Utlåtanden till gränssnittsrekommendationer för SAML- och OpenID-protokoll

1 Bakgrund

Transport- och kommunikationsverket Traficom publicerade gränssnittsrekommendationer för SAML- och OpenID Connect-protokoll av identifieringstjänster år 2018. När TUPAS-protokollet kördes ner år 2019 observerade man att det finns skäl att precisera gränssnittsrekommendationen.

År 2020 skapade Traficom en öppen e-postlista som koncentrerar sig på tekniska frågor som hänför sig till stark autentisering och betrodda elektroniska tjänster. Den tekniska gruppen som främst består av aktörer i förtroendenätet och deras experter mötte flera gånger år 2020 och dryftade revideringen av gränssnittsspecifikationen. På basis av respons och förslag av den tekniska gruppen begärde Traficom utlåtanden om ändringarna till protokollen S212 (SAML) och S213 (OIDC) på utlåtande.fi under perioden 5 mars – 6 april 2021.

Myndigheten för digitalisering och befolkningsdata DVV, OP Gruppen, Danske Bank, Ubisecure och Aktia Bank svarade på begäran om utlåtande. Utlåtandena behandlas under följande avsnitt.

1.1 Avsnitt 2.2.2 Är tabellen uppdaterad?

Ja: 5

Nej: -

Kommentarer:

- Fasta hänvisningar till algoritmer bör undvikas i specifikationen. Det skulle i stället vara bra om man ger en hänvisning till en förteckning över algoritmer som ett etablerat standardiseringsorgan har specificerat och uppdaterar aktivt.
- Vi ser inga behov för uppdatering.

Transport- och kommunikationsverkets bedömning: På basis av utlåtandena ser det ut som om det inte finns något behov att ändra rekommendationerna. Beslut: Inga förändringar

1.2 Avsnitt 2.2.3/4.2.2 Ska signering av autentiseringsbegäranden specificeras som obligatoriska (för tillfället är detta valbart)?

Ja: 5

Nej: -

Kommentarer/Varför:

- Det skulle inte finnas s.k. rum för tolkning i olika användningsfall i fråga om huruvida signatur skulle vara obligatorisk eller inte och det säkraste möjliga sättet skulle alltid användas med tanke på autentiseringsbegäranden. Det skulle alltid vara möjligt att kontrollera vem som skickat begäran.

- Skäl: Det är viktigt att ha autentiseringbegäran singerat så att vi vet som är källan för begäran. Det finns också en utgångstid för signatur och kan därför inte bedrägligt åkallas.
- Autentiseringsbegäran mellan Broker och IdP bör vara signerad. Autentiseringsbegäran innehåller vissa parametrar, t.ex. acr_values och ftn_spname, vars integritet bör vara bekräftad.
- Specificeringen av signaturen som kategoriskt obligatorisk skulle minska behovet av individuell konfiguration och göra implementeringen enklare.
- Obligatoriskhet skulle vara bra för det skulle hindra förfalskning eller kapning av autentiseringsbegäranden.

Transport- och kommunikationsverkets bedömning:

På basis av utlåtandena är det motiverat att ändra den förlitande partens signatur för autentiseringsbegäranden från frivillig till obligatorisk.

Signering av autentiseringsbegäranden inom förtroendenätet kan fortfarande vara valfri.

Samma fråga har diskuterats inför revidering av föreskrift 72 och behandlingen fortsätter också i själva beredningen av föreskriften.

Beslut: Ändras till obligatorisk

1.3 Avsnitt 3.1.1.2/3.1.2.2 Är förteckningen över icke-obligatoriska attribut tillräcklig?

Ja: 4

Nej: -

Kommentarer/Vad ska läggas till:

- Som kommentar är AuthCachingDisabled ny enligt vår uppfattning. Det viktiga är att dessa blir icke-obligatoriska attribut också i framtiden.

Transport och kommunikationsverkets bedömning:

På basis av utlåtandena ser det ut som om det inte finns något behov att ändra rekommendationerna. AutoCachingDisabled har varit i rekommendationen redan från början.

Beslut: Inga förändringar

1.4 Avsnitt 4.2 Är kommentaren om ftn_spname, som ändrades till en obligatorisk parameter för autentiseringsbegäranden, tillräckligt klar?

Ja: 3

Nej: 2

Kommentarer/Hur skulle du ändra texten:

- Skäl: Enligt beskrivningen förväntas det att tjänsteproducentens namn visas på det språk som användaren väljer. Betyder det att tjänsteleverantören måste skicka namnet på alla tre språk? Var god och förklara.

