



Sikkerhedsmodeller for OIOREST

OIOREST - REST baserede webservices



IT- og Telestyrelsen

Ministeriet for Videnskab
Teknologi og Udvikling



Sikkerhedsmodeller for OIOREST

Udgivet af:
IT- & Telestyrelsen

IT- & Telestyrelsen
Holsteinsgade 63
2100 København Ø

Telefon: 3545 0000
Fax: 3545 0010

Nederst foto på forsiden:

B Tal (<http://flickr.com/photos/b-tal/>)
Creative Commons NY-NC
(<http://creativecommons.org/licenses/by-nc/2.0/deed.en>)

Publikationen kan hentes
på IT- & Telestyrelsens
Hjemmeside: <http://www.itst.dk>
ISBN (internet): 87-92311-73-3

>

Sikkerhedsmodeller for OIOREST

Version 1.0

Indhold

>

Indledning	5
Afgrænsning	5
Model 1: Sikring af systemkald	6
Arkitektur	6
Etablering af sikkerhed	6
Sikkerhedsmæssige egenskaber	8
Praktiske forhold	8
Særlige juridiske forhold i system-til-system kald	9
Model 2: Systemkald på vegne af bruger	11
Arkitektur	11
Overførsel af brugeridentitet	11
Etablering af sikkerhed	11
Sikkerhedsmæssige egenskaber	12
Attributter i fremmede registre	12
Praktiske forhold	12
Særlige juridiske overvejelser ved systemkald på vegne af bruger	13
Juridiske forhold	14
Regler der er i spil, når man sammenkobler services	14
Personoplysningsloven	14
Scenarie A	15
Scenarie B	16
Ansvar	17
Kom godt fra start med personoplysningsloven	17
Referencer	19

Indledning

>

Denne guide er henvendt til offentlige myndigheder samt private virksomheder, der ønsker at udstille eller anvende web services baseret på [OIOREST]. Guiden beskriver sikkerhedsmodeller, der kan anvendes i forbindelse med OIOREST. Formålet er at opnå fundamentale sikkerhedsmæssige egenskaber for kommunikationen herunder autenticitet, integritet og konfidentialitet. Anvendelse af de beskrevne sikkerhedsmodeller gør det muligt at udbyde eller anvende web services, der eksponerer følsomme data eller udbyder kritiske ressourcer via internettet.

Sikkerhedsmodellerne tager udgangspunkt to alment forekommende scenarier for serviceintegration: det første scenarie består af et system-til-system kald via internettet, og det andet scenarie udvider det første med kald på vegne af en bruger.

Begge sikkerhedsmodeller er baseret på brug af sikre transportprotokoller nærmere betegnet TLS / SSL¹ (se [TLS] og [SSL]). For hver sikkerhedsmodel beskrives:

- Arkitekturen hvor modellen kan anvendes.
- Hvordan sikkerheden etableres.
- De sikkerhedsmæssige egenskaber modellen tilvejebringer.
- Praktiske forhold man skal være opmærksom på.
- Juridiske aspekter af serviceintegration.

Afgrænsning

Guiden udstikker generelle retningslinjer, og der gives således *ikke* detailanvisninger på, hvorledes specifikke servere eller programmeringsmiljøer konfigureres i praksis. Endvidere skal det påpeges, at de beskrevne sikkerhedsmodeller alene dækker *kommunikationen* mellem en serviceaftager og en serviceudbyder; generelle it-sikkerhedsaspekter i organisationer og it-systemer behandles ikke.

Den juridiske del af vejledningen er udarbejdet for at give et kortfattet overblik over de krav især personoplysningsloven stiller. Vejledningen vil derfor ikke gå i detaljer med de enkelte forhold, i stedet gives et overblik, som hjælper godt fra start i forbindelse med brug af OIOREST.

Læseren forudsættes at være bekendt med OIOREST samt gængse begreber indenfor it-sikkerhed.

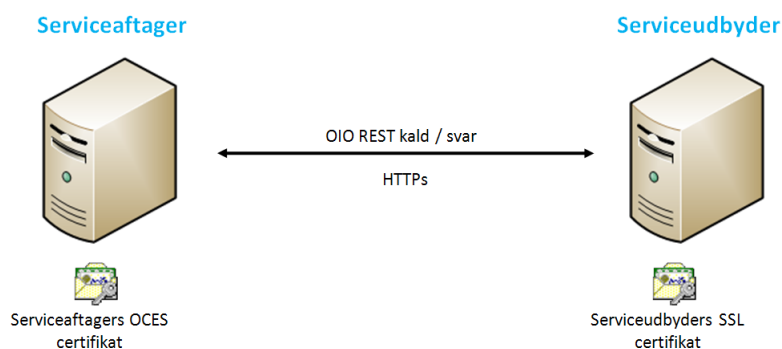
¹ I det følgende anvendes betegnelsen SSL som en fællesbetegnelse for SSL og TLS. De to protokoller er stort set ækvivalente; SSL (Secure Socket Layer) er den oprindelige protokol, der blev udviklet af Netscape, og navnet TLS (Transport Security Layer) blev indført i forbindelse med standardisering af protokollen under Internet Engineering Task Force.

