



IT- og Telestyrelsen

Ministeriet for Videnskab
Teknologi og Udvikling

Vejledning vedrørende niveauer af autenticitetssikring

Kolofon:

OIO Referencemodel for tværgående brugerstyring

Denne anbefaling kan frit anvendes af alle. Citeres fra anbefalingen i andre publikationer til offentligheden skal angives korrekt kildehenvisning.

Forslag til anbefalinger for tværgående brugerstyring udarbejdes af IT- og Telestyrelsen, IT-strategisk kontor, som sekretariat for OIO It-Arkitekturkomiteen.

Kontaktperson:

It-Arkitekt Søren Peter Nielsen, email: spn@itst.dk

Telefon 25 67 07 83 (direkte)

It-Arkitekt Anders Dalsgaard, email: ada@itst.dk

Telefon 25 65 32 08 (direkte)

Ministeriet for Videnskab, Teknologi og Udvikling

IT- og Telestyrelsen

IT-strategisk kontor

Holsteinsgade 63

DK-2100 København Ø

Telf. +45 35 45 00 00

Fax. +45 35 45 00 10

<http://www.itst.dk>

itst@itst.dk

1	Indledning.....	4
1.1	Opsummering.....	4
1.2	Formål	4
1.3	Overblik	5
1.4	Anvendelsesområde	5
2	Sikkerhedsniveauer og risikovurdering	7
2.1	Beskrivelse af sikkerhedsniveauer	7
2.2	Risici, mulige konsekvenser og sikkerhedsniveauer.....	7
2.3	Bestemmelse af niveau for autenticitetssikring og valg af system ved hjælp af risikovurdering ..	10
2.4	Niveauer af autenticitetssikring og risikoprofiler. Beskrivelse og eksempler.....	12
2.5	Risici og kontekst.....	13
3	Vurdering af tillid til akkreditiv-udbydere	14
4	Implementering af en autenticitetssikringsproces	15
4.1	Autenticitetssikringsprocessen.....	15
4.2	Anvendelse af anonyme akkreditiver.....	15
4.3	Lovmæssige krav	16
4.4	Omkostninger i forhold til nytteværdi.....	16
5	Yderligere information	18

1 Indledning

1.1 Opsummering

Denne vejledning beskriver, hvorledes ejere af systemer til digital forvaltning kan bestemme det rette sikkerhedsniveau for autenticitetssikringsprocessen i deres systemer. Der defineres og beskrives fire niveauer af autenticitetssikring for elektroniske transaktioner. Vejledningen hjælper med at bestemme behovet for autenticitetssikring i systemer til digital forvaltning.

Det er den forretningsansvarlige systemejer, der har det primære ansvar for at bestemme nødvendige sikkerhedsniveauer samt strategierne til at opnå disse niveauer. Dette gælder også for niveauer af autenticitetssikring.

Systemejere bør gennemgå de følgende trin, som er nærmere beskrevet i afsnit 2.3, for at fastsætte det nødvendige niveau af autenticitetssikring:

1. Udfør risikovurdering for det givne it-systemet.
2. Match identificerede risici til nødvendigt niveau af autenticitetssikring.
3. Vælg teknologi til autenticitetssikring.
4. Valider efter implementering, at systemet i drift har det nødvendige niveau af autenticitetssikring.
5. Revurdér periodisk, om systemet har behov for opgradering af teknologien, der er anvendt til autenticitetssikringen.

1.2 Formål

Denne vejledning vedrører autenticitetssikring af personer, der er brugere af systemer til digital forvaltning. Til trods for at autenticitetssikring typisk involverer en computer eller anden form for elektronisk udstyr, så vedrører denne vejledning ikke indbyrdes autenticitetssikring imellem servere, andre computere eller netværkskomponenter.

Denne vejledning har til formål at hjælpe systemejere med at bestemme og analysere risici forbundet med hvert enkelt trin i autenticitetssikringsprocessen. Det inkluderer (men er ikke begrænset til) validering af faktisk identitet, udlevering af akkreditiver, teknisk og forvaltningsmæssig administration, journal-føring, revision og selve anvendelsen af akkreditiverne. Hvert trin i processen har indflydelse på, hvor godt det tekniske system samlet set stemmer overens med det ønskede sikkerhedsniveau.

Denne vejledning kan anvendes på egen hånd. Den er i overensstemmelse med sikkerhedsstandarden DS484 og vil kunne anvendes supplerende til DS484.

Anbefalingerne i denne vejledning bygger på og svarer til anbefalinger fra en række andre lande herunder USA¹, England og Australien.

Sikkerhedspolitikken, hvori brugerstyring er et væsentligt element, skal for alle institutioner revurderes. Dette vil selvsagt være en oplagt lejlighed til en kritisk revision af hvilke data, der er omgærdet af hvilke sikkerhedsbestemmelser. Et godt udgangspunkt vil være DS484.

¹ Den tilsvarende amerikanske vejledning er *m-04-04 E-Authentication Guidance for Federal Agencies* fra USA's Office of Management and Budget. <http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf>

1.3 Overblik

Denne vejledning indeholder anbefalinger vedrørende elektronisk autenticitetssikring til ejere af systemer til digital forvaltning. Autenticitet defineres som

Egenskab, der sikrer, at en ressource eller person er den hævdede (anvendes fx ved log on og elektronisk underskrift/digital signatur)²

Autenticitetssikring har som fokus at bekræfte en brugers identitet på basis af pålideligheden af vedkommendes akkreditiver.

