Consent Architecture: DKMS as the Structurally Sound Foundation for EHDS Article 71

Vereign AG

2026-04-29

Architettura del Consenso: DKMS come Fondamento Strutturalmente Solido per EHDS Article 71

Vereign AG — aprile 2026

1. Sommario Esecutivo

La normativa europea sui dati sanitari ha superato una soglia decisiva. L'opt-out non è più un obiettivo di policy auspicabile — ai sensi di EHDS Article 71 è un **diritto legale** della persona fisica, applicabile in ogni Stato membro che tratta dati sanitari identificabili per uso secondario. Stratificato sugli Articoli 7(3) e 17(2) del GDPR, sull'eIDAS 2.0 Article 5a, sulla FADP e sull'HFG svizzeri, e sul PDSG tedesco, cinque regimi indipendenti convergono su un insieme unitario di invarianti ingegneristici: **identificatori riferiti alla persona, opt-out verificabile con marca temporale, reversibilità senza re-identificazione, propagazione cross-controller e unlinkability**. Il PKI centralizzato e l'identità federata ne soddisfano al massimo uno o due; X.509 non ne soddisfa nessuno al livello del cittadino. **Decentralized Key Management (DKMS) è il primo fondamento strutturalmente solido per onorare il ritiro del consenso end-to-end — *in condizioni interorganizzative, post-divulgazione, sotto vigilanza regolatoria*.** La tesi ha confini espliciti — i derivati usciti dal sistema prima del ritiro, i backup immutabili e le singole controparti disoneste rimangono fuori dalla portata

architettonica. Il dossier dei risarcimenti 2025–2026 (Kaiser USD 47,5M, Sutter USD 21,5M, procedimenti paralleli contro BJC, Northwell, Catholic Health, Aspirus e SSM Health) è l'indicatore anticipatore: ogni incidente centralizzato condivide un'unica caratteristica — l'utente non aveva alcuna agency architettonica.

---

2. Perché Adesso — Convergenza Regolatoria in 24 Mesi

Per due decenni, la gestione del consenso nell'informatica sanitaria ha trattato l'opt-out come un problema di UX. Dal 2024 in poi, cinque regimi giuridici indipendenti hanno convergito sullo stesso schema ingegneristico, lasciando ai vendor mesi — non anni — per dimostrare la conformità strutturale.

EHDS Article 71 — Reg. (EU) 2025/327. Adottato l'11 febbraio 2025; pubblicato nella Gazzetta Ufficiale dell'Unione Europea (GU L 2025/327) il 5 marzo 2025; in vigore dal 26 marzo 2025. L'Article 71(1) riconosce a ogni persona fisica il diritto di esercitare l'opt-out dal trattamento secondario di dati sanitari elettronici identificabili. L'Article 71(2) vieta il rilascio di nuovi permessi su dati identificabili una volta esercitato l'opt-out, preservando i permessi emessi in precedenza. **L'Article 71(8)** vieta ai titolari dei dati di acquisire dati identificativi aggiuntivi al solo scopo di onorare l'opt-out — il punto di svolta ingegneristico che preclude il pattern ovvio del "registro centrale degli ID con opt-out".

GDPR Articles 7(3) e 17(2) — Reg. (EU) 2016/679. L'Article 7(3) richiede che il ritiro del consenso sia «altrettanto facile da esercitare quanto il conferimento». L'Article 17(2) impone un obbligo di propagazione: il controller che onora una richiesta di cancellazione deve adottare «misure ragionevoli, incluse misure tecniche» per informare i controller downstream. L'Article 9(2)(a) innalza la soglia per i dati sanitari al consenso *esplicito*; gli Articoli 17(3)(c)/(d) prevedono deroghe per la sanità pubblica e la ricerca che rendono la cancellazione letterale strutturalmente irraggiungibile per la maggior parte delle cartelle cliniche — ed è precisamente per questo che EHDS ha configurato il diritto come **soppressione prospettica** piuttosto che come cancellazione retroattiva.

eIDAS 2.0 — Reg. (EU) 2024/1183. Modifica il Reg. (EU) 910/2014 per istituire il European Digital Identity Wallet (EUDIW). L'Article 5a(14) prescrive il «pieno controllo dell'utente» sulle operazioni del wallet. L'Article 5a(16)(a) vieta il tracciamento cross-context dell'utilizzo del wallet; l'Article 5a(16)(b) prescrive la **unlinkability** tra le presentazioni di credenziali a verifier diversi. Insieme, i punti 5a(16)(a)–(b) costituiscono la forma operativa di EHDS Article 71(8): un'architettura in cui l'operatore può correlare un cittadino tra verifier diversi non supera per definizione il test di unlinkability.

