

Ohjeita avainkoodin käyttöön: kirjaudu nettisivustoille ja -sovelluksiin ilman käyttäjätunnusta ja salasanaa

I. Standardit ja nykyinen tilanne

A. Taustaa

Nettisivustoille ja -sovelluksiin käyttäjiltä vaaditaan usein käyttäjätunnus ja salasana. Nyt tämä on muuttumassa. Nettisivustot ja -sovellukset ovat siirtymässä salasanoista turvallisempiin avainkoodeihin (toiselta suomalaiselta nimitykseltään 'pääsyavaimiin' - englanniksi termi on 'passkeys'). Tärkeimpänä syynä tähän siirtymään on lisääntyvät tietomurrot, jotka aiheuttavat suuria kustannuksia ja tappioita eri toimijoille.

Tässä kaksi Suomessa julkaistua lehtijuttua avainkoodeista: [Iltasanomien juttu 16.7.2023](#) ja [Yle:n juttu 23.10.2024](#)

Syksyllä 2025 ZDNET julkaisun 6-osainen englanninkielinen juttusarja tästä aiheesta. [Se alkaa tästä linkistä](#). Tämän ohjeen kirjoittaja on suomentanut nämä jutut; jos haluat suomennokset, ota yhteyttä tämän kirjoittajaan.

Avainkoodit perustuvat maailman suurimpien tietoyhtiöiden yhdessä laatimaan Fido2-standardiin vuodelta 2019. Se määrittelee avainkoodien kolme pääprosessia: **1.) avainkoodien rekisteröinti, 2.) todentaminen ja 3.) muuttaminen sekä poistaminen (tämän viimeisen pääprosessin toteutusta vasta suunnitellaan)**; lue asiasta tarkemmin: [Linkki 1](#) ja [Linkki 2](#).

Kaksi ensimmäistä prosessia on jo saatu 'jalkautettua' ja ne toimivat – tietyin varauksin – automaattisesti. Mutta kolmas prosessi – avainkoodin automaattinen poistaminen (decommissioning) – on vielä suunnittelijoiden pöydällä ja siksi se vaatii vielä käyttäjältä 'käsityötä'.

Tähän siirtymään arvioidaan kuluvan USA:ssa seuraavat 5 -10 vuotta, Euroopassa tähän siirtymään on vasta havahduttu.

ZDNET julkaisu kertoi 21.5.2026, että [Microsoft vaihtaa 2-vaiheisen tekstiviesteihin pohjautuvan tunnistautumisen tilalle avainkoodit](#).

Microsoftin globaalin markkina-aseman vuoksi tämän päätöksen arvellaan nopeuttavan avainkoodien käytön yleistymisen maailmanlaajuisesti myös muilla alustoilla ja muissa nettisovelluksissa.

B. Tilanne nyt

Tällä hetkellä [avainkoodiin sopivat laitteet löytyvät tässä olevasta linkistä](#). Mutta tilanne paranee koko ajan monella osa-alueella ja nämäkään nettisivut eivät pysy kehityksen perässä, mm. Linux-järjestelmissä ja Firefox-selaimissa avainkoodi toimii nykyisin hyvin.

Haasteena tässä on saavuttaa globaalisti tilanne, jossa avainkoodeilla tunnistautuminen olisi yhtä vaivatonta kuin tunnistautuminen on jo nyt 'käyttäjätunnus + salasana' -yhdistelmällä tai Suomessa niiden lisäksi pankkitunnuksilla tai mobiilivarmenteella. Tähän kuluu aikaa, koska tämä tavoite

vaatii, että lähes kaikki yritykset alkavat tukea avainkoodin käyttöä omissa nettisovelluksissaan ja avainkoodin kaikki pääprosessit saadaan automatisoitua sekä kuluttajat totutettua käyttämään avainkoodeja.

Avainkoodien kahta ensimmäistä automaattista pääprosessia (rekisteröinti ja todentaminen) voi jo kokeilla useilla nettisivuilla. Tässä joitakin linkkejä:

* [Laitteet ja käyttöjärjestelmät ja nettiselaimet, joissa avainkoodi toimii jo nyt](#)

* Nettisivustot ja -sovellukset, jotka tukevat avainkoodin käyttöä jo nyt: [Linkki 1](#) ja [Linkki 2](#).

* Muitakin jo on, mm. [Manjaro Forum](#) ja [EndeavourOS Forum](#)

Avainkoodia (toiselta suomalaiselta nimeltään 'pääsyavainta') Suomessa tukevia nettisovelluksia olen löytänyt vasta **kolme**:

* **Kansalliskirjasto**: Sen [hakupalveluun](#) voi kirjautua Google Gmail-avainkoodilla (ja yliopistojen tunnuksilla).

