Difi
Direktoratet for forvaltning og ikt

Standardiseringsrådets møte #3 2018

Referat

Standardiseringsrådet - møte #3 2018

Sted og tid: Difi Oslo, tirsdag 25 september kl 09:00 – 12:00

Agenda

Tid	Sak		Ansvarlig
0900		Velkommen og godkjenning av referat og agenda	Sekretariatet
Høring av forslag til nye eller reviderte forvaltningsstandarder			
0910	18-11	Tiltak mot uønsket trafikk på internett – reviderte standarder og høringsoppsummering	Kompetansesenter Grunnleggende datakommunikasjon
Informasjons- og drøftingssaker			
1015	18-12	Statistikk og informasjon om bruk av Referansekatalogen	Sekretariatet
1045	18-13	Status - Forslaget om opprettelse av Arkitektur- og standardiseringsråd	Sekretariatet
1105		Eventuelt	
1115		Enkel lunsj (til ca 11.45)	

Deltakere

Virksomhet og navn		Tilstede	Fravær
Faste medlemmer			
Arkivverket	Bent Vangli	X	
KS	Ingeborg Berge		X
Kartverket	Magnus Karge	X	
Oslo kommune	Per Kjetil Grotnes		X
NAV	Line Langlo Spongsveen	X	
NAV	John Martin Furseth	X	
Skatteetaten	Hans Erik Gravdahl Sørensen	X	
E-helse	Thomas Tveit Rosenlund	X	
Brønnøysundregistrene (BR)	Geir Ørnulf Olsen	X	
SSB	Trygve Falch		X
Norstella	Jon Arve Risan	X	
KMD	Sidsel Tønnesen		X
Standard Norge	Erik Winther	X	
Sekretariatet (Difi)	Rune Karlsen (møteleder)	X	
Sekretariatet (Difi)	Stine Stakkestad (referent)	X	
Deltakere i forbindelse med sakene		**Saker**	

Difi	Håkon Styri	18-11

Hovedpunkter og oppsummering

Velkommen til Standardiseringsrådets møte #3 / 2018

10 deltakere møtte. I tillegg stilte referent og presentasjonsholder.

Høring av forslag til nye eller reviderte forvaltningsstandarder

18-11 Tiltak mot uønsket trafikk på internett - reviderte standarder og høringsoppsummering

Håkon Styri fra «Kompetansesenter Grunnleggende datakommunikasjon» i Difi presenterte saken. Sendt ut en høring, fire forskjellige endringer i forslag til dette i Referansekatalogen som Håkon og kompetansesenter har sett på. Fire reviderte forslag ble presentert. Dette er et oppdrag fra KMD, og er en del av et større arbeid. Gjort ferdig fire forslag, og noen reviderte som kommer frem om to uker. Involvert i arbeidet: SMD, KMD, Nasjonal kommunikasjonsmyndighet, difi, Uninett, Norid, NSM.

Hovedpunkter fra presentasjonen er standarder og forslag til vurdering:

- Sikker datakommunikasjon (HTTPS)
- Transportsikring av e-post
- Motvirke falske avsendere (e-post)
- Sikkerhet i domenenavnsystem (DNSSEC)

Har fått 29 svar ifm. høringsrunde. Ingen negative tilbakemeldinger, men ønsket justeringer. Standarder bør være enkle og klare, må oppdatere eksisterende veiledere.

Forslag A: Sikker datakommunikasjon

- Legge til RFC 2817. Gir liten verdi, og har noen ulemper. Trekker derfor dette forslaget.
- Justert tekst slik at RFC6797 ikke er til hinder.
- Logging er et gyldig argument for å ikke bruke standarden i perioder. De fleste vil ikke logge og de som logger gjør det i et avgrenset tidsrom
- Stikkprøve: 82% hadde https. Mange har oppdatert, og 2/3 snubler i å sette det opp riktig og trenger bedre veiledere. Mye av investeringene er allerede gjort, trenger derfor bedre veiledninger og tilgjengelige testverktøy.

<u>Kommentarer og innspill:</u>

- Dersom det blir obligatoriske standarder vil det måtte fremmes for departementet (KMD). Deretter må departementet vurdere og det blir ny høring og videre prosess inkludert en samfunnsøkonomisk analyse. Denne prosessen er tidkrevende og kostbar. Fått beskjed om regjeringens sikkerhetsutvalg om å gjøre denne standarden obligatorisk, og det er derfor dette vurderes.
- På andre siden er en kostnad ved nullforslaget dårligere brukeropplevelse. Obligatoriske standarder gjør at alle må ta det i bruk.

