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

Vereign AG

2026-04-29

Arquitectura del Consentimiento: DKMS como Fundamento Estructuralmente Sólido para EHDS Article 71

Vereign AG — Abril 2026

1. Resumen Ejecutivo

La legislación europea sobre datos sanitarios ha cruzado un umbral decisivo. El opt-out ya no es una aspiración normativa: bajo EHDS Article 71 es un **derecho legal** de la persona física, exigible en cada Estado miembro que procese datos sanitarios identificables con fines de uso secundario. Superpuesto a los Artículos 7(3) y 17(2) del GDPR, el Art. 5a del eIDAS 2.0, la nDSG suiza y la HFG, y el PDSG alemán, cinco regímenes independientes convergen en un mismo conjunto de invariantes de ingeniería: **identificadores de ámbito personal, opt-out verificable con marca de tiempo, reversibilidad sin reidentificación, propagación entre responsables del tratamiento e imposibilidad de vinculación**. La PKI centralizada y la identidad federada satisfacen, como mucho, uno o dos de estos requisitos; X.509 no satisface ninguno en la capa ciudadana. **Decentralized Key Management (DKMS) es el primer fundamento estructuralmente sólido para honrar la retirada del consentimiento de extremo a extremo — *en condiciones interorganizativas, posdivulgación, bajo supervisión regulatoria*.** La tesis tiene límites explícitos: los derivados que abandonaron el sistema antes

de la retirada, las copias de seguridad inmutables y los actores individuales deshonestos quedan fuera del alcance arquitectónico. El expediente de acuerdos extrajudiciales de 2025–2026 (Kaiser USD 47.500.000, Sutter USD 21.500.000, procedimientos paralelos contra BJC, Northwell, Catholic Health, Aspirus y SSM Health) es el indicador adelantado: en cada incidente centralizado se repite la misma característica — el usuario carecía de agencia arquitectónica.

---

2. Por Qué Ahora — Convergencia Regulatoria en 24 Meses

Durante dos décadas, la gestión del consentimiento en TI sanitaria trató el opt-out como un problema de experiencia de usuario. A partir de 2024, cinco regímenes jurídicos independientes convergieron en el mismo patrón de ingeniería, dejando a los proveedores meses — no años — para demostrar el cumplimiento estructural.

EHDS Article 71 — Reglamento (UE) 2025/327. Adoptado el 11 de febrero de 2025; publicado en el Diario Oficial de la Unión Europea (DO L 2025/327) el 5 de marzo de 2025; en vigor desde el 26 de marzo de 2025. El artículo 71(1) otorga a toda persona física el derecho a ejercer el opt-out respecto al procesamiento secundario de datos sanitarios electrónicos identificables. El artículo 71(2) prohíbe la emisión de nuevos permisos de datos sobre datos identificables una vez ejercido el opt-out, mientras mantiene los permisos emitidos con anterioridad. **Article 71(8)** prohíbe a los titulares de datos obtener datos de identificación adicionales únicamente para dar cumplimiento al opt-out — el giro de ingeniería que descarta el patrón obvio de «registro central de IDs excluidos por opt-out».

GDPR Artículos 7(3) y 17(2) — Reglamento (UE) 2016/679. El artículo 7(3) exige que la retirada del consentimiento sea «tan sencilla como otorgarlo». El artículo 17(2) impone un deber de propagación: el responsable del tratamiento que atienda una solicitud de supresión debe adoptar «medidas razonables, incluidas técnicas», para informar a los responsables posteriores. El artículo 9(2)(a) eleva el umbral para datos de salud a consentimiento *explícito*; los artículos 17(3)(c)/(d) contemplan excepciones de salud pública e investigación que hacen que la supresión literal sea estructuralmente inalcanzable para la mayoría de los registros clínicos — razón por la cual el EHDS configuró el derecho como **supresión prospectiva** en lugar de eliminación retroactiva.

eIDAS 2.0 — Reglamento (UE) 2024/1183. Modifica el Reglamento (UE) 910/2014 para establecer el Monedero de Identidad Digital Europeo (EUDIW). El artículo 5a(14) exige el «control pleno del usuario» sobre las operaciones del monedero. El artículo 5a(16)(a) prohíbe el rastreo entre contextos del uso del monedero; el artículo 5a(16)(b) exige la **imposibilidad de vinculación** entre presentaciones de credenciales a distintos verificadores. Juntos, los artículos 5a(16)(a)–(b) son la forma operativa de EHDS Article 71(8): toda arquitectura en la que el operador pueda correlacionar a un ciudadano entre distintos verificadores falla por definición el requisito de imposibilidad de vinculación.

