Analyysi · 26. toukokuuta 2026

← Edellinen·Seuraava →

# Todellinen vs. näennäinen yksityisyys: kysymykset, jotka kannattaa kysyä

Toisen jakson operatiivinen synteesi: kysymykset, jotka erottavat arkkitehtonisen yksityisyyden palvelun julistuksellisen yksityisyyden palvelusta. Kyselylomake eurooppalaiselle ammattilaiselle ennen minkään digitaalisen työkalun käyttöönottoa arkaluonteisia tietoja varten.

**Sanottakoon selvästi:** Kaksi palvelua, joilla on samat käyttöehdot, voivat toimia hyvin eri tavoin. Toinen suojaa teknisellä suunnittelulla. Toinen suojaa sopimuksellisella lupauksella. Eroa ei lueta käyttöehdoista — se löytyy esittämällä konkreettiset kysymykset. Vastausten laatu kertoo tuotteesta yhtä paljon kuin niiden oma sisältö.

## Ero arkkitehtonisen ja julistuksellisen yksityisyyden välillä

Tämän jakson seitsemän edellisen artikkelin aikana olemme kulkeneet saman aiheen eri kerrosten läpi. Kansainvälisten siirtojen oikeus Schrems II:n kautta. Kryptografisen hashin matemaattinen idea, joka sinetöi jokaisen Cuadernon. Kill switchin arkkitehtoninen valinta ja institutionaalinen valtaus, joka lähes aina liittyy siihen. Päästä päähän -salauksen mekanismi ja operatiivinen kysymys siitä, missä avaimet sijaitsevat. Kannustimien linjautuminen liiketoimintamallin mukaan. Itsesuvereeni kryptografinen identiteetti. Self-hosting suhteellisena strategiana. Jokainen artikkeli käsitteli yhtä kulmaa. Tämä, jakson viimeinen, kokoaa ne yhteen kyselylomakkeeksi.

Erottelu, joka kannattaa muistaa, on yksinkertainen: on palveluita, joiden yksityisyys on *arkkitehtonista*, ja on palveluita, joiden yksityisyys on *julistuksellista*. Ensimmäinen on upotettu tekniseen suunnitteluun: tietyt yksityisyyssitoumuksen rikkomukset ovat teknisesti vaikeita tai mahdottomia, koska arkkitehtuuri ei salli niitä. Toinen on talletettu käyttöehtojen tekstiin: tietyt rikkomukset olisivat sopimuksellisesti rangaistavia, jos ne tapahtuvat, mutta teknisesti mikään ei estä niitä. Molemmat mallit voivat täyttää GDPR:n; mutta toinen suojaa rakenteen kautta ja toinen lupauksen kautta, ja ero on operatiivisesti valtava.

Seuraavat kysymykset on suunniteltu erottamaan toinen tapaus toisesta. Ne eivät ole edistyneitä teknisiä kysymyksiä. Ne ovat kysymyksiä, joihin mikä tahansa rehellinen palveluntarjoaja voi vastata julkisessa dokumentaatiossaan. Vastauksen laatu ja täsmällisyys kertoo tuotteesta yhtä paljon kuin itse vastaus. Kysymykset ryhmitellään kuuteen kerrokseen; ne kaikki kannattaa esittää ennen palvelun käyttöönottoa arkaluonteisia tietoja varten, ei vain niitä, jotka ensimmäinen vaisto tunnistaa.

## Kerros 1: arkkitehtuuri

Kiinnitetään yksi termi ennen jatkamista. *Operaattorilla* tarkoitamme yritystä, joka tarjoaa palvelun: tahoa, joka hallitsee palvelimia ja ohjelmistoa, ei yksittäistä henkilöä. Tämän selvennyksen jälkeen perustavanlaatuinen arkkitehtoninen kysymys on: mitä operaattori tekee lähettäjän ja vastaanottajan välisellä sisällöllä? Mahdollisia vastauksia on kolme, ja ne kannattaa osata erottaa toisistaan, sillä kaikkia kolmea mainostetaan toisinaan samankaltaisin sanankäänteinn.

