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

Vereign AG

2026-04-29

Architecture du consentement : DKMS comme fondement structurellement solide pour EHDS Article 71

Vereign AG — Avril 2026

1. Résumé exécutif

Le droit européen des données de santé a franchi un seuil décisif. L'opt-out n'est plus une ambition politique — en vertu de EHDS Article 71, il s'agit d'un **droit légal** de la personne physique, opposable dans chaque État membre traitant des données de santé identifiables à des fins secondaires. Superposés aux Articles 7(3) et 17(2) du RGPD, à l'Article 5a d'eIDAS 2.0, à la nLPD et à la LRH suisses, et au PDSG allemand, cinq régimes indépendants convergent vers un même ensemble d'invariants d'ingénierie : **identifiants à portée personnelle, opt-out horodaté et vérifiable, réversibilité sans réidentification, propagation inter-contrôleurs et non-liabilité**. L'ICP centralisée et l'identité fédérée n'en satisfont au plus qu'un ou deux ; X.509 n'en satisfait aucun au niveau citoyen. **La Gestion décentralisée des clés (DKMS) est le premier fondement structurellement solide pour honorer le retrait du consentement de bout en bout — *dans des conditions inter-organisationnelles, post-divulgation, sous surveillance réglementaire*.** La thèse comporte des limites explicites — les dérivés ayant quitté le système avant le retrait, les sauvegardes immuables et les contreparties

individuellement malhonnêtes restent hors de portée architecturale. Le dossier de règlements 2025–2026 (Kaiser USD 47,5 M, Sutter USD 21,5 M, procédures parallèles contre BJC, Northwell, Catholic Health, Aspirus et SSM Health) constitue l'indicateur avancé : chaque incident centralisé partage une seule caractéristique — l'utilisateur ne disposait d'aucune capacité d'action architecturale.

---

2. Pourquoi maintenant — Convergence réglementaire en 24 mois

Pendant deux décennies, la gestion du consentement dans l'informatique de santé a traité l'opt-out comme un problème d'interface utilisateur. À partir de 2024, cinq régimes juridiques indépendants ont convergé vers le même schéma d'ingénierie, laissant aux éditeurs des mois — et non des années — pour démontrer leur conformité structurelle.

EHDS Article 71 — Règlement (UE) 2025/327. Adopté le 11 février 2025 ; publié au Journal officiel de l'Union européenne (JO L 2025/327) le 5 mars 2025 ; en vigueur depuis le 26 mars 2025. L'Article 71(1) confère à toute personne physique le droit de s'opposer au traitement secondaire de ses données de santé électroniques identifiables. L'Article 71(2) interdit l'émission de nouveaux permis portant sur des données identifiables une fois l'opt-out exercé, tout en maintenant les permis délivrés avant cet exercice. **L'Article 71(8)** interdit aux détenteurs de données d'acquérir des données d'identification supplémentaires dans le seul but d'honorer l'opt-out — le pivot d'ingénierie qui ferme la voie au schéma évident du « registre central des personnes ayant exercé l'opt-out ».

Articles 7(3) et 17(2) du RGPD — Règlement (UE) 2016/679. L'Article 7(3) exige que le retrait du consentement soit « aussi aisé à retirer qu'à donner ». L'Article 17(2) impose une obligation de propagation : un responsable du traitement qui honore une demande d'effacement doit prendre « des mesures raisonnables, y compris d'ordre technique » pour informer les responsables du traitement en aval. L'Article 9(2)(a) relève le seuil applicable aux données de santé à un consentement *explicite* ; les Articles 17(3)(c)/(d) prévoient des exceptions pour la santé publique et la recherche qui rendent l'effacement littéral structurellement inaccessible pour la plupart des dossiers cliniques — raison précisément pour laquelle l'EHDS a formulé le droit comme une **suppression prospective** plutôt que comme une suppression rétrospective.

eIDAS 2.0 — Règlement (UE) 2024/1183. Modifie le Règlement (UE) 910/2014 pour créer le Portefeuille européen d'identité numérique (EUDIW). L'Article 5a(14) impose un « contrôle total de l'utilisateur » sur les opérations du portefeuille. L'Article 5a(16)(a) interdit le suivi inter-contextes de l'utilisation du portefeuille ; l'Article 5a(16)(b) impose la **non-liabilité** entre les présentations d'attestations à différents vérificateurs. Ensemble, les points 5a(16)(a)-(b) constituent la forme opérationnelle de l'Article 71(8) de l'EHDS : une architecture dans laquelle l'opérateur peut corréler un citoyen à travers différents vérificateurs échoue au test de non-liabilité par définition.