FADP e HFG svizzeri. La Legge federale sulla protezione dei dati rivista (FADP / nDSG, RS 235.1, in vigore dal 1° settembre 2023) richiede il consenso esplicito per i dati sensibili all'Article 6(6) e un diritto di ritiro assoluto all'Article 6(7), con diritti di cancellazione all'Article 32 soggetti a obblighi di conservazione. La Legge sulla ricerca sull'essere umano (HFG / HRA, RS 810.30) agli Articoli 7(2) e 17 riconosce il diritto di revoca del consenso e di opposizione all'ulteriore utilizzo dei dati sanitari. L'EGDG in arrivo (messaggio del Consiglio federale, 5 novembre 2025) inverte il modello EPD da opt-in a opt-out con entrata in vigore prevista

~2028–2030; il BDG (base giuridica per l'uso secondario di DigiSanté) è in fase di redazione. La propagazione intercantonale rende il caso svizzero strutturalmente più complesso di quello europeo.

PDSG tedesco. Il Patientendaten-Schutz-Gesetz mette in opera l'architettura di opt-out della ePA tedesca (cartella clinica elettronica), operativa dal gennaio 2025 per circa 73 milioni di assicurati nell'ambito dell'assicurazione sanitaria obbligatoria. Il PDSG codifica le meccaniche di soppressione prospettica — i cittadini che rifiutano l'ePA non possono essere trattati in base alla base giuridica opt-in — per una popolazione superiore alla maggior parte degli Stati membri dell'UE complessivamente. La pressione di implementazione nazionale sull'architettura del consenso non è quindi teorica; è operativa nel maggiore sistema sanitario a pagatore unico in Europa.

La bozza di linea guida TEHDAS2 Joint Action (settembre 2025) conferma che il meccanismo tecnico di propagazione dell'opt-out **non** è specificato dal diritto UE e viene rimesso all'implementazione degli Stati membri. Questo è il punto debole architettonico: ogni Stato potrebbe scegliere il proprio approccio, ma solo un approccio basato su chiavi controllate dal soggetto soddisfa l'Article 71(8) senza introdurre surrettiziamente un registro di re-identificazione vietato. I vendor che consegnano un'architettura conforme in uno Stato membro la venderanno in tutti e ventisette; quelli che risolvono solo la UX locale si troveranno di fronte a una conversazione architettonica diversa in ogni trasposizione.

Ciascuno di questi cinque regimi, preso singolarmente, è gestibile. **Tutti e cinque insieme, in una finestra di 24 mesi, costituiscono la funzione forzante architettonica.** I vendor di informatica sanitaria si trovano ora di fronte a un mercato in cui la «gestione del consenso» deve comporsi end-to-end, attraverso confini nazionali, tra controller diversi, nel tempo — e il pattern del registro centralizzato che ha sostenuto il settore per due decenni è precluso dal diritto primario del più grande blocco economico del pianeta.

---

3. I Cinque Invarianti Ingegneristici

I cinque regimi convergono su un insieme ristretto e preciso di requisiti ingegneristici. Non sono aspirazionali — sono predicati verificabili rispetto ai quali qualsiasi architettura del consenso può essere valutata.

3.1 Identificatori Riferiti alla Persona

Il soggetto dei dati deve controllare l'identificatore sotto cui i propri permessi, autorizzazioni e stato del consenso sono referenziati. Questo è il *prerequisito* per ogni altro invariante: se l'operatore possiede l'identificatore, possiede anche l'opt-out. EHDS Article 71(8) preclude esplicitamente i registri di re-identificazione lato operatore; il mandato di «pieno controllo dell'utente» dell'eIDAS 2.0 Article 5a(14) nomina la stessa proprietà al livello del wallet. Senza un identificatore riferito al soggetto, la propagazione, la reversibilità e la unlinkability collassano tutte nella policy dell'operatore.

3.2 Opt-Out Verificabile con Marca Temporale

Per ogni permesso di dati, il sistema deve conoscere il momento preciso del rilascio e il momento preciso del ritiro — e una terza parte (regolatore, tribunale, controller downstream) deve poter verificare entrambi senza dover fidarsi dei log dell'operatore. EHDS Article 71(2) traccia un confine temporale netto: i permessi precedenti all'opt-out rimangono validi; quelli successivi sono illeciti. Questo è inapplicabile senza una cronologia a prova di manomissione, verificabile da terze parti, dello stato del consenso del soggetto.

3.3 Reversibilità Senza Re-Identificazione

Il Recital 54 del Regolamento EHDS conferma che l'opt-out è reversibile (i cittadini possono tornare all'opt-in) e libero da vincoli formali (senza durata minima). L'Article 71(8) vieta al titolare dei dati di acquisire dati identificativi aggiuntivi al solo scopo di onorare l'opt-out. Le due clausole lette congiuntamente creano un vincolo stringente: il sistema deve supportare il cambio di stato del consenso avanti e indietro, ai tempi del cittadino, **senza** che il titolare dei dati costruisca un registro di re-identificazione parallelo per tracciare chi ha cambiato stato e quando. Qualsiasi architettura che richieda di «tenere semplicemente un elenco degli ID con opt-out» viola direttamente l'71(8).

