Otsast lõpuni krüpteerimine, tõeliselt selgitatud

Mida teenusepakkujad ütlevad, kui nad ütlevad E2EE, ja mida nad jäitavad mainimata. Mehhanismi ja selle piirangute õpetlik selgitus ilma reklaamiümbriseta.

Teeme selgeks: WhatsApp ütleb, et teie sõnumid on otsast lõpuni krüpteeritud. See on tõsi — ja sellest ei piisa. Kui varukoopia läheb iCloudi või Google Drive'i ilma täiendava krüpteerimiseta, murtakse krüpteering teie enda telefonis. Operatiivne küsimus ei ole selles, kas see on krüpteeritud, vaid kus asuvad võtmed.

Mida krüpteerimine tegelikult tähendabil

Sõnumi krüpteerimine tähendab selle muutmist millekski, mis näib mürana kõigile, kellel puudub teatud teave, mida nimetatakse võtmeks. Operatsioon toimub saatja seadmes ja õige võtmega tühistatakse see vastuvõtja seadmes. Vahepeal liigub sõnum baitide jadana, millel puudub nähtav tähendus. See on lihtne idee. Ülejäänud artikkel käsitleb nüansse, mis muudavad selle sõltuvalt juhust kas tõeliseks garantiiks või turundussildiks.

Omadussõna *otsast lõpuni* — inglise keeles *end-to-end*, lühendatult E2EE — lisab täpsust. Krüpteerimist ei tehta selleks, et vahepealne server saaks seda lugeda ja kohale toimetada. Seda tehakse selleks, et ainult kahel otsal — saatja seadmel ja vastuvõtja seadmel — oleks võti. Iga server, mida sõnum läbib, näeb müra, mitte sõnumit. See on tehniline erinevus *transiidi ajal* toimuva krüpteerimisega, kus sisu liigub krüpteeritult ühest serverist teise, kuid iga server, mida see läbib, dekrüpteerib selle edastamiseks, taastades ajutiselt teksti selgel kujul.

Jagatud saladuse paradoks

On ilmne probleem. Selleks, et kaks inimest saaksid omavahel sõnumeid krüpteerida ja dekrüpteerida, vajavad mõlemad sama võtit. Kuid kuidas nad selles võtmes kokku lepivad, kui kõik, mida nad üksteisele saadavad, läbib definitsiooni kohaselt kanali, kus keegi võib pealt kuulata? Võtmes kokkuleppimine samas kanalis, kus nad seda hiljem kasutavad, tundub võimatu: kui ründaja kuuleb seda kokkuleppimise ajal, saab ta dekrüpteerida kõik järgneva. Aastakümneid lahendas klassikaline krüptograafia selle rängal viisil: võtmed anti üle isiklikult enne kasutamise alustamist füüsilistel kohtumistel. Suursaadikud kandsid kaasas võtmetega kohvreid, mis olid õmmeldud mantli voodri sisse.

Kaasaegses e-posti suhtluses see lahendus ei scaleeru. Kui me peaksime füüsiliselt minema iga inimese juurde, kellega kavatseme krüpteeritult suhelda, ei saaks me kellegagi rääkida. Küsimus, mille krüptograafiline kogukond viiskümmend aastat tagasi esitas, oli järgmine: kas on võimalik, et kaks inimest, kes üksteist ei tunne ja jagavad vaid avalikku kanalit, lepivad samas avalikus kanalis kokku saladuses, mida keegi kanalit pealt kuulaja ei saa teada?

Diffie-Hellmani elegants

1976. aastal demonstreerisid kaks matemaatikut nimega Whitfield Diffie ja Martin Hellman midagi pealtnäha võimatut: et kaks inimest, rääkides ainult avaliku kanali kaudu — kanali kaudu, kus kõik saavad kuulda kõike, mida nad ütlevad —, saavad kokku leppida salajases paroolis ilma, et ükski kuulaja saaks seda avastada. See kõlab nagu maagia. See ei ole: see on matemaatika. Diffie-Hellmani võtmevahetus, nagu seda sellest ajast peale teatakse, on praktiliselt kogu krüpteeritud internetisuhtluse alus ning pool sajandit intensiivset kasutamist ja ülemaailmset akadeemilist kontrolli kinnitavad selle kindlust. Kes soovib näha visuaalset intuitsiooni või matemaatikat, võib lugemist jätkata. Kes eelistab usaldada, et see töötab, võib samuti jätkata ilma artikli lõime kaotamata.

