

# Auðkenning í gegnum Island.is - Leiðbeiningar um tengingu

## 1. Skilgreining stofnunar (sendist til forsætisráðuneytis)

- a. Heiti stofnunar: \_\_\_\_\_  
(Dæmi: Tryggingarstofnun)
- b. Auðkenni stofnunar (án íslenskra stafa): \_\_\_\_\_  
(Dæmi: tryggur.is, stofnun.is)
- c. Síða sem á birtast eftir auðkenningu: \_\_\_\_\_  
(Dæmi: <https://www.stofnun.is/eydublad>)
- d. Lógó stofnunar verður birt í auðkenningarglugganum ásamt lógói Island.is. Skila þarf lógóinu á gif-formi á hvítum grunni, þar sem breiddin er 200 pixlar og hæðin er 60 pixlar. Island.is getur aðstoðað við að lagfæra lógóið ef þörf krefur.

*Athugasemdir: Hægt er að senda viðbótarupplýsingar með auðkenningunni, t.d. til að vísa á ólíkar undirslóðir, sjá kafla 3 í fylgiskjali. Einnig er hægt að biðja sérstaklega um að skráð verði annað auðkenni fyrir þróunarumhverfi, sjá nánar í kafla 4 í fylgiskjali.*

## 2. Tenging við rafrænt þjónustulag Island.is

- a. Þegar auðkenningu er lokið á síðunni Island.is er notandinn sendur á síðuna sem gefin er upp í lið 1b. Þá þarf stofnunin að gera vefþjónustukall í rafræna þjónustulagið til þess að sækja SAML skírteinið sem Island.is setti þar (sjá nánar í fylgiskjali). Þetta gerir stofnunin með því að kalla á eftirfarandi þjónustu: [https://egov.webservice.is/sst/runtime.asvc/com.actional.soapstation.eGOVDKM\\_AuthConsumer.AccessPoint?WSDL](https://egov.webservice.is/sst/runtime.asvc/com.actional.soapstation.eGOVDKM_AuthConsumer.AccessPoint?WSDL)
- b. Þegar stofnunin hefur sótt SAML skírteinið þarf að aðgæta hvort að undirritun þess sé gild.
- c. Nánari upplýsingar um samskiptin má sjá í fylgiskjali.

