MEMORIA CERO

Identidad soberana, acto irrefutable

AXENKOR SpA · Primera edición, 2026

MEMORIA CERO

Identidad soberana, acto irrefutable

AXENKOR SpA

Primera edición · 2026

MEMORIA CERO Identidad soberana, acto irrefutable

> *La privacidad no es para los que no tienen nada que esconder. Es para los que entienden que la información es poder — y que el poder sobre la propia información debería pertenecer a quien la genera.*

A mis hijo, hijas —

simplemente porque su existencia me motiva, me alimenta y me hace querer y hacer más cosas cada día; porque inspiran mi deseo de aportar de alguna forma a este mundo y dejarles a mi descendencia presente y futura un legado, no sé si transcendental, pero sí muy personal, permanente, y que busca cambiar mi mundo — por ende, al mundo.

— Pedro

Nota sobre los términos

Este libro describe una arquitectura con términos específicos que no existen en el vocabulario digital convencional. Para el lector que llega sin contexto previo, esta nota define cada uno de ellos. Para el lector que los conoce, sirve como referencia rápida cuando el texto los usa en combinación.

Motor de Autoría Soberana (MAS). El protocolo criptográfico sobre el que está construido todo el sistema. Define la arquitectura de identidad soberana, los mecanismos de firma, el registro inmutable de actos, y las reglas de verificación. MAS es el protocolo. OwnTrust es su primera implementación para personas naturales en Chile.

OwnTrust. La implementación concreta de MAS para el mercado chileno. Sistema de certificación de actos soberanos de personas naturales e instituciones. Permite a cualquier titular demostrar, con certeza matemática, qué autorizó, cuándo, y con qué alcance.

MVOK. La aplicación con la que el titular interactúa con OwnTrust. Actúa como la interfaz soberana del titular para firmar actos, ejercer derechos ARCO+P, y consultar su historial certificado.

AXENKOR SpA. La empresa que desarrolla y opera OwnTrust y el protocolo MAS. Fundada en Chile en 2026. Chile es el primer territorio. El mundo es la frontera.

El Simbionte. La entidad criptográfica que representa la identidad soberana de un actor en el sistema MAS. Si el Simbionte lo firmó, ocurrió. Y eso no puede deshacerse, falsificarse ni negarse.

Simbionte Soberano. La identidad raíz permanente de la persona natural. Anclada biométricamente. Irrevocable por ninguna organización. Solo se extingue por decisión soberana del propio titular o por proceso judicial con los mecanismos del protocolo.

Simbionte Derivado. La proyección funcional generada por el Simbionte Soberano cuando el titular asume un cargo o rol. Sus capacidades están delimitadas al alcance de ese rol. Se desactiva automáticamente cuando el titular sale del cargo — sin intervención manual de ningún sistema.

AID — Identificador Autónomo. El identificador único del Simbionte. Pseudónimo matemático derivado de las claves públicas del actor. No contiene ni revela la identidad natural del titular. Verificable por cualquier tercero sin contactar ninguna autoridad central.

KEL — Registro de Eventos de Clave. El registro inmutable y cronológico de todos los actos del Simbionte. Cada entrada está firmada criptográficamente y encadenada a la anterior. No puede modificarse sin romper la cadena. Es la historia irrefutable del titular.

ADN. En el contexto de este libro: no el ácido desoxirribonucleico biológico, sino su equivalente criptográfico — la clave efímera derivada de los datos de identidad del titular durante el génesis. Existe solo durante el acto de autenticación y desaparece una vez cumplida su función. No se almacena en ningún lugar.

Fragmento A / Fragmento B. Las dos mitades de la firma soberana. El Fragmento A pertenece al titular, vive en su dispositivo personal. El Fragmento B pertenece al operador del sistema. Ninguno puede producir una firma válida sin el otro. Es el billete partido del capítulo 8, aplicado a la identidad digital.

La Bóveda. El sistema de almacenamiento distribuido donde viven los Fragmentos B y los registros del KEL. Opera bajo reglas criptográficas que ningún operador puede violar unilateralmente.

Acto soberano. Cualquier acción que el titular firma con su identidad soberana: un consentimiento, el ejercicio de un derecho ARCO+P, una declaración, una transferencia de posesión. El acto soberano es irrefutable porque nace de la firma del titular, no del registro del sistema.

Memoria cero. El principio arquitectónico central del sistema: no recordar lo que no es necesario recordar. La identidad natural del titular nunca se almacena. Lo que persiste es el registro de actos certificados, no los datos que los fundamentaron.

Génesis. El ritual inicial en el que el titular establece su identidad soberana por primera vez. Requiere su documento de identidad físico y un secreto personal. Es el único momento en que el sistema verifica la identidad en claro. A partir de él, el titular solo necesita su secreto.

ARCO+P. Los derechos que la Ley 21.719 garantiza a todo titular de datos personales: Acceso, Rectificación, Cancelación, Oposición y Portabilidad. En OwnTrust, el titular los ejerce directamente desde su aplicación, sin depender de que la organización los gestione en su nombre.

Titular. La persona natural cuyos datos personales se tratan. El protagonista de todo el sistema. El actor, no el objeto.

Hegemonía del custodio. El paradigma vigente: el poder sobre la narrativa de los hechos pertenece a quien controla el registro. El modelo que MAS desplaza estructuralmente.

Hegemonía objetiva. El paradigma que MAS instala: el poder pertenece a los hechos matemáticamente certificados, independientemente de quién los custodie. El modelo al que apunta este libro.

Índice

▸ *Los capítulos marcados incluyen sección de profundidad técnica al final.*

Capítulo

Prólogo

Imagine que la Agencia de Protección de Datos Personales llama mañana.

No es una advertencia. Es una fiscalización. Alguien presentó una reclamación contra su empresa. La APDP quiere saber si el titular Juan Pérez consintió específicamente el uso de sus datos de salud el 15 de marzo de 2024.

Tiene treinta días para responder.

¿Qué les muestra?

Si la respuesta es un log de base de datos — un registro que su propia empresa administra, que su propia empresa podría modificar, que existe porque su propia empresa dice que existe — entonces no tienen evidencia.

Tienen una afirmación.

Y una afirmación, ante un regulador con dientes y ante un tribunal con criterio, vale lo que vale: depende de si le creen.

Este libro nació de esa pregunta. No de la pregunta técnica sobre cómo construir un sistema más seguro. Sino de la pregunta más fundamental: ¿por qué en el mundo digital la evidencia de un acto — de que alguien consintió, firmó, autorizó, ejerció un derecho — existe en los registros de quien más interés tiene en que esa evidencia sea favorable?

En el mundo físico no funciona así. Un contrato firmado existe en manos de ambas partes. Una declaración notarial existe en el archivo del notario — un tercero sin interés en el resultado. Una factura existe con el sello del emisor y la aceptación del receptor.

En el mundo digital, el contrato existe en el servidor de quien lo redactó. La declaración existe en la base de datos de quien la solicitó. La aceptación existe en el log de quien la necesita.

Eso tiene un nombre en teoría legal: conflicto de interés probatorio. Y es el defecto de origen de prácticamente todo sistema digital de gestión de identidad y consentimiento que existe hoy.

* * *

Este libro habla de ese defecto. Y de cómo resolverlo.

La solución que proponemos tiene un nombre: Identidad Digital Soberana y Trazabilidad Certificada. Y su implementación concreta se llama OwnTrust. Pero este libro no es un manual de producto. Es la explicación de por qué ese defecto existe, por qué las soluciones actuales no lo resuelven, y qué arquitectura lo resuelve de verdad.

La primera parte examina el problema con la honestidad que merece. No como crítica al mercado — sino como diagnóstico técnico y legal de por qué el modelo actual es insuficiente para lo que la ley exige y para lo que el titular merece.

La segunda parte describe el modelo que resuelve el problema. Con la precisión que requiere quien lo va a implementar y con la claridad que requiere quien lo va a evaluar, contratar o regular.

La tercera parte analiza las implicaciones para cada actor: el titular, la organización, el regulador y el sistema legal. Porque un cambio de arquitectura produce cambios en la distribución del poder y la responsabilidad — y esos cambios merecen ser nombrados.

La cuarta parte mira hacia adelante. Hacia lo que es posible cuando la identidad digital es verdaderamente soberana — cuando no depende de ningún sistema, ninguna empresa, ningún Estado, ningún dispositivo. Solo del titular.

El epílogo vuelve a la escena del comienzo. La misma llamada de la APDP. La misma pregunta. Pero esta vez con una respuesta diferente.

* * *

Una nota sobre la estructura.

Este libro está escrito para dos audiencias simultáneas: quienes necesitan entender el problema y la solución en términos conceptuales, legales y estratégicos — y quienes necesitan entenderlos en términos técnicos, criptográficos y de implementación.

En lugar de escribir dos libros, elegimos una estructura diferente. Cada capítulo tiene un cuerpo principal escrito para cualquier lector comprometido con el tema — sin tecnicismos, con rigor. Algunos capítulos incluyen al final una sección de profundidad técnica, claramente señalada, para quien necesita los detalles de implementación.

El lector ejecutivo puede saltarse las secciones de profundidad sin perder el hilo. El lector técnico encontrará en ellas la especificidad que el cuerpo principal deliberadamente omite.

Ambos leerán el mismo libro. Pero no exactamente de la misma manera.

