Vahvemman uudet ominaisuudet 1-2018

Aika:	Torstai 8.3.2018 13:30-15:00
Paikka:	Espoo, Keilaniemi, CSC, Sekvenssi & https://cscfi.zoom.us/j/605121495 Join from PC, Mac, Linux, iOS or Android: https://cscfi.zoom.us/j/605121495 Or an H.323/SIP room system: H.323: 109.105.112.236 or 109.105.112.235 Meeting ID: 605 121 495 SIP: 605121495@109.105.112.236 or 605121495@109.105.112.235
Läsnä:	• Timo Alatalo (TUT) • Janne Lauros (CSC) • Jukka Karvonen (HY) • Jussi Tirkkonen (TUT) • Timo Tunturi (Aalto) • Arto Tuomi (CSC) • Kari Laalo (CSC)

Avaus

Haka-ohjausryhmä kertoi vahvemman uusista ominaisuuksista keskustellun organisaatioissa ja nimesi henkilöitä, joilla saattaa olla ideoita vahvemman tunnistamisen jatkokehittämiselle.

Esitetyt ideat vahvemman uusille ominaisuuksille ja jatkokehitykselle

- Luovutaan KT1 Hakan vahvemmassa keskitetyssä
  - Jatkossa, jos tulee tarve KT1:lle, tällaisille palveluille toteutetaan oma instanssi palvelun omalla kustannuksella
- Kysytään 2FA vain yhden kerran vuorokauden aikana tunnetulta päätelaitteelta
  - Tämä ominaisuus todettiin tärkeimmäksi toteutettavaksi, joka on toteutettava ensin
  - Totetusehdotus: Tehdään uusi moduli johon voidaan konfiguroida perussäännöt käyttäjän 2FA:n "muistamiselle". Konfiguroitavat asiat:
    - Aikamääre (organisaatio voi määrittää)
    - seuraavassa sessioilla viitataan MFA:n voimassaoloon, ei IdP:n (tai SP:) autentikaatiosessioon
      - Proriteetti 1:
        - rolling window per selain, eli sessio pysyy voimassa niin pitkään, kuin käyttäjä käy kirjautumassa nykyisellä sessiolla määritetyn ajan kuluessa
        - riittää, että toteutetaan selainkohtaisesti
        - tuki usealle samanaikaiselle sessiolle eri selaimilta
      - Prioriteetti 2:
        - session kokonaispituus, eli sessio ei voi olla ikuisesti voimassa, vaan organisaatio määrittää session kokonaispituuden
      - Prioriteetti 3:
    - Kirjautumisen kohde
      - Prioriteetti 4
        - Kohdekohtainen kokonaispituuden säätö (esim. Palvelu X vaatii totp/vuorokausi ja palvelu Y totp/2w)
    - Käyttäjän verkko
      - Epäolennaista, eikä juuri mielenkiintoista, sillä työntekijät esimerkiksi tekevät etätyötä
    - Yleiset reunaehdot
      - Käyttäjällä on oltava mahdollisuus revoikoida (kaikki) sessiot samalta tai muulta päätelaitteelta, jolla MFA on toistaiseksi luotettuna
      - Sääntö voidaan rajoittaa tiettyihin sallittuihin palveluihin (tai kaikkiin?)
      - noudatetaan forceAuth, eli forceAuth pakottaa totaalisesti uuden kirjautumisen, eli tehdään uusi tunnistus ja uusi 2FA riippumatta siitä, onko vanhoja sessioita olemassa millään tasolla
  - Tämä paketoitaisiin uuteen MFA Client- projektiin siten että IdP ei ottaisi enää käyttöön MPASS projektin geneeristä OIDC ratkaisua vaan MFA Client - projektista saisi täsmä asennuksen.
- MFA API Proposal
  - Ominaisuus 1: Organisaatiolle keino kysyä listaa omista käyttäjistä joilla token rekisteröity
    - Web-service (kyllä/ei vastaus)
      - kysytään eppn:llä, onko MFA käytössä tällä käyttäjällä
    - Web-service (json taulukko)
      - IDM voi kysyä luettelon oman organisaation käyttäjistä, joilla on MFA käytössä
      - kotiorganisaatio luovuttaa schacHomeorganisation arvon, jonka perusteella käyttäjä sidotaan kysyvään organisaatioon
  - Ominaisuus 2:.. Statistiikkaa?
  - Toteutus ehdotus: MFA projektiin luodaan API rajapinta jonka kautta tunnistetut organisaatiot voivat kysyä heitä koskevia tietoja
- Uusia rekisteröintivaihtoehtoja (järjestys määrittää prioriteetin)
  1. Tiskirekisteröinti (tokenin tallentaminen virkailijan avustamana)
  2. Suomi.fi

