Analys · 26 maj 2026

← Föregående·Nästa →

Verklig vs. skenbar integritet: de frågor man bör ställa sig

Operativ syntes av cykel 2: de frågor som skiljer en tjänst med arkitektonisk integritet från en med deklarativ integritet. Ett frågeformulär för den europeiska yrkesutövaren innan denne tar i bruk ett digitalt verktyg för känsliga uppgifter.

För att förstå varandra: Två tjänster med samma juridiska meddelande kan bete sig mycket olika. Den ena skyddar genom teknisk design. Den andra skyddar genom avtalsmässigt löfte. Skillnaden går inte att läsa i meddelandet — den upptäcks genom att ställa de konkreta frågorna. Svarens kvalitet säger lika mycket om produkten som deras eget innehåll.

Skillnaden mellan arkitektonisk och deklarativ integritet

Under de sju föregående artiklarna i denna cykel har vi rört oss genom olika lager av samma fråga. Rätten om internationella överföringar med Schrems II. Den matematiska idén om den kryptografiska hash som förseglar varje Cuaderno. Det arkitektoniska valet av kill switch och den institutionella fångst som nästan alltid åtföljer den. Mekanismen i totalsträckskrypteringen och den operativa frågan om var nycklarna finns. Anpassningen av incitamenten enligt affärsmodellen. Den självsuveräna kryptografiska identiteten. Self-hosting som proportionerlig strategi. Varje artikel behandlade en aspekt. Denna, den sista i cykeln, samlar dem i ett frågeformulär.

Den distinktion som är värd att minnas är enkel: det finns tjänster vars integritet är *arkitektonisk* och det finns tjänster vars integritet är *deklarativ*. Den första är inbäddad i den tekniska designen: vissa kränkningar av integritetsåtagandet är tekniskt svåra eller omöjliga eftersom arkitekturen inte tillåter dem. Den andra är nedlagd i texten i det juridiska meddelandet: vissa kränkningar skulle vara avtalsmässigt sanktionerbara om de inträffar, men tekniskt hindrar ingenting dem. Båda modellerna kan uppfylla GDPR; men den ena skyddar genom konstruktion och den andra skyddar genom löfte, och skillnaden är operativt enorm.

Frågorna som följer är utformade för att skilja det ena fallet från det andra. Det är inte avancerade tekniska frågor. Det är de frågor som varje ärlig leverantör kan besvara i sin offentliga dokumentation. Svarets kvalitet och precision säger lika mycket om produkten som svaret självt. Frågorna grupperas i sex lager; det är bra att ställa dem alla innan man tar tjänsten i bruk för känsliga uppgifter, inte bara de som det första instinktet identifierar.

Lager 1: arkitektur

Låt oss fastställa en term innan vi går vidare. Med *operatör* menar vi företaget som tillhandahåller tjänsten: den enhet som kontrollerar servrarna och programvaran, inte en enskild person. Med det klargjort är den grundläggande arkitektoniska frågan: vad gör operatören med innehållet mellan avsändare och mottagare? Det finns tre möjliga svar och det är värt att kunna skilja dem åt, eftersom alla tre ibland marknadsförs med liknande ordval.

- Det första: innehållet passerar genom en server hos operatören i klartext, där operatören kan läsa det även om han lovar att inte göra det.
- Det andra: innehållet passerar krypterat genom en server hos operatören, där operatören inte kan läsa det om nycklarna uteslutande finns på användarnas enheter.
- Det tredje: innehållet passerar inte genom någon server hos operatören, eftersom det inte finns någon server hos operatören i det konkreta flödet.

Skillnaden mellan dessa tre är inte en skillnad i grad: det är en skillnad i typ.

Den kompletterande frågan — redan formulerad i Cuaderno om kryptering — är: vem har de kryptografiska nycklar som gör det möjligt att läsa innehållet? Om användaren har dem och endast användaren, är krypteringen verklig. Om operatören dessutom har dem i någon form — även under namnet «kontoåterställning» eller «synkronisering mellan enheter» —, är krypteringen nominell. Frågan tillåter inget ärligt mellansvar.