PARTE I

El problema

El primer paso hacia la solución es entender el problema con más precisión que quien lo sufre.

— anónimo

Capítulo 1

El conflicto de interés que nadie nombra

Hay un momento en el que la mayoría de las empresas descubre que no tienen evidencia.

No lo saben todavía. Creen que sí la tienen. Tienen bases de datos, tienen logs, tienen registros de clics y de formularios enviados. Tienen sistemas de gestión que generan reportes con fechas y nombres y estados. Todo parece estar en orden.

El problema emerge cuando alguien externo — un regulador, un juez, un abogado de la contraparte — les pregunta: ¿pueden demostrar que ese consentimiento fue otorgado por el titular y no registrado por ustedes?

La respuesta, en la inmensa mayoría de los casos, es que no. Que lo que tienen es el registro de que ellos registraron que el titular consintió. Que la fuente y el interesado son la misma entidad.

La trampa del registro propio

En el derecho probatorio existe un principio fundamental: la prueba no puede provenir exclusivamente de quien tiene interés en el resultado que esa prueba establece.

Es por eso que un contrato requiere la firma de ambas partes — no solo la declaración de una de ellas de que la otra firmó. Es por eso que una escritura pública pasa por un notario — un tercero sin interés en el acto. Es por eso que una sentencia la dicta un juez — alguien ajeno a la disputa.

En el mundo digital, este principio se ignoró desde el principio. No por malicia — sino por inercia. Porque los sistemas se construyeron para gestionar eficientemente las operaciones de las empresas, no para generar evidencia verificable independientemente.

El resultado es un ecosistema donde la prueba del consentimiento de un titular existe en el servidor de la empresa que necesita ese consentimiento para

operar. Donde la prueba de que un derecho fue ejercido existe en la base de datos de la organización que debe responder a ese derecho. Donde la cadena de custodia de la evidencia comienza y termina en la parte interesada.

Esto no es un problema de honestidad. La mayoría de las empresas no manipulan sus registros. El problema es más sutil y más estructural: es que la arquitectura del sistema hace que la manipulación sea posible — y esa posibilidad es suficiente para que la evidencia sea jurídicamente débil.

> *La evidencia no es lo que ocurrió. Es lo que puede probarse que ocurrió ante quien tiene autoridad para determinarlo.*

Por qué todos los sistemas tienen el mismo defecto

Las plataformas de gestión de consentimiento y derechos ARCO+P que dominan el mercado hoy — OneTrust, TrustArc, Ketch y sus equivalentes locales — resuelven un problema real: ordenan el proceso interno de las organizaciones para gestionar los datos personales de sus titulares.

Lo hacen bien. Tienen flujos de trabajo, paneles de control, integraciones con sistemas empresariales, reportes para auditores. Son productos maduros, con años de desarrollo y miles de clientes.

Pero tienen un defecto de origen que ningún nivel de sofisticación puede resolver: la evidencia del acto vive en sus servidores. El certificado de que el titular consintió es un registro en su base de datos. La prueba de que el titular ejerció un derecho es un log en su sistema.

Eso significa que si la empresa necesita demostrar el consentimiento ante la APDP, presenta un documento generado por un sistema que ella contrata, que ella configura, que ella administra. El regulador puede confiar en ese sistema — o puede no hacerlo.

Y cuando hay una disputa real — cuando el titular dice que nunca consintió, cuando el regulador cuestiona la autenticidad del registro — la empresa no tiene más argumento que la palabra del sistema que ella misma opera.

No es suficiente. No debería serlo.

El titular como testigo ausente

Hay algo más profundo en este problema. Algo que va más allá de la evidencia y la ley.

En todos estos sistemas, el titular es un objeto. Es la entidad sobre la cual se registra información. Es el destinatario de formularios, el firmante de políticas, el sujeto de los datos. Pero no es el autor del acto.

El autor del acto, en prácticamente todos los sistemas existentes, es la empresa. La empresa registra que el titular hizo algo. La empresa custodia esa evidencia. La empresa puede presentarla o no presentarla, y en qué forma y contexto presentarla.

El titular no tiene ningún papel activo en la generación de la evidencia de sus propios actos.

Eso produce una paradoja curiosa: los sistemas de protección de datos personales — diseñados para empoderar al titular — están construidos de una forma que sistemáticamente lo excluye del acto más importante de su relación con la organización.

El consentimiento, en la práctica digital actual, no es un acto del titular. Es un registro de la empresa de que el titular hizo algo que la empresa necesitaba que hiciera.

* * *

La solución al conflicto de interés no es hacer más confiables los registros de las empresas. Es cambiar quién genera la evidencia del acto.

Si la evidencia del consentimiento proviene del titular — si es el titular quien la genera, quien la firma, quien la hace irrefutable — entonces el conflicto de

interés desaparece. No porque la empresa sea más honesta, sino porque ya no es la fuente de la prueba.

Eso requiere una arquitectura completamente diferente. Una donde el titular sea el actor principal. Una donde su identidad no la custodie nadie. Una donde el acto lo firme él — con evidencia que nadie más puede generar ni falsificar.

Esa arquitectura existe. Los capítulos siguientes explican por qué todavía no es la norma — y cómo puede serlo.

▸ Profundidad técnica — Anatomía de un log de base de datos como evidencia

Un log de base de datos típico de un sistema de consentimiento contiene campos como: id, titular_id, tipo_consentimiento, fecha_registro, ip_origen, version_politica, estado. Todos estos campos son generados, almacenados y administrados por la misma entidad que los presenta como evidencia.

El problema técnico es que cualquier administrador de base de datos con acceso de escritura puede modificar estos registros. Los sistemas más maduros implementan logs de auditoría que registran los cambios — pero esos logs de auditoría también están en la misma base de datos, administrada por la misma empresa.

La criptografía resuelve este problema cuando se aplica correctamente. Un registro firmado digitalmente por el titular — con una llave privada que solo el titular posee — no puede ser modificado sin invalidar la firma. Y esa invalidación es detectable por cualquier tercero con la llave pública correspondiente.

El problema es que ningún sistema comercial actual implementa firma criptográfica del titular. Implementan firma del sistema — lo cual no resuelve el conflicto de interés, sino que lo formaliza con tecnología.

Capítulo 2

El titular ausente

Existe una pregunta que ningún sistema de gestión de datos personales ha respondido satisfactoriamente: ¿cómo sabe el titular qué hizo con sus propios datos?

La respuesta honesta es que, en la mayoría de los casos, no lo sabe. Puede pedirle a la empresa un reporte de qué datos tiene y qué hizo con ellos — eso es el derecho de acceso del ARCO+P. Pero ese reporte lo genera la empresa, con la información que la empresa decide incluir, en el formato que la empresa elige, en el momento que la empresa considera oportuno.

El titular no tiene un registro propio, independiente, de sus actos soberanos en el mundo digital. No existe ningún equivalente digital a la memoria que tiene sobre los contratos físicos que firmó, las declaraciones que hizo ante un notario, las decisiones que tomó en presencia de testigos.

En el mundo digital, la memoria de sus actos la tiene la organización. No él.

La diferencia que la ley no termina de capturar

La Ley 21.719 de Chile — al igual que el GDPR europeo, la LGPD brasileña y sus equivalentes latinoamericanos — reconoce al titular como sujeto de derechos. Puede acceder a sus datos, rectificarlos, cancelarlos, oponerse a su tratamiento, exigir su portabilidad.

Pero hay una distinción que la ley reconoce en su espíritu y que los sistemas tecnológicos no han implementado en su forma: la diferencia entre ser el sujeto de un derecho y ser el autor de su ejercicio.

Cuando una persona firma un contrato en papel, es el autor de ese acto. Su firma es la evidencia. Nadie más pudo haberla producido. El documento físico existe en su mano y en la mano de la contraparte.

Cuando una persona "consiente" en un formulario web, es el sujeto del registro de la empresa de que algo ocurrió. La empresa registra el clic, el

timestamp, la IP. El titular no tiene nada en su mano. No hay acto del titular — hay registro de la empresa de un comportamiento del titular.

Esta distinción parece semántica. No lo es. Es la diferencia entre evidencia soberana y afirmación corporativa. Y esa diferencia se vuelve crítica exactamente cuando más importa: en una disputa.

> *El consentimiento digital, tal como existe hoy, no es un acto del titular. Es el registro de la empresa de que el titular hizo algo que la empresa necesitaba que hiciera.*

Lo que el titular no puede hacer — y debería poder

Piense en lo que significa ejercer soberanía real sobre los propios datos personales.

Significa poder demostrar, en cualquier momento y ante cualquier interlocutor, qué consintió y qué no. Significa tener acceso a un registro de sus propios actos — no mediado por ninguna empresa — que sea verificable matemáticamente. Significa poder decir: "Yo firmé esto. Esto tiene mi firma. Nadie más pudo haberla producido. Nadie puede modificarla sin que sea evidente."

Significa, en el fondo, que la evidencia de sus actos digitales tenga la misma solidez que la evidencia de sus actos físicos.

Eso no existe hoy. En ningún sistema comercial disponible a escala. Hay aproximaciones — la firma electrónica avanzada, los sistemas de identidad federada, los blockchain de identidad — pero todas tienen limitaciones que las hacen inadecuadas para el uso cotidiano del titular promedio: son costosas, complejas, dependientes de hardware específico, o requieren una infraestructura que el titular no controla.