nLPD et LRH suisses. La nouvelle Loi fédérale sur la protection des données (nLPD / nDSG, RS 235.1, en vigueur le 1er septembre 2023) exige un consentement explicite pour les données sensibles à l'Article 6(6) et

un droit de retrait absolu à l'Article 6(7), les droits à la suppression prévus à l'Article 32 étant soumis aux obligations de conservation. La Loi relative à la recherche sur l'être humain (LRH / HRA, RS 810.30) confère, à ses Articles 7(2) et 17, le droit de révoquer le consentement et de s'opposer à toute utilisation ultérieure de données de santé. L'EGDG en préparation (message du Conseil fédéral, 5 novembre 2025) inverse le modèle DEP du consentement opt-in à l'opt-out, avec une entrée en vigueur prévue vers 2028–2030 ; le BDG (base légale pour l'utilisation secondaire dans le cadre de DigiSanté) est en cours de rédaction. La propagation inter-cantonale rend le cas suisse structurellement plus complexe que le cas européen.

PDSG allemand. Le Patientendaten-Schutz-Gesetz opérationnalise l'architecture opt-out de l'ePA allemand (dossier de santé électronique), en exploitation depuis janvier 2025 pour environ 73 millions d'assurés au régime légal. Le PDSG codifie les mécanismes de suppression prospective — les citoyens qui refusent l'ePA ne doivent pas être traités au titre de la base légale du consentement opt-in — pour une population plus importante que celle de la plupart des États membres de l'UE réunis. La pression nationale de mise en œuvre sur l'architecture du consentement n'est donc pas théorique ; elle est opérationnelle dans le plus grand parc de soins à payeur unique d'Europe.

Le projet de directive de l'Action conjointe TEHDAS2 (septembre 2025) confirme que le mécanisme technique de propagation de l'opt-out n'est **pas** spécifié par le droit européen lui-même et est laissé à la mise en œuvre des États membres. C'est là la vulnérabilité architecturale fondamentale : chaque État pourrait choisir sa propre approche, mais seule une approche à clés contrôlées par la personne concernée satisfait à l'Article 71(8) sans introduire en contrebande un registre de réidentification prohibé. Les éditeurs qui déploient une architecture conforme dans un État membre pourront commercialiser dans l'ensemble des vingt-sept ; ceux qui ne résolvent que le problème d'interface local seront confrontés à un dialogue architectural différent dans chaque transposition.

Chacun de ces cinq régimes pris isolément est surmontable. **Tous les cinq ensemble, dans une fenêtre de 24 mois, constituent la contrainte architecturale déterminante.** Les éditeurs d'informatique de santé se trouvent désormais face à un marché dans lequel « la gestion du consentement » doit être composable de bout en bout, transfrontières, entre contrôleurs, dans le temps — et le schéma du registre centralisé qui a porté le secteur pendant deux décennies est fermé par le droit primaire du plus grand bloc économique de la planète.

---

3. Les cinq invariants d'ingénierie

Les cinq régimes convergent vers un ensemble restreint et précis d'exigences d'ingénierie. Ils ne sont pas aspirationnels — ce sont des prédicats testables à l'aune desquels toute architecture de consentement peut être évaluée.

3.1 Identifiants à portée personnelle

La personne concernée doit contrôler l'identifiant sous lequel ses permis, autorisations et état de consentement sont référencés. C'est la *condition préalable* à tous les autres invariants : si l'opérateur détient l'identifiant, il détient l'opt-out. L'Article 71(8) de l'EHDS ferme explicitement la voie aux registres de réidentification côté

opérateur ; l'Article 5a(14) d'eIDAS 2.0, qui impose un « contrôle total de l'utilisateur », nomme la même propriété au niveau du portefeuille. Sans identifiant à portée de la personne concernée, la propagation, la réversibilité et la non-liabilité s'effondrent toutes dans la politique de l'opérateur.

3.2 Opt-out horodaté et vérifiable

Pour chaque permis de données, le système doit connaître le moment précis de son émission et le moment précis de son retrait — et un tiers (régulateur, tribunal, contrôleur en aval) doit pouvoir vérifier les deux sans faire confiance aux journaux de l'opérateur. L'Article 71(2) de l'EHDS trace une frontière temporelle nette : les permis antérieurs à l'opt-out restent valides ; les permis postérieurs sont illicites. Cela est inapplicable sans une chronologie infalsifiable et vérifiable par des tiers de l'état de consentement de la personne concernée.

3.3 Réversibilité sans réidentification

Le Considérant 54 du Règlement EHDS confirme que l'opt-out est réversible (les citoyens peuvent opter à nouveau pour l'inclusion) et libre (sans durée minimale). L'Article 71(8) interdit au détenteur de données d'acquérir des données d'identification supplémentaires dans le seul but d'honorer l'opt-out. Les deux dispositions lues ensemble créent une contrainte précise : le système doit permettre de basculer l'état de consentement dans un sens ou dans l'autre, selon le calendrier du citoyen, **sans** que le détenteur de données ne constitue un registre de réidentification parallèle pour suivre qui a basculé dans quel sens. Toute architecture qui nécessite de « maintenir une liste de personnes ayant exercé l'opt-out » viole directement l'Article 71(8).