Model 1: Sikring af systemkald

>

Arkitektur

Den første sikkerhedsmodel finder anvendelse på system-til-system kald via internettet, hvor de to systemer evt. tilhører forskellige organisationer. Det ene system initierer kommunikationen og optræder i rollen som serviceaftager (forkortet SA i det følgende), og det andet optræder i rollen som serviceudbyder (forkortet SU).



Figur 1: Scenarie med system-til-system kald

Kommunikationen følger request-response mønstret, hvor serviceaftageren sender en forespørgsel og herefter (synkront) modtager et svar fra serviceudbyderen. Ønsker man asynkron kommunikation, hvor der f.eks. kaldes tilbage på et senere tidspunkt, etableres en ny OIOREST kommunikation, hvor rollerne af serviceaftager og serviceudbyder byttes om.

I dette scenarie foretages systemkaldet med serviceaftagerens identitet og serviceudbyderen får ikke direkte informationer, om hvorvidt kaldet afvikles på vegne af en bruger eller it-system hos serviceaftageren, men alene at det kommer fra den virksomhed, som serviceaftageren repræsenterer.

Etablering af sikkerhed

Sikringen af kommunikationen etableres ved, at parterne anvender SSL protokollen til den HTTP-baserede kommunikation².

SSL protokollen findes i to varianter, nemlig med eller uden klientautentifikation (se nedenfor). I denne sikkerhedsmodel anvendes varianten *med* klientautentifikation (serverautentifikation er obligatorisk). Inden kommunikationen kan etableres, skal begge parter udstyres med et såkaldt X.509 certifikat med en tilhørende privat nøgle (som illustreret på ovenstående figur):

- Serviceaftageren skal have et klientcertifikat og her anbefales enten et OCES Virksomhedscertifikat (forkortet VOCES), et OCES Funktionscertifikat (forkortet FOCES) eller et OCES Medarbejdercertifikat (forkortet MOCES)

² Når HTTP sikres med SSL benyttes ofte betegnelsen HTTPs, som angivet på figuren.

med tilhørende privat nøgle. Som regel skal disse installeres på de applikationsservere eller på den klient, der skal kalde servicen³.

- Serviceudbyderen skal konfigureres med et SSL servercertifikat med tilhørende privat nøgle. Som regel skal dette installeres på virksomhedens web servere.

Et OCES Virksomhedscertifikat identificerer indehaveren som virksomhed via et CVR nummer, og et OCES Funktionscertifikat identificerer tillige den service eller applikation, som på virksomhedens vegne anvender certifikatet. Forskellen på de to OCES certifikattyper består primært i, at VOCES kan anvendes til at indgå bindende aftaler på vegne af en virksomhed, mens FOCES alene er beregnet til sikring af teknisk kommunikation.

Forskellene mellem de to typer certifikater i OIOREST sammenhæng er opsummeret i nedenstående tabel:

Forskelle mellem FOCES og VOCES
<p>Fordele ved funktionscertifikater sammenlignet med virksomhedscertifikater:</p> <ul style="list-style-type: none"> • Mindre konsekvenser ved kompromittering, da den private nøgle ikke kan binde virksomheden. Dette kan være en fordel, hvis certifikat og privat nøgle skal installeres på en server i en demilitariseret zone (DMZ), som kan være under angreb fra internettet. • Identificerer servicen som anvender certifikatet. • Billigere end virksomhedscertifikater.
<p>Fordele ved virksomhedscertifikater sammenlignet med funktionscertifikater:</p> <ul style="list-style-type: none"> • Kan anvendes i flere sammenhænge herunder til bindende aftaleindgåelse.

Rent praktisk bestilles begge typer certifikater gennem LRA klienten fra DanID (tidligere TDC).

Et MOCES certifikat identificerer en medarbejder i en given virksomhed og adskiller sig fra de to øvrige typer ved, at der skal angives kodeord hver gang den private nøgle anvendes. MOCES certifikater er derfor i OIOREST sammenhæng kun relevante, når serviceaftager er en rig klient, der har adgang til brugerens private nøgle (efter brugeren har indtastet password). For detaljer om OCES certifikatpolitikkerne henvises til [OCES-CP].

Endelig skal det nævnes, at OCES personcertifikater og medarbejdercertifikater spiller en rolle i forbindelse med på-vegne-af scenarier (se næste kapitel), hvor de anvendes af slutbrugeren til at logge ind i serviceaftagers applikation.