* **e-kirjastoon** avainkoodi toimii nyt vain Android- tai Apple- matkapuhelimeen ladatun e-kirjasto-sovelluksen kautta. Siihen kirjaudutaan ensin Suomi.fi prosessin mukaisesti vahvalla tunnistautumisella ja sitten luodaan avainkoodi (jota e-kirjasto kutsuu '**pääsyavaimeksi**'). E-kirjaston avainkoodien web-käyttöliittymä tietokoneille julkaistaan 2026.

Katso tarkemmin tämä [havainnollinen ohje](#)

* [laakari.chat](#)

C. Todentavat alustat, ohjelmat ja laitteet:

1. Alustatodentajien ohjelmat:

Suomessa toimivia ulkomaalaisia avainkoodin käyttäjiä ovat tämän Fido2-standardin pääkehittäjät: Googlen Gmail, Microsoft ja Apple. Kukin näistä suosii oman alustansa selaimia ja todentajia (authenticator):

* Google: [Google Avainkoodi](#) → Google-tili, Gmail s-posti, Android matkapuhelimet sekä Google avainkoodia käyttävät muut tahot, jotka käyttävät sitä oman avainkoodinsa lisäksi tai, joilla ei vielä ole omaa avainkoodia

* Windows: Katso tarkemmin [Windows Hello](#) tai [Microsoft Edge/Salasanojen hallinta](#)

* Apple: [Apple ID](#) → macOS ja iOS

2. Muut todentavat ohjelmat:

* Kolmansien osapuolten automaattisesti synkronoivat salasanojen hallintaohjelmat:

Edge (Windows), Safari (Mac), Google Chrome, Firefox, Opera, Vivaldi, Brave -selaimet voivat käyttää todentajina myös kolmansien osapuolten automaattisesti synkronoivia salasanojen hallintaohjelmia (esim. 1Password, Bitwarden, LastPass, Dashlane, Proton Passi, Hanko io.) edellyttäen, että käyttäjä lataa ja asettaa selaimensa ko. salasanojen hallintaohjelman **laajennuksen** (extension). Tutustu selainten laajennusten asettamiseen (asetuksiin) erikseen, jotta ne toimivat kuten haluat.

Jokaiseen salasanojen hallintaohjelmaan tallennetut käyttäjän omat tiedot, eli käyttäjän omat käyttäjätunnukset, salasanat ja avainkoodit jne. muodostavat **käyttäjän tietokannan**. Netissä siihen tehdyt muutokset, lisäykset, poistot jne. synkronoituvat automaattisesti ns. 'konepellin alla' ja toimivat sitten samalla tavalla kaikissa avatuissa omissa laitteissa.

* Kolmansien osapuolten ei-automattisesti synkronoivat salasanojen hallintaohjelmat: Jos haluat pitää käyttäjätunnusten, salasanojen ja avainkoodien tietokannan (tai tietokannat) vain itselläsi ja synkronoida sen kaikille omille laitteille itse, voit käyttää esim. salasanojen hallintaohjelmaa [KeePassXC](#) ja sen selainlaajennusta, [käyttöohjeet](#) ja [avainkoodien luominen ja ylläpito](#).

3. Todentavat laitteet:

* Fido2-standardin täyttävät ulkoiset laitteet: esim. Yubico:n [YubiKey](#) – USB tikut / avaimet

II. Seuraavaksi kuvataan avainkoodin kolme pääprosessia tietokoneella tarkemmin.

Jos haluat kirjautua eri nettisovelluksiin helposti ja turvallisesti, ryhdy käyttämään avainkoodeja. Avainkoodien prosesseissa eri nettisovelluksilla on hieman toisistaan eroavia ja erinäköisiä toteutuksia, mutta pääpiirteissään kaikkien avainkoodien prosessit toimivat samalla tavalla, koska ne perustuvat samaan Fido2-standardiin:

A. Avainkoodin rekisteröinti tietokoneella

1. Ota käyttöön joko oman alustasi salasanojen hallintaohjelma (password manager) tai joku kolmannen osapuolen automaattisesti synkronoiva salasanojen hallintaohjelma (esim. Bitwarden) ja tee sinne eri omien nettisovellusten ja niiden käyttäjätunnusten ja salasanojen lista.

Pidä tämän salasanojen hallintaohjelman avaamiseen tarvittava salasana ja sen mahdollinen pin-koodi tallessa: aina omassa vihkossa + sen varavihkossa sekä esim. Windowsin **Enlock**-sovelluksessa tai Linuxien **Salasanat ja avaimet**-sovelluksessa jne.

2. Lataa nettiselaimesi kyseisen salasanojen hallintaohjelman laajennus (extension). Selaimen laajennus avaa automaattisesti linkin kyseiseen salasanojen hallintaohjelmaan sen pääsalasanalla (tai – jos sellainen on luotu – mahdollisesti sen pin-koodilla).

