Sydnärkes IT-förvaltning

Nuläge och klassning av Verifieds system för e-signatur och identifiering

Lennart Grahn
Atea Sverige AB
2020-09-25

Innehållsförteckning

SAMMANFATTNING 4

BAKGRUND 5

INLEDNING 5
GENOMFÖRANDE 5

NULÄGE 6

ALLMÄNT 6
VAR HANTERAS OCH LAGRAS DATA 6
ARKIVERING, GALLRING & BACKUP 6
ARBETSFLÖDE 6
LOGGHANTERING 7
SÄKERSTÄLLA IDENTITET 7
SPÅRBARHET 7
SÅRBARHETSSCANNING 7
UTVECKLING 7

KLASSNING 8

BESLUTSUNDERLAG 9

VAD SÄGER LAGEN? 9
FÖRSLAG OM HUR UPPFYLLA LAGKRAV 10
FÖRSLAG TILL MÖJLIGT BESLUT 10

CHECKLISTA INFÖR EVENTUELL IMPLEMENTATION 11

Utgåvehistorik för dokumentet

Utgåva	Datum	Kommentar	Ansvarig
0.1	2020-04-21	Grundutgåva	Lennart Grahn
1.0	2020-04-23	Uppdaterad till version för leverans till kund	Lennart Grahn
1.4	2020-08-30	Uppdaterad med beslutsunderlag och förslag till beslut	Lennart Grahn
1.5	2020-09-18	Uppdaterad efter avstämning med kund och Verified, lagt till exec.summary samt Checklista inför implementation	Lennart Grahn
1.6	2020-09-25	Mindre korrigeringar innan leverans till kund.	Lennart Grahn

Sammanfattning

Socialförvaltningarna hos de kommuner som ingår i Sydnärkes IT-förvaltning har som önskemål att kunna upphöra med fax för att hantera underskrift av olika ärenden som exempelvis hanteringen av underskrifter av vissa beslut, orosanmälningar m.m.
Med det som mål har en utvärdering skett i möjligheten att använda en produkt från det svenska företaget Verified avseende elektronisk signering och identifiering.

Utvärderingen har skett främst utifrån följande aspekter; systemets klassificering (dvs vilken information kan man tillåta att systemet hanterar), lagar och förordningar (som OSL, GDPR m.fl), påverkan av utländsk lagstiftning, val av underleverantörer samt företagets eget informationssäkerhetsarbete.

All data lagras inom Sverige och hanteras inom EU förutom kontaktpersonernas mailadresser då ett amerikanskt företag nyttjas för att skicka mailet till kontaktpersonen.
Eftersom man inte längre kan hänvisa till Privacy Shield för hantering av personuppgifter i US har ett arbete initierats av Verified för att byta underleverantör så att även den hanteringen sker inom EU.

All data (PDF:er och signaturer) lagras och hanteras i krypterad form för att eliminera risken för spridning av känsliga personuppgifter eller sekretessbelagd information.

Sist i detta dokument finns en checklista på saker som behöver verifieras eller beaktas i samband med en implementation.

Baserat på utredningen ser vi inget hinder för att kunna gå vidare med en implementation av lösningen från Verified.

Bakgrund

INLEDNING

Socialförvaltningarna hos de kommuner som ingår i Sydnärkes IT-förvaltning har som önskemål att kunna upphöra med fax för att hantera underskrift av olika ärenden som exempelvis hanteringen av underskrifter av vissa beslut, orosanmälningar m.m.
I detta syfte vill man undersöka möjligheten att använda en produkt från Verified för elektronisk signering och identifiering.
Av den anledningen har detta nuläge och systemklassning sammanställts som ska ses som ett underlag inför en riskanalys. Resultatet av nuläget, klassningen och riskanalysen kommer att sammanställas i en rapport för att utgöra beslutsunderlag om sagda lösning kan användas eller inte. Syftet med riskanalysen är att får verksamhetenas syn på lösningen i kombination med lag- och myndighetskrav samt resultatet av informationsklassningen.
Riskanalysen har genomförts i form av en workshop med representant från de berörda kommunernas socialförvaltningar.

GENOMFÖRANDE

Analysen har genomförts av Lennart Grahn från Atea Sverige AB med stöd av representanter från berörda kommuner och leverantören Verified.