Lager 2: affärsmodell

Frågan om affärsmodellen betyder lika mycket som den arkitektoniska frågan, och av samma väsentliga skäl: incitament frambringar med tiden systematiskt olika produkter, även med identiskt uttalade syften. Hur tjänar operatören pengar idag? En enda källa, två, en blandning? Om finansieringen omfattar reklam eller monetisering av data, vilka data monetiseras då och på vilken rättslig grund i GDPR sker det? Täcker det ändamål som uttalas i det juridiska meddelandet de tredjepartsuppgifter som yrkesutövaren avser att anförtro tjänsten?

Och frågan av andra ordningen, inte alltid formulerad: hur ser operatörens finansiella situation ut på tre till fem års sikt? Ett företag i riskkapitalfasen verkar under andra påtryckningar än ett företag med stabil lönsamhet. Bytet av finansieringsmodell är upprepade gånger det ögonblick då det implicita avtalet med användarna skrivs om utan förhandling.

Lager 3: jurisdiktion

För den europeiska yrkesutövaren är frågan om jurisdiktion inte retorisk. I vilken jurisdiktion är operatören registrerad? I vilket land finns de servrar som behandlar uppgifterna fysiskt? Är svaret på de två föregående frågorna detsamma eller olika, och om det skiljer sig åt, vilken lagstiftning tillämpas? En europeisk region som drivs av ett amerikanskt företag är, vad gäller Schrems II, inte ett europeiskt svar: företaget är underkastat FISA 702 oberoende av var servrarna finns.

Den kompletterande operativa frågan är: om det imorgon kom en underrättelseorder som är giltig i operatörens jurisdiktion och som krävde att mina uppgifter eller mina klienters lämnades ut, vad skulle då hända? Om det ärliga svaret börjar med «företaget skulle vara skyldigt att lämna ut dem», skyddar tjänsten inte mot den ordern hur mycket reklamen än antyder motsatsen. Om det ärliga svaret börjar med «företaget skulle inte kunna lämna ut dem eftersom det inte har dem i klartext», skyddar tjänsten verkligen; och skillnaden beror nästan helt på de två första lagren, inte på integritetspolicyns kvalitet.

Lager 4: operatör och kill switch

Vilken teknisk kapacitet behåller operatören för att på distans stänga av, blockera, radera eller försämra tjänsten? Frågan är inte paranoid: den är operativ. De digitala plattformarna har upprepade gånger utövat denna kapacitet under de senaste åren, ibland på eget initiativ, ibland på order av regeringar, ibland efter ägarbyten eller policyändringar. Om kapaciteten finns är det bra att veta under vilka avtalsmässigt uttalade förutsättningar den utövas, och att reservera en marginal för de outtalade förutsättningar som de senaste årens praktik har visat vara lika relevanta: oväntat domstolsbeslut, internationell sanktion, byte av bolagsstyrning, förvärv av en enhet med en annan policy.

Systerfrågan är den om kontinuitetsplanen: om operatören utövade kapaciteten mot yrkesutövaren — av vilken anledning som helst, rättvist eller inte —, hur mycket drifttid skulle då fortfarande vara tillgänglig, vilken procedur för export av data finns det, och till vilken alternativ leverantör skulle man kunna migrera? Om svaret börjar med «det borde inte hända» är det inte ett operativt svar; det är ett löfte.

Lager 5: identitet och åtkomst

Vem kontrollerar inloggningsuppgifterna till tjänsten? Om operatören kan återställa användarens åtkomst utan användarens medverkan — en procedur som vanligtvis kallas «kontoåterställning» —, är operatören tekniskt sett kontots förvaltare och kan också överlåta det till den som begär det via lämplig procedur. Om operatören inte kan återställa åtkomsten eftersom identiteten finns kryptografiskt på användarens enhet, kan operatören inte heller överlåta den, inte ens på order. Båda modaliteterna är legitima beroende på sammanhanget; men, återigen, de är olika, och det är bra att veta vilken man tar i bruk.