nDSG y HFG suizas. La Ley Federal de Protección de Datos revisada (nDSG, SR 235.1, en vigor desde el 1 de septiembre de 2023) exige consentimiento explícito para datos sensibles en el artículo 6(6) y un derecho absoluto de retirada en el artículo 6(7), con derechos de supresión en el artículo 32 sujetos a obligaciones de conservación. La Ley de Investigación con Seres Humanos (HFG / HRA, SR 810.30) en los artículos 7(2) y 17 otorga la revocación del consentimiento y un derecho de disenso para el uso ulterior de datos de salud. La inminente EGDG (mensaje del Consejo Federal, 5 de noviembre de 2025) invierte el modelo del EPD de opt-in a opt-out con entrada en vigor prevista para ~2028–2030; el BDG (base jurídica de uso secundario de DigiSanté) está en fase de redacción. La propagación intercantonal hace que el caso suizo sea estructuralmente más complejo que el europeo.

PDSG alemán. La Patientendaten-Schutz-Gesetz operacionaliza la arquitectura de opt-out del ePA alemán (historia clínica electrónica), en funcionamiento desde enero de 2025 para aproximadamente 73 millones de beneficiarios del seguro obligatorio. El PDSG codifica la mecánica de supresión prospectiva — los ciudadanos que rechacen el ePA no deben ser procesados en virtud del fundamento jurídico de opt-in — para una población superior a la de la mayoría de los Estados miembros de la UE en conjunto. La presión de implantación nacional sobre la arquitectura del consentimiento no es teórica; es operativa en el mayor sistema sanitario de pagador único de Europa.

El borrador de directriz de la Acción Conjunta TEHDAS2 (septiembre de 2025) confirma que el mecanismo técnico de propagación del opt-out **no** está especificado por el propio Derecho de la UE y se defiere a la implementación de cada Estado miembro. Este es el flanco débil arquitectónico: cada Estado podría adoptar su propio enfoque, pero solo un sistema de claves controladas por el sujeto satisface el Article 71(8) sin introducir subrepticiamente un registro prohibido de reidentificación. Los proveedores que implementen una arquitectura conforme en un Estado miembro venderán en los veintisiete; los que resuelvan únicamente la UX local se enfrentarán a una conversación arquitectónica diferente en cada transposición.

Cada uno de estos cinco regímenes, por separado, es superable. **Los cinco juntos, en una ventana de 24 meses, son la función de forzamiento arquitectónico.** Los proveedores de TI sanitaria se enfrentan ahora a un mercado en el que la «gestión del consentimiento» debe componerse de extremo a extremo, entre fronteras, entre responsables del tratamiento, a lo largo del tiempo — y el patrón de registro centralizado que ha sostenido al sector durante dos décadas está descartado por el Derecho primario del mayor bloque económico del planeta.

---

3. Los Cinco Invariantes de Ingeniería

Los cinco regímenes convergen en un conjunto pequeño y preciso de requisitos de ingeniería. No son aspiracionales — son predicados comprobables con los que puede evaluarse cualquier arquitectura de consentimiento.

3.1 Identificadores de Ámbito Personal

El interesado debe controlar el identificador bajo el que se referencian sus permisos, autorizaciones y estado de consentimiento. Este es el *prerrequisito* de todos los demás invariantes: si el operador posee el identificador, el

operador posee el opt-out. EHDS Article 71(8) descarta explícitamente los registros de reidentificación del lado del operador; el mandato de «control pleno del usuario» del artículo 5a(14) del eIDAS 2.0 nombra la misma propiedad en la capa del monedero. Sin un identificador de ámbito del sujeto, la propagación, la reversibilidad y la imposibilidad de vinculación colapsan en política del operador.

3.2 Opt-Out Verificable con Marca de Tiempo

Para cada permiso de datos, el sistema debe conocer el momento preciso de la emisión y el momento preciso de la retirada — y un tercero (regulador, tribunal, responsable del tratamiento posterior) debe poder verificar ambos sin confiar en los registros del operador. EHDS Article 71(2) traza una frontera temporal nítida: los permisos anteriores al opt-out permanecen válidos; los posteriores son ilegales. Este requisito no puede hacerse cumplir sin una línea temporal a prueba de manipulaciones y verificable por terceros del estado de consentimiento del sujeto.

3.3 Reversibilidad sin Reidentificación

El Recital 54 del Reglamento EHDS confirma que el opt-out es reversible (los ciudadanos pueden volver a incluirse) y libre de formalidades (sin duración mínima). El artículo 71(8) prohíbe al titular de los datos obtener datos de identificación adicionales exclusivamente para dar cumplimiento al opt-out. Ambas cláusulas leídas conjuntamente crean una restricción estricta: el sistema debe admitir el cambio del estado de consentimiento en ambos sentidos, a iniciativa del ciudadano, **sin** que el titular de los datos construya un registro paralelo de reidentificación para rastrear quién ha cambiado en qué sentido. Toda arquitectura que exija «mantener simplemente una lista de IDs que han ejercido el opt-out» viola el artículo 71(8) directamente.