3.4 Propagation inter-contrôleurs

L'Article 17(2) du RGPD exige du responsable du traitement qui honore l'effacement qu'il prenne « des mesures raisonnables, y compris d'ordre technique » pour informer les contrôleurs en aval qui détiennent des copies, réplications ou liens. L'Article 71 de l'EHDS superposé à des chaînes de permis multi-contrôleurs aggrave cette exigence : le signal d'opt-out doit atteindre chaque Organisme d'accès aux données de santé, chaque consortium de recherche, chaque sous-traitant ayant reçu des données dans le cadre d'un permis antérieur. La propagation ne peut pas se résumer à un registre documentaire — elle doit constituer un artefact vérifiable que les parties en aval peuvent revérifier.

3.5 Non-liabilité

L'Article 5a(16)(b) d'eIDAS 2.0 impose la non-liabilité entre les présentations de la même attestation à différents vérificateurs. La conséquence opérationnelle : une architecture dans laquelle une seule partie (même un intermédiaire autorisé) voit toutes les transactions entre vérificateurs échoue au test par construction. C'est la propriété qui exclut les fournisseurs d'identité fédérés du niveau citoyen des systèmes conformes à l'EHDS : le fournisseur d'identité, par conception, voit chaque connexion et chaque présentation d'attestation. La fédération peut satisfaire à la propagation, mais uniquement en violant la non-liabilité.

Ces cinq invariants forment un système interdépendant. **X.509 PKI n'en satisfait aucun au niveau citoyen. Les fournisseurs d'identité fédérés ne satisfont à la propagation qu'en violant la non-liabilité. DKMS les satisfait tous les cinq.** Telle est la thèse de solidité structurelle, que le reste de ce document examine.

4. Le piège de l’Article 71(8)

Le schéma d’implémentation le plus simple pour l’opt-out — celui qu’un éditeur d’informatique de santé esquissera lors de la première heure d’une conversation architecturale — est **un registre central des identifiants de citoyens ayant exercé l’opt-out**. Chaque détenteur de données consulte le registre avant tout traitement ; si l’identifiant du citoyen figure sur la liste, le traitement s’arrête. Simple. Familier. Auditable.

L’Article 71(8) ferme intégralement cette voie.

La disposition interdit aux détenteurs de données d’acquérir des données d’identification supplémentaires dans le seul but d’honorer l’opt-out. **La « liste des identifiants ayant exercé l’opt-out » est, par construction, exactement un tel registre.** Elle n’existe qu’à une seule fin : réidentifier les citoyens dans le cas négatif — pour déterminer que *ce citoyen a exercé l’opt-out et ne peut donc pas être traité*. La liste elle-même constitue la violation réglementaire qu’elle est censée prévenir.

Le piège est récursif. Toute tentative d’anonymiser le registre (hacher les identifiants, les pseudonymiser, les conserver dans un domaine de confiance séparé) réintroduit le problème initial : le détenteur de données a encore besoin d’*un* identifiant à tester par rapport à la liste, et cet identifiant doit être dérivable des données que le détenteur détient déjà. Le haché n’est pas anonyme pour le détenteur qui possède l’entrée ; le pseudonyme n’est pas anonyme pour le détenteur qui possède le lien. Le Considérant 54 renforce cela en imposant que l’opt-out soit réversible et libre — ce qui signifie que le registre doit pouvoir basculer, ce qui à son tour exige que le registre trace *quel* citoyen a basculé *quand* — ce qui est précisément le registre de réidentification que l’Article 71(8) interdit.

L’implication pour les éditeurs d’informatique de santé est nette. **Tout « module de gestion du consentement » dont l’architecture repose sur une liste centrale et faisant autorité des personnes ayant exercé l’opt-out est fermé par le droit primaire de l’UE.** Ce n’est pas un choix de conception d’interface ; c’est la différence entre une architecture pouvant se conformer à l’EHDS et une architecture qui ne le peut pas. Les produits génériques de gestion du consentement fondés sur le schéma de registre — qu’ils soient SaaS, on-premise ou hybrides — se heurteront à cette contrainte à chaque transposition nationale. La réponse structurelle doit placer l’identifiant sous le contrôle du citoyen, afin que le détenteur de données n’ait jamais à maintenir de registre de réidentification.