3. Etsi nettisovellus, jossa jo on tunnistautumiseesi tarvittava käyttäjätunnus ja salasana ja joka tukee myös avainkoodin käyttöä. Sovellus ilmoittaa siitä yleensä, esim. **'Log in with a passkey'** (Kirjautu avainkoodilla') tai muulla vastaavalla tavalla.

4. Avaa kyseinen nettisovellus nykyisillä tunnuksillasi (käyttäjätunnus ja salasana) ja valitse tunnusten vaihto avainkoodiin ('pääsyavaimen').

Nettisovellus ja nettiselaimen laajennus tekevät ja varmentavat keskenään uuden avainkoodisi ja sen rekisteröinnin ns. 'konepellin alla'. Kun se on valmis, saat siitä ilmoituksen. Seuraavalla kerralla voit tunnistautua valmiilla avainkoodilla.

Nykyiset tunnistautumisen tunnuksesi (käyttäjätunnus ja sitä vastaava salasana) pysyvät edelleen voimassa ja säilyvät nettisovelluksen tietokoneilla.

5. Voit käyttää tätä samaa rekisteröityä avainkoodia eri laitteista, jos niiden selaimessa on saman salasanojen hallintaohjelman (esim. Bitwarden) laajennus.

B. Avainkoodilla todentaminen tietokoneella

1. a.) Avaa tietokoneesi nettiselain.

1. b) Avaa selaimeen lataamasi salasanojen hallintaohjelman laajennus (extension) sen salasanalla.

2. Avaa sen nettisovelluksen kirjautumissivu, johon avainkoodi on jo rekisteröity.

3. Osoita hiirellä nettisovelluksen sisäänkirjautumisen käyttäjätunnuksen paikkaa, niin salasanojen hallintaohjelman laajennus avaa siihen kyseisen nettisovelluksen avainkoodin logon.

4. Klikkaa avainkoodin logoa ja nettiselaimen laajennus ottaa yhteyden kyseiseen nettisovellukseen, joka ensin todentaa sinut ja avaa sitten sinulle rekisteröidyn nettisovelluksen sivuston. Olet nyt kirjautunut kyseiseen nettisovellukseen avainkoodilla.

Kirjautuminen avainkoodilla tapahtuu ilman, että muuten pitäisi ensin (todentautumista varten) kirjoittaa tai lähettää nettisovellukselle käyttäjätunnuksesi ja salasanasi.

5. Kun lopetat kyseisen nettisovelluksen käytön → sulje se normaalisti (esim. klikkaa sovelluksen kohtaa **'Kirjautu ulos'** tai vastaava) ja kirjautumisesi päättyy ja nettiyhteys sovellukseen purkautuu.

6. Kun haluat avata kyseisen nettisovelluksen uudestaan sulkematta välillä selainta, jatka kohdasta B.2; muussa tapauksessa aloita uudestaan kohdasta B.1.

C. Avainkoodin muuttaminen ja poistaminen tietokoneella

Tässä on kuvattu avainkoodin muuttamisen ja poistamisen peruspiirteet, joiden yksityiskohdat voivat erota toisistaan eri nettisovelluksissa. Avainkoodin poistamisen prosessi automatisoituu vähitellen.

1. Käyttäjällä voi olla **useita avainkoodeja** samaan nettisovellukseen. Niitä voi luoda eri salasanojen hallintaohjelmien laajennuksilla, joita voi käyttää eri laitteilla. Ne yksilöivät sinut kuhunkin käytettävään laajennukseen ja laitteeseen (tietokoneeseen) erikseen.

2. **Voit lisätä** jonkun tietyn olemassa olevan salasanojen hallintaohjelman laajennuksen kautta jo käytettävään avainkoodiin uuden avainkoodin kytkeytymällä kyseiseen nettisovellukseen sen ensimmäisellä avainkoodilla → etsi omat henkilötietosi ja sen asetukset ('Preferences') → klikkaa **Lisää avainkoodi** ('Add Passkey') -painiketta → järjestelmä luo (rekisteröi) samaan laajennukseen toisen avainkoodin, joka toimii myös ensimmäiseksi luodun avainkoodin lisäksi sisäänkirjautumisessa.

Katso oheinen kuva, joka kertoo ensin, että kyseessä on Bitwardenilla 20.5. luotu avainkoodi ja sitä on käytetty viimeksi 3 päivää sitten ja antaa mahdollisuuden lisätä uusi avainkoodi klikkaamalla **+Add Passkey** -painiketta:

Btw Passkey

Added 20 May

Last Used 3 days ago

+ Add Passkey

3. **Voit lisätä (rekisteröidä) uuden avainkoodin toiseen** koneeseen kirjautumalla em. nettisovelluksen kohtaan käyttäjätunnuksellasi ja sitä vastaavalla salasananasi toisen laitteen toisesta salasanojen hallintaohjelman laajennuksesta (esim. LastPass) käyttäjätunnuksellasi ja sitä vastaavalla salasananasi ja klikkaamalla **+Add Passkey** -painiketta.