La pregunta que este libro responde es: ¿cómo construir soberanía digital real para el titular ordinario — no para el experto en criptografía, no para el usuario de nicho — con lo que ese titular ya tiene en su bolsillo?

Lo que el titular ya tiene

Tiene su cédula de identidad.

Este objeto físico — emitido por el Estado, con elementos de seguridad verificables, con datos únicos que solo él conoce en su combinación exacta — es la llave más poderosa que la mayoría de las personas tiene. Y es la llave que prácticamente ningún sistema digital ha sabido usar correctamente.

Los sistemas de identidad digital han tomado dos caminos con la cédula. O la ignoran completamente — y basan la identidad en algo que el usuario crea, como una contraseña, que puede ser olvidada, robada o compartida. O la usan como verificación de alta fricción — escáner, lector NFC, proceso burocrático — que la hace impráctica para el uso cotidiano.

Ninguno de los dos caminos produce soberanía. El primero porque la identidad no está anclada a nada real. El segundo porque la fricción excluye a la mayoría de los titulares.

Existe un tercer camino. Uno que usa la cédula como punto de partida — no como proceso burocrático — y que produce una identidad digital que es efímera, soberana, y verificable. Una identidad que nadie custodia porque nadie la necesita custodiar. Una identidad que existe cuando el titular la invoca y desaparece cuando el titular se va.

Una identidad de memoria cero.

* * *

El titular ausente no es un accidente de diseño. Es la consecuencia inevitable de construir sistemas de gestión de datos personales desde la perspectiva de la organización — con sus necesidades de eficiencia operacional, de integración con sistemas existentes, de reducción de fricción en el proceso de adquisición de clientes.

Esos sistemas funcionan bien para la organización. Son inadecuados para el titular.

El cambio de paradigma que este libro propone es simple en su enunciado y complejo en su implementación: construir el sistema desde la perspectiva del titular — con sus datos, su cédula, su secreto, su firma — y que la organización reciba como resultado la evidencia irrefutable que necesita.

El titular en el centro. No como sujeto. Como autor.

▸ Profundidad técnica — Qué exige realmente la Ley 21.719

El artículo 12 de la Ley 21.719 establece que el consentimiento debe ser "libre, informado, específico y otorgado de manera inequívoca". El artículo 13 agrega que la carga de la prueba del consentimiento recae en el responsable del tratamiento.

La expresión "de manera inequívoca" es clave. Un log de base de datos generado por el propio responsable no es inequívoco — es disputable. Una firma criptográfica del titular, generada con una llave privada que solo el titular posee, es inequívoca en el sentido más técnico y legal posible: no puede ser producida por nadie más.

La carga de la prueba sobre el responsable significa que, en caso de disputa, no es el titular quien debe demostrar que no consintió — es la organización quien debe demostrar que sí. Un log de base de datos modificable difícilmente satisface ese estándar en un proceso de fiscalización riguroso.

El artículo 28 establece las sanciones: hasta el 4% de los ingresos anuales del responsable para infracciones gravísimas. Para una empresa con 10 millones de dólares de facturación anual, eso representa 400.000 dólares por infracción. La inversión en evidencia irrefutable es, en cualquier análisis de costo-beneficio razonable, la decisión obvia.

Capítulo 3

Las multas que nadie está calculando bien

El 1 de diciembre de 2026 la Ley 21.719 entra en vigor en Chile con plena capacidad sancionadora. Esa fecha es conocida. Lo que no es tan conocido — o no se ha internalizado con la seriedad que merece — es lo que esa fecha significa en términos de riesgo concreto para las organizaciones que tratan datos personales.

La mayoría de las empresas están tomando medidas. Están actualizando sus políticas de privacidad, nombrando a sus Delegados de Protección de Datos, implementando sistemas de gestión. Algunas están invirtiendo en plataformas internacionales de compliance. Todo eso está bien. Nada de eso es suficiente.

Porque el riesgo no está en no tener un sistema. El riesgo está en tener un sistema cuya evidencia sea cuestionable cuando más importa — en una fiscalización real, ante una reclamación concreta, con un regulador que tiene autoridad para sancionar.

Los números reales

La Ley 21.719 establece tres categorías de infracción con montos que pocos han calculado con precisión.

Las infracciones leves — que incluyen no contar con mecanismos adecuados para que el titular ejerza sus derechos ARCO+P — tienen multas que pueden alcanzar el equivalente a cincuenta unidades tributarias anuales. Para una empresa mediana, eso puede representar montos de cinco a diez millones de pesos.

Las infracciones graves — que incluyen tratar datos sin el consentimiento válido del titular — escalan al 2% de los ingresos anuales del responsable. Para una empresa con cinco millones de dólares de facturación, eso son cien mil dólares por infracción. No por año. Por infracción.

Las infracciones gravísimas — que incluyen transferir datos personales sensibles sin autorización, o impedir sistemáticamente el ejercicio de los derechos del titular — alcanzan el 4% de los ingresos anuales. Para esa misma empresa, doscientos mil dólares. Para un banco o una aseguradora con ingresos de cien millones de dólares, cuatro millones de dólares.

Estos no son números teóricos. Son el texto de la ley.

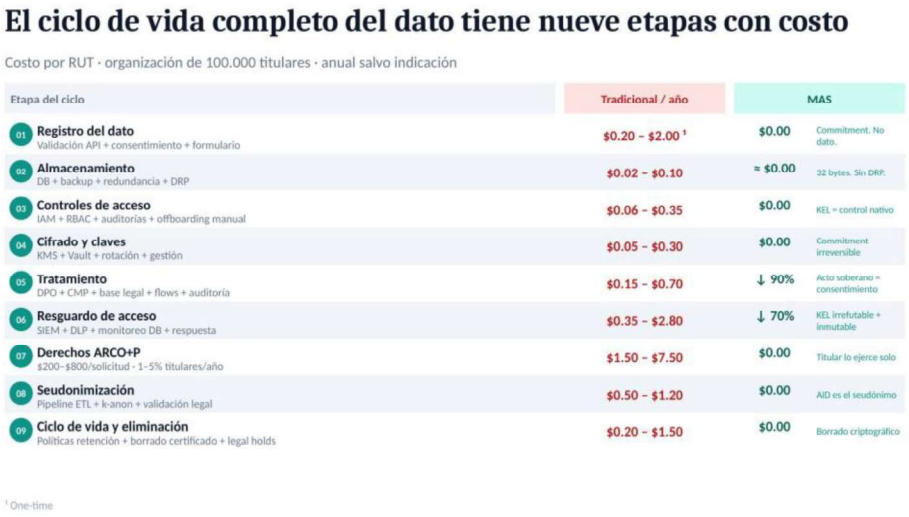
El precedente europeo

Desde que el Reglamento General de Protección de Datos entró en vigor en Europa en mayo de 2018, las multas acumuladas por las autoridades de protección de datos europeas superan los cuatro mil quinientos millones de euros.

Lo que hace ese número especialmente instructivo no es su magnitud — sino quiénes lo componen. Las multas más grandes no fueron impuestas a empresas que deliberadamente ignoraron la ley. Fueron impuestas a empresas que creían que estaban cumpliendo.

Meta recibió multas por más de mil millones de euros — no porque no tuviera sistemas de gestión de consentimiento, sino porque esos sistemas no generaban consentimiento válido en los términos que la ley exige. Google, Amazon, WhatsApp — todos con equipos legales de primer nivel, todos con recursos para implementar cualquier sistema disponible — fueron sancionados por las mismas razones.

El análisis del ciclo de vida completo del dato personal muestra que el riesgo regulatorio es solo uno de los nueve ítems de costo. La imagen que sigue ilustra cada etapa — desde el registro hasta la eliminación certificada — y el diferencial entre el modelo tradicional de custodia y el Protocolo MAS.



El ciclo de vida completo del dato tiene nueve etapas con costo

Costo por RUT · organización de 100.000 titulares · anual salvo indicación

Etapa del ciclo	Tradicional / año	MAS	
01 **Registro del dato** Validación API + consentimiento + formulario	$0.20 – $2.00 [1]	$0.00	Commitment. No dato.
02 **Almacenamiento** DB + backup + redundancia + DRP	$0.02 – $0.10	≈ $0.00	32 bytes. Sin DRP.
03 **Controles de acceso** IAM + RBAC + auditorías + offboarding manual	$0.06 – $0.35	$0.00	KEL = control nativo
04 **Cifrado y claves** KMS + Vault + rotación + gestión	$0.05 – $0.30	$0.00	Commitment irreversible
05 **Tratamiento** DPO + CMP + base legal + flows + auditoría	$0.15 – $0.70	↓ 90%	Acto soberano = consentimiento
06 **Resguardo de acceso** SIEM + DLP + monitoreo DB + respuesta	$0.35 – $2.80	↓ 70%	KEL irrefutable + inmutable
07 **Derechos ARCO+P** $200–$800/solicitud · 1–5% titulares/año	$1.50 – $7.50	$0.00	Titular lo ejerce solo
08 **Seudonimización** Pipeline ETL + k-anon + validación legal	$0.50 – $1.20	$0.00	AID es el seudónimo
09 **Ciclo de vida y eliminación** Políticas retención + borrado certificado + legal holds	$0.20 – $1.50	$0.00	Borrado criptográfico

[1] One-time

Figura 1 — Las nueve etapas del ciclo de vida del dato y su costo por titular · Modelo tradicional vs. Protocolo MAS · Org. referencia: 100.000 titulares

La lección del precedente europeo no es que las empresas grandes son el objetivo. La lección es que la calidad de la evidencia — no la existencia de un sistema — es lo que determina la sanción.