3.4 Propagación entre Responsables del Tratamiento

El artículo 17(2) del GDPR exige al responsable del tratamiento que atiende la supresión adoptar «medidas razonables, incluidas técnicas», para informar a los responsables posteriores que poseen copias, replicaciones o vínculos. EHDS Article 71 superpuesto a cadenas de permisos con múltiples responsables intensifica esto: la señal de opt-out debe alcanzar a cada Organismo de Acceso a Datos Sanitarios, a cada consorcio de investigación, a cada subencargado del tratamiento que recibió datos bajo un permiso anterior. La propagación no puede ser un registro en papel — debe ser un artefacto verificable que las partes posteriores puedan recomprobar.

3.5 Imposibilidad de Vinculación

El artículo 5a(16)(b) del eIDAS 2.0 exige la imposibilidad de vinculación entre presentaciones de la misma credencial a distintos verificadores. La consecuencia operativa: toda arquitectura en la que cualquier parte individual (incluso un intermediario autorizado) observe todas las transacciones entre verificadores falla el requisito por construcción. Esta propiedad es la que excluye a los proveedores de identidad federados de la capa ciudadana de los sistemas conformes con EHDS: el IdP, por diseño, ve cada inicio de sesión y cada presentación de credencial. La federación puede satisfacer la propagación, pero solo violando la imposibilidad de vinculación.

Estos cinco invariantes forman un sistema interconectado. **X.509 PKI no satisface ninguno de ellos en la capa ciudadana. Los IdP federados satisfacen la propagación únicamente violando la imposibilidad de vinculación. DKMS satisface los cinco.** Esta es la afirmación de solidez estructural, y el resto del documento la examina.

---

4. La Trampa del Article 71(8)

El patrón de implementación más sencillo para el opt-out — el que un proveedor de TI sanitaria esbozará en la primera hora de conversación arquitectónica — es **un registro central de IDs de ciudadanos que han ejercido el opt-out**. Cada titular de datos consulta el registro antes de procesar; si el ID del ciudadano figura en la lista, el procesamiento se detiene. Sencillo. Familiar. Auditable.

El Article 71(8) descarta por completo este patrón.

La cláusula prohíbe a los titulares de datos obtener datos de identificación adicionales exclusivamente para dar cumplimiento al opt-out. **La «lista de IDs que han ejercido el opt-out» es, por construcción, exactamente ese tipo de registro.** Existe con el único fin de reidentificar ciudadanos para el caso negativo — para determinar que *este ciudadano ha ejercido el opt-out y por tanto no puede ser procesado*. La propia lista es la infracción regulatoria que pretende prevenir.

La trampa es recursiva. Cualquier intento de anonimizar el registro (aplicar hash a los IDs, seudonimizarlos, mantenerlos en un dominio de confianza separado) reintroduce el problema original: el titular de los datos sigue necesitando *algún* identificador para cotejar con la lista, y ese identificador debe poder derivarse de los datos que el titular ya posee. El hash no es anónimo para el titular que dispone de la entrada; el seudónimo no es anónimo para el titular que dispone del vínculo. El Recital 54 refuerza esto al exigir que el opt-out sea reversible y libre de formalidades — lo que significa que el registro debe admitir cambios, lo que a su vez exige que el registro rastree *qué* ciudadano ha cambiado *cuándo*, que es exactamente el registro de reidentificación que el artículo 71(8) prohíbe.

La implicación para los proveedores de TI sanitaria es contundente. **Cualquier «módulo de gestión del consentimiento» cuya arquitectura descanse en una lista autorizada central de sujetos que han ejercido el opt-out está descartado por el Derecho primario de la UE.** No se trata de una elección de diseño de UX; es la diferencia entre una arquitectura que puede cumplir con el EHDS y una que no puede. Los productos genéricos de gestión del consentimiento construidos sobre el patrón de registro — ya sean SaaS, on-premises o híbridos — se enfrentarán a esta restricción en cada transposición de cada Estado miembro. La respuesta estructural debe situar el identificador bajo el control del ciudadano, de modo que el titular de los datos nunca tenga que mantener un registro de reidentificación.

---

5. La Tesis de DKMS

> **Decentralized Key Management es el primer fundamento estructuralmente sólido para honrar la retirada del consentimiento de extremo a extremo — *en condiciones interorganizativas, posdivulgación, bajo supervisión regulatoria*.**

DKMS — construido sobre KERI, una especificación abierta de la Trust over IP Foundation — sitúa la raíz de confianza en el ciudadano en lugar de en una autoridad centralizada. El ciudadano (o el agente de su monedero) posee un Autonomic IDentifier (AID) que es autocertificante: se deriva de una clave pública bajo el control del ciudadano, y su autenticidad no depende de ningún registrador. Todas las autorizaciones concedidas a titulares de datos, encargados del tratamiento y responsables posteriores se encadenan hasta ese AID a través de un Key Event Log (KEL) — un registro de solo adición, verificable por terceros, del estado de claves del ciudadano, incluidas las rotaciones de clave.