        a. Mobiilivarmenne
        b. Edellyttää, että organisaatio luovuttaa henkilötunnuksen
- Muut toiveet
    - Vaaditaan vahvempaa aina mennessä tiettyyn (esim. sisäiseen) palveluun
    - Käyttäjille tai adminille opt-in toiminnallisuus. Tarkoittaa, että käyttäjä (tai admin?) voisi määritellä, että kaikkiin palveuihin vaaditaan vahvempaa hänen id:llään kirjautuessa
        - Tämä ominaisuus toissijainen suhteessa päätelaitteen muistamiselle ja luettelossa edellä oleville toiveille
        - Aina aaditaan vahvempi
        - Vahvempi vaaditaan seuraavalla kirjautumiskerralla
    - Sähköposti-ilmoitus käyttäjälle uuden MFA-tokenin rekisteröimisestä
        - Edellyttää, että organisaatio luovuttaa sähköpostiosoitteen MFA-palvelulle

Aiheita uusille ominaisuuksille

- Yleisesti MFA:lle
    - HR:n UI:lla voi muuttaa tilinumeroa, jolle palkka maksetaan
    - HR:n UI:lla voi käynnistää out-prosessin (irtisanominen)
- Aikamääre MFA:n vaatimisessa
    - Jonkin virkailijan päätyötä saattaa olla laskujen hyväksyminen. Jos MFA vaaditaan jokaisella kirjautumiskerralla, saattaisi työpäivästä muotoutua hankala

Muita huomoita

- Vaikea nähdä todennäköisenä, että esim. toimikorttikirjautuminen muuttuisi luotettavaksi tai riittävän käytännölliseksi, jotta siihen voitaisiin luottaa
- Turvallista pelkästään päätelaitteeseen perustuvaa vahvaa tunnistamista on vaikea nähdä horisontissa

Eteneminen

Toteutusjonoon:

1. Toteutetaan yksittäisen selaimen muistaminen (eli ei kysytä toista tunnistetta). Osana tätä toteutaan vaihtoehtoiset konfiguraatio-optiot:
    a. Aika, jonka jälkeen kysytään toinen tunniste uudelleen. Tämä aika on aina kiinteästi asetettu suoritetusta MFA-tunnistustapahtumasta.
    b. Aika, jonka sisällä tunnistus siirtää toisen tunnisteen kysymistä eteenpäin.
2. Seuraavana optiona on liittää yllä listatut aika-asetukset SP-kohtaisesti.

Jatkokehitykseen ja -jalostukseen

- Sähköposti-ilmoitus käyttäjälle, että hän on rekisteröinyt tunnistusvälineen MFA:ssa. Samassa sähköpostissa voidaan ohjeistaa tulevaisuuden ongelmatilanteita tai ainakin linkittää ohjeisiin.
- Käyttäjä revokoi kaikki sessionsa
- Tunnistusvälineen rekisteröinti tukipisteen kautta organisaatioissa.
- Rajapinta MFA:lle
    - Web-service (kyllä/ei vastaus)
        - kysytään eppn:llä, onko MFA käytössä tällä käyttäjällä
    - Web-service (json taulukko)
        - IdM voi kysyä luettelon oman organisaation käyttäjistä, joilla on MFA käytössä
        - kotiorganisaatio luovuttaa schacHomeorganisation arvon, jonka perusteella käyttäjä sidotaan kysyvään organisaatioon