> *Las empresas europeas más multadas no carecían de sistemas de compliance. Carecían de evidencia irrefutable de que sus sistemas funcionaban como la ley exige.*

Lo que la APDP va a necesitar demostrar

La Agencia de Protección de Datos Personales de Chile va a necesitar, como toda institución regulatoria nueva, establecer su autoridad con las primeras fiscalizaciones. Las sanciones ejemplares de los primeros años son una constante en la historia de las agencias regulatorias.

Eso no significa que cualquier empresa será sancionada. Significa que las primeras empresas fiscalizadas van a ser examinadas con un nivel de escrutinio que la mayoría no anticipa. Y que el criterio de evaluación no va a ser "¿tiene un sistema?", sino "¿puede demostrar que ese sistema produce evidencia válida?"

A escala de 250.000 titulares activos con perfil completo, el costo anual de custodia en el modelo tradicional se sitúa entre 4,25 y 8,75 millones de dólares,

solo en gestión directa de datos, antes de cualquier incidente. Con el Protocolo MAS, ese mismo universo cuesta menos de 38.000 dólares anuales — una reducción del 99,6%. La imagen siguiente muestra esa comparación.

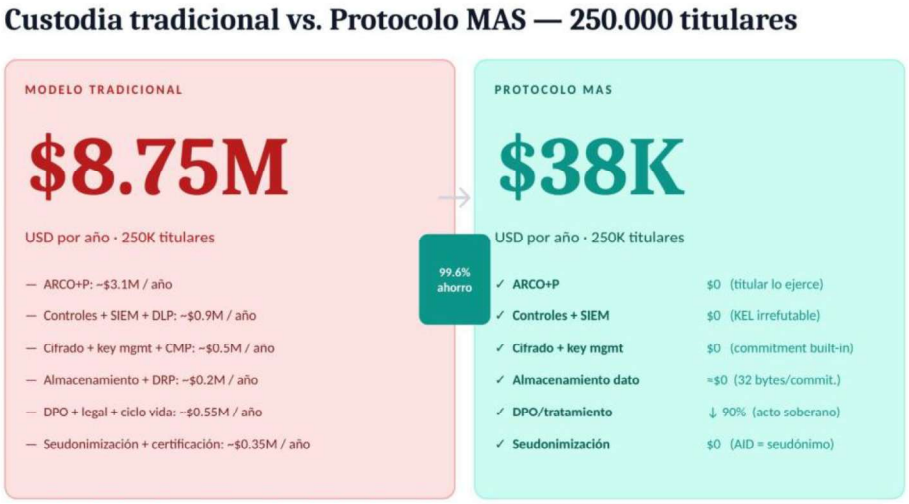


Figura 2 — Costo anual de custodia de datos · 250.000 titulares · Custodia tradicional: $8,75M USD · Protocolo MAS: $38K USD · Ahorro: 99,6%

La diferencia entre una empresa que puede responder afirmativamente a esa segunda pregunta y una que solo puede responder a la primera es, potencialmente, la diferencia entre una sanción y una exoneración.

El costo de esa diferencia, para una empresa mediana chilena, puede ser de cien mil a cuatrocientos mil dólares. Por infracción.

El costo de generar evidencia irrefutable desde el origen — de construir un sistema donde el acto del titular sea la fuente de la prueba — es significativamente menor. Y produce, además, el único sistema que resiste el escrutinio regulatorio más exigente.

* * *

Las multas que nadie está calculando bien no son las multas de la ley. Son las multas de una fiscalización real, ante una reclamación concreta, con evidencia cuestionable.

Esas multas son más probables de lo que la mayoría anticipa. Y más costosas de lo que la mayoría ha calculado.

La pregunta relevante no es si su empresa tiene un sistema de gestión de consentimiento. Es si ese sistema produce evidencia que resiste el escrutinio de quien tiene autoridad para sancionarla.

Si la respuesta es incierta — este libro es para usted.

▸ **Profundidad técnica — Análisis de los casos europeos más relevantes**

El caso Meta Ireland (2023, €1.200 millones) es el más instructivo para el contexto chileno. La sanción no fue por ausencia de sistemas de consentimiento — Meta tiene sistemas sofisticados. Fue por la base legal usada para el tratamiento: Meta argumentaba "interés legítimo" donde la ley requería consentimiento explícito. La evidencia de que el consentimiento fue obtenido no era suficiente para el estándar que el GDPR exige.

El caso Google LLC (Francia, 2019, €50 millones) es aún más relevante: Google tenía sistemas de consentimiento, pero la información sobre el uso de los datos era insuficientemente clara y el consentimiento no era suficientemente específico. La autoridad francesa determinó que los clics de "acepto" en interfaces confusas no constituyen consentimiento válido.

La implicación directa para Chile: un checkbox marcado, sin evidencia criptográfica de que el titular específico lo marcó de forma informada y libre, es vulnerable al mismo tipo de cuestionamiento. La Ley 21.719 es conceptualmente similar al GDPR en sus requisitos de validez del consentimiento.

Capítulo 4

La ilusión del cumplimiento

Existe una categoría de problema que es especialmente difícil de resolver: el problema que parece resuelto.

El mercado de gestión de datos personales tiene soluciones maduras, costosas, bien implementadas, ampliamente adoptadas. OneTrust tiene más de catorce mil clientes. TrustArc lleva décadas en el mercado. Hay docenas de plataformas locales y regionales que prometen cumplimiento regulatorio.

Esas plataformas hacen muchas cosas bien. Ordenan los procesos internos. Centralizan la gestión de políticas. Generan reportes para auditores. Facilitan el trabajo del Delegado de Protección de Datos. Reducen la fricción en la gestión de solicitudes ARCO+P.

Pero todas tienen el mismo defecto de origen que describimos en el capítulo anterior: la evidencia del acto vive en sus servidores. Y eso significa que todas producen, en el mejor de los casos, cumplimiento aparente — no evidencia irrefutable.

Lo que las soluciones existentes hacen

Las plataformas de gestión de consentimiento actuales fueron diseñadas para resolver un problema de eficiencia operacional: cómo gestionar, a escala, las obligaciones de una organización respecto a los datos personales de sus titulares.

Ese es un problema real y válido. Y lo resuelven bien. Permiten configurar flujos de consentimiento, gestionar versiones de políticas, trackear el estado de las solicitudes ARCO+P, generar reportes consolidados, integrarse con los sistemas de marketing y CRM de la organización.

El problema es que el diseño completo está orientado hacia adentro de la organización. El titular aparece como el destinatario de formularios — no como el actor que los genera. La evidencia del acto es un registro en el sistema de la organización — no una firma del titular.

Cuando se le pregunta a un sistema de este tipo "¿puede demostrar que Juan Pérez consintió?", la respuesta es: "El sistema registra que Juan Pérez marcó el checkbox el 15 de marzo de 2024 desde la IP 192.168.x.x con el navegador Safari versión 17."

Eso es todo lo que puede demostrar. Que hay un registro. Que el sistema lo generó. Que alguien — desde esa IP, en ese momento, con ese navegador — marcó ese checkbox.

No puede demostrar que fue Juan Pérez. No puede demostrar que no fue otro sistema el que hizo el clic. No puede demostrar que el registro no fue modificado posteriormente. No puede demostrar nada más allá de lo que el propio sistema dice sobre sí mismo.

El problema de escala

Hay otro problema que las soluciones existentes no resuelven — y que raramente se menciona en los catálogos de productos.

El mercado de gestión de datos personales está segmentado en dos: las grandes empresas que pueden pagar entre diez y cincuenta mil dólares anuales por plataformas internacionales, y el resto.

El "resto" es el 95% del mercado empresarial chileno. Pequeñas y medianas empresas, consultorios médicos, estudios jurídicos, centros educacionales, comercios — todos obligados por la Ley 21.719, ninguno con el presupuesto para las soluciones de referencia del mercado.

Lo que ese 95% hace hoy es improvisación: formularios de Google, hojas de Excel, procesos manuales, declaraciones en papel. Nada que produzca evidencia válida. Nada que resista una fiscalización.

La brecha entre el texto de la ley y la realidad del mercado es, para ese 95%, absoluta.

> *El cumplimiento regulatorio no debería ser un privilegio de las empresas que pueden pagar cincuenta mil dólares al año. Debería*

> *ser accesible para quien trata datos personales — independientemente de su tamaño.*

Lo que ninguna solución existente puede hacer

Hay algo que ninguna de las plataformas existentes — independientemente de su precio, su sofisticación o sus años de desarrollo — puede hacer.

No pueden hacer que la evidencia del acto provenga del titular.

No porque no quieran. Sino porque están construidas sobre una arquitectura donde el titular es un objeto del sistema — no un actor del sistema. Cambiar eso no es una actualización de funcionalidades. Es un cambio de arquitectura completo.

Una plataforma de gestión de consentimiento construida para registrar lo que las empresas hacen con los datos no puede, con una actualización de software, convertirse en un sistema donde el titular genera la evidencia de sus propios actos. Son arquitecturas incompatibles.