- Med tanke på slutanvändarens användningserfarenhet skulle det vara bra att specificera behandlingen av parametern.

  Skulle namnet på förmedlingstjänsten visas i användargränssnitt eller skulle det vara möjligt att visa det utöver applikationsnamnet? I detta sammanhang betyder användargränssnitt ofta två saker: användargränssnittet som visas på användarens webbläsare och användargränssnittet som visas i identifieringsverktyget.

  Det skulle vara viktigt att visa samma information i identifieringsverktyget och i webbläsaren så noggrant som möjligt.

  Till exempel, om webbläsaren visar att "Du håller på att logga in på Exempelbutik Ab:s tjänst" bör samma applikationsnamn visas i verktyg för mobil identifiering.

Transport- och kommunikationsverkets bedömning: För attributen ftn_spname verkar det finnas ett behov att specificera gränssnittsspecifikationen. Att visa namnet på serviceapplikationen i alla de situationer och användargränssnitt som kräver användarens åtgärder har föreslagits som obligatorisk vid revideringen av föreskrift M72. I själva rekommendationen vore det bra att specificera vad man ska göra med webbläsarinställningarna på olika språk. Beslut: Beskrivningen som hänför sig till språkversionerna specificeras vid behov senare på basis av den tekniska arbetsgruppens åsikter. Texten i den nuvarande rekommendationen kan vara tillräcklig "The name is RECOMMENDED to be in the same language as user's preferred user interface language (parameter ui_locales)." Språkversionen raderas från den rekommendation som publiceras och behandlas på nytt om den tekniska gruppen anser att det är viktigt.

1.5 Avsnitt 4.2.1 Bör antalet attribut som förmedlas i sammankoppling av inledande identifiering ökas?

Ja: -

Nej: 4

Kommentarer/Vad ska läggas till:

- Reason: A sufficient parameter "ftn_chain_level" already exists.
- Det finns inte något behov att lägga till attribut till autentiseringsbegäranden. I stället kunde de nuvarande FTN LOA-nivåerna specificeras med en vektor som beskriver den inledande identifieringens styrka; det skulle kunna anges som attribut som överlåts i autentiseringsresponsen i samband med en sammankopplad identifieringstransaktion.

Transport- och kommunikationsverkets bedömning: På basis av utlåtanden verkar det inte finnas något behov att lägga till attribut till inledande identifiering. Beslut: Inga förändringar

1.6 Avsnitt 4.3.1/4.5.1 Är den nya specificeringen av fel på tillräcklig nivå?

Ja:

Nej: 4

Kommentarer:

- De vore bra om det fanns flera än två specifikationer på error-nivån. Slutledningen bör inte överföras till datainnehållet i sektionen error_decscription; i stället bör mottagaren direkt få det korrekta error=[värdet] med en entydig betydelse. Exempelvis speciellt 'user cancel' bör vara på error-nivån så att den kan särskiljas från den egentliga access_denied-situationen.
- Skäl: Det behövs flera svarsmeddelanden för fel. Till exempel, "invalid_grant", "invalid_grant_type", "invalid_state" som anger att autentiseringskoden har upphört att gälla och att en ogiltig kod skickas.
- Villkoret av att returnera ett felmeddelande bara till en identifierad kundimplementering, som diskuterades i arbetsgrupperna, är inte med i avsnittet.
- En separat felkod bör läggas till för 'cancel'. Fel = "cancel" som sedan kan ha ett ytterligare error_description fält, eller inget ytterligare fält.

Transport- och kommunikationsverkets bedömning:

Behandling av fel diskuterades i den tekniska gruppens workshopar år 2020. Traficom önskade att medlemmarna i förtroendenätet ger ett ändringsförslag till rekommendationen. Ändringsförslaget erhölls och man gick igenom det i den tekniska gruppens workshop. På basis av kommentarerna kan man tolka att texten i rekommendationen ännu inte motsvarar det man önskat. Enligt Traficoms åsikt kan omnämnandet av returnering av felsvar läggas till i rekommendationen omedelbart. Vid behandling av fel skulle det vara önskvärt om aktörerna i förtroendenätet kunde nå enighet om en standardmetod för att behandla fel eller felsituationer. Enligt Traficoms åsikt skulle det vara bäst att arrangera en separat workshop för att harmonisera behandling av fel, där aktörerna kunde nå enighet om praxis och standardiserade felmeddelanden.

Beslut: Ett omnämnande av returnering av felsvar till en identifierad serviceapplikation läggs till. För behandlingen av fel arrangeras en separat workshop och på basis av den bildas en harmoniserad syn på de ändringar som behövs i rekommendationen.