- Offentlige virksomheter skal bruke https, noe som gir god beskyttelse for brukeren. Kan bruke nett overalt, og sikre sider. Unngår reklame, kryptominer og mindre utsatt for hacking. Sertifikater og kryptonøkler: råd fra NSM fortløpende om hvilke nøkler og kryptering som bør brukes.
- Standard Norge vil vite mer om risikogapet. Hvilke kostnader er forbundet med utredninger og de som skal gjennomføre det?
    - Håkon Styri påpeker at det er verdt å få inn gapet i forskriftene, og sterkere fokus på dette fordi det er en nødvendighet. Dumt å kaste bort penger om det ikke blir gjort ordentlig. Dersom standarder blir obligatorisk vil de 2/3 som gjør det dårlig på dette punktet få fokus på at de faktisk gjennomfører dette riktig. De blir pushet i riktig retning.
- Videre diskuteres det om pengene som brukes på en utredning fra departementets side med tilhørende samfunnsøkonomisk analyse heller bør bruker til å direkte veilede de som sliter. Forslag kommer om ny høringsrunde om det bør bli obligatorisk eller satse der det trengs. Selv om det er obligatorisk må den enkelte virksomhet velge om de skal prioritere økonomisk å gjøre det som trengs, og det er ikke sikkert.
- Veldig få kommersielle programvarer som ikke har dette innbygget. Virksomhetene må faktisk lære seg å sette opp programvaren riktig. Investeringene som kreves for å få det på plass er svært lave, men litt mer må til for å få det ordentlig i orden.
- Sekretariatet stiller spørsmål om prosess fram til en forskrift og utredning i Norge, før det går videre til EU. Hva vil det koste og hva vil det bety?
    - En forskrift vil gjøre det mer prioritert. Krever ikke masse fordi mye av investeringene er gjort. Kostbart å dytte på de som ikke gjør det bra.
    - Ikke sikkert at en ny høring vil gjøre de oppmerksom på det.
- Kommentar fra NAV om at det minimum må kjøres undersøkelser. For de som ikke bryr seg, krever det nok litt mer å få de til å gjøre det ordentlig. Verktøy og prosessrunde kan gjøre mye, men støtter utredning.
- Viktig å få med seg hvorfor noen virksomheter gjør det dårligere på dette punktet selv om de har tilgang på riktig verktøy. Hva hindrer disse virksomhetene. Verktøy og prosessrunder kan gjøre mye, trenger bedre og tydeligere veiledninger og det må være et testverktøy tilgjengelig for å kunne sjekke om man gjør ting riktig.

<u>Oppsummering fra Standardiseringsrådets leder:</u>

- Undersøker dette videre for å finne ut hva som er mest hensiktsmessig av obligatorisk eller anbefaling.
- Tar ikke en endelig beslutning i dag om denne standard skal være obligatorisk, men ønsker å gå videre med prosess for utredning/vurdering av denne som obligatorisk, inkl samfunnsøkonomisk analyse.

Forslag B: Transportsikring av e-post

Hovedpunkter:

- DANE er en mekanisme som retter opp dette punktet. Utbredelse i Norge er liten, ingen i stikkprøven bruker dette. Få som tilbyr, og derfor for dårlig til å lage en anbefaling basert på dette.

- Forslag at behandlingen av dette utsettes til neste møte fordi det skjer endringer/vedtak i standarder på området akkurat nå. Dette kan endre forslaget.

Oppsummering fra Standardiseringsrådets leder:

- Trenger ikke gjøre forslaget vanntett, men trenger å forberedes.
- Forslaget utsettes til neste møtet.

Forslag C: Motvirke falske avsendere (e-post)

DMARC, har ligget en del år, tatt i bruk av flere land som noe man ønsker å bruke. En mekanisme som gjør at man kan sjekke at avsender faktisk er den korrekte avsender.

- To mekanismer, og man kan velge hvilken man vil bruke. Trenger ikke implementere begge mekanismene når man sender ut.
- Kommet en del innspill i høringsrunder. Stikkprøver: veldig mange har satt opp teknologien, men bare 1/5 har faktisk brukt det de har kjøpt. Bør ikke være noe stort hinder, fordi mekanismene er i stor grad på plass.
- Dette vil motvirke phishing-angrep, og bidrar til økt sikkerhet.
- Offentlige virksomheter trenger bedre veiledning.

Kommentarer og innspill:

- Standard er en ting, men må prøve å få gjort noe med kompetansenivå slik at de får brukt det.
- Sekretariatet påpeker at det finnes veiledere, men problemet er at folk ikke vet at det finnes.
- Bruker man f.eks. Microsoft Office 365 er mekanismene på plass. Må bare finne ut hvordan man setter det opp. Veletablert teknologi, og ofte inkludert i prisen man betaler. Sånn sett liten investering i lisenser og avgifter: men må få peke på gode veiledere. Ikke noe grunnlag for å foreslå obligatorisk.
- Viktig informasjonstiltak slik at borgerne tror det er noe man kan forvente fra offentlige virksomheter.
- Mottaker muliggjøres og er de som kan bruke mekanismen ved å sjekke avsender. Ønsker en anbefaling slik at mottaker vet at de kan sjekke alt som kommer fra offentlig sektor.