La retirada en este modelo no es una solicitud presentada a un operador. Es una **rotación de clave que el ciudadano realiza de forma unilateral**. La rotación se publica en el KEL; a partir de ese momento, cualquier parte posterior que posea credenciales ancladas al estado de clave anterior a la rotación debe reautenticarse con el estado actual del ciudadano para continuar el procesamiento. Los permisos existentes emitidos antes de la rotación continúan operando donde la base jurídica subyacente lo permita (en correspondencia con EHDS Article 71(2)); los nuevos permisos no pueden emitirse bajo el estado de clave antiguo, porque ese estado ya no es el estado de control del ciudadano. El ciudadano ha retirado arquitectónicamente — no solo procedimentalmente — la autorización futura, y cualquier parte posterior que ignore la rotación publicada produce firmas auditables como obsoletas.

Correspondencia con los cinco invariantes:

Invariante	Mecanismo DKMS
Identificadores de ámbito personal	El AID es el identificador autocertificante del sujeto; no se requiere índice del lado del operador
Opt-out verificable con marca de tiempo	El KEL contiene eventos de clave con marca de tiempo a prueba de manipulaciones
Reversibilidad sin reidentificación	Opt-back-in = rotación de clave que restablece la autorización; sin registro paralelo
Propagación entre responsables del tratamiento	El KEL es publicable; los verificadores deben recomprobar entre dominios de confianza
Imposibilidad de vinculación	AIDs por contexto y credenciales de divulgación selectiva evitan la correlación entre verificadores

Comparación con las opciones existentes:

X.509 PKI vincula la identidad a un certificado emitido por una CA. El ciudadano no posee la raíz de confianza; la CA sí. La revocación está dirigida por el operador (CRL/OCSP) y falla silenciosamente por defecto. La imposibilidad de vinculación entre contextos está estructuralmente ausente — toda presentación de certificado es vinculable a través del número de serie, el DN del emisor y el DN del sujeto. X.509 no satisface *ninguno* de los cinco invariantes en la capa ciudadana.

IAM Federado (OIDC, SAML). El Proveedor de Identidad es, por diseño, el rastreador entre contextos que el artículo 5a(16)(b) del eIDAS 2.0 prohíbe. La federación puede satisfacer la propagación entre responsables del tratamiento (un cierre de sesión único vacía las sesiones posteriores), pero solo violando la imposibilidad de vinculación — cada inicio de sesión pasa por el IdP, que ve cada parte que confía a la que accede el ciudadano. La arquitectura puede satisfacer como máximo tres invariantes y solo a costa del quinto.

KMS Centralizado (AWS KMS, Azure Key Vault, GCP Cloud KMS). Excelente para cargas de trabajo de arrendatario único. La supresión criptográfica de NIST SP 800-88 §2.5 mediante claves gestionadas por el cliente es una primitiva de supresión terminal reconocida por los reguladores (EDPB Guidelines 01/2025; ENISA 2019 §4.2). Pero una vez que los datos abandonan el límite del arrendatario — hacia un consorcio de investigación, un responsable del tratamiento posterior, un destinatario de uso secundario permitido — la destrucción del CMK del operador no afecta en modo alguno a la copia. La propagación entre responsables del tratamiento no está resuelta. Schrems II / EDPB Recommendations 01/2020 Use Case 3 agrava esto: el importador de datos no debe poseer las claves, por definición.

DKMS no reemplaza estas arquitecturas — ocupa el nicho arquitectónico preciso que ellas no pueden cubrir. KMS centralizado para la supresión en el ámbito del arrendatario, X.509 para la revocación de clase TLS, IAM federado para el consentimiento en el ámbito de sesión — y DKMS para la capa interorganizativa y posdivulgación donde EHDS Article 71 opera realmente.

---

6. Dónde Fallan las Arquitecturas Centralizadas

Los cinco invariantes son comprobables. Cada arquitectura de consentimiento centralizada importante falla de una manera estructuralmente específica.