Et andet begreb er *Autorisation*, der på basis af politikker og tilladelser giver brugeren adgangsrettigheder efter, at vedkommende er autenticitetssikret.

I forbindelse med implementering af et system til digital forvaltning er det systemejerens ansvar at bestemme det nødvendige niveau af autenticitetssikring for de transaktioner³, som systemet inkluderer. Dette sker via en risikovurdering for hver type af transaktion. Vurderingen identificerer:

- Potentielle konsekvenser som følge af en sikkerhedshændelse
- Sandsynligheden for at hændelsen indtræffer

Denne vejledning kategoriserer en række konsekvenser og giver en fælles baggrund for at bestemme størrelser af risici. Vejledningen beskriver

- En metode til vurdering af risici
- Fire niveauer for autenticitetssikring
- Hvorledes det rette niveau af autenticitetssikring bestemmes

1.4 Anvendelsesområde

Ikke alle transaktioner, der sker i forbindelse med digital forvaltning, kræver autenticitetssikring

Denne vejledning vedrører alle transaktioner, der sker i forbindelse med digital forvaltning, som kræver autenticitetssikring, uafhængigt af om de er initieret af individuelle brugere, private virksomheder eller offentlige myndigheder. Undtaget fra vejledningens anvendelsesområde er dog transaktioner, der vedrører national og international sikkerhed. Krav i forbindelse hermed behandles i Statsministeriets sikkerhedscirkulære⁴.

I forhold til autenticitetssikring er der tale om to typer af individuel autenticitetssikring:

- a) Sikring af en identitets autenticitet, som bekræfter en brugers personlige identitet
- b) Sikring af en attributs autenticitet, som bekræfter, at brugeren tilhører en særlig gruppe (som fx "folkepensionist" eller "sagsbehandler i jobcenter")

Attributbaseret autenticitetssikring består i at etablere et bestemt niveau af tillid til, at en bestemt attribut tilhører en given bruger. Hvis attributten ikke giver mulighed for at udlede brugerens identitet, kaldes det et anonymt akkreditiv (dette diskuteres yderligere i afsnit 4). Attributbaseret autenticitetssikring behandles ikke i større grad i denne vejledning, men det er muligt for systemejere at anvende anonyme akkreditiver i visse sammenhænge.

² Definition fra DS 484:2005, Standard for informationssikkerhed

³ Til brug i denne vejledning defineres *transaktion* som: En diskret begivenhed mellem en bruger og et system, som understøtter et forretningsmæssigt formål

⁴ Der henvises til "Cirkulære vedrørende sikkerhedsbeskyttelse af informationer af fælles interesse for landene i NATO, EU eller WEU, andre klassificerede informationer samt informationer af sikkerhedsmæssig beskyttelsesinteresse i øvrigt" – også kaldet Statsministeriets sikkerhedscirkulære.

Vejledning beskæftiger sig ikke direkte med autorisation. Autorisation fokuserer på de handlinger, som en bruger efter autenticitetssikring må udføre. Det er systemejerens ansvar at sikre korrekt håndtering af autorisationer i sit system.

Vejledningen beskæftiger sig ikke med vurderinger af, om akkreditiver på et givet sikkerhedsniveau kan anvendes til elektronisk signatur. Den fælles offentlige anbefaling er at anvende OCES digital signatur⁵ til elektronisk underskrift.

Vejledningen foreskriver ikke hvilke tekniske systemer, der skal implementeres. De sikkerhedsniveauer, der defineres i denne vejledning, er ikke bundet til tekniske foranstaltninger og bliver ikke forældede i takt med forældelsen af de tekniske systemer. Anbefalinger om hvilke teknologier, der anbefales til opnåelse af de ønskede sikkerhedsniveauer, publiceres uafhængigt og kan således opdateres løbende, uden at det vil kræve ændringer til denne vejledning.

⁵ Læs mere om OCES digital signatur på <http://www.digitalsignatur.dk/>

2 Sikkerhedsniveauer og risikovurdering

2.1 Beskrivelse af sikkerhedsniveauer

Denne vejledning beskriver fire niveauer af autenticitetssikring til anvendelse indenfor digital forvaltning. Hvert sikkerhedsniveau beskriver i hvor høj grad, en organisation, på baggrund af de akkreditiver⁶ brugeren har præsenteret, kan være sikker på, at brugeren virkelig er den, vedkommende giver sig ud for at være. I denne sammenhæng defineres sikkerhed som:

1. Graden af tillid til grundigheden af den proces, der er anvendt til at fastslå brugerens identitet ved udstedelsen af akkreditiver til vedkommende
2. Graden af tillid til, at den bruger, der anvender akkreditiverne, er lig med den bruger, som akkreditiverne blev udstedt til

De fire sikkerhedsniveauer er følgende:

- Niveau 1 - Lille eller ingen tiltro til påstået identitet
- Niveau 2 - Nogen tiltro til påstået identitet
- Niveau 3 - Høj tillid til påstået identitet
- Niveau 4 - Meget høj tillid til påstået identitet

2.2 Risici, mulige konsekvenser og sikkerhedsniveauer

Dette dokument vedrører kun risici forbundet med fejlagtig autenticitetssikring. En generel tilgang til håndtering af risiko i forbindelse med it-systemer er blandt andet beskrevet i *Standard for informationssikkerhed, DS 484:2005*. Det er vigtigt at bemærke, at der er andre metoder til risikohåndtering (fx restriktioner i adgangen til det anvendte netværk, detektering af angreb⁷ og hændelsesovervågning), som kan medvirke til at nedsætte behovet for højere niveauer af autenticitetssikring.

