Käyttötapaukset

Protokollat

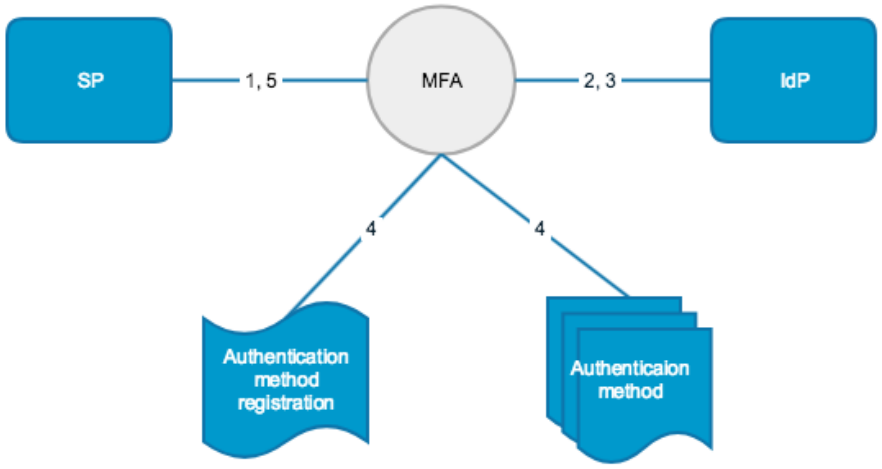
- Service Providerin ja MFA:n välisessä tiedonsiirrossa käytetään Hakassa käytössä olevaa SAML2Int-profiilia
- IdP:n ja MFA:n välisessä tiedonsiirrossa käytetään OpenID Connect protokollan Implicit Flow:ta

Tunnistusvälineet

- MFA tukee ensimmäisessä vaiheessa TOTP-tunnistusta
  - Asiakasohjelmisto vapaasti valittavissa tukevista tuotteista
- Tunnistusvälineen rekisteröinnissä hyödynnetään ensimmäisessä vaiheessa SMS-pohjaista rekisteröintiä
  - Edellyttää soveltuvaa puhelinnumeron hallintaa organisaatiossa
  - SMS-pohjainen tunnistusvälinen mahdollista toteuttaa myös

Käyttötapaus 1

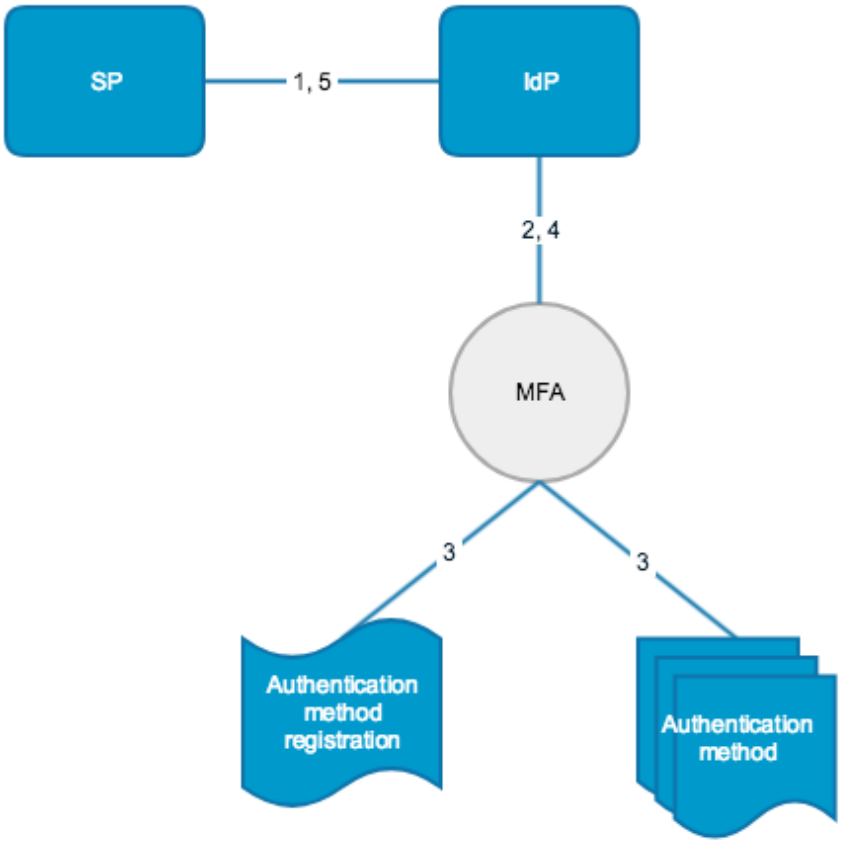
Ensimmäisessä käyttötapauksessa palvelut, jotka haluavat vahvemman tunnistuksen, ohjaavat tunnistustapahtumat Haka MFA:lle.