Neile, kes soovivad seda pildis ette kujutada, on olemas tuntud analoogia värvidega. Kujutage ette, et Alice ja Bruno lepivad avalikult kokku põhivärvis — ütleme kollases — neid pealt kuulava Eva silme all. Kumbki valib privaatselt teise salajase värvi ja segab oma saladuse kollasega. Alice saab teatud oranži; Bruno saab teatud rohelise. Nad vahetavad tulemusi Eva silme all. Nüüd segab kumbki saadud värvi oma saladusega ja mõlemad jõuavad sama lõppvärvini, sest segamise järjekord ei ole oluline. Eva on näinud kollast ja kahte vahepealset segu, kuid mitte saladusi; ilma ühegi saladuseta ei jõua ta lõppvärvini. Reaalne matemaatika asendab värvid astendamisega moodulrühmades või elliptilistes kõverates, kuid idee on sama: jagatud saladus luuakse avalikult ilma, et keegi kanalis saaks seda rekonstrueerida.

Aritmeetikas neile, kes eelistavad näha mehhanismi: Alice valib salajase arvu a, Bruno valib b. Nad vahetavad kanali kaudu avalikult g^a ja g^b. Alice arvutab $(g^b)^a$ ja Bruno arvutab $(g^a)^b$; mõlemad jõuavad sama tulemuseni g^{ab}. Eva näeb g, g^a ja g^b kanalit läbimas, kuid a taastamine g^a-st — nn diskreetse logaritmi probleem — nõuab astronoomilist arvutusaega, mis ületab universumi vanust, kui g valitakse sobivas matemaatilises rühmas.

Kellele meeldib kontrollida väikeste arvudega. Diffie-Hellmani vahetust saab algusest lõpuni läbi teha numbritega, mis on piisavalt väikesed, et peast arvutada. Kes eelistab aritmeetikasse mitte süveneda, võib selle ploki vahele jätta, kaotamata artikli järge; kes aga soovib näha mehhanismi samm-sammult töötamas, leiab selle siit. **Avalikud reeglid**, mida saavad lugeda kõik: algarv $p = 11$ (tõelises Diffie-Hellmanis on see umbes kolmesajakohaline; me kasutame ühtteist, et arvutused mahuksid ühele lehele), baas $g = 2$ ja kokkulepe, et kogu aritmeetika tehakse

modulo p — arvutatakse, jagatakse *p*-ga ja hoitakse jääki, nagu üheteistkümnepositsiooniline kell, mis läheb nulli tagasi, kui ületab kümmet. **Privaatsed valikud**, igaühel üks ja neid ei jagata kunagi: Alice valib $a = 4$. Bruno valib $b = 7$.

Samm 1. Alice arvutab $2^4 = 16$, siis $16 \bmod 11 = \mathbf{5}$. Ta saadab viie. Eva paneb selle kirja.

Samm 2. Bruno arvutab $2^7 = 128$, siis $128 \bmod 11 = \mathbf{7}$. Ta saadab seitsme. Eva paneb ka selle kirja. Pärast kahte saatmist sisaldab Eva märkmik nelja andmepunkti: $p = 11$, $g = 2$, A = 5, B = 7. Tal on puudu ühine arv, mida Alice ja Bruno on just tuletamas — ja mida Eva ei suuda rekonstrueerida.

Samm 3. Alice võtab seitsme, mille Bruno talle saatis, ja astendab selle oma isikliku astendajaga $a = 4$. Vältimaks arvu $7^4 = 2401$, arvutatakse see osade kaupa, rakendades iga sammu järel modulot:

$7^2 = 49$

$49 \bmod 11 = 5$

$7^4 = (7^2)^2 = 5^2 = 25$

$25 \bmod 11 = 3$

Alice saab arvu **3**.

Samm 4. Bruno võtab viie, mille Alice talle saatis, ja astendab selle oma isikliku astendajaga $b = 7$. Jällegi osade kaupa:

$5^2 = 25 \bmod 11 = 3$

$5^4 = (5^2)^2 = 3^2 = 9 \bmod 11 = 9$

$5^6 = 5^4 \times 5^2 = 9 \times 3 = 27 \bmod 11 = 5$

Lõpuks $5^7 = 5^6 \times 5 = 5 \times 5 = 25 \bmod 11 = \mathbf{3}$.