2.2.1 Kategorisering af konsekvenser

For at kunne bestemme det rette niveau af autenticitetssikring skal ejere af it-systemer vurdere mulige risici og identificere foranstaltninger til at minimere konsekvensen af dem.

Fejl i forbindelse med autenticitetssikring, som har relativt store konsekvenser, kræver højere niveauer af sikkerhed. Risikoen skal håndteres i den måde selve forretningsprocesserne bygges op, i de politikker som den anvendende organisation definerer og ved teknologiske foranstaltninger.

Kategorier af mulige konsekvenser inkluderer følgende

- Ulempe, kval eller tab af anseelse
- Økonomisk tab eller ansvarspådragelse
- Skade på myndighedsaktiviteter eller andre offentlige interesser
- Ikke-autoriseret frigivelse af sensitiv information
- Fysisk personskade

⁶ Akkreditiver defineres i denne sammenhæng som et objekt, hvis rigtighed godtgøres af kontrolløren i forbindelse med autenticitetssikring. Akkreditiver kan på en eller anden måde være bundet til det individ, de er udstedt til, eller de kan være gældende for det individ, der på et givet tidspunkt er ihændeher af dem. Den første slags akkreditiver anvendes til autenticitetssikring, mens den anden slags kan anvendes til autorisation.

⁷ På engelsk: Intrusion Detection

- Mulighed for at begå/modvirke opklaring af ulovligheder

Det nødvendige niveau af autenticitetssikring bestemmes ved at vurdere den mulige risiko for hver af de nævnte kategorier af konsekvenser. Den mulige risiko bestemmes som en kombination af:

- Sandsynligheden for, at hændelsen, som resulterer i konsekvensen, indtræffer
- Konsekvensens størrelse

Risikoen beskrives med en af følgende tre størrelser:

- Lille
- Moderat
- Stor

I næste afsnit defineres størrelserne af risici i forbindelse med hver af de definerede kategorier. Bemærk: Hvis fejl i forbindelse med autenticitetssikring ikke giver anledning til målelige konsekvenser, er der ingen risiko.

2.2.2 Bestemmelse af risiko i forbindelse med autenticitetssikring

Dette afsnit definerer, hvornår risikoen for en given konsekvens betegnes som lille, moderat eller stor.

Risiko for ulempe, kval eller tab af anseelse

- **Lille** – Giver højst kortvarig ulempe, kval eller forlegenhed til en organisation eller person
- **Moderat** – Giver højst mindre alvorlig kortvarig eller begrænset længerevarende ulempe, kval eller tab af anseelse til en organisation eller person.
- **Stor**– Mere alvorlig eller alvorlig længerevarende ulempe, kval eller tab af anseelse til en organisation eller person (reserveres generelt til situationer med særligt alvorlige konsekvenser, eller som vedrører mange personer).

Risiko for økonomisk tab eller ansvarspådragelse

- **Lille** – Giver højst et ubetydelig økonomisk tab til en organisation eller person eller højst en ubetydelig ansvarspådragelse for en myndighed.
- **Moderat** – Giver højst et mindre alvorligt uopretteligt økonomisk tab til en organisation eller person eller en alvorlig ansvarspådragelse for en myndighed.
- **Stor**– Giver et mere alvorligt eller katastrofalt økonomisk tab til en organisation eller person eller en alvorlig eller katastrofal ansvarspådragelse for en myndighed.

Risiko for skade på myndighedsaktiviteter eller andre offentlige interesser

- **Lille** – Giver højst en begrænset negativ effekt på organisationens aktiviteter, dens aktiver eller offentlighedens interesser. Eksempler på begrænset negativ effekt er:
 - Nedsættelse af en organisations evne omfangsmæssigt eller tidsmæssigt til udførelse af opgaver, hvilket medfører, at organisationens effektivitet indenfor dens primærområde nedsættes
 - Mindre skade på en organisations aktiver eller på offentlige interesser iøvrigt
- **Moderat** – Giver højst en mindre alvorlig negativ effekt på organisationens aktiviteter, dens aktiver eller offentlighedens interesser. Eksempler på mindre alvorlige negative effekter er:

- Betydelig nedsættelse af en organisations evne omfangsmæssigt eller tidsmæssigt til udførelse af opgaver, hvilket medfører, at organisationens effektivitet indenfor dens primærområde nedsættes betydeligt
- Betydelig skade på en organisations aktiver eller på offentlige interesser i øvrigt
- **Stor**– Giver en alvorlig eller katastrofal negativ effekt på organisationens aktiviteter, dens aktiver eller offentlighedens interesser. Eksempler på alvorlig eller katastrofal effekt er:
 - Alvorlig nedsættelse af en organisations evne omfangsmæssigt eller tidsmæssigt til udførelse af opgaver, hvilket medfører, at organisationen er ude af stand til at løse en eller flere opgaver indenfor dens primærområde
 - Stor skade på en organisations aktiver eller på offentlige interesser i øvrigt

Risiko for ikke-autoriseret frigivelse af sensitiv information

- **Lille** – Resultaterer højst i en begrænset frigivelse af personlig, myndighedssensitiv eller kommerciel sensitiv information til uautoriserede parter, hvor følgen er tab af fortrolighed i lille omfang.
- **Moderat** – Resultaterer højst i en frigivelse af personlig, myndighedssensitiv eller kommerciel sensitiv information til uautoriserede parter, hvor følgen er tab af fortrolighed i moderat omfang.
- **Stor** – Resultaterer i en frigivelse af personlig, myndighedssensitiv eller kommerciel sensitiv information til uautoriserede parter, hvor følgen er tab af fortrolighed i stort omfang.