³ Langt de fleste applikationsservere og netværksstakke kan konfigureres til at anvende SSL, så programmøren ikke behøver at udvikle programkode.

Et SSL servercertifikat identificerer indehaveren via et domænenavn på internettet (f.eks. www.itst.dk), hvilket er et krav i forbindelse med SSL protokollen. Disse certifikater kan anskaffes fra en lang række udbydere.

Sikkerhedsmæssige egenskaber

Ved anvendelse af ovenstående sikkerhedsmodel opnår man følgende sikkerhedsmæssige egenskaber:

- Konfidentialitet af kommunikationen – såvel HTTP headere og body, der bærer OIOREST kommunikationen, holdes hemmelige under transport.
- Integritet af kommunikationen.
- Autentifikation af serviceaftager som virksomhed eller evt. medarbejder i en virksomhed overfor serviceudbyder. Ved anvendelse af softwarebaserede OCES certifikater opnås i udgangspunktet autentifikation på niveau 3 i forhold NIST's klassificeringer af autenticitetssikring⁴ svarende til ”høj tillid til påstået identitet” (se evt. [AUTH-LEV] for detaljer). Er der brug for et højere niveau af autenticitetssikring (dvs. 4), skal man i udgangspunktet anvende kryptografisk hardware til beskyttelse af den private nøgle.
- Autentifikation af serviceudbyder (i form af domænenavn) overfor serviceaftager.

Det skal bemærkes, at ovenstående egenskaber opnås mellem serviceaftagers applikationsserver og den (web) server hos serviceudbyderen, der terminerer SSL forbindelsen. Hvis serviceudbyderen har en it-arkitektur bestående af flere sikkerhedszoner adskilt af firewalls, vil SSL termineringen typisk ske i en demilitariseret zone (DMZ). Her skal man være opmærksom på sikring af kommunikationen videre ind i bagvedliggende zoner hos serviceudbyderen, hvilket typisk også vil ske med SSL forbindelser.

Endvidere skal det nævnes, at modellen *ikke* giver uafviselighed på de enkelte transaktioner / servicekald. Har man brug for dette, kan man evt. indføre digitale signaturer over de data, som transporteres i HTTP kaldet. Dette beskrives dog ikke yderligere i denne guide. Guiden [SIG-BEV] beskriver, hvorledes bevisværdien af digitale signaturer kan sikres.

Praktiske forhold

Ved implementering af ovenstående model er der en række praktiske forhold, man bør overveje:

- Inden kommunikationen kan etableres, skal parterne konfigurere systemerne med en liste af certifikatudstedere, der skal accepteres for modpartens certifikat.
- Serviceudbyderen skal konfigurere hvilke serviceaftagere, der må kalde servicen dvs. opsætte adgangskontrol. Dette kan typisk ske ved at identificere

⁴ http://csrc.nist.gov/publications/drafts/800-63-rev1/SP800-63-Rev1_Dec2008.pdf

certifikater eller andre referencer for de serviceaftagere, man vil give adgang, samt opsætte regler for, hvad de må tilgå.

- De private nøgler hørende til certifikaterne skal beskyttes mod uautoriseret adgang. Hvis hackere kan få adgang til de private nøgler, er kommunikationen usikker, og en hacker vil bl.a. kunne udgive sig for at være den part, der er angivet i det tilhørende certifikat.
- SSL protokollen kan anvende forskellige krypteringsalgoritmer, hashalgoritmer og forskellige nøglelængder (såkaldte "cipher suites"; se evt. [TLS] afsnit A.5), hvoraf nogle giver ringe eller ingen sikkerhed. Man bør derfor konfigurere sine servere, så der kun accepteres cipher suites med stærk kryptering (minimum 128 bit).
- Serviceudbyderen skal konfigurere sin server til at kræve klientautentifikation, da dette er krævet i sikkerhedsmodellen men valgfrit i SSL. Tillader man kald uden klientautentifikation, har man ikke vished for serviceaftagers identitet.
- SSL protokollen findes i forskellige versioner, og man bør ikke tillade gamle versioner. Serverne bør derfor kræve mindst version 3.0 af SSL og mindst version 1.1 af TLS.
- Certifikaterne har en udløbsdato (typisk to år efter udstedelse), og parterne bør etablere en procedure, der sikrer, at de fornys i god tid inden udløb. I modsat fald vil systemerne pludselig holde op med virke den dag, certifikatet udløber.
- Man skal konfigurere sine servere til at foretage et spærrecheck af certifikatet enten via spærreliste (CRL) eller on-line opslag hos certifikatudstederen (OCSP protokollen). Hvis man ikke foretager spærrecheck, bliver det muligt at få adgang med et spærret certifikat.
- I ovenstående beskrivelse har udgangspunktet været, at kommunikationen består af et enkelt request-response kald. Det skal dog nævnes, at SSL protokollen etablerer en session, hvor man vil kunne sende mange OIOREST kald/svar. I situationer, hvor der er behov for mange servicekald indenfor en kort tidsperiode (f.eks. såkaldte batch jobs), kan man overveje at genbruge sessionen med henblik på at opnå bedre performance. Dette kræver dog, at begge systemer kan håndtere dette.