5. La thèse DKMS

> **La Gestion décentralisée des clés est le premier fondement structurellement solide pour honorer le retrait du consentement de bout en bout — *dans des conditions inter-organisationnelles, post-divulgation, sous surveillance réglementaire*.**

DKMS — s'appuyant sur KERI, une spécification ouverte de la Trust over IP Foundation — place la racine de confiance chez le citoyen plutôt que chez une autorité centralisée. Le citoyen (ou son agent portefeuille) détient un Identifiant Autonomique (AID) auto-certifiant : il est dérivé d'une clé publique sous le contrôle du citoyen, et son authenticité ne dépend d'aucun registraire. Toutes les autorisations accordées aux détenteurs de données, aux sous-traitants et aux contrôleurs en aval s'ancrent sur cet AID par le biais d'un Journal des événements de clés (KEL) — un enregistrement en ajout seul, vérifiable par des tiers, de l'état de chiffrement du citoyen, y compris les rotations de clés.

Le retrait dans ce modèle n'est pas une demande soumise à un opérateur. C'est une **rotation de clé que le citoyen effectue unilatéralement**. La rotation est publiée dans le KEL ; à partir de ce moment, toute partie en aval détenant des attestations ancrées à l'état de clé pré-rotation doit se réauthentifier par rapport à l'état actuel du citoyen pour continuer à traiter. Les permis existants émis avant la rotation continuent de fonctionner là où la base légale sous-jacente le permet (conformément à l'Article 71(2) de l'EHDS) ; les nouveaux permis ne peuvent pas être émis sous l'ancien état de clé, car cet ancien état n'est plus l'état de contrôle du citoyen. Le citoyen a architecturalement — et non seulement procéduralement — retiré l'autorisation future, et toute partie en aval qui ignore la rotation publiée produit des signatures auditables comme étant périmées.

Mise en correspondance avec les cinq invariants :

Invariant	**Mécanisme DKMS**
Identifiants à portée personnelle	L'AID est l'identifiant auto-certifiant de la personne concernée ; aucun index côté opérateur n'est requis
Opt-out horodaté et vérifiable	Le KEL contient des événements de clés horodatés et infalsifiables
Réversibilité sans réidentification	Opt-back-in = rotation de clé rétablissant l'autorisation ; aucun registre parallèle
Propagation inter-contrôleurs	Le KEL est publiable ; les vérificateurs doivent revérifier entre domaines de confiance
Non-liabilité	Les AID par contexte et les attestations à divulgation sélective évitent la corrélation inter-vérificateurs

Comparaison avec les options existantes :

X.509 PKI lie l'identité à un certificat émis par une autorité de certification. Le citoyen ne détient pas la racine de confiance ; l'autorité de certification le fait. La révocation est pilotée par l'opérateur (CRL/OCSP) et échoue sans signaler d'erreur par défaut. La non-liabilité inter-contextes est structurellement absente — chaque présentation de certificat est liée par le numéro de série, le DN de l'émetteur et le DN du sujet. X.509 ne satisfait *aucun* des cinq invariants au niveau citoyen.

IAM fédéré (OIDC, SAML). Le fournisseur d'identité est par conception le traceur inter-contextes que l'Article 5a(16)(b) d'eIDAS 2.0 interdit. La fédération peut satisfaire à la propagation inter-contrôleurs (une déconnexion unique vide les sessions en aval), mais uniquement en violant la non-liabilité — chaque

connexion transite par le fournisseur d'identité, qui voit chaque partie utilisatrice visitée par le citoyen. L'architecture ne peut satisfaire au plus que trois invariants, et uniquement au prix du cinquième.

KMS centralisé (AWS KMS, Azure Key Vault, GCP Cloud KMS). Excellent pour les charges de travail mono-locataire. L'effacement cryptographique via les Clés gérées par le client (CMK) selon la section 2.5 du NIST SP 800-88 est un primitif d'effacement terminal reconnu par les régulateurs (Lignes directrices EDPB 01/2025 ; ENISA 2019 §4.2). Mais une fois que les données quittent le périmètre du locataire — vers un consortium de recherche, un contrôleur en aval, un destinataire autorisé pour une utilisation secondaire — la destruction de la CMK de l'opérateur ne touche pas la copie. La propagation inter-contrôleurs reste non résolue. Schrems II / Recommandations EDPB 01/2020 Cas d'utilisation 3 aggrave encore le problème : l'importateur de données ne doit pas détenir les clés, par définition.

DKMS ne remplace pas ces architectures — il occupe le créneau architectural précis qu'elles ne peuvent pas combler. KMS centralisé pour l'effacement dans le périmètre, X.509 pour la révocation de classe TLS, IAM fédéré pour le consentement à portée de session — et DKMS pour la couche inter-organisationnelle et post-divulgation où l'Article 71 de l'EHDS s'applique réellement.

---

6. Les points de défaillance des architectures centralisées

Les cinq invariants sont testables. Chaque architecture de consentement centralisée majeure échoue selon une modalité structurellement spécifique.