Risiko for fysisk personskade

- **Lille** – Resultaterer højst i risiko for en mindre skade, som ikke kræver lægelig behandling.
- **Moderat** – Resultaterer højst i moderat risiko for en mindre skade, eller begrænset risiko for en skade, der kræver lægelig behandling.
- **Stor** – Resultaterer i risiko for en alvorlig skade eller død.

Risiko for mulighed for at begå/modvirke opklaring af ulovligheder

- **Lille** – Resultaterer højst i risiko for ulovligheder, som normalt ikke giver anledning til myndighedshåndhævelse.
- **Moderat** – Resultaterer højst i moderat risiko for ulovligheder, som kan give anledning til myndighedshåndhævelse.
- **Stor** – Resultaterer i risiko for ulovligheder, som giver anledning til myndighedshåndhævelse.

2.2.3 Bestemmelse af niveau for autenticitetssikring

Niveau for autenticitetssikring bestemmes ud fra den mulige størrelse af de identificerede risici i tabel 1 nedenfor. Det nødvendige niveau er det laveste niveau, som matcher eller overgår de mulige størrelser af de risici, der er identificeret i en risikovurdering (se punkt 2 nedenfor).

Tabel 1 – Maksimale størrelser af risici for hvert sikkerhedsniveau

Risiko i forhold til sikkerhedsniveau				
Kategorier af konsekvenser ved fejl i forbindelse med autenticitetssikring	1	2	3	4
Ulempe, kval eller tab af anseelse	Lille	Moderat	Moderat	Stor
Økonomisk tab eller ansvarspådragelse	Lille	Moderat	Moderat	Stor
Skade på myndighedsaktiviteter eller andre offentlige interesser	-	Lille	Moderat	Stor
Ikke-autoriseret frigivelse af sensitiv information	-	Lille	Moderat	Stor
Fysisk personskade	-	-	Lille	Moderat Stor
Mulighed for at begå/modvirke opklaring af ulovligheder	-	Lille	Moderat	Stor

Tegnet ”-” angiver ikke tilstrækkeligt sikkerhedsniveau til hændelser med den givne konsekvens

I forbindelse med analysen af potentielle risici skal systemejeren overveje alle direkte og indirekte følger af en fejl i forbindelse med autenticitetssikring, herunder muligheden for, at der kan opstå mere end én fejl, og at det kan have følger for mere end én person. Definitionerne af risici anvender relative termer som ”alvorlig” eller ”begrænset”. Betydningen af disse termer vil afhænge af den konkrete sammenhæng, som de optræder i. Systemejeren må vurdere den konkrete sammenhæng og beskaffenheden af de personer/entiteter, der påvirkes for at udlede den betydning af de skader, der kan opstå. Efterhånden som risici vurderes for flere systemer, vil der oparbejdes en praksis, som gør det nemmere at lægge en mere definitiv betydning i termer som ”alvorlig” eller ”begrænset”. I forbindelse med risikovurderingen af skade på myndighedsaktiviteter eller andre offentlige interesser skal systemejeren være ekstra opmærksom på afhængigheden af den konkrete kontekst i sine vurderinger.

I nogle tilfælde, som vist i tabel 1, kan mere end ét sikkerhedsniveau være bedste match til en given størrelse af en risiko. Fx i tabel 1 kan det ses, at moderat risiko for økonomisk tab svarer til både sikkerhedsniveau 2 og 3. I sådanne tilfælde må systemejeren inddrage yderligere kontekst vedrørende systemet i sin beslutning. Yderligere kontekst kan fx være, at der også er en moderat risiko for ulovligheder i forbindelse med fejl i autenticitetssikringen, hvilke så afgør, at der skal anvendes sikkerhedsniveau 3.

2.3 Bestemmelse af niveau for autenticitetssikring og valg af system ved hjælp af risikovurdering

Systemejere finder det rette niveau af autenticitetssikring ved at gennemgå følgende skridt:

1. Udfør risikovurdering for det givne it-system.

Risikovurderingen⁸ vil sætte størrelser på det relative omfang af konsekvenser og sandsynligheden

⁸ Yderligere vejledning om risikovurdering kan findes i Dansk Standard ”Standard for informationssikkerhed”, DS 484:2005 Anneks B, Risikovurdering.

for en lang række hændelser forbundet med systemet i tilfælde af en fejl i forbindelse med autenticitetssikring.

Bemærk: Et it-system kan have flere typer eller kategorier af transaktioner, som det kan være nødvendigt at udføre separate vurderinger af i forbindelse med den samlede risikovurdering. Vær også opmærksom på, at et it-system kan involvere flere organisationer. Det er ikke nok at vurdere risiko for den organisation, som "ejer" systemet.