- Ensimmäinen: sisältö kulkee operaattorin palvelimen kautta selväkielisenä, jolloin operaattori voi lukea sen, vaikka lupaisi olla tekemättä niin.
- Toinen: sisältö kulkee operaattorin palvelimen kautta salattuna, jolloin operaattori ei voi lukea sitä, jos avaimet sijaitsevat yksinomaan käyttäjien laitteissa.
- Kolmas: sisältö ei kulje minkään operaattorin palvelimen kautta, koska tuossa nimenomaisessa virrassa ei ole operaattorin palvelinta.

Ero näiden kolmen välillä ei ole asteen ero: se on tyypin ero.

Täydentävä kysymys —jo muotoiltu salausta käsittelevässä Cuadernossa— on: kenellä on kryptografiset avaimet, jotka mahdollistavat sisällön lukemisen? Jos ne ovat käyttäjällä ja vain käyttäjällä, salaus on todellista. Jos ne ovat lisäksi operaattorilla missä tahansa muodossa —jopa nimellä »tilin palautus» tai »laitteiden välinen synkronointi»—, salaus on nimellistä. Kysymykseen ei ole rehellistä välimuotoista vastausta.

## Kerros 2: liiketoimintamalli

Liiketoimintamallia koskeva kysymys on yhtä tärkeä kuin arkkitehtoninen kysymys, ja samasta olennaisesta syystä: kannustimet tuottavat ajan myötä järjestelmällisesti erilaisia tuotteita, vaikka julkilausutut tarkoitukset olisivat identtisiä. Miten operaattori ansaitsee rahaa tänään? Yksi lähde, kaksi, sekoitus? Jos rahoitus sisältää mainontaa tai tietojen rahaksi muuttamista, mitä tietoja muutetaan rahaksi ja millä GDPR:n oikeusperustalla se tehdään? Kattaako käyttöehdoissa julkilausuttu käyttötarkoitus kolmansien osapuolten tiedot, jotka ammattilainen aikoo uskoa palvelulle?

Ja toisen asteen kysymys, jota ei aina muotoilla: mikä on operaattorin taloudellinen tilanne kolmen tai viiden vuoden tähtäimellä? Pääomasijoitusvaiheessa oleva yritys toimii eri paineiden alaisena kuin vakaasti kannattava yritys. Rahoitusmallin muutos on toistuvasti se hetki, jolloin käyttäjien kanssa tehty implisiittinen sopimus kirjoitetaan uudelleen ilman neuvotteluja.

## Kerros 3: lainkäyttöalue

Eurooppalaiselle ammattilaiselle lainkäyttöalueen kysymys ei ole retorinen. Millä lainkäyttöalueella operaattori on rekisteröity? Missä maassa sijaitsevat fyysisesti palvelimet, jotka käsittelevät tietoja? Onko vastaus kahteen edelliseen kysymykseen sama vai erilainen, ja jos se eroaa, mitä lainsäädäntöä sovelletaan? Yhdysvaltalaisen yrityksen operoima eurooppalainen alue ei ole Schrems II:n kannalta eurooppalainen vastaus: yritys on FISA 702:n alainen riippumatta siitä, missä palvelimet sijaitsevat.

Täydentävä operatiivinen kysymys on: jos huomenna saapuisi operaattorin lainkäyttöalueella pätevä tiedustelumääräys, joka vaatisi luovuttamaan minun tai asiakkaideni tiedot, mitä tapahtuisi? Jos rehellinen vastaus alkaa sanoilla »yritys olisi velvollinen luovuttamaan ne», palvelu ei suojaa tuota määräystä vastaan, vaikka mainonta antaisi ymmärtää päinvastaista. Jos rehellinen vastaus alkaa sanoilla »yritys ei voisi luovuttaa niitä, koska sillä ei ole niitä selväkielisinä», palvelu kyllä suojaa; ja ero riippuu lähes kokonaan kahdesta ensimmäisestä kerroksesta, ei tietosuojakäytännön laadusta.