Bruno saab samuti arvu **3**.

Mõlemad on jõudnud sama arvuni, 3, töötades paralleelselt. Kumbki ei saatnud ühelgi hetkel oma privaatset astendajat. Alice ei tea, et $b = 7$; Bruno ei tea, et $a = 4$. Kumbki kasutas teise saadetud avalikku väärtust kombineerituna oma privaatse astendajaga ja nad kohtusid samas sihtpunktis. **Miks nad jõuavad sama arvuni?** Mida kumbki arvutas: Alice, $(g^b)^a = 2^{7\times4} = 2^{28} \bmod 11$. Bruno, $(g^a)^b = 2^{4\times7} = 2^{28} \bmod 11$. See on sama kogus, sest astendajate korrutamise järjekord ei ole oluline ($7 \times 4 = 4 \times 7$). Kumbki jõudis erinevat teed pidi samasse sihtpunkti.

Aga Eva? Tal on märkmikus $p = 11$, $g = 2$, A = 5, B = 7 ja ta tahaks 3-e. Selle arvutamiseks peaks ta teadma *a*-d või *b*-d — kuid kumbki neist pole kanalit läbinud. Ainus võimalus on küsida endalt: «millise astendaja a korral kehtib $2^a \bmod 11 = 5$?». Nii väikese p puhul võib ta proovida 0, 1, 2, 3, 4... ja leida selle vähem kui minutiga. Kuid asendades arvu 11 kolmesajakohalise algarvuga, on võimalike astendajate ruumis rohkem elemente kui jälgitavas universumis aatomeid. **Tänapäeval ei tea inimkond ühtegi algoritmi, mis suudaks selle ruumi läbida kiiremini kui miljardite aastatega.** See on niinimetatud *diskreetse logaritmi probleem*: edaspidi lihtne, tagurpidi arvutuslikult võimatu. Ja see on põhjus, miks krüpteering peab vastu isegi siis, kui Eva on jälginud kogu vestlust täht-tähelt.

Kolm lihtsat koostisosa — kella-aritmeetika, astendamine ja korrutamise kommutatiivsus ($a \cdot b = b \cdot a$) — toodavad kombineerituna protokolli, millest pool inimkonda sõltub iga päev oma privaatsuhtluses. Ükski neist kolmest osast ei tundu eraldi võetuna eriline. Otsustav on nende kokkupanek.

Diffie-Hellmanist Signal-protokollini

Otsast lõpuni krüpteerimine, mida tänapäevased professionaalsed sõnumirakendused kasutavad, tugineb peaaegu ilma eranditeta Diffie-Hellmani vahetuse elegantsele ja tugevdatud versioonile. Signal-protokoll, mille disainisid Trevor Perrin ja Moxie Marlinspike aastatel 2013–2016, on etaloniks. See kombineerib kahte põhiideed. Esimene on võtmevahetus elliptilistes kõverates (X25519), mis loob algse jagatud saladuse kahe seadme vahel. Teine on nn Double Ratchet — kahekordne hammasratas —, mis uuendab võtmeid automaatselt iga sõnumiga, nii et seadme kompromiteerimine täna ei võimalda dekrüpteerida varasemaid sõnumeid ega tulevasi sõnumeid pärast hammasratta pööramist.

Zig-is mahub kahe seadme vahel jagatud saladust loov X25519 vahetus kuuele reale, kasutades standardraamatukogu:

```
const std = @import("std");
const X25519 = std.crypto.dh.X25519;

// Alicia y Bruno generan cada uno un par (privada, pública).
const par_alicia = X25519.KeyPair.generate(io);
const par_bruno  = X25519.KeyPair.generate(io);

// Cada parte recibe la clave pública de la otra y deriva el mismo secreto.
const secreto_alicia = X25519.scalarmult(par_alicia.secret_key, par_bruno.public_key) catch unreachable;
const secreto_bruno  = X25519.scalarmult(par_bruno.secret_key,  par_alicia.public_key) catch unreachable;
// secreto_alicia == secreto_bruno  (32 bytes)
```

Mis neil kuuel real toimub: Avalikud võtmed liiguvad avalikult. Privaatvõtmed ei lahku kunagi vastavast seadmest. Kumbki pool tuletab oma privaatvõtmest ja teise poole avalikust võtmest sama kolmekümne kahe baidise saladuse, mida keegi kanalis ei saa taastada. See saladus toimib hiljem seemnena vahetatavate sõnumite krüpteerimiseks. Signal-protokolli Double Ratchet lisab sellele materjalile pideva rotatsiooni, nii et ühe hetke kompromiteerimine ei kompromiteeri ülejäänud vestlust.