6.1 X.509 PKI Falla los Cinco Invariantes en la Capa Ciudadana

X.509 vincula la identidad a una Autoridad de Certificación. La CA genera o cofirma el certificado del ciudadano, es propietaria de la decisión de emisión y controla la revocación. Los identificadores de ámbito personal fallan en la raíz — la firma de la CA es la fuente de confianza, no la del ciudadano. El opt-out con marca de tiempo está dirigido por el operador (el ciudadano presenta una solicitud de revocación; la CA decide si la atiende y cuándo publicarla), y la revocación se propaga solo tan rápido como los intervalos de actualización de CRL o la disponibilidad del respondedor OCSP — ambos fallan silenciosamente en los navegadores por defecto. La reversibilidad sin reidentificación falla porque la reemisión exige que la CA vuelva a validar la identidad del sujeto, lo que en contextos sanitarios requiere que la CA adquiera de nuevo los datos de identificación que EHDS Article 71(8) prohíbe al titular de datos poseer. La propagación entre

responsables del tratamiento depende de que cada parte que confía verifique correctamente CRL/OCSP, algo que los incidentes de DigiNotar y Comodo demostraron que es operativamente frágil. La imposibilidad de vinculación es estructuralmente imposible: todo certificado X.509 lleva un número de serie y un DN del emisor que vinculan cada presentación al mismo ciudadano.

6.2 IAM Federado (OIDC/SAML) Falla la Imposibilidad de Vinculación por Definición

OIDC y SAML federan la autenticación a través de un Proveedor de Identidad que intermedia la relación entre el ciudadano y la parte que confía. Cada inicio de sesión que el ciudadano realiza ante cualquier verificador pasa por el IdP. El IdP sabe qué ciudadano accedió a qué servicio y cuándo. No se trata de una elección de configuración ni de una infracción de política — es la función arquitectónica del IdP. El artículo 5a(16)(b) del eIDAS 2.0 exige la imposibilidad de vinculación entre presentaciones de la misma credencial a distintos verificadores; el IdP federado es, por construcción, el punto único donde se correlaciona cada presentación. La federación puede proporcionar una propagación real entre responsables del tratamiento (Single Logout, OAuth Token Revocation, OIDC Back-Channel Logout) — pero el precio es la violación del invariante de imposibilidad de vinculación para cada presentación de credencial que el IdP intermedia.

6.3 KMS Centralizado No Puede Alcanzar la Propagación entre Responsables del Tratamiento

AWS KMS, Azure Key Vault y GCP Cloud KMS ofrecen custodia de claves auditable, backends FIPS 140-2 L3 / 140-3, destrucción programada de claves (`ScheduleKeyDeletion`, soft-delete + purga, `DESTROY_SCHEDULED`) y cifrado en sobre con separación DEK/KEK. Dentro de un arrendatario único, esta es una primitiva de supresión GDPR Article 17 plenamente adecuada — NIST SP 800-88 §2.5 reconoce explícitamente el borrado criptográfico como técnica de saneamiento de nivel Purga, y las EDPB Guidelines 01/2025 consideran la custodia de claves como determinante del resultado en cuanto a si los datos son anónimos para un destinatario concreto. La arquitectura funciona **dentro del límite del arrendatario**.

No cruza ese límite. Una vez que los datos han sido copiados lícitamente a un consorcio de investigación, a un responsable del tratamiento posterior permitido o a un subencargado del tratamiento en otro dominio de confianza, la destrucción del KMS del arrendatario no afecta en modo alguno a la copia. La propagación del artículo 17(2) del GDPR se convierte en una obligación contractual — papel, no arquitectura. La estructura de cadena de permisos de EHDS Article 71 hace que esta brecha sea estructural y no incidental: cada permiso es potencialmente el inicio de una cadena con múltiples responsables del tratamiento, y el CMK centralizado carece de medios para alcanzar más allá del primer eslabón.

---

7. Dónde DKMS NO Cumple — Análisis Riguroso

La tesis es estructural, no absoluta. Una formulación honesta hace el argumento defendible; el exceso lo destruye. La afirmación sobre DKMS tiene cuatro límites explícitos.

7.1 Derivados — EDPB Opinion 28/2024

Una vez que los datos han sido transformados en un derivado — agregados analíticos, pesos de modelos de aprendizaje automático, extractos estadísticos, informes regulatorios ya presentados — la destrucción de claves sobre el texto cifrado de origen no afecta al derivado. El EDPB Opinion 28/2024 sobre aspectos de protección de datos en modelos de IA (adoptado el 17 de diciembre de 2024) confirma explícitamente que las obligaciones de supresión no se propagan de manera limpia a los pesos del modelo una vez completado el entrenamiento. DKMS no mejora en este aspecto al CMK centralizado. Si un consorcio de investigación permitido ha entrenado un modelo con datos de un ciudadano que posteriormente ejerce el opt-out, los pesos del modelo permanecen. La contribución arquitectónica es la auditabilidad de la cadena de derivación, no la anulación retroactiva de la derivación.