## Kerros 4: operaattori ja kill switch

Mitä teknistä kykyä operaattori säilyttää keskeyttääkseen, estääkseen, poistaakseen tai heikentääkseen palvelua etänä? Kysymys ei ole vainoharhainen: se on operatiivinen. Digitaaliset alustat ovat käyttäneet tätä kykyä toistuvasti viime vuosina, joskus omasta aloitteestaan, joskus hallitusten määräyksestä, joskus omistus- tai politiikkamuutosten jälkeen. Jos kyky on olemassa, on hyvä tietää, millä sopimuksellisesti julkilausutuilla edellytyksillä sitä käytetään, ja varata marginaali julkilausumattomille edellytyksille, jotka viime vuosien käytäntö on osoittanut yhtä merkityksellisiksi: odottamaton tuomioistuimen määräys, kansainvälinen pakote, yritysjohdon muutos, yritysosto sellaisen tahon toimesta, jolla on toisenlainen politiikka.

Sisarkysymys koskee jatkuvuussuunnitelmaa: jos operaattori käyttäisi tätä kykyä ammattilaista vastaan —mistä syystä tahansa, oikeutetusti tai ei—, kuinka paljon toiminta-aikaa olisi vielä käytettävissä, mikä tietojen vientimenettely on olemassa ja mille vaihtoehtoiselle palveluntarjoajalle voitaisiin siirtyä? Jos vastaus alkaa sanoilla »ei sen pitäisi tapahtua», se ei ole operatiivinen vastaus; se on lupaus.

## Kerros 5: identiteetti ja pääsy

Kuka hallitsee palvelun pääsytunnuksia? Jos operaattori voi palauttaa käyttäjän pääsyn ilman käyttäjän osallistumista —menettely, jota tyypillisesti kutsutaan »tilin palautukseksi»—, operaattori on teknisesti tilin haltija ja voi myös luovuttaa sen sille, joka pyytää sitä asianmukaisen menettelyn kautta. Jos operaattori ei voi palauttaa pääsyä, koska identiteetti sijaitsee kryptografisesti käyttäjän laitteessa, operaattori ei voi myöskään luovuttaa sitä, ei edes määräyksen alaisena. Molemmat tavat ovat asiayhteyden mukaan oikeutettuja; mutta jälleen kerran, ne ovat erilaisia, ja on hyvä tietää, kumpaa ollaan ottamassa käyttöön.

Mitä tapahtuu ammattilaisen tiedoille, jos ammattilainen menettää pääsyn? Onko olemassa palautusmekanismeja —tilin, arkiston, istunnon— jotka riippuvat operaattorista? Ovatko nämä mekanismit yhteensopivia alan ammattieettisten sääntöjen kanssa, jos operaattori pakotetaan käyttämään niitä?

## Kerros 6: tulevaisuus

Tämä viimeinen kerros jää usein huomiotta, koska se vaatii ennakointia. Mitä tapahtuisi, jos toinen yritys ostaisi palvelun? Lähes kaikkiin yritysostoihin liittyy palveluehtojen tarkistus seuraavien kuukausien aikana. Mitä tapahtuisi, jos sääntelyvaatimukset muuttuisivat? Eurooppalainen oikeus on lisännyt poisto- ja estovelvoitteita vuodesta 2022 lähtien, ei vähentänyt niitä. Mitä tapahtuisi, jos operaattori katoaisi? Merkittävällä osalla pilvipalveluista ei ole dokumentoitua poistumissuunnitelmaa operaattorin sulkeutumisen varalta; ammattilainen huomaa ongelman, kun aikaa sen valmisteluun ei enää ole.

On muotoilu, joka kannattaa muistaa tälle kerrokselle: arkkitehtuurit, jotka riippuvat vähemmän operaattorista, ovat kestävämpiä operaattorin muutoksia vastaan. Self-hosting missä tahansa muodossaan, itsesuvereeni kryptografinen identiteetti, ilman välissä olevaa palvelinta toimiva viestintä, kaikki nämä vähentävät tulevaa riskipinta-alaa vähentämällä nykyistä riippuvuuspinta-alaa. Ne eivät poista sitä; ne vähentävät sitä.

## Ero rakenteen ja lupauksen välillä

Jos meidän pitäisi tiivistää jakso yhteen lauseeseen, se olisi tämä: rakenteelliset vastaukset säilyvät, vaikka operaattori, hallinto tai lainsäädäntö muuttuisi; lupaukseen perustuvat vastaukset säilyvät niin kauan kuin lupaaja voi ja haluaa pitää ne. Molemmat voivat olla oikeita käyttöönottohetkellä. Vain toinen niistä kestää ajan kulumisesta ja olosuhteiden muutoksista riippumatta.