3.4 Propagazione Cross-Controller

Il GDPR Article 17(2) richiede al controller che onora la cancellazione di adottare «misure ragionevoli, incluse misure tecniche» per informare i controller downstream che detengono copie, repliche o link. EHDS Article 71 sovrapposto a catene di permessi multi-controller aggrava questo requisito: il segnale di opt-out deve raggiungere ogni Health Data Access Body, ogni consorzio di ricerca, ogni sub-responsabile del trattamento che ha ricevuto dati in base a un permesso precedente. La propagazione non può essere un registro cartaceo — deve essere un artefatto verificabile che le parti downstream possono ricontrollare.

3.5 Unlinkability

L'eIDAS 2.0 Article 5a(16)(b) prescrive la unlinkability tra le presentazioni della stessa credenziale a verifier diversi. La conseguenza operativa: un'architettura in cui qualsiasi singola parte (anche un intermediario autorizzato) vede ogni transazione tra verifier diversi non supera il test per costruzione. Questa è la proprietà che esclude i provider di identità federata dal livello del cittadino dei sistemi conformi a EHDS: l'IdP, per progettazione, vede ogni accesso e ogni presentazione di credenziale. La federazione può soddisfare la propagazione, ma solo violando la unlinkability.

Questi cinque invarianti formano un sistema interlocked. **X.509 PKI non ne soddisfa nessuno al livello del cittadino. Gli IdP federati soddisfano la propagazione solo violando la unlinkability. DKMS li soddisfa tutti e cinque.** Questa è l'affermazione di solidità strutturale, e il resto del documento la esamina.

---

4. La Trappola dell’Article 71(8)

Il pattern di implementazione più semplice per l’opt-out — quello che un vendor di informatica sanitaria elaborerà nella prima ora di conversazione architettonica — è **un registro centrale degli ID dei cittadini con opt-out**. Ogni titolare dei dati interroga il registro prima del trattamento; se l’ID del cittadino è nella lista, il trattamento si interrompe. Semplice. Familiare. Verificabile.

L’Article 71(8) preclude completamente questo pattern.

La clausola vieta ai titolari dei dati di acquisire dati identificativi aggiuntivi al solo scopo di onorare l’opt-out. **La «lista degli ID con opt-out» è, per costruzione, esattamente un tale registro.** Esiste per nessun altro scopo che re-identificare i cittadini nel caso negativo — per determinare che *questo cittadino ha esercitato l’opt-out e quindi non può essere trattato*. La lista stessa è la violazione regolatoria che dovrebbe prevenire.

La trappola è ricorsiva. Qualsiasi tentativo di anonimizzare il registro (hashare gli ID, pseudonimizzarli, mantenerli in un dominio di fiducia separato) reintroduce il problema originale: il titolare dei dati ha comunque bisogno di *qualche* identificatore da confrontare con la lista, e quell’identificatore deve essere derivabile dai dati già in possesso del titolare. L’hash non è anonimo per chi possiede l’input; lo pseudonimo non è anonimo per chi possiede il collegamento. Il Recital 54 rafforza questo punto prescrivendo che l’opt-out sia reversibile e libero da vincoli — il che significa che il registro deve supportare il cambio di stato, richiedendo a sua volta che il registro tracci *quale* cittadino ha cambiato stato *quando*, che è esattamente la registrazione di re-identificazione che l’71(8) vieta.

L’implicazione per i vendor di informatica sanitaria è netta. **Qualsiasi «modulo di gestione del consenso» la cui architettura si basi su una lista centrale autorevole dei soggetti con opt-out è preclusa dal diritto primario dell’UE.** Non si tratta di una scelta di design UX; è la differenza tra un’architettura che può conformarsi a EHDS e una che non può. I prodotti generici di gestione del consenso costruiti sul pattern del registro — che siano SaaS, on-prem o ibridi — si troveranno di fronte a questo vincolo in ogni trasposizione degli Stati membri. La risposta strutturale deve porre l’identificatore sotto il controllo del cittadino, così che il titolare dei dati non debba mai mantenere un registro di re-identificazione.

---

5. La Tesi DKMS

> **Decentralized Key Management è il primo fondamento strutturalmente solido per onorare il ritiro del consenso end-to-end — *in condizioni interorganizzative, post-divulgazione, sotto vigilanza regolatoria*.**

DKMS — il cui Decentralized Key Management si basa su KERI, una specifica aperta della Trust over IP Foundation — pone la radice di fiducia nel cittadino piuttosto che in un’autorità centralizzata. Il cittadino (o il proprio wallet agent) detiene un Autonomic IDentifier (AID) auto-certificante: è derivato da una chiave

pubblica sotto il controllo del cittadino e la sua autenticità non dipende da alcun registro. Tutte le autorizzazioni concesse ai titolari dei dati, ai responsabili del trattamento e ai controller downstream si concatenano a quell'AID attraverso un Key Event Log (KEL) — un registro append-only, verificabile da terze parti, dello stato di keying del cittadino, incluse le rotazioni delle chiavi.