## Fylgiskjal

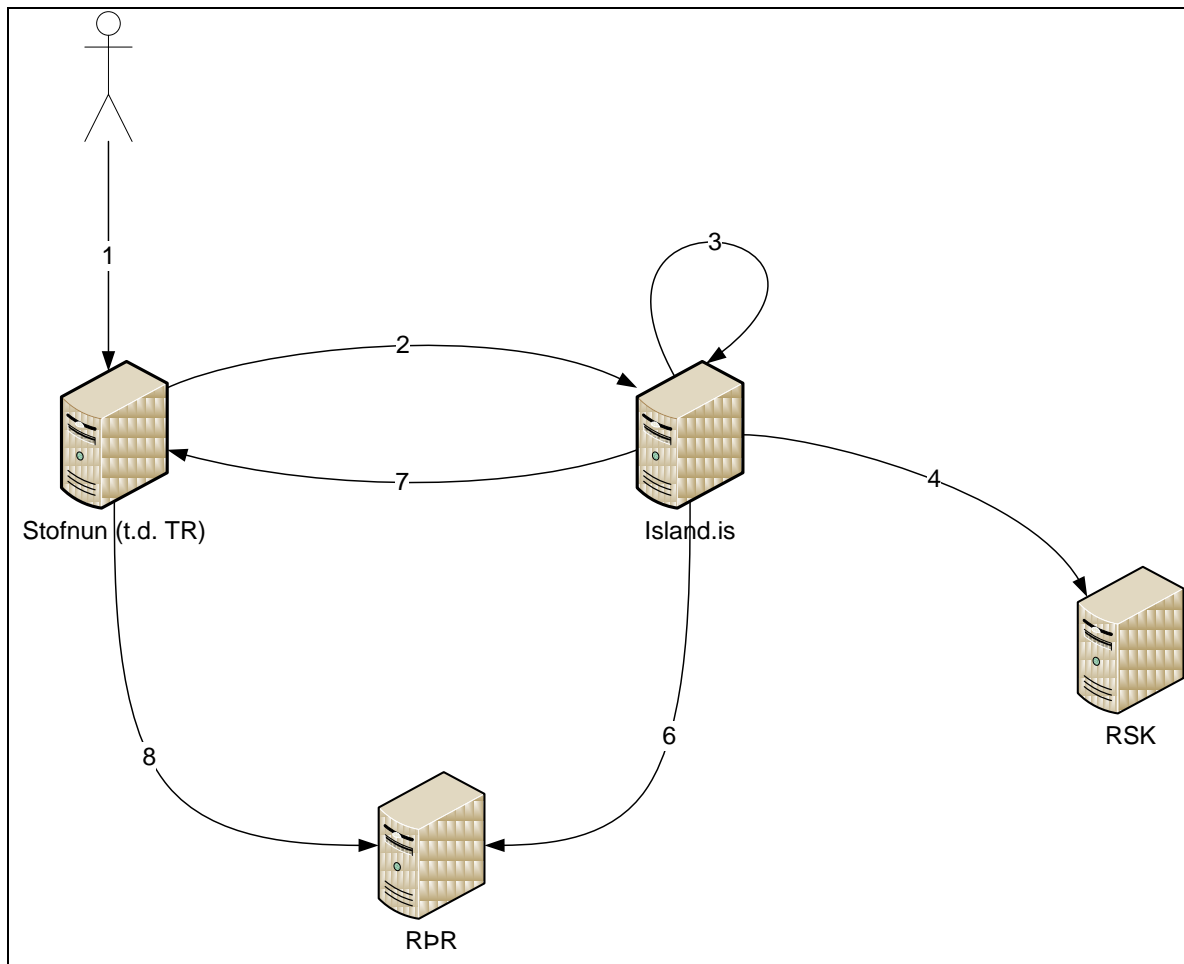
### 1. Yfirlit

Skjal þetta lýsir í grófum dráttum hvernig auðkenning fer fram á Island.is með veflykli Ríkisskattstjóra. Notkun rafrænna skilríkja fylgir svipuðu mynstri.

Auðkenningin getur verið með tvennum hætti. Notandinn getur annað hvort hafið ferlið hjá vef stofnunar, verið auðkenndur hjá Island.is og flust svo tilbaka til vefs stofnunar eða notandinn byrjar á Island.is og velur að vera fluttur á stofnun með auðkenningu. Hér á eftir er lýst ferlinu þegar notandinn byrjar hjá stofnun.

### 2. Samskipti milli kerfa (notandi byrjar hjá stofnun)

Á mynd 2.1 má sjá hvernig og í hvaða röð samskipti eiga sér stað milli kerfa. Sérhverjum lið í ferlinu er svo lýst nánar hér fyrir neðan.



Mynd 2.1

1. Notandi fer inn á vef hjá stofnun og ætlar að fá aðgang að kerfi stofnunar þar sem krafist er auðkenningar. Notandanum birtist hlekkur þar sem honum er boðið að auðkenna sig hjá Island.is með veflykli Ríkisskattstjóra.

2. Þegar notandi smellir á hlekkinn er hann sendur á innskráningarsíðu Island.is þar sem auðkenni stofnunar er notað til að lesa hvert á að senda hann að auðkenningu lokinni. Dæmi: <https://www.island.is/audkenning/?id=tryggur.is> eða <https://www.island.is/audkenning/?id=stofnun.is>. Notandinn sér innskráningarsíðu á Island.is þar sem kemur fram að hann geti auðkennt sig með því að slá inn kennitölu, veflykil Ríkisskattstjóra og smella á innskráningarhnapp.
3. Þegar notandinn hefur smellt á innskráningarhnappinn kallar Island.is í vefþjónustu hjá RSK þar sem send er inn kennitala og veflykill. Vefþjónustan skilar svári um hvort kennitalan og veflykillinn stemmi. Ef kennitalan og veflykillinn stemma ekki þá birtist villa á Island.is síðunni.
6. Ef vefþjónusta RSK skilar jákvæðri niðurstöðu þá útbýr Island.is SAML skírteini sem er undirritað með skilríki hjá Island.is. SAML skírteinið er síðan sent í vefþjónustuna verifyUserAuthentication í rafrænu þjónustulagi Island.is (RPR).  
Samkvæmt núverandi högun inniheldur skilríkið eftirfarandi breytur:
  - SSN – Kennitala Endanotanda
  - Token – Token. Hakkað með SHA1
  - SYSID - Upprunakerfi skírteinis. RSK eða eGOVDKM
  - AUTHMETHOD – Auðkenningaraðferð RSK/CERTIFICATE/... (Upplýsingar um hvernig notandinn var auðkenndur)
7. Næst sendir Island.is vefurinn notandann tilbaka á vefinn sem bað um auðkenninguna ásamt tóka (e. token) sem var settur í SAML skírteinið. Nánar tiltekið á þá síðu sem skilgreind var sem skilasíða í lið 1 (<https://www.stofnun.is/eydublad> í dæminu að ofan). Engin regla gildir um hvernig tókinn er búinn til, hann þarf aðeins að vera þannig að ekki sé hægt að reikna út hvaða tóki kemur næst. Dæmi: <https://www.stofnun.is/eydublad?token=342KJ342LKJ2OSHY4523HWE93LJL2>
8. Þegar stofnunin hefur tekið aftur við notandanum ásamt tókanum þá kallar hún á vefþjónustuna generateSAMLFromToken þar sem tókinn er sendur inn ásamt vistfangi (e. ip address) notandans. Vefþjónustan skilar til baka SAML skírteini sem inniheldur upplýsingar um notandann.

