1.1 Fysiskt skydd

Fysiskt skydd omfattar bland andra följande fysiska säkerhets- och skyddsåtgärder.

- **skalskydd** - samlingsbegrepp för en eller flera samverkande fysiska skyddskomponenter, t.ex. lås-, larm-, inbrottsskyddssystem
- **tillträdesbegränsning** - system för begränsning och kontroll av tillträde till utrymmen innanför skalskyddet

- **säkrade utrymmen** - avser de utrymmen inom ett avgränsat skalskydd som kräver ett förstärkt fysiskt skydd, t.ex. server-, växel- och korskopplingsutrymmen, datorhallar, arkivutrymmen
- **behörig** - avser person som medgivits åtkomst till information och/eller tillträde till lokaler vilka ingår i verksamheten som omfattar att tillhandahålla underskriftstjänsten.

7.1.2 Skalskydd och tillträde

Det ska finnas skalskydd som skyddar de lokaler som används för att tillhandahålla underskriftstjänsten.

Lokaler ska skyddas med lämplig tillträdesbegränsning för att säkerställa att enbart behörig personal har tillträde.

Utveckling och test av den fristående underskriftstjänsten ska ske i skyddade miljöer där åtkomst är begränsad till dem som behörigen ska ha tillträdde.

Det ska finnas medel för att kontrollera fysiskt tillträde. Till exempel bemannad reception/expedition och/eller kortstyrda och låsbara dörrar.

Endast behöriga personer får ha tillträde innanför skalskyddet. Rätt till tillträde innanför skalskyddet ska dokumenteras samt granskas och uppdateras regelbundet.

Besökare som inte är behöriga att vistas innanför skalskyddet kan tillåtas tillträde men ska då åtföljas av behörig person.

Datum samt tidpunkterna för in- och utpassering ska registreras.

7.1.3 Datamiljöer

Utvecklings- och testmiljöer ska vara separerade från driftmiljön.

Utrustning för att skapa, hantera och/eller administrera krypteringsnycklar ska placeras i säkrat utrymme med loggfunktion avseende tillträde.

7.2 IT-säkerhet

De system som används för att tillhandahålla underskriftstjänsten ska konstrueras och arrangeras på ett sådant sätt att det säkerställs att tjänsten kan upprätthållas utan brister i tillgänglighet och kapacitet.

7.2.1 Datasäkerhet

Underskriftsnycklar samt nycklar för signering av certifikat och spärrlistor, ska skapas och användas i en kvalificerad anordning, så kallad säker hårdvarumodul (HSM), som lägst är certifierad enligt FIPS 140-2 nivå 3 eller EN 419 221-5. Varje underskriftsnyckel ska raderas direkt efter det att den använts för underskrift och den tillhörande publika nyckeln lästs ut och inkluderats i ett underskriftscertifikat. Underskriftsnycklar får förekomma utanför hårdvarumodulen endast om de är krypterade och under förutsättning att följande krav uppfylls:

- Krypteringsnycklar som används för kryptering av underskriftsnycklar får inte förekomma utanför hårdvarumodulen.
- Krypteringsalgoritm och nycklar för kryptering av underskriftsnycklar ska följa de krav på krypteringsalgoritmer som framgår av tjänstespecifikation fristående underskriftstjänst.
- Underskriftsnycklar i krypterad form får inte förekomma utanför underskriftstjänstens säkra driftmiljö.
- Efter att en underskriftsnyckel raderats får ingen kopia av underskriftsnyckeln existera i eller utanför HSM modulen. Detta gäller oavsett om den är krypterad eller inte.

System för att skapa certifikat ska separeras från system för att skapa underskrifter på sådant sätt att intrång i det ena systemet inte ska kunna ge kontroll över det andra systemet.

Förändringar i driftmiljö ska hanteras på ett säkert och kontrollerat sätt så att det inte uppstår funktionella eller säkerhetsmässiga felaktigheter vid införande av ny eller ändrad funktionalitet i driftmiljön.

Vid förändringar i driftmiljö ska alla relaterade konfigurationsenheter hanteras under kontroll så att nödvändiga och önskade åtgärder vidtas i alla delar av systemet.

Genomförande av förändringar i systemets programvara ska strikt kontrolleras, godkännas och testas genom att använda formella processer för detta.