Risikovurdering er til en vis grad en subjektiv proces, hvor systemejeren må overveje skader som følge af bl.a. tekniske fejl, ondsindede tredjeparter, misforståelser og menneskelige fejl. Systemejeren bør overveje et bredt udsnit af scenarier i arbejdet med at finde de potentielle skader, der kan blive påført vedkommendes forretningsproces. Det er bedre at inkludere for meget end for lidt i denne fase. Når risici er identificeret, er det måske muligt at justere forretningsprocessen og afbøde mulige risici ved at mindske sandsynligheden for, at de opstår (se trin 4)

2. Match identificerede risici til nødvendigt niveau af autenticitetssikring.

De identificerede risici indplaceres i kategorierne beskrevet i 2.2.

For at finde det nødvendige niveau af autenticitetssikring bør systemejeren i første omgang identificere risici, uafhængigt af hvilken teknisk løsning, der anvendes til autenticitetssikring. Dernæst matches de identificerede risici til det laveste niveau af autenticitetssikring, som er dækkende for alle de identificerede risici. Fx hvis der er fem risici med potentielle størrelser, som matches af niveau 1, og der er en risiko, som svarer til niveau 2, så kræver transaktionen autenticitetssikring på niveau 2. Fx. hvis misbrug af en brugers elektroniske identitet/akkreditiver under lægelig behandling kan resultere i risiko for alvorlig personskade eller død, skal niveau 4 anvendes til trods for, at størrelsen af andre risici er minimal.

3. Vælg teknologi til autenticitetssikring.

Efter at have bestemt nødvendigt niveau af autenticitetssikring vælges en teknisk løsning, som kan understøtte dette niveau. Dette kan fx gøres på basis af "Electronic Authentication Guideline" fra det amerikanske National Institute of Standards and Technology (NIST)⁹.

4. Valider efter implementering, at systemet i drift har det nødvendige niveau af autenticitetssikring.

Baggrunden for dette er, at selve implementeringen af systemet kan indføre nye risici eller forstærke eksisterende risici. Systemejeren bør kontrollere, at processen til autenticitetssikring opfylder systemets behov for autenticitetssikring som led i en generel sikkerhedsgodkendelse af systemet (såsom certificering, akkreditering eller lignende)

5. Revurdér periodisk, om systemet har behov for opgradering af teknologien, der er anvendt til autenticitetssikringen.

Systemejeren skal periodisk kontrollere om teknologisk forældelse eller ændringer i forretningsprocessen, som it-systemet understøtter, har betydning for niveauet af autenticitetssikring. Det er oplagt at foretage denne kontrol sammen med generelle årlige reviews af it-sikkerheden. Bemærk: Teknologisk forældelse af en autenticitetssikringsløsning behøver ikke at resultere i, at der

⁹ Publikationsnummeret er 800-63, og vejledning findes online på denne adresse:

http://www.csrc.nist.gov/publications/nistpubs/800-63/SP800-63v6_3_3.pdf

Det forventes, at NIST opdaterer "Electronic Authentication Guideline" i trit med udviklingen teknisk og risikomæssigt indenfor autenticitetssikringsløsninger.

skal implementeres ny teknologi. Det er muligt for systemejeren at forbedre niveauet af autenticitetssikring for en given teknisk løsning ved indførelse af andre risiko-afbødende foranstaltninger.

2.4 Niveauer af autenticitetssikring og risikoprofiler. Beskrivelse og eksempler

Niveau 1 - Lille eller ingen tiltro til påstået identitet. Anvendes for eksempel til at lade brugere registrere bogmærker på en web-side, som de så kan anvende på et senere tidspunkt.

Eksempler:

- I nogle tilfælde vil en persons indsendelse af en formular være en transaktion, som ikke kræver autenticitetssikring ud over niveau 1. Dette er tilfældet, når al information sendes til en offentlig organisation; der ikke sendes nogen information den anden vej, og der ikke er andre behov for højere niveau af autenticitetssikring. Det kunne fx dreje sig om en formular til indrapportering af gadelygter uden lys i.
- Lokal registrering på et netsted med selvangivet brugerid og kodeord, som blot resulterer i mulighed for at tilrette måden, netstedet præsenterer sin information på, kan anvende niveau 1. Hvis en tredjepart aflurer bruger-id og kodeord, kan vedkommende muligvis få adgang til personlig og forretningsmæssig information om den retmæssige bruger på baggrund af den tilretning, vedkommende har foretaget. Hvis der ikke er tale om en meget høj grad af tilretning, er risikoen herved sandsynligvis minimal.
- Et online debat-forum, som ikke beder om anden information end navn og geografisk område fra bruger, der vil deltage, kan også anvende niveau 1. Såfremt debatforummet ikke vedrører sensitive eller private emner, er der ingen oplagte risici herved.

Niveau 2 – Overordnet betraget er der tillid til, at den påståede identitet er korrekt. Niveau 2 akkrediterer kan anvendes til mange offentlige tjenester, hvor den offentlige myndighed har behov for at kende brugerens identitet fra starten (denne identitet skal dog verificeres på anden måde, før der foretages sagsbehandling eller lignende af den offentlige myndighed).