Il ritiro in questo modello non è una richiesta inoltrata a un operatore. È una **rotazione di chiave che il cittadino esegue unilateralmente**. La rotazione viene pubblicata nel KEL; da quel momento in poi, qualsiasi parte downstream che detenga credenziali ancorate allo stato pre-rotazione della chiave deve ri-autenticarsi rispetto allo stato attuale del cittadino per continuare il trattamento. I permessi esistenti emessi prima della rotazione continuano a operare dove la base giuridica sottostante lo consente (in corrispondenza con EHDS Article 71(2)); i nuovi permessi non possono essere emessi sotto il vecchio stato della chiave, perché quel vecchio stato non è più lo stato di controllo del cittadino. Il cittadino ha ritirato architettonicamente — non solo proceduralmente — l'autorizzazione futura, e qualsiasi parte downstream che ignori la rotazione pubblicata produce firme verificabili come non aggiornate.

Mappatura rispetto ai cinque invarianti:

Invariante	**Meccanismo DKMS**
Identificatori riferiti alla persona	L'AID è l'identificatore auto-certificante del soggetto; non è richiesto alcun indice lato operatore
Opt-out verificabile con marca temporale	Il KEL contiene eventi chiave a prova di manomissione con marca temporale
Reversibilità senza re-identificazione	Ritorno all'opt-in = rotazione di chiave che ristabilisce l'autorizzazione; nessun registro parallelo
Propagazione cross-controller	Il KEL è pubblicabile; i verifier devono ricontrollare attraverso i domini di fiducia
Unlinkability	AID per contesto e credenziali a disclosure selettiva evitano la correlazione cross-verifier

Confronto con le opzioni esistenti:

X.509 PKI vincola l'identità a un certificato emesso da una CA. Il cittadino non detiene la radice di fiducia; la detiene la CA. La revoca è guidata dall'operatore (CRL/OCSP) e in caso di errore si risolve per default in soft-fail. La unlinkability cross-context è strutturalmente assente — ogni presentazione di certificato è collegabile attraverso il numero di serie del certificato, il DN dell'emittente e il DN del soggetto. X.509 soddisfa *zero* dei cinque invarianti al livello del cittadino.

IAM federato (OIDC, SAML). L'Identity Provider è per progettazione il tracker cross-context che l'eIDAS 2.0 Article 5a(16)(b) vieta. La federazione può soddisfare la propagazione cross-controller (un single logout svuota le sessioni downstream), ma solo violando la unlinkability — ogni accesso transita attraverso l'IdP, che vede ogni relying party visitata dal cittadino. L'architettura può soddisfare al massimo tre invarianti e solo a scapito del quinto.

KMS centralizzato (AWS KMS, Azure Key Vault, GCP Cloud KMS). Eccellente per workload single-tenant. La cancellazione crittografica tramite Customer-Managed Key ai sensi di NIST SP 800-88 §2.5 è una primitiva di cancellazione terminale riconosciuta dai regolatori (EDPB Guidelines 01/2025; ENISA 2019 §4.2). Ma una volta che i dati lasciano il confine della tenancy — in un consorzio di ricerca, un controller downstream, un destinatario autorizzato per uso secondario — la distruzione della CMK dell'operatore non ha effetto sulla copia. La propagazione cross-controller è irrisolta. Schrems II / EDPB Recommendations 01/2020 Use Case 3 aggrava ulteriormente questo punto: per definizione, l'importatore di dati non deve detenere le chiavi.

DKMS non sostituisce questi stack — occupa lo slot architettonico preciso che essi non possono riempire. KMS centralizzato per la cancellazione riferita alla tenancy, X.509 per la revoca di classe TLS, IAM federato per il consenso riferito alla sessione — e DKMS per il livello interorganizzativo, post-divulgazione dove EHDS Article 71 vive concretamente.

---

6. Dove le Architetture Centralizzate Falliscono

I cinque invarianti sono verificabili. Ogni architettura di consenso centralizzata fallisce in modo strutturalmente specifico.