6.1 X.509 PKI échoue aux cinq invariants au niveau citoyen

X.509 lie l'identité à une autorité de certification. L'autorité de certification génère ou co-signe le certificat du citoyen, détient la décision d'émission et contrôle la révocation. Les identifiants à portée personnelle échouent à la racine — la signature de l'autorité de certification est la source de confiance, non celle du citoyen. L'opt-out horodaté est piloté par l'opérateur (le citoyen soumet une demande de révocation ; l'autorité de certification décide de l'honorer et du moment de la publication), et la révocation ne se propage qu'à la vitesse des fenêtres de rafraîchissement des CRL ou de la disponibilité du répondeur OCSP — deux mécanismes qui échouent sans signaler d'erreur dans les navigateurs par défaut. La réversibilité sans réidentification échoue car la réémission exige que l'autorité de certification re-valide l'identité du sujet, ce qui dans le contexte de la santé requiert que l'autorité de certification réacquière les données d'identification précisément interdites par l'Article 71(8) de l'EHDS. La propagation inter-contrôleurs dépend du fait que chaque partie utilisatrice vérifie correctement les CRL/OCSP — ce que les incidents DigiNotar et Comodo ont démontré comme étant opérationnellement fragile. La non-liabilité est structurellement impossible : chaque certificat X.509 porte un numéro de série et un DN d'émetteur qui lie chaque présentation au même citoyen.

6.2 L'IAM fédéré (OIDC/SAML) viole la non-liabilité par définition

OIDC et SAML fédèrent l'authentification par l'intermédiaire d'un fournisseur d'identité qui assure la médiation de la relation entre le citoyen et la partie utilisatrice. Chaque connexion du citoyen auprès d'un vérificateur quelconque transite par le fournisseur d'identité. Celui-ci sait quel citoyen a accédé à quel service et quand. Ce n'est pas un choix de configuration ou une violation de politique — c'est la fonction architecturale du fournisseur d'identité. L'Article 5a(16)(b) d'eIDAS 2.0 impose la non-liabilité entre les présentations de la même attestation à différents vérificateurs ; le fournisseur d'identité fédéré est, par construction, le point unique où chaque présentation est corrélée. La fédération peut assurer une propagation inter-contrôleurs réelle (déconnexion unique, révocation de jeton OAuth, déconnexion OIDC par canal arrière) — mais à un coût : la violation de l'invariant de non-liabilité pour chaque présentation d'attestation que le fournisseur d'identité traite.

6.3 Le KMS centralisé ne peut atteindre la propagation inter-contrôleurs

AWS KMS, Azure Key Vault et GCP Cloud KMS offrent une custody de clés auditable, des backends FIPS 140-2 L3 / 140-3, la destruction programmée des clés (`ScheduleKeyDeletion`, soft-delete + purge, `DESTROY_SCHEDULED`) et le chiffrement d'enveloppe avec séparation DEK/KEK. Dans un seul périmètre de locataire, il s'agit d'un primitif d'effacement RGPD Article 17 entièrement adéquat — la section 2.5 du NIST SP 800-88 reconnaît explicitement l'effacement cryptographique comme une technique de purge, et les Lignes directrices EDPB 01/2025 traitent la custody de clés comme déterminante du résultat quant au caractère anonyme des données pour un destinataire donné. L'architecture fonctionne **à l'intérieur du périmètre du locataire**.

Elle ne franchit pas ce périmètre. Une fois que les données ont été légalement copiées vers un consortium de recherche, un contrôleur en aval autorisé ou un sous-traitant dans un autre domaine de confiance, la destruction KMS du locataire ne touche pas la copie. La propagation selon l'Article 17(2) du RGPD devient une obligation contractuelle — de la documentation, non de l'architecture. La structure des chaînes de permis de l'Article 71 de l'EHDS rend cette lacune structurelle plutôt qu'accessoire : chaque permis est potentiellement le début d'une chaîne multi-contrôleurs, et la CMK centralisée n'a aucun moyen d'atteindre au-delà du premier maillon.

---

7. Les limites de DKMS — Examen objectif

La thèse est structurelle, non absolue. Une formulation honnête rend l'argument défendable ; le dépasser le détruit. La thèse DKMS comporte quatre limites explicites.

7.1 Les dérivés — Avis EDPB 28/2024

Une fois que des données ont été transformées en dérivé — agrégats analytiques, poids de modèles d'apprentissage automatique, extraits statistiques, rapports réglementaires déjà déposés — la destruction des clés sur le texte chiffré source ne touche pas le dérivé. L'Avis EDPB 28/2024 sur les aspects de la protection des données dans les modèles d'IA (adopté le 17 décembre 2024) confirme explicitement que les obligations d'effacement ne se propagent pas aisément aux poids de modèles une fois l'entraînement effectué. DKMS ne fait pas mieux que la CMK centralisée ici. Si un consortium de recherche autorisé a entraîné un modèle sur des données dont le citoyen exerce ensuite l'opt-out, les poids du modèle subsistent. La contribution architecturale est l'auditabilité de la chaîne de dérivation, non le dénouement rétroactif de cette dérivation.