Ja mis täpselt asub `std.crypto.dh.X25519` sees? Ei mingit varjatud maagiat. Need on kaks lühikest funktsiooni, mida saab täies mahus lugeda Zigi enda standardraamatukogust. Esimene tuletab privaatvõtmest avaliku võtme — vahetuse «g^a»:

```
pub fn recoverPublicKey(secret_key: [secret_length]u8) IdentityElementError![public_length]u8 {
    const q = try Curve.basePoint.clampedMul(secret_key);
    return q.toBytes();
}
```

Artikli keeles: privaatvõtit «korrutatakse» — elliptilises, mitte elementaarses aritmeetilises mõttes — Curve25519 kõvera baaspunktiga ja tulemus serialiseeritakse kolmekümne kaheks baidiks. Operatsioon `clampedMul` on selle skalaarkorrutise tugevdatud versioon: see sisaldab kaitsemeetmeid, mida krüptograafiline kogukond on aastate jooksul lisanud, et seista vastu teadaolevatele rünnakuperekondadele. Kaks rida funktsiooni keha.

Teine funktsioon kombineerib sinu privaatvõtme avaliku võtmega, mille teine pool sulle saadab. See on vahetuse «$(g^b)^a$», mis toodab kolmekümne kahe baidise jagatud saladuse, mida kumbki teist kunagi ei edastanud:

```
pub fn scalarmult(secret_key: [secret_length]u8, public_key: [public_length]u8) IdentityElementError![shared_length]u8 {
    const q = try Curve.fromBytes(public_key).clampedMul(secret_key);
    return q.toBytes();
}
```

Veel kaks rida. Saadud avalikku võtit tõlgendatakse punktina kõveral ja «korrutatakse» enda privaatvõtmega. Kõvera operatsiooni kommutatiivsuse tõttu — mis on analoogne numbrilises näites nähtud astendajate korrutamise kommutatiivsusega — lõpetavad mõlemad osapooled sama serialiseeritud punktiga: täpselt selle jagatud saladusega, millest artikkel räägib.

See on kõik. See, mis rakenduses tundub maagiana, on tegelikult kaks funktsiooni, kumbki kolm rida pikk. Tehniline keerukus on koondunud ühte operatsiooni, `clampedMul`, mis on kirjutatud samas standardraamatukogus allpool, mida on aastakümneid üle vaadanud rahvusvaheline krüptograafiline kogukond ja mis on kättesaadav kõigile, kes soovivad seda täht-tähelt lugeda. Meie rakenduses ega Zigi standardraamatukogus pole musta kasti. On avatud lähtekood, mida inimene suudab mõista, valides tempo, millega ta soovib sellesse süveneda.

Mida otsast lõpuni krüpteerimine kaitseb

Mida E2EE hästi kaitseb, eeldades korrektset teostust, on sõnumi sisu edastamise ajal. Vahepealne server, mis krüpteeritud andmeid vastu võtab ja edasi saadab, näeb arusaamatute baitide jada. Ründaja, kellel on juurdepääs kaablile, ruuterile või wifi pääsupunktile, näeb sama. Teenusepakkuja, kes säilitab liiklusest koopiaid, ei saa seda hiljem lugeda. Valitsus, kes kohustab teenuseoperaatorit sisu üle andma, saab samad arusaamatud baidid, mis serveril algselt olid.

See on praktilises mõttes palju. See on vahe kirja kirjutamise vahel läbipaistmatusse ümbrikusse ja selle kirjutamise vahel postkaardile. Mõlemad jõuavad kohale. Ainult üks säilitab sisu postiljoni eest.

