Pedersen, Klaus Vilstrup

Fra: Hagen, Erik
Sendt: onsdag 9. mai 2018 22:34
Til: Pedersen, Klaus Vilstrup
Emne: Mine notater fra i dag

Hei Klaus,

Håper du er vel hjemme!

Her er mine notater fra i dag – for hva det er verdt:

Tilstede:
Anne Lise Furmyr, Skatteetaten
Erik Nygren, Skatteetaten
Øivind Syrstad, Skatteetaten
Stig Dørmænen, Brønnøysundregistrene
Rolf Næss, Acando/Brønnøysundregistrene
Anders Nordin, Politiet
Håkon Jendal, NAV
Klaus Vilstrup Pedersen, Difi
Svanhild Gundersen, Difi
Jørgen Binningsbø, Difi
Erik Hagen, Difi

Token-mekanismer

Jørgen, presentasjon

Åpne standarder!
Med begrepsapparat
Token: handler om autentiseringsbevis ... OpenID Connect

Oauth2 - autentiseringsnær autorisasjon, access_token vs. refresh_token
access_token

Eksempel: SVV, der eu regnr. gis sammen med access_token, svar med personnr, slik at verksetdet slipper å holde rede på poersonnr

Tokenberikelse fra auoritative kilder

I scope her: Virksomhetsautorisasjon /svært enkel), Difi-løsning tatt fra ifm. KRR. Kan gjenbrukes
=> Virksomhetssertifikat gir access token til tjeneste

Skatt, Nav: Veldig bra, dette svarer på våre behov (men glem OpenID Connect her, bare Oauht)

Jørgen: Vil ikke trekke inn SMP-en her

Håkon + Øivind: Det som er viktig for NAV (og andre) er at en slipper å finne opp kruttet selv , og at behovet for utviklerkompetansen begrenses	

Rolf Næss: Hva med vedlikehold av katalogen som gir kopling fra virksomhetssertifikat til access_token

På vegne av-funksjonalitet finnes.. ID-porten som komponent!

Rolf N: Tre ulike problemstillinger (som jeg ikke fikk notert riktig - her følger bare deler av dette): Hassle med sertifikater, …PKI-validering i offentlig sektor?
Hvilke behov har en API-eier… hva skal en API-er bestemme for alle konsumentene

Rolf M. Vi har dykket rett ned i detaljer om løsning, om f.eks. access token uten å ha definert scenarier og problemstillinger. Behov for top down?!
Øivind: Iterativt - båe høyt og lavt
Klaus: Middle out!

Tore: Brreg har ikke infrastruktur for token, så vi vil gjerne lære av dere
Øivind; Det har ikke Skatt heller.
Håkon, Det har ikek NAV heller

Om Openshift vs, Kubernetes for Container Management: …?

Konklusjon: Neste workshop med alle fysisk tilstede, med "dette" (token) som eneste tema. 22. mai 12-16.

Rolf, gjennomgang av sitt dokument

Rolf har oppsummert hva vi holder på med og noen forutsetninger - "top-down"
Svar med en gang..
…
Ser kun på virksomheter!? (Jørgen hadde senere også en kommentar om at personer kanskje kan dekkes av samme mekanismer
Klient som opptrer på vegne av virksomhet, eller på vegne av borger? Klaus: Begge deler! To ulike scenarier.
Hjemmel?
API fra private virksomheter (eks. bank)
API-er fra private (f.eks. utviklet på en offentlig plattform)
Om personnr er sensitivt er kontekstbasert
Anders, Politiet vil ikke…. URL ikke beskyttet av TLS… Øivind sier Anders tar feil!?

Håkon: Referansearkitektur finnes på flere nivåer - der f.eks. bruk av get eller post blir en "løsningsreferansearkitektur"

Hovedproblem som ble diskutert: Aksesslogger der get-kallene finnes, dvs. mye sensitiv informasjon i loggene

Hvor langt skal en gå i å "forutsette" at aksessloggene sikret?

Ang. OWASP: OWASP funker i en browser-kontekst, men ikke nødvendigvis maskin-maskin

Stig: Debatten tyder på at REST er så problematisk at det kan virke som vi bør gå tilbake til SOAP, men det kan da umulig være tilfelle, eller?

Avklaring: Overordnet referansearkitektur for eOppslag er ikke begrenset til Rest!

Merk: Aksesslogger kan inneholde payload, ikke bare header

Spørsmål: hva er ende-til-ende? Applikasjon til applikasjon?
TLS ende-til-ende som løsning… ? Hva er forskjellen på enveis og toveis…

Spørsmål, Øivind, Erik (Skatt): Stick to REST-prinsipper?

Aksjonspunkt: Håkon gir overordnet oppsummering av problemstillingene rundt aksesslogger og måter å håndtere det på

Håkon, gjennomgang av sin presentasjon

Slide:Forutsetninger
Engelsk vs. norsk.
Konklusjon: Beholder norsk inntil videre

Slide om Stegvis oppbygging av sikkerhet..
Hvordan indentifisere krav til sikkerhet: Detaljert metodikk for dette har vi ikke (Difis veiledere er ikke spesifikke nok?)

Utestående:
Dokumentere hvilke krav/trusler som vil medføre an trenger ende-til-ende integritet på respons
Dokumentere tilsvarende for "delvis uavviselighet" (ikke mulig å oppnå full uavviselighet)

Nivåer av sikkerhet: 0-3…

Integritet og konfidensialitet på transport: VPN, ikke TLS???
… enveis TLS…

STS (Security Token Service) som ABB er OK -> oauth2 auhorization server

ABB-er… skille mot SSB?

Slide: Noen fordeler med å benytte OAUth2.0 access token fra ID-porten

Ulike nivåer av tilgangskontroll: Scope, ikke Audience, ref. Jørgen

Håkon oppfordrer alle til å gi innspill til dokumentet

Snakkes!

Vennlig hilsen
Erik Hagen
seniorrådgiver
M: 906 31 013
A: Grev Wedels Plass 9, 0151 Oslo

Difi
Direktoratet for forvaltning og ikt

Postboks 8115 Dep., 0032 Oslo
www.difi.no