Alla systemklockor ska vara synkroniserade sinsemellan och med tillförlitlig tidkälla. Tidskällan ska vara synkroniserad med UTC via NTP (Network Time Protocol, RFC 5905).

Systemet ska innan drifttagande ”härdas” i enlighet med vedertagna standarder och ”best practice” för att god säkerhetnivå ska uppnås i systemet.

Felmeddelanden som exponeras för användare ska utformas så att de inte ger sådan information som kan användas i fientligt syfte för att kartlägga eventuella svagheter i systemet.

Endast den programvara/programkod som behövs för uppgiften ska användas. All programvara/programkod innebär risker för sårbarheter och mängden programvara ska därför minimeras för att minska risken för sårbarheter.

Systemet ska vara försett med intrångsskydd och funktioner för intrångs-detektering. Det ska finnas lämpliga analysverktyg för att spåra och följa upp intrång och intrångsförsök.

Leverantören ska vidta integritetssäkrande åtgärder, för viktiga säkerhets-funktioner så som säkerhetsloggar och motsvarande, som gör det möjligt att läsa men inte manipulera denna typ av information.

System ska så långt det är praktiskt och lämpligt delas upp i olika säkerhetszoner för att förhindra att sårbarheter i en del av systemet kan sprida sig till andra delar.

Extern kommunikation mot tjänsten ska ske enligt TLS standarden version 1.2 eller högre. Kommunikation med underskriftstjänsten för begäran av underskrift samt retur av underskriftssvar ska endast vara åtkomligt via HTTPS på port 443. Krypteringsalgoritmer ska väljas i enlighet med tjänstespecifikationen för fristående underskriftstjänst.

Säkra funktioner ska användas för att särskilja användares sessioner mot tjänsten.

Signerad data från extern källa så som begäran om underskrift och identitetsintyg ska verifieras med avseende på ursprung och integritet innan användning. Signerad data ska kontrolleras för att verifiera att signaturen är giltig samt att signaturen omfattar all data som signaturen avses skydda. Om möjligt ska signerad data även kontrolleras med avseende på syntax så att den endast innehåller information i enlighet med uppgjorda protokollspecifikationer.

Systemet ska vara skyddat mot CSRF-attacker (Cross Site Request Forgery), XSS (Cross Site Scripting), injektionsbaserade attacker och motsvarande kända attackmönster.

Filtrering ska ske av all data vars ursprung inte kan säkerställas komma från en betrodd part.

Användarsessioners livslängd ska vara så kort som möjligt och får aldrig sträcka sig över flera begärda underskrifter. Varje begärd underskrift ska hanteras som en ny session.

Information ska raderas och överskrivas från utrustning före kassering eller återanvändning.

Programvara som skyddar mot skadlig kod ska finnas och uppdateras kontinuerligt.

Användning och modifiering av tredjepartsprogramvara ska där det är praktiskt möjligt kontrolleras och undersökas för att skydda mot eventuella dolda kanaler och trojansk kod.

7.2.2 Infrastruktur

Det ska finnas en aktuell beskrivning av all infrastruktur som är fysiskt och logisk kopplad till de system och tjänster som omfattar att tillhandahålla underskriftstjänsten.

Det ska finnas skyddsbarriärer såsom brandvägg eller motsvarande i alla externa nätanslutningar. Tjänsten ska också skyddas internt för obehörig åtkomst på motsvarande sätt.

Systemet ska skyddas mot belastningsattacker som DDoS och motsvarande. Företrädesvis görs detta i internetoperatörens domäner.

Det ska finnas en aktuell förteckning över samtliga externa anslutningar som berör systemet.

All inblandad infrastruktur ska låsas ner ”härdas” i enlighet med vedertagna standarder och ”best practice” för att minska eventuell attackyta.

Regelbundna uppdateringar ska genomföras av systemets infrastruktur (servrar, routrar, brandväggar etc). Det gäller felrättningar och säkerhetsuppdateringar till operativsystem, mellanprogramvara och annan relaterad programvara i infrastrukturen. Säkerhetsuppdateringar ska verifieras och genomföras utan fördröjning, i övrigt ska utrustningsleverantörens rekommendationer följas.