7.2 Les sauvegardes déjà effectuées

Aucune architecture de révocation de clé en temps réel, qu'elle soit DKMS ou centralisée, ne peut rappeler des données déjà répliquées sur des supports de sauvegarde immuables. Les sauvegardes hors ligne effectuées avant le retrait se situent en dehors de l'espace de clés actif. La réponse pragmatique est une destruction documentée et programmée des clés sur une fenêtre de conservation connue — ce que les lignes directrices de l'ICO, de la CNIL et du BfDI approuvent toutes comme suffisant pour les données personnelles résiduelles dans les sauvegardes. DKMS s'aligne sur cette discipline ; il ne la remplace pas.

7.3 Une seule contrepartie malhonnête

Dans un réseau de N parties dont l'une ignore la rotation de clé publiée et continue d'agir sur la base d'attestations périmées, DKMS offre une **détection forensique** — les signatures périmées sont auditables après l'événement de rotation publié — mais non une **prévention**. Un sous-traitant en aval totalement non coopératif qui exfiltre le texte en clair et le stocke hors de l'enveloppe chiffrée échappe à la portée architecturale de tout système de gestion de clés. DKMS renforce la position probatoire du régulateur ; il ne résout pas le problème sous-jacent de non-coopération. Comparé à un parc de CMK centralisées bien gouverné contractuellement, DKMS renforce la détection sans éliminer le besoin d'une application par contrat, régulateur ou tribunal contre les mauvais acteurs.

7.4 Les charges de travail mono-locataire

Pour les charges de travail résidant entièrement dans un seul domaine de confiance — données d'entreprise internes sous un seul contrôleur, SaaS mono-locataire avec CMK à portée du locataire, TLS public sous les SLO de révocation de 24 heures du CA/Browser Forum — l'effacement cryptographique via CMK centralisée selon la section 2.5 du NIST SP 800-88 est entièrement adéquat. Les Lignes directrices EDPB 01/2025 et l'ENISA 2019 §4.2 reconnaissent toutes deux la destruction de clés comme un effacement terminal dans le périmètre du locataire. **L'ajout de DKMS à ces charges de travail impose une charge opérationnelle sans bénéfice architectural.** La réponse honnête est que, pour les scénarios mono-locataire, l'architecture centralisée fonctionne.

7.5 La frontière décisive

DKMS domine lorsque les **quatre** conditions suivantes sont simultanément satisfaites :

1. Les données franchissent **au moins deux domaines de confiance**.
2. Le consentement doit **survivre post-divulgation** (c'est-à-dire que le traitement se poursuit au-delà de la frontière).
3. Le régulateur traite la **custody de clés comme déterminante du résultat** (Schrems II / Recommandations EDPB 01/2020 Cas d'utilisation 3 / Article 71(8) de l'EHDS).
4. Les parties composent DKMS **de bout en bout** (un vérificateur qui ignore le KEL annule la chaîne).

En dehors de ces quatre conditions, la CMK centralisée est le choix rationnel, et le dire rend la thèse DKMS plus solide — non plus faible — car cela localise précisément la thèse là où les preuves la soutiennent. La thèse n'est pas que DKMS résout les bannières de cookies ou la suppression SaaS mono-locataire. La thèse est que DKMS est le bon choix structurel pour *précisément* les cas qui comptent pour le consentement de santé inter-cantonal, inter-organisationnel, sous surveillance réglementaire et post-divulgation.

---

8. Preuves en production

Vereign opère l'architecture DKMS en production aujourd'hui, avec des réserves explicites sur ce qui est en production par rapport à ce qui est architectural.

SEAL est la couche de communication en production : livraison en essaim chiffrée pour les communications sortantes, avec des clés par message et une capacité de déchiffrement sous contrôle du destinataire. SEAL transporte **800 000+ messages vérifiés chaque mois** pour des utilisateurs institutionnels — l'ancre de référence à l'échelle de production pour l'architecture. Chaque message mobilise le même substrat d'événements de clés qui sous-tend la thèse de consentement : chiffrement sous contrôle de la personne concernée, horodatages vérifiables par des tiers et non-liabilité par contexte entre destinataires.

Stargate — la couche d'autorisation ancrée sur AID où les permis de données s'ancrent sur le KEL du citoyen — entre en production initiale depuis juin 2026 avec HIN comme premier déploiement opérationnel. Stargate est la surface de consentement au cœur de la thèse : les autorisations accordées aux détenteurs de données sont ancrées sur l'AID du citoyen ; la rotation de clé par le citoyen se propage par le KEL ; les vérificateurs en aval revérifient. Le déploiement HIN est un lancement à portée limitée ; **le récit de déploiement à grande échelle est réservé à l'après-été 2026**, une fois que la cohorte de production initiale aura accumulé des preuves opérationnelles sous conditions réglementaires réelles.