Vaihe	Suorittaja	Tehtävät	Huomiot
1	Palvelu (SP)	1. Palvelu on konfiguroinut MFA:n luotetuksi tunnistusvälineeksi palvelussa. Tämä voidaan suorittaa lataamalla Haka-metadata, jossa MFA mukana tai lisäämällä erillinen metadata palveluun luotetuksi. Palvelun ei tarvitse tehdä muuta kuin ottaa käyttöön annettu metadatatiedosto. 2. Palvelu tekee oman käyttöliittymänsä mukaisen ohjauksen tunnistukseen, joka vie käyttäjän MFA:lle.	
2	MFA	1. MFA näyttää käyttäjälle listan tuetuista organisaaioista, joista käyttäjä valitsee haluamansa. 2. MFA ohjaa normaalin SAML2-tunnistuspyynnön valitulle tunnistuslähteelle.	
3	IdP	1. Organisaation tunnistuslähde suorittaa tunnistuksen käyttäjätunnus-salasana -parilla ja palauttaa tunnistusvastauksen käyttäjäattribuutteineen MFA:lle.	
4	MFA	1. MFA vastaanottaa tunnistusvastauksen ja käsittelee vastaanotetut attribuutit. 2. MFA käynnistää vahvemman tunnistuksen vaiheen valitulla metodilla. a. Jos metodia ei ole käyttäjälle rekisteröity, tehdään ensin rekisteröinti mikäli väline sallii lennossa tehtävän rekisteröinnin. 3. Lisätunnistuksen jälkeen MFA paketoi IdP:lta saadut attribuutit ja lähettää tunnistusvastauksen palvelulle	
5	Palvelu (SP)	1. Palvelu vastaanottaa tunnistusvastauksen. Tunnistusvastauksessa tieto suoritetusta vahvemmasta tunnistuksesta, alkuperäisestä IdP:sta sekä käyttäjäattribuutit. 2. Palvelu voi tehdä tietojen perusteella haluamiaan toimenpiteitä.	

Käyttötapaus 2

Toisessa käyttötapauksessa kaikki tunnistustapahtumat menevät organisaation IdP:n kautta. IdP on konfiguroitu käyttämään vahvempiin tunnistusvälineisiin SUIdP:n rajapintaa.