6.1 X.509 PKI Fallisce Tutti i Cinque Invarianti al Livello del Cittadino

X.509 vincola l'identità a una Certification Authority. La CA genera o co-firma il certificato del cittadino, possiede la decisione di rilascio e controlla la revoca. Gli identificatori riferiti alla persona falliscono alla radice — la firma della CA è la fonte di fiducia, non quella del cittadino. L'opt-out con marca temporale è guidato dall'operatore (il cittadino invia una richiesta di revoca; la CA decide se onorarla e quando pubblicarla), e la revoca si propaga solo alla velocità delle finestre di aggiornamento delle CRL o della disponibilità dei responder OCSP — entrambi i quali per default si risolvono in soft-fail nei browser. La reversibilità senza re-identificazione fallisce perché la riemissione richiede che la CA ri-validi l'identità del soggetto, il che in contesti sanitari richiede alla CA di riappropriarsi degli stessi dati identificativi che EHDS Article 71(8) vieta al titolare dei dati di detenere. La propagazione cross-controller dipende dal fatto che ogni relying party controlli correttamente CRL/OCSP, il che gli incidenti DigiNotar e Comodo hanno dimostrato essere operativamente fragile. La unlinkability è strutturalmente impossibile: ogni certificato X.509 porta un numero di serie e un DN dell'emittente che collegano ogni presentazione allo stesso cittadino.

6.2 L'IAM Federato (OIDC/SAML) Fallisce la Unlinkability per Definizione

OIDC e SAML federano l'autenticazione attraverso un Identity Provider che fa da intermediario tra il cittadino e la relying party. Ogni accesso del cittadino a qualsiasi verifier transita attraverso l'IdP. L'IdP sa quale cittadino ha acceduto a quale servizio e quando. Non si tratta di una scelta di configurazione o di una

violazione di policy — è la funzione architettonica dell'IdP. L'eIDAS 2.0 Article 5a(16)(b) prescrive la unlinkability tra le presentazioni della stessa credenziale a verifier diversi; l'IdP federato è, per costruzione, il punto unico in cui ogni presentazione è correlata. La federazione può garantire una vera propagazione cross-controller (Single Logout, OAuth Token Revocation, OIDC Back-Channel Logout) — ma il costo è la violazione dell'invariante di unlinkability per ogni presentazione di credenziale intermediata dall'IdP.

6.3 Il KMS Centralizzato Non Può Raggiungere la Propagazione Cross-Controller

AWS KMS, Azure Key Vault e GCP Cloud KMS forniscono custodia delle chiavi verificabile, backend FIPS 140-2 L3 / 140-3, distruzione programmata delle chiavi (`ScheduleKeyDeletion`, soft-delete + purge, `DESTROY_SCHEDULED`) e cifratura a busta con separazione DEK/KEK. All'interno di una singola tenancy, questa è una primitiva di cancellazione ai sensi del GDPR Article 17 pienamente adeguata — NIST SP 800-88 §2.5 riconosce esplicitamente la Cryptographic Erase come tecnica di sanitizzazione di livello Purge, e EDPB Guidelines 01/2025 tratta la custodia delle chiavi come determinante per stabilire se i dati siano anonimi per un dato destinatario. L'architettura funziona **all'interno del confine della tenancy**.

Non attraversa il confine. Una volta che i dati sono stati legittimamente copiati in un consorzio di ricerca, in un controller downstream autorizzato, o in un sub-responsabile del trattamento in un altro dominio di fiducia, la distruzione del KMS del tenant non ha effetto sulla copia. La propagazione ai sensi del GDPR Article 17(2) diventa un obbligo contrattuale — documentazione, non architettura. La struttura delle catene di permessi di EHDS Article 71 rende questo gap strutturale piuttosto che incidentale: ogni permesso è potenzialmente l'inizio di una catena multi-controller, e la CMK centralizzata non ha mezzi per raggiungere oltre il primo link.

---

7. Dove DKMS Non Produce Risultati — Analisi Critica

La tesi è strutturale, non assoluta. Una formulazione onesta rende l'argomento difendibile; l'eccesso lo distrugge. La tesi DKMS ha quattro confini espliciti.

7.1 I Derivati — EDPB Opinion 28/2024

Una volta che i dati sono stati trasformati in un derivato — aggregati analitici, pesi di modelli di ML, estrazioni statistiche, relazioni normative già depositate — la distruzione della chiave sul testo cifrato di origine non ha effetto sul derivato. EDPB Opinion 28/2024 sugli aspetti di protezione dei dati dei modelli di IA (adottata il 17 dicembre 2024) conferma esplicitamente che gli obblighi di cancellazione non si propagano in modo netto ai pesi del modello una volta avvenuto l'addestramento. DKMS non fa meglio del CMK centralizzato in questo caso. Se un consorzio di ricerca autorizzato ha addestrato un modello su dati rispetto ai quali il cittadino esercita successivamente l'opt-out, i pesi del modello rimangono. Il contributo architettonico è la verificabilità della catena di derivazione, non il disfare retroattivo della derivazione.

7.2 Backup Già Effettuati

Nessuna architettura di revoca delle chiavi attive — DKMS o centralizzata — può richiamare i dati già replicati su supporti di backup immutabili. I backup offline effettuati prima del ritiro si trovano al di fuori del keyspace attivo. La risposta pragmatica è la distruzione documentata e programmata delle chiavi su una finestra di conservazione nota — che le linee guida di ICO, CNIL e BfDI approvano tutte come sufficiente per i dati personali residui nei backup. DKMS si allinea a questa disciplina; non la sostituisce.