Særlige juridiske forhold i system-til-system kald

Ved at følge ovenstående anbefalinger etableres stærk kryptering, hvilket er et krav, hvis følsomme persondata skal udveksles. Dette er et krav som følger af Sikkerhedsbekendtgørelsen § 14.

Sikkerhedsmodellen forudsætter generel tillid fra serviceudbyder til serviceaftager, herunder at der kun foretages kald, som serviceaftageren er berettiget til.

Man bør forud for integrationen af systemerne udforme en skriftlig aftale / kontrakt mellem parterne, der regulerer væsentlige forhold som f.eks.:

- Teknisk kvalitet af den udbudte service herunder svartider, opetid, tilladte antal transaktioner. Hvis serviceudbyder f.eks. lukker servicen ned for vedligehold, kan det betyde, at serviceaftagers it-systemer holder op med at fungere korrekt.
- Vilkår for anvendelse af servicen – f.eks. at det kun må ske som led i sagsbehandling, som serviceaftager lovmæssigt er pålagt. Et andet vilkår kan være betaling for servicen.

>

- Parternes ansvar og samarbejde, herunder om begge myndigheder er dataansvarlige eller om den ene er databehandler på vegne af den anden. Hvis den ene myndighed er databehandler på vegne af den anden myndighed, så er den skriftlige kontrakt et lovkrav jf. personoplysningsloven §42, stk. 2.

Der kan være lovgivningsmæssige eller forretningsmæssige forhold der medfører, at serviceudbyderen skal etablere en logning af, hvilke serviceaftagere, der har kaldt servicen, samt hvilke data der er blevet udleveret. Hvis der eksempelvis behandles fortrolige eller følsomme personoplysninger, står der i sikkerhedsbekendtgørelsen, at logning skal ske, se hertil § 15, 18 og 19.

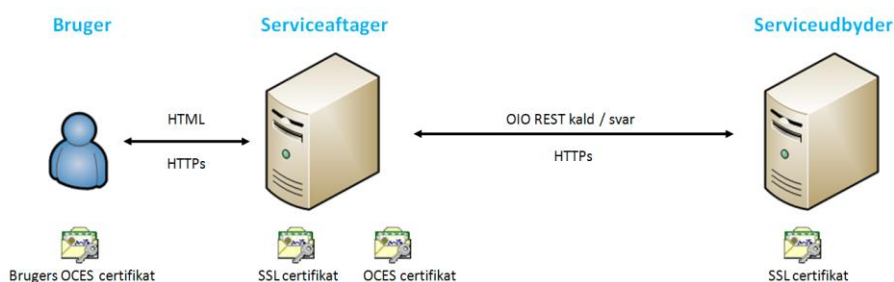
For en nærmere perspektivering af de lovgivningsmæssige forhold der vil være i forbindelse med anvendelsen af OIOREST henvises til vejledningens afsnit om juridiske forhold.

Model 2: Systemkald på vegne af bruger

>

Arkitektur

Det andet scenarie er en udvidelse af det første, hvor serviceaftageren foretager et OIOREST servicekald på vegne af en bruger. Det antages, at serviceaftageren udbyder en web applikation (f.eks. en portal), hvor brugeren er logget ind med et OCES person- eller medarbejdercertifikat. Applikationen hos serviceaftageren har på et tidspunkt behov for at kalde en service hos serviceudbyderen – det kunne eksempelvis være for at hente data om brugeren i et fremmed system, som skal bruges i applikationen:



Figur 2: Scenarie med systemkald på vegne af bruger

Servicekaldet adskiller sig i forhold til den første model ved, at man overfører såvel brugerens identitet som serviceaftagerens identitet til serviceudbyderen. Der er således mange lighedspunkter til den første model, og nedenfor fokuseres derfor kun på nye aspekter.

Overførsel af brugeridentitet

Brugerens identitet overføres fra serviceaftager til serviceudbyder ved at anvende en HTTP header med navnet "X-On-Behalf-Of". Det specifikke indhold af headeren specificeres af serviceudbyderen afhængigt af, hvad hans service har brug for at vide om brugeren⁵. Oplagte eksempler kan være overførsel af brugernavn, CPR- eller CVR-nummer, PID- eller RID-nummer fra OCES certifikat, Subject serialnumber fra OCES certifikat mv. For indholdet af OCES certifikater henvises til certifikatpolitikkerne [OCES-CP].