Eksempler:

- En bruger anvender et e-learning-site. Systemet er nødt til at kende brugeren for at kunne vise vedkommende en passende oversigt over kurser, for at kunne tildele karakterer og vise, hvorledes vedkommende har klaret sig i alle kurser, som vedkommende har gennemgået. Den eneste risiko i denne forbindelse er, at en ondsindet tredjepart kan få adgang til brugeren karakterliste, som kan resultere i en krænkelse af brugerens privatliv eller anseelse. Hvis systemejeren vurderer, at omfanget af denne konsekvens er lille, kan niveau 2 anvendes.
- Et bibliotek tilbyder borgeren mulighed for at kunne se listen over sine lån og reservere nye bøger. Dette involverer højst en lille risiko for at privatlivs-sensitive informationer afsløres, hvorfor autenticitetssikring på niveau 2 kan anvendes.
- En offentlig ansat udfører sagsbehandling, som kan involvere følsomme personlige oplysninger om en borger. Sagsbehandlingssystemets autenticitetssikring svarer til niveau 2, hvilket betyder, at risikoen for ikke-autoriseret frigivelse af sensitiv information er vurderet at være lille. Dette skyldes anvendelse af tekniske tiltag (som fx brug virtual private network), som gør det muligt at begrænse den ansattes anvendelse af systemet til, når vedkommende fysisk befinder sig på sin organisations adresse. Hvis sagsbehandlingssystemet anvendes i mindre sikre omgivelser, vurderes risikoen for ikke-autoriseret frigivelse af sensitiv information at være moderat. Dette betyder i dette tilfælde, at

brugeren skal autenticitetsikres på niveau 3. Fx kan en kommunal sagsbehandler logge på sit ESDH-system med bruger-id og kodeord, men *kun* når vedkommende befinder indenfor rådhusets afgrænsede område. Hvis vedkommende tilgår systemet udefra, kræves bedre autenticitetssikring, fx ved kombination af den bestående login-metode og afgivelse af et en-gangs-kodeord.

Niveau 3 – Anvendes til transaktioner, der kræver høj tillid til påstået identitet. Niveau 3 akkreditiver kan anvendes til at give adgang til systemer med begrænset adgang via Internettet uden behov for yderligere kontrol af brugerens identitet.

Eksempler:

- Et firma indgiver statistik-data via en erhvervsportal, som andre firmaer kunne få en konkurrencemæssig fordel af at se. Hvis det vurderes, at såvel risikoen for frigivelse af sensitiv information samt risikoen for økonomisk tab er moderat (men ikke katastrofal), kræver det autenticitetssikring på niveau 3
- En borger kan på en sundheds-/helseportal se sin egen medicin-profil med en oversigt over hvilken medicin, der har været og er recept-udskrevet til vedkommende. Hvis det vurderes, at konsekvensomfanget ved frigivelse den sensitive medicin-information er moderat (og risikoen for tab af anseelse er moderat, samt risikoen for fysisk personskade højst er lille), anvendes niveau 3.
- En offentlig ansat anvender en anden myndigheds it-system, hvilket giver vedkommende adgang til potentielt sensitiv information om borgere. Den ansatte arbejder i en bygning, som kun ansatte og autoriserede besøgende har adgang til, men transaktionerne med den anden myndigheds it-system sker over Internettet. Vedkommendes adgang til potentielt sensitiv information resulterer i moderat omfang i en risiko for kompromittering af personoplysninger, hvorfor der skal anvendes autenticitetssikring på niveau 3.

Niveau 4 – Anvendes til transaktioner, der kræver meget høj tillid til påstået identitet. Brugere kan anvende niveau 4 akkreditiver til at præsentere deres identitet og få adgang til stærkt beskyttede ressourcer via Internettet uden behov for yderligere kontrol af brugerens identitet.

Eksempler:

- En ansat i politiet skal via Internettet have fuld adgang til et register med yderst sensitiv information, som fx en oversigt over alle straffede personer i Danmark indenfor de sidste 10 år. Her er der risiko for frigivelse af sensitiv information såvel som risiko for tab af anseelse, og konsekvensen kan i begge tilfælde være af stort omfang, hvorfor der skal anvendes autenticitetssikring på niveau 4.
- En offentlig sagsbehandler anvender et it-system, som giver vedkommende adgang til potentielt personfølsom information. Adgangen sker via sagsbehandleren bærbare computer fra forskellige geografiske steder som private hjem, virksomheder, og der anvendes forskellige opkoblingsmetoder. Konsekvensomfanget ved potentiel frigivelse af den sensitive information er kun moderat, men på grund af den bærbare computers sårbarhed og fordi der anvendes en række forskellige net-forbindelser ind til systemet, vurderes den samlede risiko til at være større med behov for at kræve anvendelse af autenticitetssikring på niveau 4.

2.5 Risici og kontekst

Når niveau af autenticitetssikring bestemmes, skal risikoen for, at en modtager af elektronisk overført information vil afvise den som utroværdig, også vurderes. Denne risiko kan imødegås ved at få den afgivende person med et akkreditiv af passende niveau til at validere den afgivne information, fx med digital signatur

Mens det måske er muligt ved hjælp af teknologi at fastslå en persons identitet bedre end, hvad man kan opnå med en personlig underskrift, så er det også et faktum, at ondsindet anvendelse af digitale løsninger kan

resultere i større risiko og større skader end ved ikke-digitale metoder. Lovgivning og behovet for ordenshåndhævelse kan påvirke designet af et given autenticitetssikringssystem og kan også resultere i krav om driftsmæssig dokumentation.