Les passerelles HIN permettent à l'opt-out d'interopérer avec les contreparties utilisant X.509 via le pont S/MIME ancré sur KERI documenté dans la base de connaissance sur la sécurité de l'e-mail. C'est la reconnaissance pragmatique que DKMS composera avec — sans remplacer du jour au lendemain — le parc de santé X.509 existant.

FHIR-over-Stargate est architectural — le déploiement en production dépend de l'onboarding hospitalier ; au plus tôt septembre 2026. Le récit architectural est genuinement solide : les ressources FHIR transitant par Stargate héritent du modèle d'autorisation ancré sur AID, de sorte que l'état de consentement au niveau de la ressource réside là où le citoyen le contrôle. Mais l'ingénierie de l'adoption hospitalière — intégration des systèmes cliniques, homologation réglementaire, gouvernance opérationnelle — est un chantier de plusieurs trimestres. Nous ne revendiquons pas FHIR-over-Stargate comme déployé. Nous le revendiquons comme la prochaine étape délibérée, avec une date minimale connue, et nous anticipons que le déploiement opérationnel sera en retard sur l'état de préparation architectural par un intervalle mesurable. Confondre les deux est le mode de défaillance que ce document est écrit pour éviter.

Les résultats en production importent parce qu'ils sont ce qui distingue cette thèse d'une présentation. Les organisations d'ingénierie rencontrent régulièrement l'argument centralisation-contre-décentralisation ; ce qu'elles rencontrent rarement, c'est une décentralisation opérant à l'échelle, sous régulation institutionnelle réelle, dans un secteur régulé. Le substrat de messagerie vérifiée transporte du trafic institutionnel réel depuis assez longtemps pour exposer les angles opérationnels de DKMS — discipline de rotation de clés, découverte inter-organisations, conservation des journaux d'audit, capacité d'action du destinataire — et ces angles ont été affinés en production plutôt qu'en théorie. Lorsque Stargate entrera en production initiale depuis juin 2026, il fonctionnera sur le même substrat. L'argument architectural n'est donc pas une prévision ; c'est une extrapolation à partir d'opérations observées à l'échelle.

---

9. Cinq incidents qui établissent le schéma structurel

Cinq incidents — trois de 2026, deux cas fondateurs plus anciens — illustrent pourquoi les architectures centralisées échouent sous la pression réglementaire et comment le mode de défaillance est architectural plutôt qu'opérationnel.

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

Kaiser Foundation Health Plan a conclu un règlement de recours collectif d'un montant de USD 47,5 millions pour le suivi par pixel sur les portails patients, avec approbation définitive prononcée le 30 avril 2026 (Class Action Center, dossier Kaiser Foundation Health Plan). Les plaignants allèguent que des pixels de suivi Meta et Google intégrés dans le portail patient authentifié de Kaiser ont transmis des informations de santé protégées à des plateformes publicitaires tierces — notamment des diagnostics, des types de rendez-vous et des requêtes de médicaments — accompagnées d'identifiants suffisants pour relier les données à des patients spécifiques. La défaillance architecturale est précise : le consentement du patient existait au niveau de l'enregistrement dans le portail, mais le flux de données était déterminé par les SDK intégrés, non par les préférences déclarées du patient. Le retrait du consentement ne touchait pas les événements pixel déjà transmis, et le patient ne disposait d'aucun moyen architectural de détecter ou révoquer les flux vers des tiers.

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

Sutter Health a conclu un règlement d'un montant de USD 21,5 millions dans le même schéma de dossier, avec approbation définitive le 27 février 2026. Des règlements parallèles ont été conclus ou sont en attente contre BJC HealthCare, Northwell Health, Catholic Health, Aspirus et SSM Health sur des faits essentiellement identiques. Le dossier de règlements 2025–2026 dans son ensemble constitue l'indicateur avancé : chaque grand système de santé américain ayant intégré des pixels de suivi tiers dans ses surfaces orientées patients paie désormais l'absence architecturale de frontières cryptographiques par patient sur le flux de données. Le consentement était une case à cocher ; le flux était décidé ailleurs.

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

NHS England a consolidé les anciens opt-outs de type 1 et de type 2 dans le National Data Opt-Out (NDOO) à partir de 2018, avec valeur légale. La documentation du programme et les commentaires de l'ICO ont ultérieurement confirmé que l'opt-out était manifestement **non rétroactif** : les données déjà extraites des systèmes de médecine générale avant que le citoyen n'enregistre l'opt-out sont restées dans des jeux de données de recherche et pouvaient continuer à être traitées. NHS Digital ne disposait d'aucune infrastructure technique pour rappeler les dossiers déjà extraits. Le programme successeur GPDPR (General Practice Data for Planning and Research) devait démarrer le 1er juillet 2021 et a été indéfiniment reporté en juin 2021 précisément parce qu'il n'existait aucun moyen technique de supprimer les données de médecine générale déjà extraites lorsqu'un opt-out de type 1 était enregistré après le fait. À ce jour en 2026, l'extraction n'a toujours pas commencé. La leçon architecturale : lorsque l'opérateur détient le chemin des données, le « veto du patient » ne dispose d'aucun primitif d'application — et le mécanisme politique s'effondre sous son propre poids forensique.