Mida otsast lõpuni krüpteerimine ei kaitse

Seda tasub sama hästi teada. E2EE ei kaitse metaandmeid: server teab endiselt, et kasutaja A saadab andmeid kasutajale B, mis kellaajal, kui sagedasti ja kust, isegi kui ta ei tea, mida öeldakse. Need metaandmed, nagu me juba väitsime artiklis *Krüpteerimine ei tähenda privaatsust*, on sageli paljastavamad kui sisu. Teadmine, kad keegi helistas lahutustele spetsialiseerunud advokaadibüroosse reedel kell 22:00 kolmekümneks minutiks, räägib loo, mida kõne sisu kunagi ei rääkinud. See on sama olukord nagu näha inimest mitu korda onkoloogiakliinikusse sisenemas ja selt väljumas: pole vaja kuulda midagi siseräägitust, et kujutada ette, mis toimub. Üksik eraldiseisev metaandmeühik ei pruugi tähendada midagi; mitu omavahel ristatud joonistavad midagi tõele liiga sarnast. E2EE ei kaitse otspunkte: kui vastuvõtja seade on pahavaraga kompromiteeritud, dekrüpteeritakse sõnum selle vastuvõtja jaoks tavapäraselt ja pahavara loeb seda. E2EE ei kaitse suhtluspartneri identiteedi enda eest: kui Alice usub, et räägib Brunoga, kuid ründaja on end alguses vahele seganud (*man in the middle*) ja protokoll ei sisalda sõltumatut kontrolli, lõpetavad mõlemad osapooled sissetungijaga rääkimisega, arvates, et nad räägivad omavahel.

On neljas asi, mida tasub ilma kahemõttelisuseta sõnastada. E2EE ei takista pakkujat, kes väidab end seda pakkuvat, hoidmast lisaks krüpteerimata sõnumi koopiat oma süsteemides. Väide „minu sõnumid on otsast lõpuni krüpteeritud“ ja väide „pakkuja ei säilita minu sisu“ ei ole samad. Rakendus võib täita esimest, rikkudes samal ajal teist; oleme seda alates 2018. aastast korduvalt pressi pealkirjades näinud. Kasutajal puudub tehniline viis ühe juhu eristamiseks teisest ilma ekspertuuringuta, välja arvatud juhul, kui kliendi kood on kontrollitav. Üldsusele tuntuim juhtum: WhatsApp krüpteerib sõnumid transiidi ajal otsast lõpuni, kuid kui kasutaja aktiveerib varundamise iCloudi või Google Drive'i ilma täiendava krüpteerimiseta, salvestatakse see koopia loetavana kolmanda osapoole infrastruktuuris ja krüpteerimine tühistatakse kasutaja enda poolt.

Küsimus, mida operaator ei soovi kuulda

Rakendus, mis väidab, et krüpteerib otsast lõpuni, võib tehniliselt teha võtmete osas ühte kolmest asjast:

1. **Võtmed asuvad ainult seadmetes.** Need luuakse ja asuvad eranditult kasutajate seadmetes; operaator ei tea neid ega salvesta neid. See on optimaalne juhtum.
2. **Operaator saab soovi korral ligi.** Operaatoril on kasutajate võtmed (või ta saab neid soovi korral genereerida) ja ta hoiab neid oma andmebaasides. Kui ta soovib või teda sunnitakse, saab ta sisu lugeda. Nii on see enamiku pilveteenuste puhul.
3. **Operaatoril puudub disaini poolest ligipääs, kuid ta kontrollib ligipääsu.** Operaatoril ei ole võtmeid, kuid tal on kontroll rakenduse üle, mis neid genereerib. Sunni korral saab ta saata pahatahtliku uuenduse, mis püüab võtmed või sisu kinni enne krüpteerimist. Nii on see paljude kommertsiaalsete E2EE teenuste puhul.

Seega ei ole operatiivküsimus selles, kas miski on krüpteeritud, vaid selles, kelle kontrolli all on seade ja tarkvara, mis võtmeid haldab. Solo2-s asuvad võtmed ainult sinu Hoidlas (Sinu parooliga krüpteeritud IndexedDB) ja tarkvara on kontrollitav avatud lähtekood.

Professionaalsele lugejale

Otsast lõpuni krüpteerimine on digitaalse suveräänsuse tööriist. Kuid nagu iga tööriista puhul, sõltub selle tõhusus käest, mis seda hoiab, ja pinnasest, millele see toetub.