7.2 Copias de Seguridad ya Realizadas

Ninguna arquitectura de revocación en clave activa — DKMS ni centralizada — puede recuperar datos ya replicados en soportes de copia de seguridad inmutables. Las copias de seguridad fuera de línea realizadas antes de la retirada quedan fuera del espacio de claves activo. La respuesta pragmática es la destrucción de claves documentada y programada en una ventana de retención conocida — práctica que la ICO, la CNIL y el BfDI avalan como suficiente para datos personales residuales en copias de seguridad. DKMS se alinea con esta disciplina; no la sustituye.

7.3 Contraparte Individual Deshonesta

En una red de N partes con una parte que ignora la rotación de clave publicada y continúa actuando sobre credenciales obsoletas, DKMS proporciona **detección forense** — las firmas obsoletas son auditables más allá del evento de rotación publicado — pero no **prevención**. Un subencargado del tratamiento totalmente no cooperativo que exfiltra texto sin cifrar y lo almacena fuera del sobre cifrado queda fuera del alcance arquitectónico de cualquier sistema de gestión de claves. DKMS fortalece la posición probatoria del regulador; no soluciona la falta de cooperación subyacente. Comparado con un conjunto de CMK centralizado bien gobernado contractualmente, DKMS refuerza la detección pero no elimina la necesidad de contrato, regulador o tribunal contra los actores malintencionados.

7.4 Cargas de Trabajo de Arrendatario Único

Para cargas de trabajo que residen íntegramente en un único dominio de confianza — datos corporativos internos bajo un único responsable del tratamiento, SaaS de arrendatario único con CMK de ámbito del arrendatario, TLS web público bajo los SLO de revocación de 24 horas del CA/Browser Forum — la supresión criptográfica mediante CMK centralizado conforme a NIST SP 800-88 §2.5 es plenamente adecuada. Las EDPB Guidelines 01/2025 y ENISA 2019 §4.2 reconocen la destrucción de claves como supresión terminal dentro del límite del arrendatario. **Añadir DKMS a estas cargas de trabajo impone carga operativa sin ningún beneficio arquitectónico.** La respuesta honesta es que para los escenarios de arrendatario único, la arquitectura centralizada funciona.

7.5 El Límite Decisivo

DKMS es la opción dominante cuando se cumplen **las cuatro** condiciones siguientes:

1. Los datos cruzan **al menos dos dominios de confianza**.
2. El consentimiento debe **sobrevivir posdivulgación** (es decir, el procesamiento continúa más allá del límite).
3. El regulador considera la **custodia de claves como determinante del resultado** (Schrems II / EDPB Recommendations 01/2020 Use Case 3 / EHDS Article 71(8)).
4. Las partes componen DKMS **de extremo a extremo** (un verificador que ignora el KEL anula la cadena).

Fuera de esas cuatro condiciones, el CMK centralizado es la elección racional, y afirmarlo hace la tesis de DKMS más sólida — no más débil — porque localiza la afirmación precisamente donde la evidencia la sustenta. La afirmación no es que DKMS resuelva los banners de cookies ni la supresión en SaaS de arrendatario único. La afirmación es que DKMS es la elección estructural correcta para *exactamente* los casos que importan para el consentimiento sanitario intercantonal, interorganizativo, bajo supervisión regulatoria y posdivulgación.

---

8. Evidencia en Producción

Vereign opera la arquitectura DKMS en producción en la actualidad, con advertencias explícitas sobre qué está en producción y qué es arquitectónico.

SEAL es la capa de comunicación en producción: entrega en enjambre cifrada para comunicaciones salientes, con claves por mensaje y agencia de descifrado controlada por el destinatario. SEAL transporta **más de 800.000 mensajes verificados al mes** para usuarios institucionales — el ancla canónica de escala en producción para la arquitectura. Cada mensaje ejercita el mismo sustrato de eventos de clave que subyace a la tesis del consentimiento: claves controladas por el sujeto, marcas de tiempo verificables por terceros e imposibilidad de vinculación por contexto entre destinatarios.

Stargate — la capa de autorización anclada en AID donde los permisos de datos se encadenan al KEL del ciudadano — entra en producción anticipada a partir de junio de 2026 con HIN como primer despliegue operativo. Stargate es la superficie de consentimiento de la tesis: las autorizaciones concedidas a los titulares de datos están ancladas al AID del ciudadano; la rotación de clave por parte del ciudadano se propaga a través del KEL; los verificadores posteriores recomprueban. El despliegue en HIN es un lanzamiento de alcance limitado; **el relato de despliegue masivo está reservado para después del verano de 2026**, una vez que el grupo de producción anticipada haya acumulado evidencia operativa bajo condiciones regulatorias reales.

Los puentes HIN permiten que la retirada interopere con contrapartes que usan X.509 a través del puente S/MIME anclado en KERI documentado en la base de conocimiento de seguridad del correo electrónico. Este es el reconocimiento pragmático de que DKMS compondrá con — no reemplazará de la noche a la mañana — el ecosistema X.509 sanitario existente.