Oppsummering fra Standardiseringsrådets leder:

- Virker som alle støtter anbefalt standard, men forutsetter gode veiledninger.
- Tekst oppdateres/legges inn i Referansekatalogen

Forslag D: Sikkerhet i domenenavnsystemet.

- Offentlig sektor ligger langt bak privat sektor på dette feltet. Mulig forklaring: enkelte tilbydere krever litt ekstra betaling og offentlige anskaffelsesregler sier at vi skal bruke det billigste.
- Høy grad av avlytting i domenenavnforslag. Trenger konfidensialitet og ingen forfalskning. Det er ofte litt for lett at det er mulighet for å gjøre det.

- Vurderer ikke en obligatorisk standard. Men ønsker erfaring med gjennomføring og kostnader for et godt grunnlag for å gå videre til obligatorisk. Først anbefalt og sjekker effekt og hvis det er godt nok så kan man fortsette det. Men må det skrus litt til og sterkere virkemidler kan det vurderes obligatorisk, men kan ikke si noe om det nå.
- Utbredelse og innsikt om standarder trengs. Viktig for de som vurderer budsjettene. Trenger gode argumenter gjennom god forståelse og innsikt.
- Skatteetaten legger fram at man bør vurdere å ha en samlepakke for offentlige virksomheter. Visse punkter som må være oppfylt, og samla bilde av økt sikkerhet bør være anbefalt. Dette er kompetansekrevende for virksomhetene. Kan Norid hjelpe til her? Kanskje burde man vært mer tjent med referansekatalog?
- Hovedproblemet er at svært mange bruker programvare som er ti år gamle eller eldre. Da er det ganske mange sikkerhetshull. Trenger å bytte på standarder. Men er en prioritering og trenger et spark bak. Andre ting som haster mer.
- NAV påpeker at når man har en standard så er det lettere å ha default settinger. Når du setter opp ting helt på egenhånd er det mer risiko.

Oppsummering fra Standardiseringsrådets leder:

- Trenger god veiledning som er veldig viktig. Behovet for obligatorisk standard er ikke så viktig, fordi egeninteresse er at det er viktig å ha et sikkert system.
- Støtter forslaget og ser på det som at man er på vei til en helhetlig sikkerhetspakke. Må se ting i sammenheng.
- Forslaget til anbefaling tas inn i Referansekatalogen og publiseres når en oppdatert veiledning for bruk er på plass.

Informasjons- og drøftingssaker

18-12 Statistikk og informasjon om bruk av Referansekatalogen

Rune Karlsen ved sekretariatet presenterte saken. Innholdet er webstatistikk for Referansekatalogen og webstatistikk for standardiseringssider på Difi.no. Standardiseringssrådet tar informasjon til etterretning.

Hovedpunkter:

- Jan-Aug 2017 mot Jan-aug 2018: økt 61 %. Fra 2016 til 2017: 150%.
- Sekretariatet foreller at det ikke er gjort noen detaljerte undersøkelser på hva som har skjedd i løpet av perioden hvor det oppleves økning.
    - Mye i mars, april, mai 2017: lagt ut en del høringer og saker som kom opp og bidro til bruken.
    - Prøvd å nevne i forskjellige fora, internt i Difi og eksternt, men ikke noe grep utenom det vanlige.
- Veldig mange brukere kommer inn fra andre sider enn via Bruksområder. Det med søk er viktig, men ikke nødvendigvis på Referansekatalogen som begrep. Søker direkte på det de vil inn på.
- Trend om økning på sidevisninger, spesielt på høsten som kan være at mange prosjekter som skal være klar på høsten (anskaffelser) dermed korrelasjon.

Kommentarer og innspill:

- NAV ytrer at veilederne er kanskje det som gir størst nytteverdi. Kanskje når man f.eks. snakker om sikkerhet så kan man kjøre kampanjer. Promotere gode veiledere.
- Fra Difi sin side, kan de promotere på stands og arrangementer.
- NAV lurer på om det finnes en engelsk oversettelse. Dette trengs når det er utenlandske aktører, dette gjelder spesielt i store anskaffelser.
    - Standard Norge meddeler at det finnes masse standarder på deres sider som er på engelsk. Hvis man linker mellom standard Norges og Difis sider så får man opp bruken gjensidig. Link til de engelske variantene og legge rett inn i offentlige og private anbud. Sekretariatet (Rune) og Standard Norge vil ta dette med hverandre på et senere tidspunkt.