Nuläge

ALLMÄNT

Verified arbetar aktivt med informationssäkerhet och har infört ett ledningssystem för informationssäkerhet (LIS) i enlighet med ISO 27001. Man har också ett pågående arbete med att bli certifierad på ISO 27001 under Q1 – Q2 2021.
I och med detta vet vi att vi kan förvänta oss en viss kvalitet och nivå på leverantörens informationssäkerhets-arbete.

Bakgrundskontroll av arbetssökande sker för att säkerställa säkerheten.

Med hänsyn till företagets verksamhet och hantering av information som faller under olika sekretsslagar (GDPR, OSL, SOSFS, Banksekretess m.m.) är tjänsterna uppbyggda runt AWS ramverk för kryptering kombinerat med underleverantörer vilka tillhandahåller e-identifiering som Finansiell ID-teknik vilka tillhandahåller mobilt BankID.

VAR HANTERAS OCH LAGRAS DATA

All lagring av data sker hos AWS (Amazon Web Services) i deras svenska datacenter, viss bearbetning sker hos AWS i Irland.
All data lagras krypterat och all datatrafik är krypterad. Kryptonycklarna är unika för varje kund och roteras.

Alla PDF:er, inklusive inkodad underskrift, lagras och i form av en hash från vilken både PDF och underskrift kan återskapas och verifieras.

PDF:er som ska signeras lämnar normalt inte den krypterade lagringen, inför att ett dokument ska signeras skickas ett mail ut som enbart innehåller en URL-länk till dokumentet för signering som då enbart visas i skärmen. Men det finns också möjlighet att tillåta att dokumentet laddas ned.

För att kunna hantera de mail vilka innehåller länk till dokumenten som ska undertecknas, använder Verified en underleverantör, Postmark i USA, med vilket man har ett avtal. Inom ramen för tjänsten hanterar de enbart en personuppgift dvs. email-adressen vilken sparas under en förbestämd tid för att möjliggöra spårning.

Verified eller dess underleverantörer använder aldrig kundernas data för eget bruk.

ARKIVERING, GALLRING & BACKUP

Datat, dvs PDF:erna med inbäddad underskrift, lagras hos AWS i 10 år om inte dessa gallras av kunden. Ingen regelrätt arkivering utförs. Gallringsbeslut finns för informationen utifrån verksamhet och dokumenttyp.
Backup i dess traditionella mening existerar inte, istället säkras datat genom replikering och versionshantering vilket är inbyggt i AWS plattform.
En möjlighet att automatisera informationsflödet och säkerställa kontinuerlig gallring av information från tjänsten, skulle kunna vara att använda RPA (Robot Process Automation) vilket innebär en automatiserad process för att flytta signerade dokument till ProCapita med en automatisk radering av dokumentet från Verified.

ARBETSFLÖDE

Kortfattat beskrivet är arbetsflödet som följer; Inloggning, uppladdning av dokument, distribution av email med URL-länk för signering/nedladdning. För att kunna signera krävs verifiering av identitet genom mobilt BankID.

LOGGHANTERING

Alla aktiviteter, som uppladdning, läsning, nedladdning, signaturer, tilldela eller tabort rättigheter, m.m. i lösningen loggas. Loggarna sparas i 3 månader innan gallring sker.

Kontroll av loggarna genomförs regelbundet och automatiserat genom AWS Cloudwatch och Cloud inspector.

SÄKERSTÄLLA IDENTITET

Följande görs för att säkerställa identitet.

1. För att administrera lösningen eller ladda upp dokument, loggas användaren in med hjälp av användarnamn och lösenord. Det finns möjlighet att spärra denna inloggningsmöjlighet så enbart kan användas av personer från kundens IP-adresser.

2. För att signera eller ladda ned dokument måste individen använda utskickad länk samt identifiera sig med BankID (i dagsläget; svenskt, norskt och danskt).

3. Det finns möjlighet att signera och ladda ned utan krav på BankID, dvs med enbart användarnamn och lösenord. För att kunna hantera den typ av data som avses för socialförvaltningen (sekretessbelagd eller likställd), får inte denna möjlighet vara aktiverad.