Eso significa que el mercado no está esperando que alguien mejore las soluciones existentes. Está esperando que alguien construya algo diferente desde el origen.

Ese es el punto de partida de lo que sigue en este libro.

* * *

La ilusión del cumplimiento es cómoda. Da a las organizaciones la sensación de que el problema está resuelto, que los formularios están configurados, que los procesos están documentados, que el sistema genera los reportes que el auditor necesita.

No es una ilusión malintencionada. Es el resultado de construir soluciones para el problema que los compradores de tecnología empresarial saben articular — y no para el problema que el regulador les va a plantear cuando fiscalice.

El problema que el regulador va a plantear no es "¿tiene un sistema?". Es "¿puede demostrar que ese sistema produce evidencia válida del acto del titular?"

La respuesta a esa segunda pregunta requiere una arquitectura diferente. Una donde la evidencia no provenga del sistema de la empresa — sino del acto del titular.

Esa arquitectura es el tema de la Parte II.

▸ Profundidad técnica — Comparativa de arquitecturas de consentimiento

Existen tres arquitecturas básicas para la gestión de consentimiento digital, con diferentes niveles de solidez probatoria:

Arquitectura 1 — Registro de comportamiento: El sistema registra que un usuario realizó una acción (clic, submit, scroll). La evidencia es un log en la base de datos de la empresa. Nivel probatorio: débil. Disputable por definición.

Arquitectura 2 — Firma electrónica simple: El sistema genera una firma sobre el registro usando la identidad del usuario en el sistema (correo, ID de usuario). La evidencia incluye una firma, pero la llave privada la custodia el sistema, no el usuario. Nivel probatorio: moderado. Mejor que el registro puro, pero aún dependiente del sistema.

Arquitectura 3 — Firma criptográfica soberana: El usuario genera la evidencia con una llave privada que solo él posee. La firma es verificable por cualquier tercero. El conflicto de interés desaparece porque la fuente de la evidencia es el propio usuario. Nivel probatorio: máximo. Irrefutable matemáticamente.

Ninguna plataforma comercial disponible a escala implementa la Arquitectura 3. OwnTrust es, en este contexto, una implementación de la Arquitectura 3 con el adicional de que la llave privada del usuario es efímera — no existe almacenada en ningún lugar — y se reconstituye en cada sesión a partir de los datos del documento de identidad y el secreto personal del titular.

—

Fin de la Parte I

La Parte II — El modelo — comienza en el capítulo siguiente.

PARTE II

El modelo

La solución no es hacer más confiables los registros de las empresas. Es cambiar quién genera la evidencia del acto.

— Del capítulo anterior

Capítulo 5

Memoria cero

Hay una pregunta que ningún sistema de identidad digital ha respondido satisfactoriamente: ¿qué debería hacer un sistema con los datos de identidad del titular una vez que los ha procesado?

La respuesta que la industria ha dado históricamente es: guardarlos. Crear un perfil. Enriquecer la base de datos. Usar esa información para personalizar, segmentar, mejorar el servicio, hacer más eficiente el proceso la próxima vez.

Esa respuesta tiene una lógica operacional impecable. Y produce, como consecuencia inevitable, que la identidad del titular viva en los servidores de cada sistema con el que ha interactuado. Fragmentada. Replicada. Fuera de su control.

La pregunta que nos hicimos fue diferente: ¿qué pasa si la respuesta correcta es destruirlos?

El principio de la identidad efímera

Existe una distinción fundamental entre dos cosas que la industria trata como equivalentes: la identidad del titular y la evidencia del acto del titular.

La identidad del titular — quién es, qué datos tiene su documento, cuál es su RUT — es información que el sistema necesita para verificar que la persona es quien dice ser. Una vez hecha esa verificación, esa información no tiene ningún propósito adicional que justifique su almacenamiento.

La evidencia del acto — que el titular firmó algo, que ejerció un derecho, que otorgó un consentimiento — es información que necesita persistir. Es la razón por la que el sistema existe. Es lo que tiene valor probatorio. Es lo que el titular y la organización necesitan que quede registrado.

La confusión entre estas dos cosas — tratar la identidad del titular como si fuera evidencia del acto, y almacenarla porque "podría ser útil" — es la raíz del problema que describimos en la Parte I.

La arquitectura de memoria cero separa estas dos cosas con precisión quirúrgica: la identidad se usa — en milisegundos, en el momento preciso en que se necesita — y luego se destruye. La evidencia del acto se preserva — permanentemente, de forma inmutable, verificable por cualquier tercero.

> *La identidad no necesita vivir en ningún servidor. Necesita existir el tiempo suficiente para firmar la verdad del acto. Después, lo único que importa es la firma — no quien la hizo.*

Por qué la memoria cero es una ventaja — no una limitación

La primera reacción de cualquier arquitecto de sistemas al escuchar "memoria cero" es la misma: ¿cómo funciona si no recuerda nada?

Es la pregunta equivocada. La pregunta correcta es: ¿qué necesita recordar y qué no?

Un sistema de identidad necesita recordar que Juan Pérez firmó el consentimiento el 15 de marzo de 2024. No necesita recordar el RUT de Juan Pérez, su fecha de nacimiento, el número de su documento de identidad. Esa información fue el medio para verificar que era él. No es el fin.

La arquitectura de memoria cero recuerda exactamente lo que necesita recordar — la evidencia del acto — y destruye exactamente lo que no necesita — la identidad que sirvió para producirla.

El resultado es un sistema que es, paradójicamente, más poderoso en lo que importa y más liviano en lo que no. Más poderoso porque la evidencia que produce es irrefutable — no un log de base de datos sino una firma criptográfica del propio titular. Más liviano porque no acumula la carga operacional, legal y de seguridad de custodiar millones de identidades.

Un sistema de memoria cero no puede ser hackeado para robar identidades. Porque no las tiene.

Esa no es una limitación. Es la ventaja más poderosa del modelo.

Lo que el titular siente

Desde la perspectiva del titular, la arquitectura de memoria cero es transparente.

Llega a OwnTrust con su cédula de identidad. Ingresa cuatro datos que están impresos en ella. El sistema los procesa en milisegundos. Genera su identidad soberana. Le permite firmar el acto que necesita firmar. Y cuando termina, esos datos desaparecen.

El titular no tiene que crear una cuenta. No tiene que elegir una contraseña. No tiene que instalar una aplicación. No tiene que recordar credenciales. No tiene que preocuparse de que sus datos están almacenados en algún servidor que podría ser comprometido.

Lo que tiene que traer es lo que siempre ha tenido: su cédula de identidad.

Y lo que tiene que recordar — a partir de la primera vez — es su secreto personal. Un texto libre. Lo que quiera. Lo que solo él recuerda. No una contraseña de ocho caracteres con mayúscula y número. Algo suyo.

La próxima vez que llegue a OwnTrust no necesitará la cédula. Solo su secreto. Treinta segundos. El acto firmado. Todo destruido excepto la evidencia.

* * *

La memoria cero no es una característica técnica. Es una declaración filosófica sobre cuál es el propósito de un sistema de identidad digital.

Su propósito no es conocer al titular. Es permitirle actuar soberanamente. Y una vez que actuó, preservar la evidencia de ese acto. Nada más.

Todo lo que va más allá de ese propósito — almacenar la identidad, enriquecer el perfil, recordar los datos para la próxima vez — es una decisión de conveniencia operacional que tiene un costo que la industria ha ignorado sistemáticamente: el costo de custodiar lo que no necesita custodiar.

OwnTrust no custodia identidades. Custodia verdades.

▸ Profundidad técnica — ADN, AID e IS: los tres identificadores del sistema

La arquitectura de memoria cero opera con tres identificadores distintos, cada uno con un propósito específico y un ciclo de vida diferente.

El ADN es el identificador primario de sesión. Se calcula localmente en el navegador del titular mediante una función hash criptográfica de estándar internacional aplicado a los cuatro datos del documento más una sal interna de Axenkor que nunca sale de sus servidores. El ADN existe solo durante la sesión — segundos o minutos — y se destruye al terminar. Nadie lo almacena. Nadie puede reconstruirlo sin los cuatro datos originales y la sal.

El AID — Identificador Soberano — se deriva del ADN mediante derivación criptográfica estándar. Es el identificador que aparece en el KEL. Es efímero en la sesión pero permanente en el registro: el KEL lo contiene, pero el AID en sí no revela ningún dato personal del titular. Es un hash de un hash — sin posibilidad de ingeniería inversa hacia el RUT o cualquier dato del documento.

El IS — Índice Estable — se calcula como una derivación criptográfica adicional sobre el identificador del titular de Axenkor. Nunca sale de los servidores de Axenkor. Su propósito es vincular los diferentes AIDs del titular a lo largo del tiempo — cuando renueva su cédula, cuando cambia de dispositivo — sin exponer ningún dato personal. Es el hilo invisible que mantiene la coherencia del historial soberano del titular.

Los tres identificadores operan en capas: el ADN es la semilla efímera, el AID es la evidencia pública del acto, el IS es el índice privado de la continuidad. Juntos permiten un sistema que no almacena identidades pero sí mantiene el historial de actos soberanos del titular de forma coherente y verificable.