Juridiske overvejelser kan også have væsentlig indflydelse, når det nødvendige niveau af autenticitetssikring skal bestemmes for en given transaktion. Risikovurderingen bør inkludere de potentielle konsekvenser af ulovligheder samt proces-fejl i forbindelse med:

- Prioritering af myndighedsudøvelse
- Gennemførelse af myndighedens overordnede mål
- Brede offentlige interesser som miljøbeskyttelse, en sund finansiel sektor, terrorbekæmpelse etc.

Det betyder, at selv om sigtet for en given risiko-vurdering er en enkelt it-system, skal risikoen vurderes ud fra en holistisk synsvinkel.

Nogle skader (som fx økonomisk tab eller frigivelse af sensitiv information) er allerede beskrevet for hvert niveau af autenticitetssikring. Andre potentielle skader afhænger af, hvilke mål og opgaver en given organisation har. Vurdering og analyse af risici er meget afhængige af den sammenhæng, systemet anvendes i, og systemejeren bør vurdere, om der er specielle risici i forbindelse med systemet ud over de kategorier, som denne vejledning indeholder.

Ved vurdering af risiko for ulovligheder bør systemejeren konsultere sin juridiske ekspertise i forbindelse med bedømmelsen af, hvor stort skadesomfanget kan være som konsekvens af en ulovlighed¹⁰. Det er i vurdering af disse risici vigtigt både at overveje konsekvenser af enkeltstående handlinger såvel som gentagne handlinger (handlingsmønstre), der kan påvirke en myndigheds opgaver.

Det er også vigtigt at huske, at det nødvendige niveau af autenticitetssikring skal ses i sammenhæng med øvrigt sikkerhedsforanstaltninger i et system. Eksempelvis kan en given forretningsproces, der er vurderet til at skulle anvende niveau 3 akkreditiver, sænke it-systemets behov til niveau 2 akkreditiver ved at foretage andre afbødende aktiviteter som fx yderligere systemkontroller, yderligere autenticitetssikring foreholdt kritiske grene af forretningsprocessen etc.

3 Vurdering af tillid til akkreditiv-udbydere

Den identitet, som en bruger eller organisation repræsenteres med i en elektronisk transaktion, beror på akkreditiver. Den registrerings- og vedligeholdelsesproces, som akkreditivudbyderen anvender, er kritisk ved vurderingen af troværdigheden af de akkreditiver, der udstedes. For at kunne vælge akkreditiver til et system, som beskrevet i denne vejledning, må akkreditivudbyderens udstedelsesproces også være vurderet i forhold til niveauerne af autenticitetssikring.

¹⁰ Dette er fx relevant for risici, hvor konsekvenserne alligevel involverer juridisk ekspertise. Et eksempel er, hvor en virksomhed svindler ved at indberette forkerte data, hvilket resulterer i udbetaling af for store tilskud. Bestemmelse af hvor stort et erstatningskrav, det offentlige skal rejse overfor virksomheden, involverer juridisk ekspertise.

4 Implementering af en autenticitetssikringsproces

4.1 Autenticitetssikringsprocessen

Hvert trin i en autenticitetssikringsproces påvirker niveauet af sikkerhed. Fra validering af faktisk identitet, til udstedelse af akkreditiver, over anvendelse af akkreditiver i et robust og sikkert system, til journalisering, logning og kontrol. Ingen kæde er stærkere end det svageste led. Hvis et trin i en proces anvender et lavere niveau af autenticitetssikring end i resten af processen, kan dette trin kompromittere sikkerheden i de andre trin. En systemejer opnår det bedste niveau af autenticitetssikring via god kontrol i forbindelse med udstedelsen af akkreditiverne, anvendelse af stærke akkreditiver og robust administration (herunder en god arkiverings- og kontrolproces).

For at kunne bestemme det rette niveau for akkreditiver, der skal anvendes til at fastslå en bruger identitet, må systemejereren forstå, hvorledes it-systemet anvender akkreditiverne. Systemejereren må bestemme behovene for hvert trin i autenticitetssikrings- og autorisationsprocessen. Dette inkluderer følgende trin:

- Oprindelige registrering
- Efterfølgende anvendelse af it-systemet
- Verificering af akkreditiverne
- Transaktionshåndtering
- Dokumentjournalisering, historik, logning etc.
- Suspendering, inddragelse af akkreditiver og genudstedelse
- Revision

Ansvar for disse procestrin ligger hos systemejereren.

4.2 Anvendelse af anonyme akkreditiver

Det kan være passende at anvende ”anonyme akkreditiver”, når autenticitetssikringen ikke forudsætter, at akkreditiverne direkte eller indirekte (fx XRI) kan tilknyttes et individ med en kendt personlig identitet. Af hensyn til privatlivets fred er det vigtigt at finde den rette balance mellem behovet for at vide, hvem man kommunikerer med og den enkeltes behov for privatliv. Dette inkluderer, ud over hvad der lovmæssigt er bestemt, kun at anvende afgiven information til det formål, det er afgivet. I nogle tilfælde kan det være unødvendigt for et givet system, at identifikationen af brugeren også betyder, at man kommer til at kende brugerens personlige identitet. Det kan være tilstrækkeligt at autenticitetssikre på de følgende måder:

- Sikring af, at brugeren er medlem af en given gruppe og/eller har en given rolle
- Sikring af, at brugeren er den samme, som tidligere har afgivet og oprettet information
- Brugeren har ret til at anvende et givent pseudonym

Det forventes, at sådanne anonyme akkreditiver kan anvendes i specielle tilfælde, hvor det for hvert enkelt system vurderes, om det vil være passende at anvende anonyme akkreditiver. Det vil være muligt for brugere både at have anonyme akkreditiver såvel som akkreditiver, som beviser vedkommende identitet. Generelt er anonyme akkreditiver kun passende for systemer, der kræver autenticitetssikring på niveau 1 eller 2. Dette skyldes, at data, der kan få adgang til på niveau 3 eller 4, generelt er mere følsomme og derfor kræver, at akkreditiverne kan tilknyttes et individ med en kendt personlig identitet.