SPÅRBARHET

Man kan gå tillbaka för att verifiera dokumentets äkthet samt vem som signerat då det görs integrerat i PDF:erna.
Om man över tid behöver kunna bevisa dokumentets/signaturens äkthet även i ett sådant fall där tjänsten har avvecklats eller upphört, utgör PDF:en i sig tillräckligt bevis.

SÅRBARHETSSCANNING

Minst 2ggr/år genomförs scanning efter sårbarheter och säkerhetsbrister (OWASP). De rapporter som genereras utgör underlag för hur plattformen ytterligare kan säkras. Kunderna har möjlighet att ta del av dessa rapporter.

UTVECKLING

Utveckling sker av företaget Code 11 (Norge, Rumänien och Tyskland) vilka också är delägare i Verified. All utveckling sker i enlighet med OWASP med olika testfunktioner.

Det finns en separat utvecklingsmiljö och ”staging”miljö vilken är ett ytterligare ett steg innan nya funktioner eller versioner lanseras i produktionsmiljön.

Klassning

Baserat på Verified's arbete med, och inställning, till säkerhet och utveckling utifrån min undersökning vilken baseras på ISO27001 (samma som verktyget Klassa), drar jag slutsatsen att lösningen med god marginal uppfyller de krav som finns för en tjänst och leverantör som ska hantera data som är sekretessbelagd, dvs nivå 3 för konfidentialitet, riktighet och tillgänglighet enligt MSB klassningsmodell.

Denna bedömning styrks också sett till den kundbas som redan använder Verified's tjänster.

Beslutsunderlag

Detta kapitel utgör ett beslutsunderlag som kan användas för att besluta om Sydnärkes IT-förvaltning ska gå vidare med, och därmed implementera, den beskrivna lösningen.

Informationen som hanteras i de PDF:er som ska signeras, klassas till nivå 3 enligt MSB/SKR klassningsmodell. Det är information som omfattas av sekretess enligt Offentlighets- och Sekretesslagen (2009:400) eller likställs med sekretess utifrån myndighetskrav. Dessutom kan informationen innehålla känsliga personuppgifter vilka faller under Dataskyddsförordningen.

VAD SÄGER LAGEN?

Offentlighets- och sekretesslagen

OSL 26 kap. behandlar; sekretess till skydd för enskild inom socialtjänst, vid kommunal bostadsförmedling, adoption, m.m.
1§ Sekretess gäller inom socialtjänsten för uppgift om en enskilds personliga förhållanden, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till denne lider men.

Övriga paragrafer berör följande områden med vad som gäller specifikt för dem:

- Underårigs vistelseort
- Familjerådgivning
- Omhändertagande av personakt
- Anmälningar m.m.

Den del som vi behöver fokusera på är 7§, vilken berör undantag från sekretess:
7 § Sekretessen enligt 1 § gäller inte

1. beslut om omhändertagande av en enskild,
2. beslut om vård utan samtycke,
3. beslut om sluten ungdomsvård,
4. beslut i ärende om klagomål mot kommunal hälso- och sjukvård eller dess personal, eller
5. beslut i ärende enligt 8 kap. patientsäkerhetslagen (2010:659).

Oavsett om OSL skulle ge möjligheten att undanta beslut om omhändertagande av enskild från sekretess, kan ett sådant beslut ändå innehålla personuppgifter (även känsliga) och annan information som aggregerat ger en mycket hög känslighet för individen.

Av den anledningen bör man ändå likställa sådana beslut med sekretess och därmed också hantera dessa efter samma regler/riktlinjer.

Hur påverkas tjänsten av Schrems II målet?

Baserat på det förhandsbesked som lämnades av EU Grand Chamber, kan man inte längre hänvisa till Privacy Shield för hantering av personuppgifter.
Det påverkar också hur avtalen med leverantör och underleverantör tecknas, där man bl.a. pekar på hur överföring av personuppgifter i kommersiellt syfte till företag i tredje land (läs US) ska tolkas.
Det pågår ett arbete inom svenska myndigheter hur man ska tolka målets olika delar.
Det som är viktigt att poängtera är att man främst pekar på hantering/överföring i kommersiellt syfte.

FÖRSLAG OM HUR UPPFYLLA LAGKRAV

Genom att all data krypteras, både i transit och övrig hantering, uppfylls de lagkrav som pekar på hanteringen av sekretessbelagd och känsliga personuppgifter.