9.4 SingHealth — 1,5 million de dossiers compromis (2018)

Le rapport public du Comité d'enquête de Singapour sur la cyberattaque contre Singapore Health Services (10 janvier 2019) a constaté que 1,5 million de dossiers patients de SingHealth avaient été compromis, y compris le dossier de santé personnel du Premier ministre de Singapour. La conclusion technique est architecturale : il n'existait **aucune compartimentation** dans le système de dossiers médicaux électroniques de SingHealth. Une fois qu'un attaquant avait atteint l'application Allscripts Sunrise via un compte de service à privilèges élevés, tous les dossiers patients étaient accessibles. Le consentement du patient était un artefact de politique au niveau de la couche d'accès ; la couche de données ne disposait **d'aucune frontière cryptographique par patient**. La surface d'exposition à la violation était précisément l'absence de cette frontière.

9.5 Compromission de l'autorité de certification DigiNotar (2011)

L'enquête Fox-IT publiée sous le titre « Black Tulip » (13 août 2012) a constaté que les huit serveurs CA de DigiNotar avaient été compromis. 531+ certificats frauduleux avaient été émis, dont un certificat générique `*.google.com` utilisé pour une attaque de l'homme du milieu contre environ 300 000 utilisateurs iraniens de

Gmail. La remédiation — la méfiance envers DigiNotar — a été décidée unilatéralement par Mozilla, Microsoft et Google et propagée aux utilisateurs finaux par des mises à jour du magasin de racines. La propre chaîne Staat der Nederlanden – G2 du gouvernement néerlandais avait été omise lors du retrait initial et a nécessité un suivi. Les utilisateurs finaux ne disposaient **d'aucune capacité d'action** dans la décision de confiance à aucun stade : ni à l'émission, ni à la détection, ni à la remédiation. Ils ont appris la compromission par l'interruption de leurs propres services.

Chaque incident centralisé partage une seule caractéristique : l'utilisateur ne disposait d'aucune capacité d'action architecturale. Les patients de Kaiser et de Sutter ne contrôlaient pas le flux des pixels. Les patients du NHS ne pouvaient pas rappeler les données extraites. Les patients de SingHealth ne disposaient d'aucune frontière cryptographique par dossier. Les utilisateurs de DigiNotar ne pouvaient pas voter sur les décisions de confiance. Le schéma est structurel, et il persiste sur cinq décennies de preuves incidentelles quel que soit le régulateur, le secteur ou la juridiction.

---

10. Conclusion et comment s'engager

L'opt-out est passé de l'aspiration politique au droit légal opposable en vertu de EHDS Article 71, RGPD 7(3) et 17(2), eIDAS 2.0 5a(14)/(16)(b), nLPD et LRH suisses, et du PDSG allemand. Cinq invariants d'ingénierie en découlent directement : identifiants à portée personnelle, opt-out horodaté et vérifiable, réversibilité sans réidentification, propagation inter-contrôleurs et non-liabilité. X.509 PKI n'en satisfait aucun au niveau citoyen ; l'IAM fédéré ne satisfait à la propagation qu'en violant la non-liabilité ; le KMS centralisé satisfait au cas mono-locataire mais ne peut pas s'étendre à travers les domaines de confiance. **DKMS est le premier fondement structurellement solide pour honorer le retrait du consentement de bout en bout — dans des conditions inter-organisationnelles, post-divulgation, sous surveillance réglementaire** — avec des limites explicites concernant les dérivés, les sauvegardes et les contreparties individuellement malhonnêtes. Le dossier de règlements 2025–2026 (Kaiser, Sutter, BJC, Northwell, Catholic Health, Aspirus, SSM Health) constitue la preuve vivante que chaque architecture centralisée sous ce type de pression réglementaire partage une seule caractéristique : l'utilisateur ne disposait d'aucune capacité d'action architecturale.

Si vous êtes responsable de l'architecture du consentement dans un parc d'informatique de santé confronté à la transposition de l'EHDS, à la mise en œuvre de l'EGDG / BDG suisse, ou aux opérations du PDSG allemand, Vereign propose une revue d'architecture du consentement de 30 minutes. Nous cartographierons votre surface de consentement actuelle par rapport aux cinq invariants, identifierons les pièges de l'Article 71(8) dans votre feuille de route, et localiserons le périmètre précis où DKMS est — et n'est pas — la bonne réponse architecturale. **Contact : contact@vereign.com.**

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