4. **Voit muuttaa** jonkun salasanojen hallintaohjelman (esim. Bitwarden) laajennuksen kautta käytettävän avainkoodin tai sen nimen toiseksi → kytkeydy kyseiseen nettisovellukseen sen nykyisellä avainkoodilla → etsi omat henkilötietosi ja sen asetukset ('Preferences') → etsi nykyinen avainkoodisi ja sen vieressä oleva **työkalu-kuvake** – avaa kuvake → **Muuta (Edit) avainkoodia** klikkaamalla kyseistä valikon kohtaa. Eri nettisovelluksissa nämä kuvakkeet ja niiden tarjoama sisältö voivat olla erilaisia.



 Edit

 Delete

5. Voit **poistaa** jonkun tietyn salasanojen hallintaohjelman (esim. Bitwarden) laajennuksen kautta käytettävän avainkoodin → kytkeydy kyseiseen nettisovellukseen ko. laajennukseen tallennetulla avainkoodilla → etsi omat henkilötietosi ja sen asetukset → etsi nykyinen avainkoodisi ja sen vieressä oleva **työkalu -kuvake** → avaa kuvake → **Poista (Delete) avainkoodi** klikkaamalla kyseistä valikon kohtaa. Avainkoodi poistuu nettisovelluksen palvelimelta, mutta ei koneesi kyseessä olevasta salasanojen hallintaohjelman laajennuksesta.

6. Kun olet **poistanut** avainkoodin nettisovelluksesta, kuten edellä kuvattu, niin sen jälkeen se tulee poistaa myös nettiselaimesi kyseessä olevasta salasanojen hallintaohjelman laajennuksesta. Toistaiseksi tämä poistamisen prosessi ei tapahdu – ainakaan kaikkien avainkoodien julkaisijoiden kanssa – automaattisesti, vaan **poistaminen on tehtävä ns. ’käsityönä’ molemmissa päässä erikseen.**

Tämä avainkoodin poistamisen prosessi automatisoituu vähitellen, joten seuraa tilannetta.

III. Tämän kirjoittajan omia testejä Windows-, Linux- ja Android-laiteympäristöissä

Testeissäni olen luonut avainkoodin (rekisteröinti) ja käyttänyt (todentaminen) sitä näillä tekniikkavalinnoilla:

1.) Salasanojen hallintaohjelma [Bitwarden](#) +

2.) Windows 10 ja 11 käyttöjärjestelmät

- + **Edge** -selain, johon asensin **Bitwarden-laajennuksen** → esim. Google tili, Walmart
 - + **Firefox**-selain, johon asensin **Bitwarden-laajennuksen** → esim. Google -tili, Walmart
 - + **Opera**-selain, johon asensin **Bitwarden-laajennuksen** → esim. Google tili, Walmart
 - + **Vivaldi**-selain, johon asensin **Bitwarden-laajennuksen** → esim. Google tili, Walmart
- Huom. Microsoft Store ei tarjoa Google Chrome -selainta

3.) Linux käyttöjärjestelmät

- + **Firefox**-selain, johon asensin **Bitwarden-laajennuksen** → esim. Google-tili, Walmart
- + **Chrome**-selain, johon asensin **Bitwarden-laajennuksen** → esim. Google-tili, Walmart
- + **Opera**-selain, johon asensin **Bitwarden-laajennuksen** → Kansalliskirjaston <https://digi.kansalliskirjasto.fi/etusivu> → Kirjaudu → **Gmail-avainkoodi** → avaa 'Kansalliskirjaston digitaaliset aineistot' -hakemiston
- + **Opera**-selain, johon asensin **Bitwarden-laajennuksen** → esim. Google-tili, Walmart
- + **Vivaldi**-selain, johon asensin **Bitwarden-laajennuksen** → esim. Google-tili, Walmart

4.) Android-kännykässä käytin näistä tekniikkavalintoja

- + **Firefox**-selain → Gmail → kirjautu sisään → avainkoodi tulee Googelta automaattisesti
- + tarvittaessa pyytää kännykän näytönlukitsijan pin-koodia
- + **e-kirjasto**-sovellus (Play-kaupasta) → e-kirjasto- sovellukseen pitää kirjautua ensin pankkitunnuksilla tai mobiilivarmenteella ja luoda sitten avainkoodi (jota e-kirjasto kutsuu **pääsyavaimeksi**)