7.3 Singola Controparte Disonesta

In una rete di N parti con una parte che ignora la rotazione di chiave pubblicata e continua ad agire su credenziali non aggiornate, DKMS fornisce **rilevamento forense** — le firme non aggiornate sono verificabili rispetto all'evento di rotazione pubblicato — ma non **prevenzione**. Un responsabile del trattamento downstream completamente non cooperante che esfiltri il testo in chiaro e lo archivi al di fuori dell'involucro con chiave non è alla portata architettonica di alcun sistema di gestione delle chiavi. DKMS rafforza la posizione probatoria del regolatore; non risolve la non-cooperazione sottostante. Rispetto a un patrimonio di CMK centralizzato ben governato contrattualmente, DKMS rafforza il rilevamento ma non elimina la necessità di applicazione contrattuale, regolatoria o giudiziaria nei confronti degli attori in malafede.

7.4 Workload Single-Tenant

Per i workload che vivono interamente all'interno di un solo dominio di fiducia — dati aziendali interni sotto un unico controller, SaaS single-tenant con CMK riferita alla tenancy, TLS pubblico web sotto i SLO di revoca 24 ore del CA/Browser Forum — la cancellazione crittografica tramite CMK centralizzato ai sensi di NIST SP 800-88 §2.5 è pienamente adeguata. EDPB Guidelines 01/2025 ed ENISA 2019 §4.2 riconoscono entrambi la distruzione delle chiavi come cancellazione terminale all'interno del confine della tenancy. **Aggiungere DKMS a questi workload impone oneri operativi senza alcun beneficio architettonico.** La risposta onesta è che per gli scenari single-tenant lo stack centralizzato funziona.

7.5 Il Confine Decisivo

DKMS è dominante quando **tutte e quattro** le seguenti condizioni sono soddisfatte:

1. I dati attraversano **almeno due domini di fiducia**.
2. Il consenso deve **sopravvivere post-divulgazione** (ovvero il trattamento continua oltre il confine).
3. Il regolatore tratta **la custodia delle chiavi come determinante** (Schrems II / EDPB Recommendations 01/2020 Use Case 3 / EHDS Article 71(8)).
4. Le parti compongono DKMS **end-to-end** (un verifier che ignora il KEL annulla la catena).

Al di fuori di queste quattro condizioni, il CMK centralizzato è la scelta razionale, e affermarlo rende la tesi DKMS più forte — non più debole — perché localizza l'affermazione esattamente dove le evidenze la supportano. L'affermazione non è che DKMS risolva i banner dei cookie o la cancellazione in SaaS single-

tenant. L’affermazione è che DKMS è la scelta strutturale corretta per *esattamente* i casi che contano per il consenso sanitario intercantonale, interorganizzativo, sotto vigilanza regolatoria, post-divulgazione.

---

8. Prova di Produzione

Vereign opera oggi l’architettura DKMS in produzione, con avvertenze esplicite su cosa è consegnato rispetto a cosa è architettonico.

SEAL è il layer di comunicazione in produzione: consegna a swarm cifrata per la comunicazione in uscita, con chiavi per messaggio e agenzia di decifratura controllata dal destinatario. SEAL ha trasportato **800.000+ messaggi verificati ogni mese** per utenti istituzionali — l’ancora di produzione a scala canonica per l’architettura. Ogni messaggio esercita lo stesso substrato di key-event che sta alla base della tesi sul consenso: keying controllato dal soggetto, marca temporale verificabile da terze parti e unlinkability per contesto tra i destinatari.

Stargate — il layer di autorizzazione ancorato all’AID dove i permessi di dati si concatenano al KEL del cittadino — entra in early production da giugno 2026 con HIN come primo deployment operativo. Stargate è la superficie del consenso per la tesi: le autorizzazioni concesse ai titolari dei dati sono ancorate all’AID del cittadino; la rotazione di chiave da parte del cittadino si propaga attraverso il KEL; i verifier downstream ricontrollano. Il deployment HIN è un soft launch in termini di scope; **la narrativa del roll-out di massa è riservata al post-estate 2026**, dopo che il gruppo early-production avrà accumulato evidenza operativa in condizioni regolatorie live.

I bridge HIN consentono al ritiro di interoperare con controparti che usano X.509 tramite il bridge S/MIME ancorato a KERI documentato nella knowledge base sulla sicurezza email. Questo è il riconoscimento pragmatico che DKMS si comporrà con — e non sostituirà nell’immediato — il patrimonio sanitario X.509 esistente.