Etablering af sikkerhed

Sikkerheden består i etablering af to sikre kommunikationskanaler:

- Mellem brugerens browser og serviceaftagerens web server etableres en SSL session. Brugeren kan blive autentificeret på flere måder:

⁵ Indholdet skal URL-encodes i UTF-8 (som beskrevet i RFC 2616) for sikre, at specialtegn ikke forvanskes under transport.

>

- Der anvendes klientautentificeret SSL og browseren vil anvende brugerens digitale signatur og OCES certifikat til at etablere forbindelsen med.
- Der anvendes SSL *uden* klientautentifikation og browseren autentificeres efter SSL sessionen er oprettet f.eks. ved at anvende en login applet, der tilgår hans digitale signatur, eller eksempelvis via en fællesoffentlig single sign-on løsning baseret på [OIO-SAML] standarden som NemLog-in eller Virk BRS.
- Mellem serviceaftager og serviceudbyder etableres en SSL forbindelse på samme måde som beskrevet for den første sikkerhedsmodel.

Sikkerhedsmæssige egenskaber

Ved anvendelse af ovenstående sikkerhedsmodel opnår man samme sikkerhedsmæssige egenskaber som i model 1 for *hver* af de to transportkanaler.

Bemærk at serviceaftageren står inde for, at den overførte brugeridentitet er korrekt. Eksempelvis kan dette indgå i aftalevilkår for brug af servicen. Serviceudbyderen har således ikke nogen mulighed for at fastslå, om denne er korrekt eller om brugeren virkelig har aktiv browsersession med serviceaftageren eller evt. har afgivet samtykke til kaldet (se nedenfor). Hvis serviceudbyderen skal være sikker på dette, kan man evt. anvende protokoller, hvor serviceaftageren sender brugerens browser forbi serviceudbyderen, så han selv kan indhente samtykke. Denne teknik anvendes bl.a. i OAuth protokollen (se oauth.net).

Attributter i fremmede registre

Hvis serviceudbyderen har brug for ekstra informationer om brugeren eksempelvis i forbindelse med autorisationsbeslutninger for afvikling af servicekaldet, kan serviceudbyderen vælge at kontakte eksterne attributservices. Som eksempel kan nævnes, at NemLog-in samt Virk.dk's brugerrettighedsløsning tilbyder services, hvormed man kan slå attributter op for en bruger; sidstnævnte giver mulighed for at hente rettigheder for medarbejdere administreret via portalen.

Praktiske forhold

Ved implementering af ovenstående model er der en række praktiske forhold, man bør overveje (udover dem der allerede er nævnt for den første model):

- Serviceudbyderen skal specificere det forventede indhold af HTTP headeren, der angiver brugerens identitet.
- Serviceaftageren skal etablere brugerautentifikation til hans web-applikation med en af de beskrevne mekanismer (klientautentificeret SSL, login applet eller SAML 2.0 baseret SSO løsning).
- Serviceaftager og serviceudbyder bør overveje at anskaffe et såkaldt "Extended Validation"⁶ SSL certifikat til deres web servere. Disse certifikater kræver en ekstra grundig validering af indehaverens identitet før udstedelse,

⁶ For detaljer henvises til http://en.wikipedia.org/wiki/Extended_Validation_Certificate

og modparten kan derfor have højere tillid til sådanne certifikater end normale SSL certifikater. Endvidere skal det nævnes, at certifikaterne genkendes af nyere browsere, og at deres tilstedeværelse afspejles i brugeroplevelsen (en grøn adresselinje i browseren), hvilket giver en større tryghed for brugerne.

- Serviceudbyderen skal afvikle kaldet i kontekst af brugeren, hvilket kan få indflydelse på den måde, adgangskontrollen er indrettet på. I nogle situationer skal servicen blot hente data for den angivne bruger, i andre situationer vil brugerens identitet få indflydelse på, om servicekaldet må udføres eller ej, eller om der er særlige rettigheder forbundet med kaldet.

Særlige juridiske overvejelser ved systemkald på vegne af bruger

Udover de allerede beskrevne problemstillinger, bør man overveje implikationerne af, at servicekaldet sker på vegne af en bruger.

Det kan eksempelvis være relevant at indhente brugerens samtykke til, at servicekaldet udføres (f.eks. at man henter brugerens helbredsoplysninger i et fremmed system). I den forbindelse bør man overveje samtykkets form, virkefelt, og hvordan man senere kan dokumentere, at alle data er hentet på baggrund af specifikke samtykker.