FHIR-over-Stargate es arquitectónico hoy — el despliegue en producción depende del onboarding por parte de los hospitales; la fecha realista más temprana es septiembre de 2026. La historia arquitectónica es genuinamente sólida: los recursos FHIR que fluyen a través de Stargate heredan el modelo de autorización anclado en AID, de modo que el estado de consentimiento a nivel de recurso reside donde el ciudadano lo controla. Pero la ingeniería de la adopción hospitalaria — integración con sistemas clínicos, aprobación regulatoria, gobernanza operativa — es un proceso que abarca varios trimestres. No afirmamos que FHIR-over-Stargate esté en producción. Lo afirmamos como el próximo paso deliberado, con una fecha mínima conocida, y esperamos que el despliegue operativo se retrase respecto a la disponibilidad arquitectónica en un intervalo medible. Confundir ambos aspectos es el modo de fallo que este documento pretende evitar.

El historial en producción importa porque es lo que separa esta tesis de una presentación de diapositivas. Las organizaciones de ingeniería se encuentran habitualmente con el argumento centralización frente a descentralización; lo que raramente encuentran es la descentralización operando a escala, bajo regulación institucional real, en un sector regulado. El sustrato de mensajería verificada ha transportado tráfico institucional real durante el tiempo suficiente para exponer los rincones operativos de DKMS — disciplina de rotación de claves, descubrimiento entre organizaciones, retención de registros de auditoría, agencia del destinatario — y esos rincones han sido refinados en producción, no en teoría. Cuando Stargate entre en producción anticipada a partir de junio de 2026, funcionará sobre el mismo sustrato. El argumento arquitectónico no es, por tanto, una previsión; es una extrapolación a partir de operaciones observadas a escala.

---

9. Cinco Incidentes que Demuestran el Patrón Estructural

Cinco incidentes — tres de 2026 y dos casos fundacionales más antiguos — ilustran por qué las arquitecturas centralizadas fallan bajo presión regulatoria y cómo el modo de fallo es arquitectónico y no operativo.

9.1 Kaiser Foundation Health Plan — Acuerdo por USD 47.500.000 (2026)

Kaiser Foundation Health Plan alcanzó un acuerdo de acción colectiva por USD 47.500.000 relacionado con el rastreo mediante píxeles en el portal del paciente, con aprobación definitiva el 30 de abril de 2026 (Class Action Center, expediente del acuerdo de Kaiser Foundation Health Plan). Los demandantes alegaron que los píxeles de rastreo de Meta y Google integrados en el portal autenticado del paciente de Kaiser transmitían información sanitaria protegida a plataformas publicitarias de terceros — incluidos diagnósticos, tipos de citas e historial de consultas sobre medicamentos — junto con identificadores suficientes para vincular de nuevo los datos a pacientes concretos. El fallo arquitectónico es preciso: el consentimiento del paciente existía en la capa de registro del portal, pero el flujo de datos estaba determinado por los SDK integrados, no por la preferencia declarada del paciente. La retirada del consentimiento no afectaba en modo alguno a los eventos de píxel ya transmitidos, y el paciente carecía de medios arquitectónicos para detectar o revocar los flujos hacia terceros.

9.2 Sutter Health — Acuerdo por USD 21.500.000 (2026)

Sutter Health alcanzó un acuerdo por USD 21.500.000 en el mismo patrón de expediente, con aprobación definitiva el 27 de febrero de 2026. Acuerdos paralelos han sido suscritos o están pendientes contra BJC HealthCare, Northwell Health, Catholic Health, Aspirus y SSM Health en hechos esencialmente idénticos. El expediente de acuerdos de 2025–2026 en su conjunto es el indicador adelantado: todo gran sistema sanitario estadounidense que integró píxeles de rastreo de terceros en superficies orientadas al paciente está pagando ahora por la ausencia arquitectónica de límites criptográficos por paciente en el flujo de datos. El consentimiento era una casilla de verificación; el flujo se decidía en otro lugar.

9.3 Opt-Out Nacional de Datos del NHS (NDOO) — No Retroactividad, 2018–2021

NHS England consolidó los opt-outs legacy de Tipo 1 y Tipo 2 en el National Data Opt-Out (NDOO) a partir de 2018, con fuerza estatutaria. La documentación del programa y los comentarios de la ICO confirmaron posteriormente que el opt-out era demostrablemente **no retroactivo**: los datos ya extraídos de los sistemas de médicos de cabecera antes de que el ciudadano registrara el opt-out permanecían en los conjuntos de datos de investigación y podían seguir siendo procesados. NHS Digital no disponía de infraestructura técnica para recuperar los registros ya extraídos. El programa sucesor GPDPR (General Practice Data for Planning and Research) estaba programado para comenzar el 1 de julio de 2021 y fue aplazado indefinidamente en junio de 2021 precisamente porque no existía un medio técnico para eliminar los datos de médicos de cabecera ya extraídos cuando se registraba un opt-out de Tipo 1 a posteriori. A fecha de 2026, la extracción aún no ha comenzado. La lección arquitectónica: cuando el operador es propietario de la ruta de datos, el «veto del paciente» carece de primitiva de aplicación — y el mecanismo normativo colapsa bajo su propio peso forense.