FHIR-over-Stargate è architetturale oggi — il deployment in produzione dipende dall’onboarding ospedaliero; la data più realistica è settembre 2026. L’architettura è genuinamente solida: le risorse FHIR che transitano attraverso Stargate ereditano il modello di autorizzazione ancorato all’AID, quindi lo stato del consenso a livello di risorsa vive dove il cittadino lo controlla. Ma l’ingegneria dell’adozione ospedaliera — integrazione con i sistemi clinici, approvazione regolatoria, governance operativa — è un’impresa che si misura in trimestri. Non affermiamo FHIR-over-Stargate come consegnato. Lo affermiamo come il passo successivo deliberato, con una data più realistica nota, e ci aspettiamo che il deployment operativo segua la disponibilità architettonica con un intervallo misurabile. Conflare i due è la modalità di fallimento che questo documento è scritto per evitare.

Il track record di produzione è importante perché è ciò che distingue questa tesi da una presentazione. Le organizzazioni di ingegneria incontrano routinariamente l’argomento centralizzazione-vs-decentralizzazione; quello che incontrano raramente è la decentralizzazione che opera a scala, sotto regolazione istituzionale live, in un settore regolamentato. Il substrato di messaggistica verificata ha trasportato traffico istituzionale reale

abbastanza a lungo da esporre i dettagli operativi di DKMS — disciplina di rotazione delle chiavi, discovery cross-organizzazione, conservazione dei log di audit, agenzia del destinatario — e quei dettagli sono stati raffinati in produzione piuttosto che in teoria. Quando Stargate entrerà in early production da giugno 2026, funzionerà sullo stesso substrato. L'argomento architettonico non è quindi una previsione; è un'estrapolazione dalle operazioni osservate a scala.

---

9. Cinque Incidenti che Provano lo Schema Strutturale

Cinque incidenti — tre del 2026, due casi fondazionali più datati — illustrano perché le architetture centralizzate falliscono sotto pressione regolatoria e come la modalità di fallimento sia architettonica piuttosto che operativa.

9.1 Kaiser Foundation Health Plan — Accordo da USD 47,5M (2026)

Kaiser Foundation Health Plan ha raggiunto un accordo in class-action da USD 47,5 milioni per il tracciamento tramite pixel nel portale pazienti, con approvazione finale il 30 aprile 2026 (Class Action Center, Kaiser Foundation Health Plan settlement docket). I querelanti hanno sostenuto che i pixel di tracciamento di Meta e Google incorporati nel portale pazienti autenticato di Kaiser trasmettevano informazioni sanitarie protette a piattaforme pubblicitarie di terze parti — incluse diagnosi, tipi di appuntamento e ricerche su farmaci — insieme a identificatori sufficienti per ricondurre i dati a pazienti specifici. Il fallimento architettonico è preciso: il consenso del paziente esisteva al layer di registrazione del portale, ma il flusso dei dati era determinato dagli SDK incorporati, non dalla preferenza dichiarata dal paziente. Il ritiro del consenso non aveva alcun effetto sugli eventi pixel già trasmessi, e il paziente non disponeva di alcun mezzo architettonico per rilevare o revocare i flussi verso terze parti.

9.2 Sutter Health — Accordo da USD 21,5M (2026)

Sutter Health ha raggiunto un accordo da USD 21,5 milioni nello stesso schema di procedimenti, con approvazione finale il 27 febbraio 2026. Accordi paralleli sono stati stipulati o sono pendenti contro BJC HealthCare, Northwell Health, Catholic Health, Aspirus e SSM Health su fatti sostanzialmente identici. Il dossier degli accordi 2025–2026 nel suo complesso è l'indicatore anticipatore: ogni grande sistema sanitario statunitense che ha incorporato pixel di tracciamento di terze parti nelle superfici rivolte ai pazienti sta ora pagando per l'assenza architettonica di confini crittografici per paziente sul flusso dei dati. Il consenso era una casella da spuntare; il flusso era deciso altrove.

9.3 NHS National Data Opt-Out (NDOO) — Non-Retroattività, 2018–2021

NHS England ha consolidato gli opt-out di tipo 1 e 2 dell'era precedente nel National Data Opt-Out (NDOO) a partire dal 2018, con efficacia normativa. La documentazione del programma e i commenti dell'ICO hanno successivamente confermato che l'opt-out era dimostrabilmente **non retroattivo**: i dati già estratti dai sistemi dei medici di medicina generale prima che il cittadino registrasse l'opt-out rimanevano nei dataset di ricerca e potevano continuare ad essere trattati. NHS Digital non disponeva di infrastruttura tecnica per richiamare i dati già estratti. Il programma successore GPDPR (General Practice Data for Planning and Research) era previsto per l'avvio il 1° luglio 2021 ed è stato rinviato a tempo indeterminato nel giugno 2021 precisamente perché non esisteva alcun mezzo tecnico per cancellare i dati dei medici di medicina generale già estratti quando veniva registrato a posteriori un opt-out di tipo 1. Al 2026 l'estrazione non è ancora iniziata. La lezione architettonica: quando l'operatore possiede il percorso dei dati, il «veto del paziente» non dispone di una primitiva di applicazione — e il meccanismo politico collassa sotto il proprio peso forensico.