Tämä ei tarkoita, että jokaisen ammattilaisen pitäisi vaatia rakenteellisia vastauksia kaikilta käyttöönottamiltaan palveluilta. Suhteellisuus pysyy oikeutettuna: sisäisen kirjanpidon laskentataulukko ei tarvitse samaa vastausta kuin potilaan kliininen kertomus. Se tarkoittaa kuitenkin, että ammattimaisuus on sitä, että tietää, millaisen vastauksen on kussakin tapauksessa hyväksynyt, ja että on tietoisesti päättänyt, että tuonkaltainen vastaus on suhteessa kyseiseen tietoon.

## Kyselylomake järjestyksessä

Kaksitoista konkreettista kysymystä, jotka tiivistävät jakson, järjestettynä niin, että vastaus kuhunkin pohjustaa seuraavaa:

1. Kulkeeko sisältö operaattorin palvelimen kautta? Jos kulkee: selväkielisenä, operaattorin avaimilla salattuna vai yksinomaan käyttäjän avaimilla salattuna?

2. Jos vedotaan päästä päähän -salaukseen, missä kryptografiset avaimet sijaitsevat? Tunteeko tai säilyttääkö operaattori jotakin osaa niistä missään muodossa, mukaan lukien »palautus»?
3. Mitä metatietoja palvelu tuottaa ja säilyttää? Kuinka kauan? Kenelle ne ovat näkyvissä?
4. Miten operaattori rahoittaa toimintansa? Jos rahoitus sisältää mainontaa tai tietojen rahaksi muuttamista, kattaako julkilausuttu käyttötarkoitus kolmansien osapuolten tiedot, jotka ammattilainen on uskonut palvelulle?
5. Mikä on operaattorin taloudellinen tilanne kolmen tai viiden vuoden tähtäimellä? Onko tekijöitä, jotka viittaavat mallin välittömään muutokseen (vireillä oleva pörssilistautuminen, ehtymässä oleva rahoituskierros, todennäköinen yritysosto)?
6. Millä lainkäyttöalueella operaattori on rekisteröity? Missä maassa palvelimet fyysisesti sijaitsevat? Jos ne eroavat, mitä kansallista lainsäädäntöä käsittelyyn sovelletaan?
7. Mitä tapahtuisi, jos operaattorin lainkäyttöalueella pätevä tiedustelumääräys vaatisi luovuttamaan tietoni? Voisiko yritys teknisesti noudattaa sitä?
8. Mitä teknistä kykyä operaattori säilyttää keskeyttääkseen, estääkseen tai poistaakseen palvelun? Millä sopimuksellisilla edellytyksillä? Millä historiallisesti dokumentoiduilla sopimuksen ulkopuolisilla edellytyksillä?
9. Mikä poistumissuunnitelma on olemassa, jos operaattori käyttäisi tätä kykyä minua vastaan, oikeutetusti tai oikeudettomasti? Onko olemassa dokumentoitu menettely tietojen viemiseksi vaihtoehtoiselle palveluntarjoajalle?
10. Kuka hallitsee pääsyn tunnuksia? Voiko operaattori palauttaa ne ilman minun osallistumistani? Suojaako se minua vai altistaako se minut?
11. Onko tälle nimenomaiselle toiminnolle olemassa eurooppalaista, itse hostattua tai ilman välissä olevaa palvelinta toimivaa vaihtoehtoa? Mikä on sen todellinen kustannus verrattuna arvioituun riskiin?
12. Jos tämänpäiväistä päätöstä tarkasteltaisiin viiden vuoden kuluttua tarkastajan, tilintarkastajan tai tietomurron kohteeksi joutuneen asiakkaan toimesta, olisiko nykyinen valinta puolustettavissa tänään käytettävissä olevin perustein, vai vaatisiko se anteeksipyyntöä siitä, ettei kohtuullisia kysymyksiä esitetty?