Den modell med roterande och kundunika kryptonycklar, i kombination med de rutiner och regelverk som finns hos leverantören och AWS, måste anses tillhandahålla en mycket hög säkerhetsnivå.
Det finns inget direkt mervärde i att kunden själv hanterar kryptonycklarna, då det inte finns något US lagstöd som tvingar molntjänstleverantören att lämna ut dessa.

Avtalen måste ändå ses över, både vad gäller Verified och deras underleverantörer, då inga hänvisningar i avtalstext längre kan göras till Privacy Shield. Istället måste standardavtal användas som mer i detalj beskriver vad som tillåts, ansvar och att EU-lag tillämpas.

En av underleverantörerna vilken tillhandahåller mail-tjänsten lagrar sin data i US (Postmark). Ett arbete pågår med att ersätta Postmark med annan leverantör inom EU.
Det finns även andra alternativ till detta som; skriva om avtalet med Postmark så det inte längre hänvisar till Privacy Shield, eller förändra hanteringen och brukandet av mail-adresser som exempelvis tilldela de personer som ska nyttja systemet med ett s.k. mail-alias alternativt skapa en personlig funktionsmailbox som all sådan mail skickas till. Det sistnämnda sättet skulle helt eliminera överföringen av personuppgifter till US.
Ytterligare ett sätt att minimera risken för spridning av personuppgifter (både känsliga och vanliga) avseende den berörda individen, skulle kunna vara att utvärdera vilken information som är nödvändig att ta med i beslutsunderlaget som ska undertecknas.

FÖRSLAG TILL MÖJLIGT BESLUT

Enligt min personliga tolkning och åsikt, går det utmärkt att använda Verified-lösningen vilket är ett nordiskt företag, detta trots att man använder US baserade företag som underleverantörer.

Detta baserat på det som tidigare angetts i detta dokument, men kan sammanfattas som följande:

- All data som hanteras via AWS lagras inom Sverige och vissa funktioner hanteras från Irland (dvs all hantering inom EU).
- Alla dokument lagras och hanteras krypterat.
- Viss data (mailadresser) hanteras i US hos underleverantören Postmark. Leverantören är tänkt att ersättas med leverantör inom EU, efter en sådan förändring sker ingen lagring eller hantering av personuppgifter utanför EU.
- Identifiering av användare som ansluter från internet, sker via mobilt bankId, som också används för signering av dokumentet.

Vid ett beslut om att implementera och använda Verified-lösningen behöver följande genomföras:

- Se över avtalen med Verified och deras angivna underleverantörer.
- Byte av underleverantören Postmark, till annan EU-baserad likvärdig leverantör är planerat.

Baserat på utredningen ser vi inget hinder för att kunna gå vidare med en implementation av lösningen från Verified.

Checklista inför eventuell implementation

Denna checklista beskriver ett antal steg som behöver verifieras eller genomföras innan eller i samband med en implementation av lösningen från Verified. Punkterna är inte nödvändigtvis uppsatta i den ordning som de behöver utföras.

- Se över avtalet med Verified och deras underleverantörer, så att dessa inte hänvisar till Privacy Shield.
- Verifiera att underleverantören Postmark, byts till en leverantör som hanterar informationen inom EU om det är möjligt.
- Om bytet inte är möjligt, skulle man istället kunna använda sättet som beskrivs i sista avsnittet i kapitlet ”Förslag om hur uppfylla lagkrav”.
- Se över hur man kan minimera informationen i beslutet, kan man hänvisa till ett aktnummer för att minska informationen eller på andra sätt minska dokumentets känslighet?
- Upprätta ett gallringsbeslut för dokumenten som hanteras i lösningen, som innebär att de kan gallras direkt efter att de flyttats till ProCapita.
- Automatisera informationsflödet med en sk RPA (Robotic Process Automation) i så stor omfattning som möjligt, om detta är praktiskt och ekonomiskt möjligt. Det är ett bra sätt att minimera risken för hanteringsfel av användare.
- Skapa en användarhandledning riktad till användarna ute i verksamheterna.
- Genomför utbildning av användarna, denna kan vara i formen av workshop, videoinspelning eller nano-learning.