9.4 SingHealth — 1,5 Milioni di Cartelle Compromesse (2018)

Il rapporto pubblico del Committee of Inquiry di Singapore sull'attacco informatico a Singapore Health Services (10 gennaio 2019) ha accertato che 1,5 milioni di cartelle di pazienti SingHealth erano state compromesse, inclusa la cartella clinica personale del Primo Ministro di Singapore. La conclusione tecnica è quella architettonica: nel sistema di cartelle cliniche elettroniche di SingHealth non esisteva **alcuna compartimentazione**. Una volta che l'attaccante aveva raggiunto l'applicazione Allscripts Sunrise tramite un account di servizio privilegiato, tutte le cartelle dei pazienti erano accessibili. Il consenso del paziente era un artefatto di policy al layer di accesso; il layer dei dati non aveva **alcun confine crittografico per paziente**. La superficie di violazione era precisamente l'assenza di quel confine.

9.5 Compromissione della Certification Authority DigiNotar (2011)

L'indagine di Fox-IT pubblicata come rapporto «Black Tulip» (13 agosto 2012) ha accertato che tutti e otto i server CA di DigiNotar erano stati compromessi. Erano stati emessi 531+ certificati fraudolenti, incluso un certificato wildcard `*.google.com` usato per condurre un attacco man-in-the-middle contro circa 300.000 utenti Gmail iraniani. La remediation — la revoca della fiducia in DigiNotar — è stata effettuata unilateralmente da Mozilla, Microsoft e Google e propagata agli utenti finali tramite aggiornamenti del root store. La catena Staat der Nederlanden – G2 del governo olandese è stata trascurata nella prima rimozione e ha richiesto un intervento successivo. Gli utenti finali non avevano **alcuna agency** nella decisione di fiducia in nessuna fase: né nell'emissione, né nel rilevamento, né nella remediation. Hanno appreso della compromissione dai propri servizi che smettevano di funzionare.

Ogni incidente centralizzato condivide un'unica caratteristica: l'utente non aveva alcuna agency architettonica. I pazienti di Kaiser e Sutter non controllavano il flusso dei pixel. I pazienti del NHS non potevano richiamare i dati estratti. I pazienti di SingHealth non avevano confini crittografici per cartella. Gli

utenti finali di DigiNotar non potevano votare sulle decisioni di fiducia. Lo schema è strutturale e persiste attraverso cinque decenni di evidenze di incidenti, indipendentemente da regolatore, settore o giurisdizione.

---

10. Conclusione e Come Contattarci

L'opt-out è passato da aspirazione politica a diritto legale applicabile ai sensi di EHDS Article 71, GDPR 7(3) e 17(2), eIDAS 2.0 5a(14)/(16)(b), FADP e HFG svizzeri, e PDSG tedesco. Ne derivano direttamente cinque invarianti ingegneristici: identificatori riferiti alla persona, opt-out verificabile con marca temporale, reversibilità senza re-identificazione, propagazione cross-controller e unlinkability. X.509 PKI non ne soddisfa nessuno al livello del cittadino; l'IAM federato soddisfa la propagazione solo violando la unlinkability; il KMS centralizzato soddisfa il caso single-tenant ma non può raggiungere oltre i domini di fiducia. **DKMS è il primo fondamento strutturalmente solido per onorare il ritiro del consenso end-to-end in condizioni interorganizzative, post-divulgazione, sotto vigilanza regolatoria** — con confini espliciti riguardo a derivati, backup e singole controparti disoneste. Il dossier degli accordi 2025–2026 (Kaiser, Sutter, BJC, Northwell, Catholic Health, Aspirus, SSM Health) è l'evidenza live che ogni architettura centralizzata sotto questo tipo di pressione regolatoria condivide un'unica caratteristica: l'utente non aveva alcuna agency architettonica.

Se Lei è responsabile dell'architettura del consenso in un patrimonio di informatica sanitaria che affronta la trasposizione di EHDS, l'implementazione svizzera di EGDG / BDG, o le operazioni PDSG tedesche, Vereign offre una revisione dell'architettura del consenso di 30 minuti. Mapperemo la Sua superficie di consenso attuale rispetto ai cinque invarianti, identificheremo le trappole dell'Article 71(8) nella Sua roadmap e individueremo lo scope preciso in cui DKMS è — e non è — la risposta architettonica corretta. **Contatti: contact@vereign.com.**

Vereign AG — Dammstrasse 16, 6300 Zug, Svizzera — UID CHE-240.299.384 — LEI 50670056G9BYC736YR76