9.4 SingHealth — 1.500.000 Registros Comprometidos (2018)

El Informe Público del Comité de Investigación de Singapur sobre el Ciberataque a Singapore Health Services (10 de enero de 2019) constató que 1.500.000 registros de pacientes de SingHealth habían sido comprometidos, incluido el historial clínico personal del Primer Ministro de Singapur. El hallazgo técnico es el arquitectónico: no había **ninguna compartimentación** en el sistema de registros médicos electrónicos de SingHealth. Una vez que un atacante accedió a la aplicación Allscripts Sunrise a través de una cuenta de servicio con privilegios, todos los registros de pacientes eran accesibles. El consentimiento del paciente era un artefacto de política en la capa de acceso; la capa de datos **carecía de límites criptográficos por paciente**. La superficie de la brecha era precisamente la ausencia de ese límite.

9.5 Compromiso de la Autoridad de Certificación DigiNotar (2011)

La investigación de Fox-IT publicada como informe «Black Tulip» (13 de agosto de 2012) constató que los ocho servidores CA de DigiNotar habían sido comprometidos. Se habían emitido más de 531 certificados fraudulentos, incluido un certificado comodín `*.google.com` utilizado para llevar a cabo un ataque de intermediario contra aproximadamente 300.000 usuarios iraníes de Gmail. La remediación — la revocación de

la confianza en DigiNotar — fue llevada a cabo unilateralmente por Mozilla, Microsoft y Google, y se propagó a los usuarios finales a través de actualizaciones del almacén de certificados raíz. La propia cadena Staat der Nederlanden – G2 del gobierno neerlandés fue pasada por alto en la eliminación inicial y requirió un seguimiento adicional. Los usuarios finales tuvieron **cero agencia** en la decisión de confianza en ninguna fase: ni en la emisión, ni en la detección, ni en la remediación. Se enteraron del compromiso a través de sus propios servicios interrumpidos.

Todos los incidentes centralizados comparten una característica: el usuario carecía de agencia arquitectónica. Los pacientes de Kaiser y Sutter no controlaban el flujo de píxeles. Los pacientes del NHS no podían recuperar los datos extraídos. Los pacientes de SingHealth no tenían límites criptográficos por registro. Los usuarios finales de DigiNotar no podían votar sobre las decisiones de confianza. El patrón es estructural y persiste a lo largo de cinco décadas de evidencia de incidentes, independientemente del regulador, el sector o la jurisdicción.

---

10. Conclusión y Cómo Colaborar

El opt-out ha pasado de aspiración normativa a derecho legal exigible bajo EHDS Article 71, GDPR 7(3) y 17(2), eIDAS 2.0 5a(14)/(16)(b), nDSG y HFG suizas, y el PDSG alemán. Se derivan directamente cinco invariantes de ingeniería: identificadores de ámbito personal, opt-out verificable con marca de tiempo, reversibilidad sin reidentificación, propagación entre responsables del tratamiento e imposibilidad de vinculación. X.509 PKI no satisface ninguno en la capa ciudadana; el IAM federado satisface la propagación únicamente violando la imposibilidad de vinculación; el KMS centralizado satisface el caso de arrendatario único pero no puede alcanzar entre dominios de confianza. **DKMS es el primer fundamento estructuralmente sólido para honrar la retirada del consentimiento de extremo a extremo — en condiciones interorganizativas, posdivulgación, bajo supervisión regulatoria** — con límites explícitos en torno a derivados, copias de seguridad y contrapartes individuales deshonestas. El expediente de acuerdos de 2025–2026 (Kaiser, Sutter, BJC, Northwell, Catholic Health, Aspirus, SSM Health) es la evidencia viva de que toda arquitectura centralizada bajo este tipo de presión regulatoria comparte una característica: el usuario carecía de agencia arquitectónica.

Si usted es responsable de la arquitectura del consentimiento en un ecosistema de TI sanitaria que afronta la transposición del EHDS, la implementación del EGDG / BDG suizo u operaciones bajo el PDSG alemán, Vereign ofrece una revisión de arquitectura de consentimiento de 30 minutos. Mapearemos su superficie de consentimiento actual frente a los cinco invariantes, identificaremos las trampas del Article 71(8) en su hoja de ruta y localizaremos el alcance preciso donde DKMS es — y no es — la respuesta arquitectónica correcta. **Contacto: contact@vereign.com.**

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