Rent praktisk kan man overveje at give brugeren en mulighed for at underskrive en samtykkeerklæring med sin digitale signatur. I den forbindelse er det vigtigt at kommunikere tydeligt, hvilke data, man vil hente i servicekaldet. Derudover bør brugeren til enhver tid kunne vedligeholde sine samtykker i applikationen herunder tilbagekalde samtykker.

Et andet aspekt er, hvor meget et samtykke kan dække, f.eks. om der skal gives samtykke ved alle servicekald eller om samtykket kan genbruges. Det kommer an på den konkrete anvendelse af data, hvad der er muligt, og det er væsentligt at skabe en balance imellem brugerens mulighed for hele tiden at kontrollere anvendelsen af data og selve anvendeligheden af applikationen.

I forbindelse med overvejelserne omkring indhentelse af samtykke hos borgeren er det væsentligt at gøre klart, om serviceudbyderen eller serviceaftageren er dataansvarlig, idet det er den dataansvarlige, der har pligten til at indhente borgerens samtykke. I situationer hvor serviceaftager indhenter brugerens samtykke til udvekslingen af data, skal serviceudbyder sikre sig, at håndteringen af samtykket sker forsvarligt og opfylder lovgivningen. Se mere om ansvarsfordelingen under afsnittet om juridiske forhold.

Juridiske forhold

>

OIOREST giver mulighed for servicekald imellem forskellige offentlige myndigheder over internettet. Dermed opnås nye, fleksible muligheder for betjening af borgere f.eks. ved automatisk indhentning af nødvendige oplysninger i andre myndigheders registre. Med den øgede funktionalitet kommer dog udfordringer i forhold til overholdelse af regler, hvor hver myndighed har et ansvar overfor borgeren. I særligt fokus er personoplysningsloven, men også overholdelse af andre regler kan have betydning, især hvis den ene myndighed opererer under specialregler som det eksempelvis er tilfældet på sundhedsområdet.

Regler der er i spil, når man sammenkobler services

For at bringe et OIOREST projekt godt fra start er det vigtigt at få sat fokus på, hvilke regler man skal have for øje. Nedenfor er listet de regler, som umiddelbart vil have interesse:

Lov / bekendtgørelse	Hvornår
Personoplysningsloven. Nr. 429 af 31/5 - 2000	Når der udveksles persondata. Der er forskellige krav til behandlingen alt efter om det drejer sig om eksempelvis et navn eller om det er udveksling af eksempelvis sygdomsoplysninger. Forkortes POL.
Sikkerhedsbekendtgørelsen Nr. 528 af 15/6-2000.	Når der udveksles persondata indenfor det offentlige. Bekendtgørelsen uddyber tekniske og administrative krav til personoplysningsloven.
Forvaltningsloven Nr. 1365 af 7/12-2007	Når myndigheden behandler data for borgere. Eksempelvis kan der være forhold at afklare imellem myndighederne vedrørende svarfrister og notatpligt.
Lov om elektroniske signaturer Nr. 417 af 31/5-2000	OIOREST løsningen kan ikke i sig selv fungere som signaturløsning, og der skal derfor kobles et ekstra lag på, hvis man skal anvende løsningen til at modtage et uafviseligt samtykke.
Specialregler	Den enkelte myndighed kan være underlagt særlige regler, som kan have betydningen for dataudvekslingen. Som eksempel kan sundhedsområdet nævnes.

Personoplysningsloven

I det følgende fokuseres på personoplysningsloven i forhold til servicekald, hvor der hentes data fra en myndighed til en anden.

Det er vigtigt at huske, at man kan have sikkerhed uden privacy, men man kan ikke have privacy uden sikkerhed. Privacy er således mere end teknisk sikkerhed, fordi der stilles krav til, hvem der må tilgå data og hvordan administrationen skal være. Kravene som stilles afhænger af, hvilke data der udveksles.

Generelt kan data klassificeres i følgende 3 kategorier:

Følsom		Fortrolig		Generel
POL § 7	POL § 8	POL § 11	POL § 6	POL § 6
Racemæssig / etnisk baggrund, politisk, religiøs, eller filosofisk overbevisning, fagforeningsforhold, seksuelle forhold, helbredsmæssige forhold. Eksempel hvis der er angivet registreret partnerskab.	Strafbare forhold, væsentlige sociale problemer, andre rent private forhold. Eksempel herpå er selvmordsforsøg, bortvisning fra job.	CPR-nummer.	Private oplysninger om eks. økonomi, skatteforhold, gæld, sygedage, tjenestelige forhold og familieforhold	Bolig, bil, eksamen, ansøgning, CV, ansættelsesdato, stilling, arbejdsområde, arbejdstelefon, stamoplysninger. Eksempler er Navn, adresse og fødselsdato.

Når data er blevet inddelt i en af de 3 kategorier, kan man ud fra den paragraf, data hører under (se tabellen ovenfor) se, hvilke krav der stilles til data og behandlingen heraf.