1. Kus krüptograafilised võtmed genereeritakse ja kus need füüsiliselt asuvad? Kui operaator saab neile juurde (isegi ajutiselt, isegi taastamise ettekäändel), on E2EE ainult nimeline.
2. Kas eksisteerib vestluspartneri sõltumatu kontroll (turvanumbrid, QR-koodid, väljaspool kanalit võrdlemine), mis hoiab ära man-in-the-middle rünnaku vestluse loomise ajal?
3. Kas kliendi kood on auditeeritav — avatud, avaldatud, reprodutseeritav — või nõuab see pakkuja sõna usaldamist selle osas, mida klient tegelikult teeb?
4. Milliseid metaandmeid teenus genereerib ja säilitab ning kui kaua? Isegi kui sisu on läbipaistmatu, saavad metaandmed rekonstrueerida suure osa tundlikust teabest.

Need neli küsimust ei küsi keerulist tehnilist teavet; nad küsivad teavet, millele iga aus operaator suudab oma avalikus dokumentatsioonis vastata. Vastuse kvaliteet ja täpsus räägib toote kohta sama palju kui vastus ise.

Otsast lõpuni krüpteerimine, kui see on õigesti tehtud, on üks peenemaid konstruktsioone, mida kaasaegne krüptograafia on igapäevasesse praktika toonud. Algne idee — kaks inimest saavad avaliku kanali kaudu saladuses kokku leppida — kuulub Whitfield Diffie'le ja Martin Hellmanile (1976); pool sajandit hiljem elame endiselt selle tagajärgedes. Kuid nagu iga tehnilise lubaduse puhul, sõltub selle väärtus tegelikust täitmisest, mitte sildist. Ausa professionaali küsimus ei ole „kas see on krüpteeritud?“, vaid „kelle käes on võtmed?“. Vastustel on erinevad tagajärjed. Neid tasub teada.

Allikad ja täiendav lugemine

- Diffie, W.; Hellman, M. — *New Directions in Cryptography*, IEEE Transactions on Information Theory, november 1976. Avaliku võtme krüptograafia alusartikkel.
- Perrin, T.; Marlinspike, M. — *The Double Ratchet Algorithm*, Open Whisper Systemsi avalik spetsifikatsioon, 2016. aasta versioon. Signal-protokolli ja selle tööstuslike tuletiste alus.
- RFC 7748 — Elliptic Curves for Security (IETF, jaanuar 2016). Kaasaegsetes võtmevahetustes kasutatavate kõverate X25519 ja X448 normatiivne spetsifikatsioon.
- Ferguson, N.; Schneier, B.; Kohno, T. — *Cryptography Engineering: Design Principles and Practical Applications* (Wiley, 2010). Peatükid võtmevahetuse ja autenditud krüpteerimisprotokollide kohta.
- Määrus (EL) 2024/1183 Euroopa digitaalse identiteedi raamistiku kohta (eIDAS 2) — kehtestab raamistikud, kus vestluspartneri sõltumatu kontroll omandab institutsionaalse toe ja kus erinevusel nimelise ja tegeliku krüpteerimise vahel on erinevad õiguslikud tagajärjed.

← EelmineKill switch ja institutsionaalne hõivamineJärgmine →Ärimudel kui usalduse signaal

Viimased lugemised

- Analüüs · 18. mai 2026 Tõeline vs näiline privaatsus: küsimused, mida tasub endalt küsida
- Analüüs · 18. mai 2026 Self-hosting kui professionaalne praktika
- Kontseptsioon · 18. mai 2026 Need 24 sõna: mis on krüptograafiline identiteet

Võtke see artikkel endaga kaasa kuhu iganes vaja.

↓ Markdown ↓ Lihttekst ↓ PDF

Fail laaditakse alla teie seadmesse. Sealt saate selle salvestada, importida Solo2-sse või jagada kus iganes soovite. Cuadernos ei otsusta sihtkohta teie eest.

Lakipitsat · SHA-256 b5d12068ed1d478ccd905b8afbcc5134f10abe8f32d9d5fb5fabe642b9b24eec

Cuadernos Lacre · Ettevõtte Menzuri Gestión S.L. väljaanne ·
kirjutanud R.Eugenio · toimetanud Solo2 meeskond.

See veebisait ei kasuta küpsiseid ega laadi kolmandate osapoolte ressursse. See kasutab ise hostitud anonüümset külastajate loendurit (Umami, meie Euroopa serveris) ja minimaalset JavaScripti valgus/tume teema eelistuse haldamiseks. Ei mingeid jälitajaid, profileerimist ega andmete jagamist. Kui soovite meid jälgida: RSS.