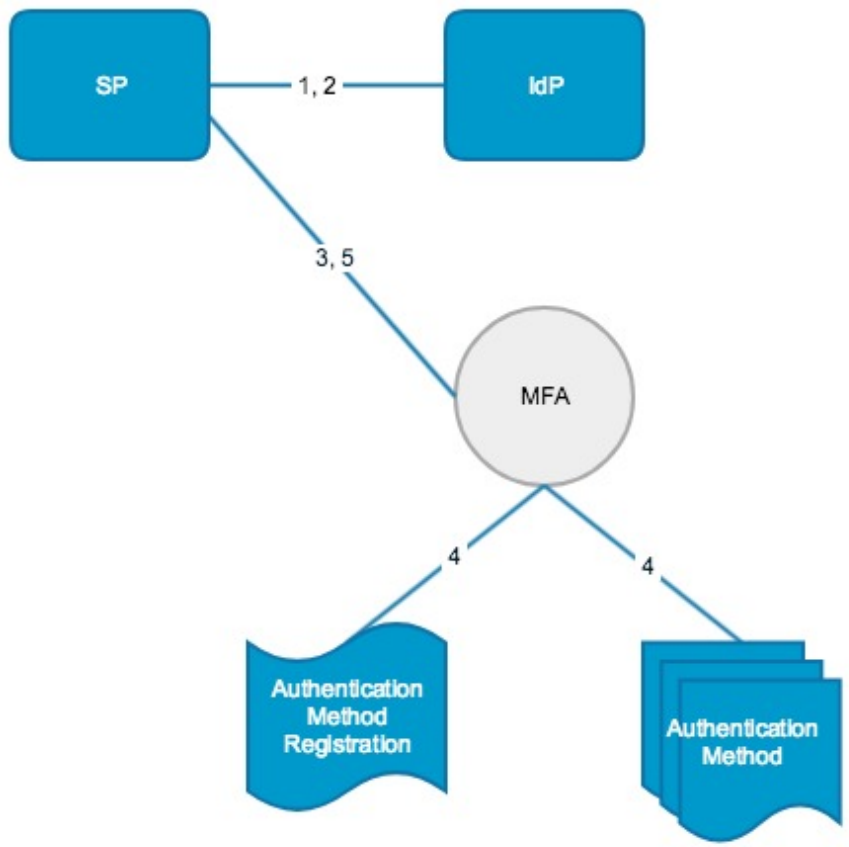
Vaihe	Suorittaja	Tehtävät	Huomiot
1	Palvelu	1. Palvelu tekee oman käyttöliittymänsä mukaisen ohjauksen tunnistukseen, joka vie käyttäjän IdP:lle	
2	IdP	1. IdP tekee käyttäjätunnus-salasana autentikaation 2. Pyytää rajapinnan kautta step-up tunnistusta MFA:lta	
3	MFA	1. MFA käynnistää vahvemman tunnistuksen vaiheen halutulla metodilla. a. Jos metodia ei ole käyttäjälle rekisteröity, tehdään ensin rekisteröinti mikäli väline sallii lennossa tehtävän rekisteröinnin. 2. Palauttaa IdP:lle tiedon tunnistustapahtumasta	
4	IdP	1. Saatuaan vastauksen tunnisuksesta MFA:lta, palauttaa tunnistusvastauksen käyttäjäattribuutteineen SUIdP:lle.	
5	Palvelu	1. Palvelu vastaanottaa tunnistusvastauksen. Tunnistusvastauksessa tieto suoritetusta vahvemmasta tunnistuksesta, alkuperäisestä IdP:sta sekä käyttäjäattribuutit. 2. Palvelu voi tehdä tietojen perusteella haluamiaan toimenpiteitä.	

Käyttötapaus 2:n vaihtoehtoinen toteutus

MFA toiminnallisuus on mahdollista integroida osaksi organisaation IdP:ta. Organisaatio saa tällöin halutessaan käyttöönsä kehitetyn ohjelmiston, mutta vastaa tällöin itse sen asentamisesta ja ylläpidosta. Tämä edellyttää riittävää asiantuntemusta IdP:n sisäisestä toiminnasta.

Käyttötapaus 3

Kolmannessa käyttötapauksessa palvelu pyytää tiettyihin toimenpiteisiin vahvempaa tunnistusta. Peruskäyttöön palvelussa riittää salasanatunnistus, joten vain osaan toimenpiteistä pyydetään vahvempaa tunnistusta.