Vad händer med yrkesutövarens uppgifter om yrkesutövaren förlorar åtkomsten? Finns det återställningsmekanismer — för konto, fil, session — som är beroende av operatören? Är dessa mekanismer förenliga med branschens yrkesetik om operatören tvingas att använda dem?

Lager 6: framtid

Detta sista lager försummas ofta eftersom det kräver projektion. Vad skulle hända om tjänsten förvärvades av ett annat företag? Nästan alla förvärv medför en översyn av tjänstevillkoren under de följande månaderna. Vad skulle hända om de regulatoriska kraven ändrades? Den europeiska rätten har ökat skyldigheterna att avlägsna och blockera sedan 2022, inte minskat dem. Vad skulle hända om operatören försvann? En betydande del av molntjänsterna har ingen dokumenterad exit-plan för scenariot att operatören lägger ned; yrkesutövaren upptäcker problemet när det inte längre finns tid att förbereda det.

Det finns en formulering som är värd att minnas för detta lager: arkitekturer som är mindre beroende av operatören är mer motståndskraftiga mot förändringar hos operatören. Self-hosting i alla dess modaliteter, den självsuveräna kryptografiska identiteten, kommunikationen utan server emellan — allt detta minskar den framtida riskytan genom proceduren att minska den nuvarande beroendeytan. De eliminerar den inte; de minskar den.

Skillnaden mellan struktur och löfte

Om vi skulle destillera cykeln till en enda mening skulle det vara denna: de strukturella svaren består även om operatören, förvaltningen eller lagstiftningen ändras; svaren per löfte består så länge den som lovar kan och vill upprätthålla dem. Båda kan vara korrekta i det ögonblick de antas. Endast det ena av de två håller oberoende av tidens gång och omständigheternas förändring.

Detta betyder inte att varje yrkesutövare måste kräva strukturella svar av alla de tjänster han tar i bruk. Proportionaliteten förblir legitim: ett kalkylblad för intern bokföring behöver inte samma svar som en patients journal. Det betyder dock att professionalism består i att veta vilken sorts svar man har accepterat i varje enskilt fall, och i att medvetet ha beslutat att den sortens svar är proportionerlig mot den konkreta uppgiften.

Frågeformuläret, ordnat

Tolv konkreta frågor som sammanfattar cykeln, ordnade så att svaret på var och en informerar nästa:

1. Passerar innehållet genom en server hos operatören? Om så: i klartext, krypterat med operatörens nycklar, eller krypterat med nycklar som uteslutande tillhör användaren?

2. Om totalsträckskryptering åberopas, var finns de kryptografiska nycklarna? Känner till eller bevarar operatören någon del av dem i någon form, inklusive «återställningen»?
3. Vilka metadata genererar och bevarar tjänsten? Hur länge? För vem är de synliga?
4. Hur finansieras operatören? Om finansieringen omfattar reklam eller monetisering av data, täcker det uttalade ändamålet då tredjepartsuppgifter som anförtrotts av yrkesutövaren?
5. Hur ser operatörens finansiella situation ut på tre till fem års sikt? Finns det faktorer som tyder på en förestående modelländring (förestående börsintroduktion, finansieringsrunda som håller på att ta slut, sannolikt förvärv)?
6. I vilken jurisdiktion är operatören registrerad? I vilket land finns servrarna fysiskt? Om de skiljer sig åt, vilken nationell lagstiftning tillämpas då på behandlingen?
7. Vad skulle hända om en underrättelseorder som är giltig i operatörens jurisdiktion krävde att mina uppgifter lämnades ut? Skulle företaget tekniskt kunna efterleva den?
8. Vilken teknisk kapacitet behåller operatören för att stänga av, blockera eller radera tjänsten? Under vilka avtalsmässiga förutsättningar? Under vilka historiskt dokumenterade icke-avtalsmässiga förutsättningar?
9. Vilken exit-plan finns om operatören utövade denna kapacitet mot mig, rättvist eller orättvist? Finns det en dokumenterad procedur för export av data till en alternativ leverantör?
10. Vem kontrollerar inloggningsuppgifterna? Kan operatören återställa dem utan min medverkan? Skyddar det mig eller utsätter det mig?
11. Finns det ett europeiskt, självhostat eller serverlöst alternativ för denna konkreta funktion? Vad är dess verkliga kostnad jämfört med den bedömda risken?
12. Om dagens beslut om fem år granskades av en inspektör, en revisor eller en kund som drabbats av ett intrång, skulle det nuvarande valet då vara försvarbart med de argument som finns tillgängliga idag, eller skulle det kräva en ursäkt för att inte ha ställt rimliga frågor?