Kysymykset eivät odota täydellisiä vastauksia. Ne odottavat rehellisiä vastauksia, joita rehellinen operaattori osaa antaa ja joita vähemmän rehellinen operaattori välttää muotoilemasta täsmällisesti. Operatiivinen ero näiden kahden operaattorityypin välillä, sanomme tämän ilman dramatiikkaa, havaitaan yleensä lukemalla hitaasti vastaukset, joita ne vapaaehtoisesti tarjoavat, jo ennen kuin on tarpeen pyytää lisää.

---

*Tällä artikkelilla päätämme Cuadernos Lacren toisen jakson. Aloitimme Schrems II:n perimästä toimituksellisesta velasta ja päätämme operatiiviseen kyselylomakkeeseen. Matkan varrella olemme käyneet läpi käsitteitä —hash, salaus, identiteetti— ja soveltavia analyyseja —kill switch, liiketoimintamalli, self-hosting—. Julkaisun julkilausuttu toimituksellinen tarkoitus ei ollut hukuttaa lukijaa tyhjentävällä luettelolla ongelmista, vaan antaa hänelle työkaluja, joilla erottaa minkä tahansa uuden palvelun edessä, millaista vastausta hän on hyväksymässä. Tämä erottelu —arkkitehtuurin ja lupauksen välillä— on se työkalu. Muun kukin ammattilainen asettaa niiden tietojen palvelukseen, jotka katsoo käytännössään kysymyksen arvoisiksi.*

## Lähteet ja lisälukemista

- Tämä julkaisu, jakso 2 (toukokuu 2026) — *Schrems II, viisi vuotta myöhemmin*, *Mitä SHA-256 todellisuudessa on*, *Kill switch ja institutionaalinen valtaus*, *Päästä päähän -salaus, todellinen selitys*, *Liiketoimintamalli luottamuksen merkkinä*, *24 sanaa: mikä on kryptografinen identiteetti*, *Self-hosting ammatillisena käytäntönä*. Ne seitsemän artikkelia, joiden varaan tämä kyselylomake nojaa.
- Asetus (EU) 2016/679 — yleinen tietosuoja-asetus. Oikeudellinen viitekehys kaikille kysymyksille, joita kyselylomake esittää, erityisesti artiklat 5, 6, 25, 28, 32, 33 ja luku V.
- Euroopan tietosuojaneuvosto — operatiiviset suuntaviivat ja lausunnot Schrems II:sta, kansainvälisistä siirroista, vaikutustenarvioinneista ja proaktiivisesta vastuusta (julkaisut 2020–2024).
- Espanjan tietosuojavirasto — vuosina 2022–2024 julkaistut seuraamukset rekisterinpitäjille riittämättömistä siirtovälineistä tai muodollisista vaikutustenarvioinneista, joilla ei ole sisällöllistä sisältöä.

- noyb.eu — Euroopan digitaalisten oikeuksien keskus, jota johtaa Maximilian Schrems. Julkinen arkisto valituksista, muutoksenhauista ja analyyseista, jotka koskevat Euroopan tietosuojasääntöjen todellista, ei näennäistä, noudattamista.

← EdellinenSelf-hosting ammatillisena käytäntönäSeuraava →Mitä allekirjoitus ei voi korjata

## Viimeaikaiset lukemiset


- Pohdintaa · 29. kesäkuuta 2026 Et ole anonyymi
- Pohdintaa · 27. toukokuuta 2026 Mitä allekirjoitus ei voi korjata
- Analyysi · 25. toukokuuta 2026 Self-hosting ammatillisena käytäntönä


Ota tämä artikkeli mukaasi minne tarvitset.

↓ Markdown ↓ Pelkkä teksti ↓ PDF

Tiedosto ladataan laitteellesi. Voit tallentaa sen, tuoda sen Solo2-sovellukseen tai jakaa sen haluamallasi tavalla. Cuadernos ei päätä tiedoston kohtaloa puolestasi.

Sinetti · SHA-256 e5a3edf618ba2d64e2a929e0a0fdee456613b3de0c949a41c27e8b7ad0a6980c



Cuadernos Lacre · Menzuri Gestión S.L. -julkaisu ·
kirjoittanut R.Eugenio · toimittanut Solo2-tiimi.