Capítulo 6

La cédula como llave efímera

La cédula de identidad es el objeto físico más poderoso que la mayoría de las personas tiene. Emitida por el Estado. Con elementos de seguridad que ningún particular puede replicar fácilmente. Con datos únicos que identifican a una persona de forma inequívoca en el sistema civil de un país.

Y sin embargo, el mundo digital la ha ignorado casi completamente como mecanismo de identidad.

Los sistemas de identidad digital han elegido, casi sin excepción, construir sus propios mecanismos: nombres de usuario, contraseñas, preguntas de seguridad, códigos de un solo uso, autenticación de dos factores con aplicaciones propietarias. Cada uno de estos mecanismos crea una nueva capa de datos que el usuario debe gestionar, que el sistema debe custodiar, y que puede ser comprometida.

La cédula, mientras tanto, permanece en el bolsillo del titular. Infrautilizada. Ignorada por el mundo digital. Usada únicamente cuando hay que cruzar una frontera o abrir una cuenta bancaria en persona.

Por qué la cédula es la llave correcta

Hay cuatro razones por las que la cédula de identidad es el mecanismo de autenticación más adecuado para la identidad digital soberana.

La primera es la universalidad. En Chile, prácticamente toda persona mayor de edad tiene cédula de identidad. No hay que crear una nueva infraestructura de identidad. No hay que distribuir tokens de hardware. No hay que instalar aplicaciones. La llave ya existe — en el bolsillo del titular.

La segunda es la especificidad. Los cuatro datos del documento — RUT, número de documento, fecha de nacimiento, fecha de vencimiento — son únicos para cada persona y cada emisión del documento. Su combinación exacta no es

replicable sin el documento físico o acceso a información que no está disponible públicamente.

La tercera es la trazabilidad institucional. La cédula es emitida por el Registro Civil, bajo procedimientos verificables, con historia documentada. Cuando alguien usa su cédula, hay un ancla institucional detrás de ese acto que ningún sistema de credenciales digitales puede igualar.

La cuarta — y más importante — es la soberanía. La cédula pertenece al titular. No a una empresa. No a un sistema. No a una plataforma. Si OwnTrust desaparece mañana, el titular sigue teniendo su cédula. Y con ella, puede reconstituir su identidad soberana en cualquier sistema que use el mismo protocolo.

El Agente IA que verifica sin retener

La cédula de identidad, sin embargo, tiene un problema cuando se usa en el contexto digital: cualquiera puede escribir los datos de la cédula de otro. El número de RUT está en registros públicos. La fecha de nacimiento no es un secreto. El número de documento podría ser conocido por quien tuvo acceso al documento físico.

Por eso el uso de la cédula en OwnTrust no termina con el ingreso de los cuatro datos. Termina con la verificación visual del documento.

En el génesis — la primera vez que el titular accede al sistema — y en los momentos críticos que lo requieren, el titular fotografía su cédula. Anverso y reverso. El sistema procesa esas imágenes con un agente de inteligencia artificial especializado en documentos de identidad chilenos, que verifica en menos de tres segundos que el documento es auténtico, que los datos ingresados coinciden con lo que el documento muestra, que no es una impresión en papel, que no es una pantalla fotografiada, que los elementos de seguridad están presentes.

Con una certeza del 98 por ciento o superior, el sistema determina si el documento es válido.

Y luego — esto es crítico — la imagen se destruye.

No se almacena en ningún servidor. No se indexa en ninguna base de datos. No contribuye a ningún perfil biométrico. Existe en memoria por un máximo de cinco segundos. El sistema recibe solo el resultado: válida o inválida, con su nivel de certeza. Y la imagen desaparece.

> *La foto de la cédula existe el tiempo necesario para demostrar que el documento es real. Después desaparece. Como debería ser.*

Los cinco momentos

La imagen de la cédula no se pide en cada acceso. Eso sería insoportablemente invasivo y contradice el principio de proporcionalidad que debe guiar cualquier sistema de privacidad.

La imagen se pide exactamente en cinco momentos, y en ningún otro.

El primero es el génesis: la primera vez que el titular accede al sistema. Es el momento fundacional. La cédula establece la confianza inicial. El titular define su secreto personal. La identidad soberana queda constituida.

El segundo es el re-génesis: cuando el titular cambia de dispositivo o renueva su cédula. El documento cambió — es necesario verificar nuevamente que la persona es la misma.

El tercero es la recuperación: cuando el titular olvida su secreto personal. La cédula es el mecanismo de respaldo — el único mecanismo de respaldo. Si no tiene la cédula, no puede recuperar el acceso.

El cuarto es el acto de alto impacto: cuando el acto que el titular va a firmar tiene consecuencias irreversibles. Revocar todos sus consentimientos activos. Ejercer el derecho de supresión total. Actos que no tienen marcha atrás y que merecen el nivel más alto de verificación.

El quinto es el acto crítico declarado: cuando la organización determina que un acto específico — un procedimiento médico mayor, una modificación contractual significativa, una autorización de alto riesgo — requiere verificación reforzada.

En todos los demás casos — que son la inmensa mayoría — el titular necesita solo su secreto personal. Treinta segundos. Sin foto. Sin fricción.

* * *

La cédula de identidad lleva décadas en el bolsillo del titular, ignorada por el mundo digital. No porque no fuera útil — sino porque nadie había encontrado la forma de usarla sin convertirla en una carga.

La carga es la retención. Si el sistema guarda la foto de la cédula, guarda datos biométricos. Si guarda los datos del documento, guarda información personal sensible. Si guarda el historial de verificaciones, construye un perfil.

La solución es usar la cédula sin retenerla. Verificar sin almacenar. Establecer la confianza sin custodia.

Eso es lo que hace la arquitectura de memoria cero con el documento de identidad más poderoso que el titular ya tiene.

▸ Profundidad técnica — El proceso de verificación del documento

En la versión 1, la verificación de la imagen se realiza mediante un servicio externo de verificación de identidad especializada — AWS herramientas de análisis de imagen, Google Document AI o Incode — con un Acuerdo de Procesamiento de Datos firmado que garantiza la destrucción inmediata de la imagen. La API recibe la imagen, la procesa, y devuelve solo el resultado: válida o inválida, con un score de certeza. El tiempo de vida de la imagen en el proveedor externo es de tres a cinco segundos.

La versión 2 implementará un modelo WASM propio entrenado por Axenkor sobre un dataset de documentos chilenos. Este modelo correrá completamente en el navegador del titular — la imagen nunca saldrá del dispositivo. La certeza estimada para esta versión es entre el 95 y el 97 por ciento, ligeramente inferior a la API externa pero con la ventaja de soberanía total: ningún tercero ve la imagen en ningún momento.

El agente verifica seis atributos: autenticidad del soporte (no es papel impreso ni pantalla), coherencia de los datos ingresados con los visibles en la imagen, presencia de elementos de seguridad (hologramas, microimpresión, guilloché), coherencia entre anverso y reverso (mismo documento, misma persona), calidad de la imagen (resolución suficiente, iluminación adecuada, documento completo), y ausencia de manipulación digital evidente.

El resultado que llega a OwnTrust es un certificado digital con tres campos: válida (booleano), score (número entre 0 y 1), y tipo_documento (string que identifica la versión de la cédula chilena). La imagen en sí nunca llega a los servidores de OwnTrust en ninguna versión del sistema.

Capítulo 7

El secreto que nadie conoce

Después de verificar el documento, el sistema pide algo que ningún otro sistema pide de la misma manera: un secreto personal.

No una contraseña. No un PIN de seis dígitos. No la respuesta a "¿cuál es el nombre de tu primera mascota?". Un secreto personal — texto libre — lo que el titular quiera escribir. Sin reglas de formato. Sin requisitos de longitud mínima. Sin obligación de incluir mayúsculas, números o caracteres especiales.

La primera vez. Solo la primera vez. Y nunca más se le pedirá que lo repita en ese contexto de génesis.

A partir de ese momento, ese secreto es la única llave que el titular necesita para acceder a OwnTrust y firmar sus actos soberanos. No su cédula. No sus datos. Solo el secreto.

Por qué texto libre

La decisión de usar texto libre en lugar de una contraseña con formato definido no es casual. Es el resultado de entender cómo funciona la memoria humana y qué tipo de secreto es verdaderamente soberano.

Las contraseñas con formato definido — ocho caracteres, mayúscula, número, símbolo — son fáciles de olvidar y difíciles de personalizar. El resultado es que la mayoría de las personas usa las mismas contraseñas en múltiples sistemas, las escribe en algún lugar, o las delega en un gestor de contraseñas. Ninguna de esas prácticas es soberana.

Un secreto personal en texto libre puede ser cualquier cosa que el titular recuerde sin esfuerzo porque tiene significado para él. Una frase. Una palabra en un idioma que solo él habla. El nombre de un lugar que solo él recuerda. El año de algo que solo él sabe. Una combinación de elementos que solo él conectaría.

Ese tipo de secreto no necesita ser escrito en ningún lado. No necesita ser recordado con esfuerzo. No puede ser adivinado por quien no conoce al titular. Y no puede ser revelado por OwnTrust — porque OwnTrust no lo conoce.

El secreto que OwnTrust no puede leer

Esta afirmación requiere explicación, porque es contraintuitiva: el titular ingresa su secreto en el sistema, y el sistema no puede leerlo.

No es un eufemismo. Es una descripción técnica precisa.