4.3 Lovmæssige krav

I forbindelse med udvikling af processer til autenticitetssikring er systemejeren ansvarlig for at overholde alle relevante lovkrav først og fremmest fra persondataloven vedrørende datafangst og lagring af information, som vedrører validering af en brugers identitet.

De fleste digitale processer til autenticitetssikring foretager følgende datafangst:

- Information vedrørende individer/virksomheder/myndigheder, der anvender systemet
- Digitale akkreditiver (fx certifikater fra digital signatur, bruger-id'er, kodeord, PIN, mm)
- Transaktionsinformation fra autenticitetssikringen, herunder metode til validering af akkreditiv
- Logdata/sikkerhedsinformation

Systemejeren skal sikre korrekt behandling af data, der anvendes i autenticitetssikringsprocessen i forhold til gældende lovkrav. Det drejer sig først og fremmest om persondataloven, men andre love som forvaltningsloven, patientsikkerhedsloven etc. kan også være relevante.

Autenticitetssikringsdata skal beskyttes imod ikke-autoriseret offentliggørelse og ændring, men skal kunne oplyses ved indsigtbegæring, som opfylder de lovmæssige krav herfor.

4.4 Omkostninger i forhold til nytteværdi

På samme måde som enhver anden anskaffelse skal omkostningerne for et autenticitetssikringssystem overvejes i forhold til nytteværdien. Det er vigtigt at matche det nødvendige niveau af autenticitetssikring med de omkostninger og andre byrder, som forretningsmæssige, politik-bestemte og tekniske krav til systemet i øvrigt medfører.

Nytteværdier inkluderer typisk:

- Tidsbesparelse i forbindelse med en transaktion
- Større anvendelse af samarbejdspartnere og bedre kundetilfredshed
- Bedre registrering/journalisering og mulighed for bedre analyser/statistikker
- Bedre produktivitet blandt de ansatte og forbedret kvalitet af den endelige ydelse
- Bedre indsigt/viden til offentligheden
- Bedre sikkerhed generelt og omfattende sikkerhed for yderst sensitiv information

Omkostninger omfatter typisk:

- Udgifter til løsningsdesign
- Anskaffelse af teknisk system
- Testning
- Idriftsættelse af det implementerede system
- Løbende vedligehold

I nogle tilfælde kan den initiale omkostning ved etablering af et system være relativt lille, mens der er højere omkostninger forbundet med den løbende vedligeholdelse. Det er derfor vigtigt at vurdere omkostninger i forhold til nytteværdi over hele levetiden for systemet, herunder også hvad det vil koste at migrere væk fra den givne implementering til et system, som baserer sig på anden teknologi. Understøttelse af åbne standarder, som er indeholdt i 'OIO - Kataloget over offentlige it-standarder', bør være et vigtigt kriterium i forbindelse med anskaffelse af teknisk system.

Det er også vigtigt at vurdere om omkostningerne kan nedbringes ved etablering af en fælles autenticitetssikringservice imellem flere organisationer eller ved anvendelse af en service fra en kommerciel virksomhed.

Fejl i forbindelse med autenticitetssikring kan resultere i væsentlige omkostninger for myndigheder, borgere og private virksomheder. Disse mulige omkostninger bestemmes i forbindelse med risikovurderingen, som beskrevet i afsnit 2, og de bør inddrages i en eventuel costbenefitanalyse for systemet.

Andre byrder dækker over

- a) Omkostninger som andre organisationer, virksomheder eller borgere påtvinges
- b) Tidsforbrug, der ikke er indeholdt i omkostnings-estimatet, men som er et resultat af u hensigtsmæssigheder i den tekniske system

Systemer, som medfører en overdreven mængde af andre byrder, vil måske ikke opnå den forventede anvendelse og dermed heller ikke den estimerede nytteværdi. Hvis det tekniske system til et givent niveau af autenticitetssikring medfører for store omkostninger eller andre byrder, bør systemejereren overveje at anvende et lavere niveau af autenticitetssikring og kompensere via styringskontroller og justeringer i forretningsprocessen til at opnå det samme samlede niveau for sikkerhed. Hvis omkostningerne ikke kan reduceres til et acceptabelt niveau via sådanne afbødende foranstaltninger, kan systemejereren blive nødt til justere sine visioner for systemet.

5 Yderligere information

Dette fællesoffentlige arbejde i forbindelse med tværgående brugerstyring er beskrevet på

<http://www.oio.dk/arkitektur/brugerstyring>

Information om nogle af de aktiviteter inden for it-sikkerhed, som Videnskabsministeriet varetager findes på

<http://www.oio.dk/sikkerhed>