Generelt stilles der krav indenfor følgende 4 hovedområder:

- Behandlingssikkerhed – administration.
- Den registreredes rettigheder.
- Anmeldelse.
- Teknisk sikkerhed.

Kravene retter sig imod al behandling af data, fordi en databehandling i personoplysningslovens forstand vedrører al brug af data. Det betyder at læsning, registreringen, opbevaring, brug, videregivelse og sletning alt sammen er databehandlinger. Ingen behandlinger går derfor fri, men kravene til procedurer og sikkerhed bliver større eller mindre alt efter datas klassifikation og den påtænkte anvendelse.

Scenarie A

Der tages i det følgende udgangspunkt i et scenarie, hvor myndighed A kalder en service hos myndighed B for at læse data. Data kopieres ikke over i et særskilt register. Alligevel er det en databehandling, der er omfattet af personoplysningsloven. Kravene, som stilles til behandlingen, vil naturligvis kun rette sig imod datalæsningen. I denne situation er det derfor vigtigt at overveje, om myndighed B må give myndighed A ret til at læse data. Dertil kommer om det kun er bestemte medarbejdere i myndighed A, der skal gives adgang og hvordan der følges op på, at det er de rigtige der rent faktisk gives adgang.

I det beskrevne tilfælde er myndighed B dataansvarlig, fordi det er myndighed B, der forvalter data. Som dataansvarlig skal myndighed B sikre, at det er lovligt at lade medarbejderne hos myndighed A tilgå data. Det vil være tilladt at give adgang, hvis det eksempelvis står i en lov, at data skal gives videre.

>

Når vi omtaler en videregivelse af data, er det vigtigt at huske, at de informationer data indeholder, bliver givet videre allerede, når en person læser dem. Af denne grund bliver en læseadgang, som gives til en anden myndighed, anset som en videregivelse af data.

Myndighed A's rolle som enten databehandler eller dataansvarlig afhænger af, om der er indgået en skriftlig kontrakt der regulerer, hvem der må tilgå data, hvordan data må anvendes, og hvordan sikkerheden skal være hos myndighed A. Kontrakten kan kun indgås for behandlinger, Myndighed B har ret til at foretage. Kravene til udformning af kontrakten findes i personoplysningslovens §42. Eksisterer en sådan kontrakt er myndighed A databehandler på vegne af myndighed B, som er dataansvarlig. I modsat fald er myndighed A også dataansvarlig.

Scenarie B

Hvis vi tager fat i samme situation som i scenarie A med den ændring, at myndighed A indlæser data i et eget system, så skal myndighed A skal sørge for it-sikkerheden for de data, som ligger i dette system. Om myndighed A bliver dataansvarlig for oplysningerne afhænger som nævnt ovenfor af, om der foreligger en kontrakt med myndighed B, som binder Myndighed A i forhold til anvendelsen af data.

Foreligger der ikke en kontrakt, bliver myndighed A dataansvarlig på lige fod med myndighed B, og begge parter skal løfte det ansvar, som påhviler den dataansvarlige efter personoplysningsloven.

Det ansvar, som påhviler den dataansvarlige, er blandt andet, at:

- Sikre, at der er tilladelse til behandlingen af data og eventuelle samtykker er indhentet.
- Sørge for it-sikkerheden.
- Sikre, at de rigtige personer har adgang til data.
- Sikre, at der er historik i forhold til adgangen af data.
- Foretage de nødvendige anmeldelser til datatilsynet.
- Udarbejde skriftlige aftaler med databehandlere.
- Sikre, at borgeren er orienteret om brugen af data.
- Sikre borgerens ret til at gøre indsigelse imod databehandlingen.
- Sikre at data er korrekte.
- Sikre at data bruges til saglige formål.
- Slette data, når de ikke længere er nødvendige.

Kravene, som specifikt skal overholdes, afhænger af datas klassifikation og ganske kort kan følgende overordnede krav nævnes indenfor de 3 kategorier:

Konsekvens		
Følsom	Fortrolig	Generel
Der er et generelt forbud mod at dele data med mindre der er lovhjemmel eller uafviseligt samtykke fra borger. Med uafviseligt menes, at samtykkes skal gives af en borger, der er tydeligt oplyst om formål og anvendelse. Desuden skal samtykket	Der stilles krav til sikkerheden såvel teknisk som administrativt. Ikke alle behandlinger af fortrolige data skal anmeldes til Datatilsynet, men forholdet skal undersøges. Borgerens ret til eksempelvis at	Der stilles ikke så store sikkerhedskrav til generelle persondata. Behandlingen er dog stadig omfattet af personoplysningsloven.