### 3. Viðbótarupplýsingar í vefslóð (url-breytur)

Í mörgum tilvikum hafa stofnanir þörf fyrir að senda inn viðbótarupplýsingar með auðkenningu, til dæmis ef notendum er boðið upp á að auðkenna sig fyrir ákveðnar umsóknir og því þörf á að geta vísað þeim á ólíkar undirslóðir eftir auðkenningu.

Til að senda viðbótarupplýsingar með auðkenningu er það gert með valkvæmu url-breytunni **path**, gildi hennar er bætt aftan við slóð skilasíðu þegar notandi er sendur þangað. Gildi *path* þarf að vera “url-encoded” og má ekki innihalda XSS veikleika (e. *cross-site scripting*). Ef *path* uppfyllir ekki þessi skilyrði er gildi þess ekki sent áfram eftir auðkenningu.

**Dæmi 1:** Stofnun hefur útbúið ólík eyðublöð á vefslóðunum [www.stofnun.is/eydublad1](http://www.stofnun.is/eydublad1), [www.stofnun.is/eydublad2](http://www.stofnun.is/eydublad2), o.s.frv., sem taka við auðkenndum notendum. Stofnunin skráir þá skilasíðuna <https://www.stofnun.is/eydublad> og býr til tengla á auðkenningarsíðuna á sniðinu: [www.island.is/audkenning?id=stofnun.is&path=123](http://www.island.is/audkenning?id=stofnun.is&path=123). Eftir auðkenningu er notanda í þessu dæmi vísað sjálfkrafa á slóðina: <https://www.stofnun.is/eydublad123?token=342KJ342LKJ2OS>

**Dæmi 2:** Stofnun hefur gefið upp skilasíðuna <https://www.stofnun.is/eydublad>. Með aðstoð path-breytunnar á að skila gildinu “?nr=123”, sem url-umkóðað er “%3Fnr%3D123”. Þá er tengillinn á auðkenningarsíðuna: [www.island.is/audkenning?id=stofnun.is&path=%3Fnr%3D123](http://www.island.is/audkenning?id=stofnun.is&path=%3Fnr%3D123). Eftir auðkenningu er notanda í þessu dæmi vísað sjálfkrafa á slóðina:

<https://www.stofnun.is/eydublad?nr=123&token=342KJ342LKJ2OS> .

Athugið að í þessu dæmi gæti stofnunin einnig skráð “?nr=” sem hluta af slóð skilaslóðunnar (<https://www.stofnun.is/eydublad?nr=>) en það gefur ekki sama sveigjanleika í notkun.

**Dæmi 3:** Ef gildi path er **ekki** encoded (eða inniheldur þekkta XSS veikleika), sbr.

<http://www.island.is/audkenning?id=stofnun.is&path=?nr=123> er þeim upplýsingum hent og notanda vísað á <https://www.stofnun.is/eydublad?token=342KJ342LKJ2OS>.

## 4. Þróunarumhverfi á sérstöku léni

Ef stofnun er með þróunarumhverfi á sérstökum vefslóðum (t.d. öðru léni) og vill geta prófað auðkenninguna þar, er einfaldast að óska eftir því að stofnað verði sérstakt viðbótar-auðkenni fyrir stofnunina sem eingöngu verður notað við prófanir.

**Dæmi 4:** Stofnun hefur með þróunarumhverfi á léninu <http://development.stofnun.is> og vill geta prófað auðkenninguna þar. Stofnað er prófunarauðkennið *d.stofnun.is* og fyrir það er skráð skilaslóðin <http://development.stofnun.is/eydublad> (sbr. dæmi 1 hér fyrir ofan). Þá er tengill á auðkenningarsíðu: [www.island.is/audkenning?id=d.stofnun.is&path=123](http://www.island.is/audkenning?id=d.stofnun.is&path=123).

Athugið að ekki er gerð krafa um að prófunarauðkenni endurspegli raunverulegt undirlén.