Oppsummering fra Standardiseringsrådets leder:

- Ser på gjennomgangen nå som en grei oversikt over hvordan Referansekatalogen blir brukt og bruke det som bakteppe.
- Tror det er potensiale for forbedringer for sidevisninger, ikke alle virksomheter vet om dette.
- Hvis mulig, reklamere på egne sider.
- Reklamere i forbindelse med deltagelse på seminarer hvor Difi er med, promotere referansekatalogen.
- Standard Norge og Difi koordinerer.

18-13 Status - Forslaget om opprettelse av Arkitektur- og standardiseringsråd

Rune Karlsen ved sekretariatet presenterte saken.

Først repetisjon.

- Felles kjøreregler (ikke bare på standarder)
- Prinsipper, standarder og løsninger
- Behov for også å gjøre arkitekturprodukter til anbefalt/obligatorisk.
- Vurderes lite effektivt med to råd med overlappende ansvarsområder.

Veien videre:

- Avklaring med KMD 5. sept.: la frem modellen som er foreslått, videre prosess og mandat, krever kanskje justering av forskrift (men ikke så stor endring). Kan utvide og starte opp arbeidet i et råd uten at den formelle forskriftsendringer er godkjent, og det bør ikke være en bremsekloss.
- Skatemøte 26. sept.: tilslutning til anbefalt forvaltningsmodell og tilslutning på innretning til mandatarbeidet.
- Utforming av mandatet: bred involvering, ta med det beste fra eksisterende mandat og erfaringer (standardiseringsrådet), tar med viktige innspill fra høringsrunden våren 2018.
- Mandat og veien videre forankres med KMD. KMD og Difi vurderer en mulig opprettelse. Nullalternativ er at det fortsetter som i dag. *Rune endrer fra opprettelse, til utvidelse.*
- Tidsplan: ikke avklart, men mandatarbeidet settes i gang med tilslutning fra skate 26.9. Høsten vil gå til å få mandatet på plass.
- Sendes ut spørreskjema til standardiseringsrådet og kompetansesenter. Ønskelig med innspill for hva som fungerer og ikke. Hva kan justeres?
- Arkivverket forteller at det er kurs om dette på NOKIOS, fokuserer på praktiske case og hvordan bygge tjenester som går på tvers i offentlig sektor og diskusjon.

- På Difi.no sider for det som finnes på arkitektur, kan orientere seg her. Rammeverk (NIF og EIF).

Oppsummering fra Standardiseringsrådets leder:

- Må ta den tiden som trengs før man gjør noe vedtak. 1 eller 3 måneder ekstra har ikke noe å si. Viktig med en god og riktig prosess for å utvide til et felles Arkitektur- og standardiseringsråd.

Eventuelt

Rune Karlsen ved sekretariatet hadde to punkter under eventuelt, og standardiseringsrådsleder hadde to korte punkter. Det var for øvrig skryt av Rune fra leder som pusher framdrift av forskriftsendring og tar tak i ting.

1) **ELMER**
   - BRREG har intern runde, og har kommet frem til at ELMER ikke er så relevant lenger. Man har gått bort fra skjema, og over til dialoger. Har utarbeidet internt notat og innstillinger, og venter nå på godkjennelse/forankring fra toppledelsen. Meddeler at ingen tar kontakt med BRREG om ELMER lenger. Dette vil tas opp på neste møte etter forankring med toppledelse i BRREG.
2) **Forskriftsendring**
   - Sekretariatet har Dialog med KMD på forskriftsendringen.
   - Difi la frem sitt forslag om endring av forskrift i oktober 2017. KMD skal formelt behandle videre i EU-høring osv. Dette har feilet i første forsøk og må gjøres/startes på nytt.
   - Overføring til ESA tar 3 måneder, så går det til regjeringsbehandling/statsråd osv. Tar tid og derfor har KMD antydet januar 2019 som dato ny for ferdigbehandling og ikrafttredelse av oppdatert forskrift.
3) **Arkivverket gjennomfører høring.** Skal leveres en ny rapport om Norsk Arkivstandard
4) **Tema for standardiseringsrådsmøter**
   - Innspill om tema til Rune/Sekretariatet når det er noe dere vil ta opp.
   - Alle medlemmer og kompetansesentra oppfordres til å melde inn aktuelle saker til sekretariatet.

Neste møte: 11. desember.

Dato og referent
Oslo, 04.10.2018
Difi/Standardiseringssekretariatet
Rune Karlsen/Stine Stakkestad

Versjon og status
0.5 - Under arbeid
0.9x - Utkast – til kommentarer hos deltakerne
1.0 - Ferdig – forbehold om formell godkjenning
1.0 - Endelig