1.7 Fritt formulerad respons på OIDC-rekommendationen
Var god och ge fritt formulerad respons på utkastet (OIDC).

- Fri OIDC-respons

  Ange vissa primära krav för visning av UI, t.ex. knappen Avbryt, visa namnet på tjänsteleverantören, val av språk, osv.

  Det vore bra att visa logg/fel ID så att det kan användas för utredning.

- I avsnitt 2.2.1 uppmanas till användning av på förhand pin-försedda nycklar, men processen för nyckelutbyte beskrivs inte. Detta har lett till variationer i förfarandena med nyckelutbyte i nätverket. I nyckelutbyte

skulle det vara bättre att agera på det i OIDC Core-specifikationen vedertaget sätt.

Transport- och kommunikationsverkets bedömning: En av frågorna som diskuterades i de tekniska workshoparna år 2020 var att harmonisera användargränssnitt och föra in dem i rekommendationen. Ämbetsverket önskade få ett förslag av aktörerna men inga förslag kom in. Det är möjligt att lägga till en enhetlig grafisk utformning eller element i rekommendationen men detta behöver en omfattande godkännande av aktörerna i förtroendenätet. Dessutom är det väsentligt att förslaget till ändring av rekommendationen skulle komma från aktörerna i nätverket som deras enhetliga syn. Vid revideringen av föreskrift M72 har det framhävts att namnet på serviceapplikationen bärs och syns genom hela identifieringsprocessen. När föreskriften blir färdig kommer texterna i rekommendationerna att ändras för att avspegla den nya föreskriften och motiveringen till föreskriften. Pinförsedda nycklar (certificate/key pinning) och nyckelutbyte både på telekommunikations- och applikationsnivån tydliggörs i samband med revideringen av föreskrift 72. Efter att föreskriften blivit färdig kommer Traficom också att ändra gränssnittsspecifikationerna så att de avspeglar de eventuella ändringarna i föreskriften eller i motiveringen. Tidtabellen för ändringarna som hänför sig till föreskriften är början av 2022. Beslut: Inga ändringar i rekommendationen. Önskan som framfördes för användargränssnitt kommer också att diskuteras i den tekniska gruppen.

1.8 Kommentarerna om SAML-rekommendationen Var god och ge fritt formulerad respons på utkastet (SAML).

- Fritt formulerad respons på SAML

  Standardisera förnyelse av nyckel i SAML-flödet.

Transport- och kommunikationsverkets bedömning: Saken behandlades i föregående avsnitt (pinförsedda nycklar/nyckelutbyte)

1.9 Övriga kommentarer/Utlåtanden

- Traficom har begärt att Myndigheten för digitalisering och befolkningsdata (DVV) ger sitt utlåtande om förtroendenätets SAML- och OIDC-gränssnittsrekommendationer. Myndigheten för digitalisering och befolkningsdata tackar för möjligheten att få yttra sig och konstaterar följande.

  DVV anser att det är bra att gränssnittsspecifikationen uppdateras och att uppdateringsarbetet har gjorts i samarbete med förtroendenätet och andra marknadsaktörer. DVV anser också att det är bra att gränssnittsspecifikationerna publiceras enbart på engelska för att vara direkt tillgängliga för många och att det inte ska bli några tolkningsskillnader mellan olika språkversioner.

  Avsnitt 2.2.3 / 4.2.2

  DVV anser att det är bra om signering av autentiseringsbegäranden skulle specificeras som obligatorisk i gränssnittsrekommendationen. Signering av

en autentiseringsbegäran är redan nu en ganska vanlig praxis, men om den skulle specificeras som obligatorisk skulle det inte finnas rum för tolkning i olika användningsfall i fråga om huruvida signatur skulle vara obligatorisk eller inte och det säkraste möjliga sättet skulle alltid användas med tanke på autentiseringsbegäranden. Det skulle alltid vara möjligt att kontrollera vem som skickat begäran.

Avsnitt 4.3.1 / 4.5.1

DVV föreslår att ordlistan för specificering av felsituationer skulle kunna vara mera omfattande än två termer. Slutledningen bör inte överföras till datainnehållet i sektionen error_decscription; i stället bör mottagaren direkt få det korrekta error=[värdet] med en entydig betydelse. Exempelvis speciellt 'user cancel' bör vara på error-nivån så att den kan särskiljas från den egentliga access_denied-situationen.

Annars har DVV inte någonting att yttra sig över gränssnittsrekommendationerna.