være givet skriftligt, så der ingen tvivl er om omfanget. Endelig skal der anvendes en teknik der er sikker nok til, at man kan stole på data. Der stilles store krav til såvel administrativ som teknisk sikkerhed. Der skal ske anmeldelse til Datatilsynet og borgerens ret til eksempelvis at se og rette data skal sikres.	se og rette data skal sikres.	Behandlingen skal generelt ikke anmeldes til Datatilsynet. Borgerens ret til eksempelvis at se og rette data skal sikres.
--	-------------------------------	--

Ansvar

Såvel serviceaftager som serviceudbyder har ansvar og opgaver, når personoplysningsloven skal overholdes. For at afklare ansvarsforholdet er det nødvendigt at finde ud af, om man er dataansvarlig eller databehandler. Begreberne findes i personoplysningsloven §3 nr. 4 og 5.

Den dataansvarlige er den, som kan bestemme, hvordan og hvornår data anvendes. I OIOREST sammenhæng vil dette som udgangspunkt være serviceudbyderen, som har data liggende. Hvis data videregives på en måde, så data kan behandles selvstændigt af serviceaftageren, vil denne også blive dataansvarlig.

Gives data derimod til serviceaftager med baggrund i en skriftlig aftale med nøje instruktioner om brug, så vil serviceaftager blive databehandler i stedet for dataansvarlig. Denne model bruges til outsourcing af driftopgaver og dette kaldes efter personoplysningsloven en overladelse. En overladelse er derfor en videregivelse af data, hvor der er en skriftlig kontrakt som sikrer, at databehandleren ikke kan handle frit og hvor den dataansvarlige giver en opgave videre, som denne ellers selv skulle løse.

Den dataansvarlige bærer det overordnede ansvar for brugen af oplysningerne, og har kontakten med borgeren. Databehandleren skal overholde kontrakten med den dataansvarlige og sørge, for at sikkerheden er i orden.

Kom godt fra start med personoplysningsloven

Nedenfor er angivet en lille huskeliste til komme godt fra start, når man skal finde ud, af hvilke krav, der skal opfyldes.

- Få overblik over hvilke data der deles.
- Er der personoplysninger? Hvis ikke, så gælder personoplysningsloven ikke.
- Hvis der er personoplysninger, så skal disse klassificeres, så der er overblik over, om de er generelle, fortrolige eller følsomme.
- Afklar, hvem der har ansvaret for data og dermed er dataansvarlig. Hvis man er serviceudbyder, er det vigtigt at finde ud af, om man er i gang med at videregive data på en måde så serviceaftager selvstændigt kan anvende data. Hvis ikke skal der laves en skriftlig kontrakt om, hvordan data må bruges.

>

Hvis serviceaftager ikke begrænses skriftligt i brugen af data, og der ikke føres kontrol med serviceaftageren, så regnes det som en videregivelse af data, hvor serviceaftager kan anvende data selvstændigt.

- Tilladelsen til at videregive data skal undersøges – er der eksempelvis en lov der siger, at data skal videregives eller har man et skriftligt samtykke fra brugeren? Hvis ikke skal man undersøge, om man på anden måde har ret til at videregive data, Hvis man videregiver data, skal man i de fleste tilfælde have borgerens samtykke. Som tommelfingerregel er det vigtigt at huske, at borgeren skal kunne forstå, hvor data er og hvem han/hun kan henvende sig til for indsigt, rettelser i data m.m.
- Hvis serviceaftager skal fungere som databehandler på vegne af serviceudbyder, så er det vigtigt, at man husker at udarbejde en skriftlig kontrakt, der tager højde for datasikkerheden.

Referencer

>

- [OIOREST] <http://oiorest.dk>
- [SSL] ”SSL 3.0 Specification”:
<http://www.freesoft.org/CIE/Topics/ssl-draft/3-SPEC.HTM>
- [TLS] ”The Transport Layer Security (TLS) Protocol Version 1.2”, Internet Engineering Task Force.
<http://www.ietf.org/rfc/rfc5246.txt>
- [OCES-CP] <https://www.signatursekretariatet.dk/certifikatpolitikker.html>
- [OIO-SAML] <http://www.oiosaml.info>
- [SIG-BEV] ”Signatur- og Systembevis – teknisk vejledning i sikring af digitale signaturers bevisværdi”, IT- og Telestyrelsen.
<http://www.itst.dk/arkitektur-og-standarder/infrastruktur-og-felles-losninger/brugerstyring/signatur-og-systembeviser>
- [AUTH-LEV] ”Vejledning vedrørende niveauer af autenticitetssikring”.
<http://www.itst.dk/arkitektur-og-standarder/Standardisering/standarder-for-serviceorienteret-infrastruktur/standarder-for-brugerstyring/filer-til-standarder-for-brugerstyring/Horing.B.st.niv.autenticitetssikring.v5.pdf>