Cuando el titular ingresa su secreto en el génesis, ese secreto nunca viaja a los servidores de OwnTrust en claro. Se usa localmente, en el navegador del titular, para cifrar un fragmento aleatorio. Lo que llega al servidor de OwnTrust es el resultado cifrado — no el secreto.

El servidor de OwnTrust almacena ese resultado cifrado. Pero sin el secreto original — que nunca llegó al servidor — no puede descifrar nada. La clave para descifrar el fragmento es el secreto, y el secreto solo lo tiene el titular.

La organización que usa OwnTrust nunca ve el secreto. Los ingenieros de Axenkor nunca ven el secreto. Si los servidores de OwnTrust son comprometidos, el atacante obtiene fragmentos cifrados que no puede descifrar sin el secreto del titular.

Eso es soberanía real. No la promesa de que el sistema cuida el secreto. La garantía matemática de que el sistema no puede conocerlo.

> *La organización conoce los datos del titular. OwnTrust procesa esos datos. Nadie conoce el secreto del titular. Eso es lo que hace la diferencia.*

Lo que el secreto habilita

El secreto personal no es solo un mecanismo de autenticación. Es la llave que habilita dos cosas simultáneamente, mediante el mismo método aplicado dos veces.

La primera es la validación de identidad. Cuando el titular ingresa su secreto, el sistema puede verificar que es el mismo titular que definió ese secreto en el génesis — sin almacenar el secreto, sin transmitirlo, sin exponerlo a ningún tercero. Si el secreto es correcto, la identidad está verificada.

La segunda es la firma soberana. Una vez verificada la identidad, el sistema puede firmar el acto que el titular quiere firmar — con una firma criptográfica que ningún otro puede producir, que nadie puede negar, que cualquier tercero puede verificar.

El secreto no hace ambas cosas directamente. Las habilita mediante el método del billete partido — que es el tema del capítulo siguiente.

* * *

Hay algo profundamente correcto en la arquitectura del secreto personal.

Los sistemas de identidad digital han fallado históricamente no porque la tecnología sea insuficiente — sino porque han tratado de resolver un problema humano con soluciones puramente técnicas. Han creado credenciales que los humanos no pueden recordar, procesos que los humanos no pueden entender, y mecanismos que los humanos terminan subvirtiendo con prácticas inseguras.

El secreto personal en texto libre reconoce que la memoria humana funciona mejor con significado que con formato. Que un secreto que tiene sentido para el titular es más seguro que una contraseña aleatoria — porque el titular lo recuerda sin esfuerzo y por eso nunca necesita escribirlo.

La soberanía real no requiere que el titular sea un experto en criptografía. Requiere que el sistema sea suficientemente honesto para admitir que el titular es el único que debería conocer su propio secreto.

▸ Profundidad técnica — Cómo el secreto se convierte en billete partido

En el génesis, cuando el titular define su secreto, el sistema ejecuta el siguiente proceso localmente en el navegador:

1. Se generan dos fragmentos aleatorios de 256 bits mediante un generador criptográficamente seguro de números aleatorios (CSPRNG). Estos fragmentos — el primer componente de identidad y el segundo componente de identidad — no se derivan del secreto. Son completamente aleatorios.

2. El secreto del titular se usa como llave para calcular el valor esperado: valor_esperado = una función de derivación criptográficaHA256(el segundo componente de identidad, una función de derivación criptográficaHA256(el primer componente de identidad, secreto)). Este valor esperado se almacena en OwnTrust. El secreto no se almacena en ningún lugar.

3. el primer componente de identidad queda protegido con cifrado simétrico de grado militar usando el ADN efímero del titular como llave, y el resultado cifrado se almacena en OwnTrust indexado por el IS del titular. el segundo componente de identidad se almacena en la Bóveda Axenkor, también indexado por IS.

4. En cada acceso posterior, el titular ingresa su secreto. El sistema descifra el primer componente de identidad usando el ADN recalculado, recupera el segundo componente de identidad de la Bóveda, y calcula una función de derivación criptográficaHA256(el segundo componente de identidad, una función de derivación criptográficaHA256(el primer componente de identidad, secreto_ingresado)). Si el resultado coincide con el valor esperado almacenado, la identidad está verificada. Si no coincide, el acceso se deniega.

El secreto nunca viaja al servidor. El servidor nunca puede recalcular el valor esperado sin el secreto. La verificación ocurre sin exposición del secreto a ningún tercero.

Capítulo 8

El método del billete partido

Existe en criptografía un concepto elegante en su simplicidad y poderoso en sus implicaciones: el secreto compartido. La idea de que un secreto puede dividirse en partes de tal forma que ninguna de ellas, por sí sola, revela nada — pero que juntas reconstituyen el secreto original.

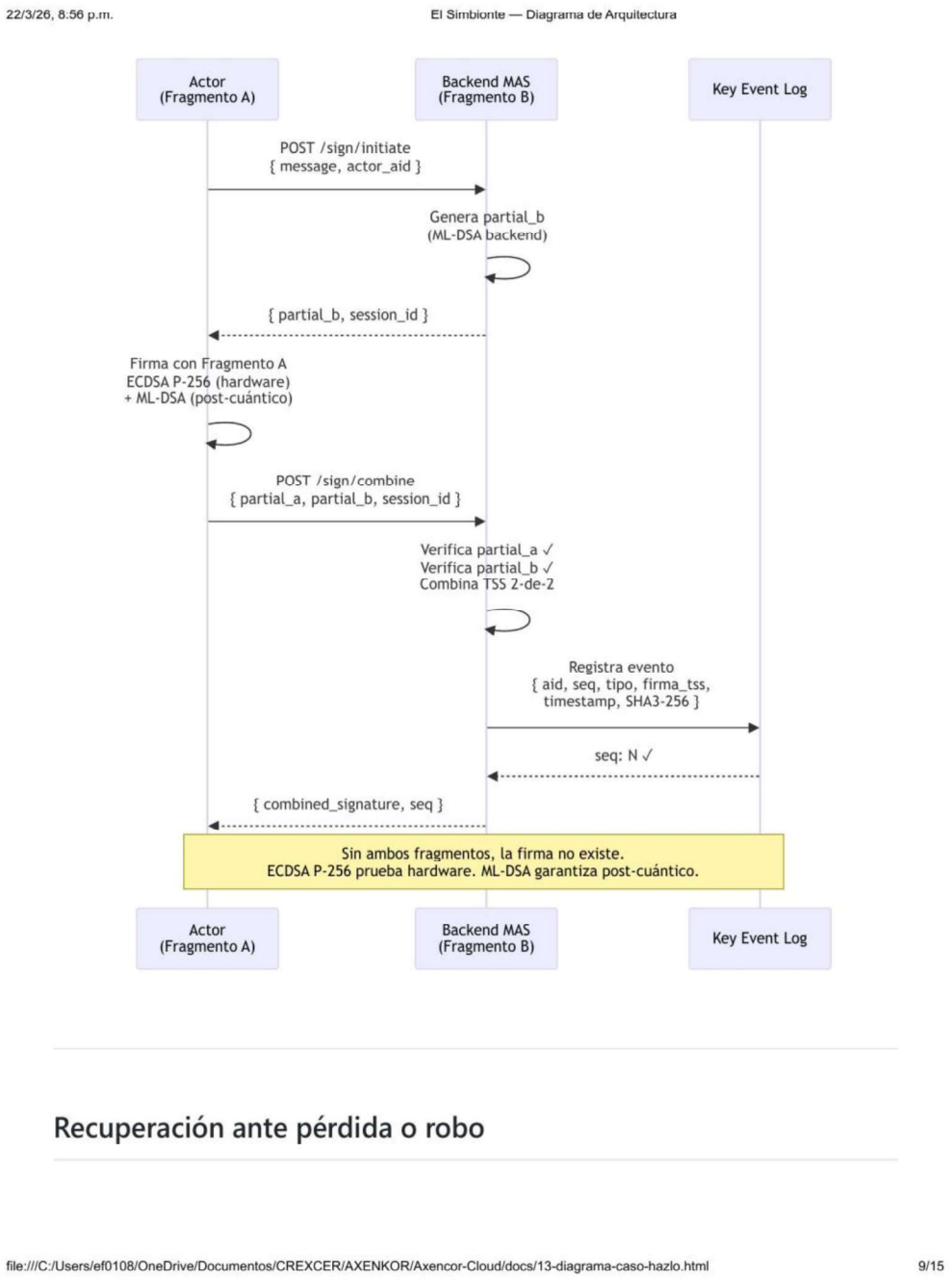


Figura 3 — Protocolo de firma TSS 2-de-2 · El Fragmento A (titular) y Fragmento B (Bóveda) co-firman sin reunirse jamás en el mismo lugar · ECDSA P-256 + ML-DSA FIPS 204 · Cada evento encadenado con SHA3-256

El billete partido es la aplicación de ese concepto al problema de la identidad soberana. Un billete — cualquier billete — puede cortarse en dos mitades. Cada mitad es inútil sin la otra. Juntas demuestran que las dos partes tenían, en algún momento, el mismo billete.

En OwnTrust, el método del billete partido se aplica dos veces. Con propósitos distintos. Con fragmentos distintos. Con resultados distintos. Pero con el mismo principio: ninguna mitad es suficiente — ambas son necesarias.

Dos instancias del mismo método

Es importante ser preciso aquí, porque la imprecisión lleva a confusiones que tienen consecuencias técnicas y legales.

