Icke funktionella krav

Underskriftstjänst

Svensk e-legitimation

INNEHÅLL

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 Inledning

De krav som specificeras i detta dokument skall gälla för den verksamhet som bedrivs för att tillhandahålla Underskriftstjänst för Svensk e-legitimation.

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

2 Tillgänglighet och kapacitet

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

Totalt inom offentlig sektor kan, med den kunskap vi har idag om tjänster och tjänsteutveckling, finnas ett behov av upp till 100 miljoner elektroniska underskrifter om året när Svensk e-legitimation har varit i full drift några år. I bråd tid kan behovet komma att vara att genomföra upp till 200 underskrifter per sekund.

2.1 Svarstider

Följande krav på svarstider skall gälla för Underskriftstjänsten såvida inte annat framgår av enskilt avrop/leverans.

Svarstider skall vara max 3 sekunder i 90 % av fallen.
Svarstid i lågt belastad tjänst skall 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 sådant som utförs hos annan part, till exempel utställande av identitetsintyg som ska användas vid underskrift.

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

3 Administrativ säkerhet

3.1 Policy och regelverk

3.1.1 Policy och processer

Säkerhetspolicy, processer och rutiner som omfattar informationssäkerhetsarbetet, hantering av risker och förbättring av informationssäkerheten skall finnas. Dessa skall vara baserade på ISO-27001 eller motsvarande.

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

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

3.1.2 Säkerhetsorganisation

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

3.1.3 Roller och ansvar

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

3.2 Rutiner

3.2.1 Riskanalys

Det skall upprättas en riskanalys gällande hot mot verksamheten som omfattar att tillhandahålla Underskriftstjänsten som skall ligga till grund för säkerhetsarbetet.

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

3.2.2 Åtkomstskontroll

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

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

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

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

3.3 Övervakning och kontroll

Leverantören skall ha en process för informationsspridning i samband med driftavbrott och incidenter.

Säkerhetsincidenter som påverkar eller kan påverka verksamheten som omfattar att tillhandahålla Underskriftstjänsten skall rapporteras omedelbart till part och i format som E-legitimationsnämnden bestämmer.

4 Teknisk säkerhet

4.1 Fysisk säkerhet

4.1.1 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.

4.1.2 Skalskydd och tillträde

Leverantören skall använda skalskydd för skydd av de lokaler som omfattar att tillhandahålla Underskriftstjänsten.

Lokaler skall skyddas med lämpliga tillträdesskydd för att säkerställa att enbart behörig personal har tillträde.

Det skall 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 skall granskas, uppdateras och dokumenteras regelbundet.

Besökare som inte är anställda av Leverantören och som vistas innanför skalskyddet skall åtföljas.

Datum samt tidpunkterna för in- och utpassering skall registreras.

4.1.3 Datamiljöer

Utvecklings- och testmiljöer skall vara separerade från driftmiljön.

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

4.2 IT-säkerhet

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

4.2.1 Datasäkerhet

Underskriftsnycklar samt nycklar för signering av certifikat och spärrlistor, skall skapas och användas i en säker hårdvarumodul (HSM) som lägst är certifierad enligt FIPS 140-2 nivå 3. Varje underskriftsnyckel skall 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 skall följa de krav på krypteringsalgoritmer som framgår av Tjänstespecifikation för underskriftstjänst avsnitt 4.17.
- 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 skall separeras från system för att skapa underskrifter på sådant sätt att intrång i det ena systemet inte skall kunna ge kontroll över det andra systemet.

Förändringar i driftmiljö skall 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 skall alla relaterade konfigurationsenheter hanteras under kontroll så att nödvändiga och önskade åtgärder vidtas i alla delar av systemet.

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

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

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

Felmeddelanden som exponeras för externa användare skall 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 skall användas. All programvara/programkod innebär risker för sårbarheter och mängden mjukvara skall därför minimeras för att minska risken för sårbarheter.

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

Leverantören skall 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 skall 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 skall ske enligt TLS standarden version 1.1 eller högre. Kommunikation med signeringstjänsten för begäran av underskrift samt retur av underskriftssvar skall endast vara åtkomligt via HTTPS på port 443. Krypteringsalgoritmer skall väljas i enlighet med avsnitt 4.17 i Tjänstespecifikationen för Underskriftstjänsten.

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

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

Systemet skall vara skyddat mot CSRF-attacker (Cross Site Request Forgery), XSS (Cross Site Scripting) och injektionsbaserade attacker.

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

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

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

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

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

4.2.2 Infrastruktur

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

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

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

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

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

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