Frågorna väntar sig inte perfekta svar. De väntar sig ärliga svar, som den ärliga operatören vet att ge och som den mindre ärliga operatören undviker att formulera med precision. Den operativa skillnaden mellan de två sorternas operatör, det säger vi utan dramatik, brukar märkas genom att långsamt läsa de svar de erbjuder frivilligt, redan innan man behöver be om mer.

Med denna artikel avslutar vi den andra cykeln av Cuadernos Lacre. Vi började med den redaktionella skuld som ärvts från Schrems II och avslutar med ett operativt frågeformulär. På vägen har vi rört oss genom begrepp — hash, kryptering, identitet — och tillämpade analyser — kill switch, affärsmodell, self-hosting. Publikationens uttalade redaktionella avsikt var inte att överväldiga läsaren med den uttömmande listan över problem, utan att ge denne verktyg så att han inför varje ny tjänst kan urskilja vilken sorts svar han accepterar. Den distinktionen — mellan arkitektur och löfte — är verktyget. Resten kommer varje yrkesutövare att ställa i tjänst för de uppgifter som han i sin praktik anser värda frågan.

Källor och vidare läsning

- Denna publikation, cykel 2 (maj 2026) — *Schrems II, fem år senare*, *Vad SHA-256 egentligen är*, *Kill switch och institutionell fångst*, *End-to-end-kryptering, förklarat på riktigt*, *Affärsmodellen som ett tecken på förtroende*, *De 24 orden: vad en kryptografisk identitet är*, *Self-hosting som professionell praxis*. De sju artiklar som detta frågeformulär vilar på.
- Förordning (EU) 2016/679 — Allmänna dataskyddsförordningen. Juridisk referensram för alla de frågor som frågeformuläret väcker, i synnerhet artiklarna 5, 6, 25, 28, 32, 33 och kapitel V.
- Europeiska dataskyddsstyrelsen — operativa riktlinjer och yttranden om Schrems II, internationella överföringar, konsekvensbedömningar och proaktiv ansvarsskyldighet (publikationer 2020-2024).
- Spanska dataskyddsmyndigheten — offentliggjorda sanktioner 2022-2024 mot personuppgiftsansvariga för olämpliga överföringsinstrument eller för formella konsekvensbedömningar utan väsentligt innehåll.
- noyb.eu — Europeiska centret för digitala rättigheter, lett av Maximilian Schrems. Offentligt arkiv över klagomål, överklaganden och analyser om den verkliga, inte skenbara efterlevnaden av de europeiska dataskyddsreglerna.

← FöregåendeSelf-hosting som yrkespraxisNästa →Det en signatur inte kan fixa

Senaste läsning

- Reflektion · 29 juni 2026 Du är inte anonym
- Reflektion · 27 maj 2026 Det en signatur inte kan fixa
- Analys · 25 maj 2026 Self-hosting som yrkespraxis

Ta med dig den här artikeln dit du behöver den.

↓ Markdown ↓ Klartext ↓ PDF

Filen laddas ner till din enhet. Därifrån kan du spara den, importera den till Solo2 eller dela den var du vill. Cuadernos bestämmer inte destinationen åt dig.

Lacksigill · SHA-256 078d9cebe22169210d3f1f7e65493d5a257f45a9a6cf89fb433370b09d233212

Cuadernos Lacre · En utgåva från Menzuri Gestión S.L. ·
skriven av R.Eugenio · redigerad av teamet bakom Solo2.