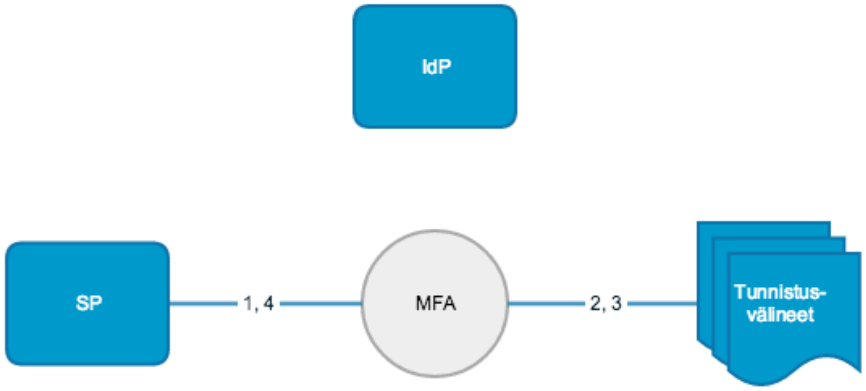


Vaihe	Suorittaja	Tehtävät	Huomiot
1	SP	**1.** Palvelu tekee oman käyttöliittymänsä mukaisen ohjauksen tunnistukseen.	
2	IdP	**1.** IdP tunnistaa käyttäjän käyttäjätunnus - salasana -parilla	
3	SP	**1.** Palvelu tarvitsee toimenpiteeseen vahvemman tunnistuksen. Tekee tunnistuspyynnön MFA:lle	
4	MFA	**1.** MFA tekee vahvemman tunnistuksen käyttäjästä. **2.** MFA palauttaa tunnistusvastauksen vahvemmasta tunnistustapahtumsta.	
5	SP	**1.** Palvelu vastauksen perusteella oikeuttaa käyttäjän suorittamaan toimenpiteen.	

Käyttötapaus 4

Neljännessä käyttötapauksessa käyttäjä ei käy lainkaan IdP:lla, vaan suorittaa vahvan tunnistuksen ulkoisessa palvelussa. Käytännön sovellus esimerkiksi salasanan unohtaminen, jolloin käyttäjä ei voi IdP:lla tunnistautua.

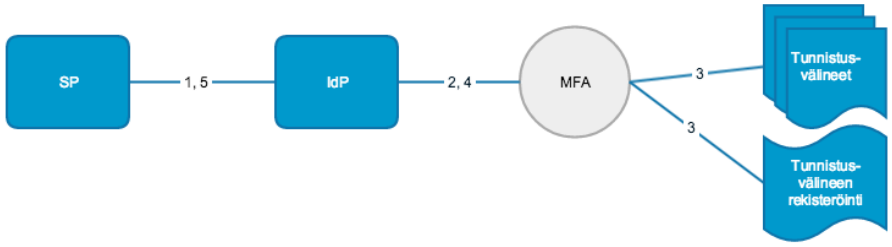
Liittyminen MFA:iin on normaali Haka-liitos, joten palvelun ei tarvitse integroida erikseen vahvaa tunnistusvälinettä.



Vaihe	Suorittaja	Tehtävät	Huomiot
1	SP	1. Palvelu tekee oman käyttöliittymänsä mukaisen ohjauksen tunnistukseen.	
2	MFA	1. MFA ohjaa käyttäjän tunnistautumaan vahvalla välineellä	
3	Tunnistusväline	1. Vahva tunnistusväline palauttaa tunnistetun käyttäjän MFA:lle	
4	MFA	1. MFA ohjaa tunnistetun käyttäjän takaisin palveluun.	

Käyttötapaus 5

Viides käyttötapaus muistuttaa käyttötapausta 2:ta, mutta tässä tilanteessa luotetaan pelkkään MFA:lta saatuun tunnistukseen. Käytännössä MFA:lta tulee käyttäjästä tunniste, jolla käyttäjän attribuutit haetaan organisaation hakemistosta.



Vaihe	Suorittaja	Tehtävät	Huomiot
1	Palvelu	1. Palvelu tekee oman käyttöliittymänsä mukaisen ohjauksen tunnistukseen, joka vie käyttäjän IdP:lle	
2	IdP	1. IdP pyytää rajapinnan kautta vahvaa tunnistusta MFA:lta	
3	MFA	1. MFA käynnistää tunnistuksen vaiheen halutulla metodilla. 2. Palauttaa IdP:lle tiedon tunnistustapahtumasta ja käyttäjätunnisteen.	
4	IdP	1. Saatuaan vastauksen tunnistuksesta MFA:lta, hakee käyttäjäattribuutit saamallaan käyttäjätunnisteella ja palauttaa tunnistusvastauksen käyttäjäattribuutteineen SUIdP:lle.	

5	Palvelu	1. Palvelu vastaanottaa tunnistusvastauksen. Tunnistusvastauksessa tieto suoritetusta vahvemmasta tunnistuksesta, alkuperäisestä IdP:sta sekä käyttäjäattribuutit. 2. Palvelu voi tehdä tietojen perusteella haluamiaan toimenpiteitä.	