No hay un billete partido en OwnTrust. Hay dos. Cada uno con sus propios fragmentos. Cada uno con su propio propósito. El método es el mismo — la instancia es diferente.

El primero es el billete partido del secreto. Sus dos fragmentos — llamados el primer componente de identidad y el segundo componente de identidad — sirven para un único propósito: verificar que quien ingresa el secreto es el mismo titular que lo definió en el génesis. Es un mecanismo de autenticación. Prueba identidad. No produce ninguna evidencia pública.

El segundo es el billete partido de la firma. Sus dos fragmentos — un componente de identidadF_A y un componente de identidadF_B — sirven para un único propósito diferente: generar la llave criptográfica efímera con la que el titular firma el acto soberano. Es un mecanismo de firma. Produce evidencia. Esa evidencia es pública y verificable por cualquier tercero.

La distinción no es trivial. El primer billete prueba que el titular es quien dice ser. El segundo billete produce la prueba de que el titular hizo lo que hizo. Son dos afirmaciones distintas, verificables de formas distintas, con consecuencias legales distintas.

> *El método del billete partido hace dos cosas en la misma sesión: primero valida que el secreto es correcto. Luego firma el acto con los fragmentos correspondientes. Un método. Dos instancias. En orden inamovible.*

La distribución de los fragmentos

Cada billete partido tiene cuatro fragmentos en total — dos por cada instancia del método. Y cada uno de esos fragmentos vive en un lugar diferente, bajo custodia de una entidad diferente.

Los fragmentos A — tanto del secreto como de la firma — viven en los servidores de OwnTrust, cifrados. OwnTrust los puede entregar al titular para que los use, pero no puede usarlos por sí mismo: para descifrar el primer componente de identidad se necesita el ADN efímero del titular, que OwnTrust nunca almacena. Para que un componente de identidadF_A produzca una firma, necesita combinarse con un componente de identidadF_B, que no está en OwnTrust.

Los fragmentos B — tanto del secreto como de la firma — viven en la Bóveda Axenkor, que es un sistema separado e independiente de OwnTrust. La Bóveda puede entregar el segundo componente de identidad y un componente de identidadF_B cuando recibe una solicitud válida, pero no puede generar ninguna firma por sí misma: le falta la mitad A de cada billete.

Para que el sistema funcione, las dos mitades de cada billete deben estar presentes simultáneamente, en la sesión del titular, durante los segundos que dura el proceso. Después se destruyen.

Ninguna entidad tiene todo lo que necesita. El titular necesita a OwnTrust y a la Bóveda. OwnTrust necesita al titular y a la Bóveda. La Bóveda necesita al titular y a OwnTrust. Si cualquiera de los tres falla — si los servidores de OwnTrust son comprometidos, si la Bóveda es atacada, si el secreto del titular es robado — el sistema no puede producir una firma válida.

Eso es lo que hace el billete partido más robusto que cualquier sistema de llave única: no existe un punto único de falla.

El orden inamovible

Hay una regla en la arquitectura del billete partido que no tiene excepciones: el billete de la firma nunca actúa sin que el billete del secreto haya validado primero.

Primero el secreto se verifica. Solo si la verificación es exitosa — solo si el titular demostró que conoce su secreto, que es quien dice ser — el sistema procede a generar la firma del acto.

La razón de esta regla es simple: la firma es irrevocable. Una vez que el acto queda registrado en el KEL con la firma del titular, esa evidencia existe permanentemente. No hay mecanismo de corrección. No hay manera de decir que la firma fue un error.

Por eso la autenticación previa no es opcional. Es la condición necesaria para que la firma tenga validez. Y es la condición que garantiza que nadie puede firmar en nombre del titular sin conocer su secreto.

El orden es: secreto válido — identidad verificada — acto firmado — evidencia permanente. Siempre. Sin excepciones.

* * *

El billete partido es elegante precisamente porque es simple en su concepto y poderoso en sus consecuencias.

No requiere hardware especial. No requiere que el titular entienda criptografía. No requiere que la organización confíe en OwnTrust ni que OwnTrust confíe en la organización. Requiere que cada parte tenga lo que le corresponde — y que ninguna tenga más de lo que necesita.

Esa arquitectura de mínimo privilegio — donde nadie tiene acceso a más de lo estrictamente necesario — es el principio más poderoso en el diseño de sistemas seguros. Y es el principio que el billete partido implementa de forma natural.

La próxima vez que alguien le pregunte cómo puede ser que un sistema tan poderoso no dependa de ningún actor central — la respuesta es el billete partido. Ningún actor tiene todo. Todos tienen algo. Y la verdad del acto emerge solo cuando todos contribuyen lo que les corresponde.

▸ Profundidad técnica — Los cuatro fragmentos y su ciclo de vida

En el génesis se generan los cuatro fragmentos mediante un generador criptográficamente seguro. el primer componente de identidad y un componente de identidadF_A se cifran con cifrado simétrico de grado militar usando el ADN efímero como llave y se almacenan en OwnTrust. el segundo componente de identidad y un componente de identidadF_B se almacenan en la Bóveda Axenkor, indexados por IS.

En cada sesión de acceso, el proceso de los cuatro fragmentos sigue este orden: (1) el primer componente de identidad se descifra localmente usando el ADN recalculado; (2) el segundo componente de identidad se recupera de la Bóveda; (3) el billete del secreto valida la identidad mediante función de autenticación criptográfica encadenado; (4) si la validación es exitosa, un componente de identidadF_A se descifra; (5) un componente de identidadF_B se recupera de la Bóveda; (6) el billete de la firma genera la llave firma digital de curva elíptica efímera mediante el protocolo el protocolo de firma umbral simplificado; (7) el acto se firma; (8) todos los fragmentos en claro, la llave efímera y el secreto se destruyen de memoria.

Un protocolo de firma umbral permitete generar una firma firma digital de curva elíptica estándar a partir de dos fragmentos que nunca se combinan completamente en ningún servidor — la combinación ocurre en la sesión efímera del titular. El resultado es una firma firma digital de curva elíptica estándar, verificable con cualquier implementación estándar de firma digital de curva elíptica, sin necesidad de OwnTrust ni de ningún componente propietario.

Capítulo 9

El acto soberano

Todo lo que hemos descrito hasta aquí — la memoria cero, la cédula efímera, el secreto personal, el billete partido — converge en un momento concreto y verificable: el acto soberano.

El acto soberano es el momento en que el titular firma. No hace clic en un checkbox. No envía un formulario. No registra una preferencia en la base de datos de una empresa. Firma — con una firma criptográfica que solo él puede producir, que nadie puede negar, que cualquier tercero puede verificar.

Ese momento dura treinta segundos. Lo que queda de ese momento dura para siempre.

Qué ocurre en esos treinta segundos

La experiencia del titular es simple. Ingresa su secreto. Lee el documento que va a firmar — y el sistema registra que lo leyó, midiendo el tiempo de exposición y verificando que hizo scroll hasta el final. Hace clic en firmar. El sistema produce la evidencia. Y en menos de un segundo, esa evidencia está en el KEL y en los sistemas de la organización.

Lo que ocurre debajo de esa experiencia simple es una cadena de pasos criptográficos que produce algo que ningún sistema anterior ha podido producir a esta escala: evidencia irrefutable de que este titular específico, en este momento específico, tomó esta decisión específica.

El billete del secreto valida que quien ingresó el secreto es el titular que lo definió en el génesis. El billete de la firma genera la llave efímera y firma el acto. El KEL registra ese acto con su timestamp, su hash encadenado al acto anterior, y la firma del titular. El certificado se genera y se envía a la organización.

Y luego todo desaparece. El secreto ingresado. Los fragmentos en claro. La llave efímera. El ADN calculado. La sesión termina sin rastro de quién fue el titular — solo con la verdad de lo que hizo.

La irreversibilidad como garantía

El acto soberano es irrevocable por diseño. Una vez que queda registrado en el KEL, no puede ser eliminado, modificado ni repudiado.

Esto puede sonar restrictivo. En realidad es la garantía más poderosa que el sistema ofrece — y opera en beneficio del titular tanto como de la organización.

Para el titular: ninguna organización puede negar que recibió su solicitud ARCO+P, que procesó su revocación de consentimiento, que firmó el contrato con las condiciones que el titular acordó. El acto quedó registrado. Nadie puede pretender que no ocurrió.

Para la organización: ningún titular puede negar que otorgó el consentimiento, que ejerció el derecho que dice haber ejercido, que firmó el documento con el contenido que el documento tenía. El acto quedó registrado con la firma del titular. Es irrefutable.

La irreversibilidad no es un defecto del sistema. Es la condición que hace que la evidencia tenga valor. Un registro que puede ser modificado no es evidencia — es una afirmación. Un registro que no puede ser modificado, firmado por quien lo generó, verificable por cualquier tercero, es evidencia en el sentido más estricto del término.

> *El titular firmó. La firma es irrefutable. El acto ocurrió. Eso es todo lo que el sistema necesita decir — y es todo lo que el regulador necesita escuchar.*

El certificado que no depende de nadie

Cada acto soberano produce un certificado. Un documento digital autocontenido que incluye todo lo necesario para verificar que el acto ocurrió, quién lo firmó, cuándo, sobre qué, y bajo qué condiciones.

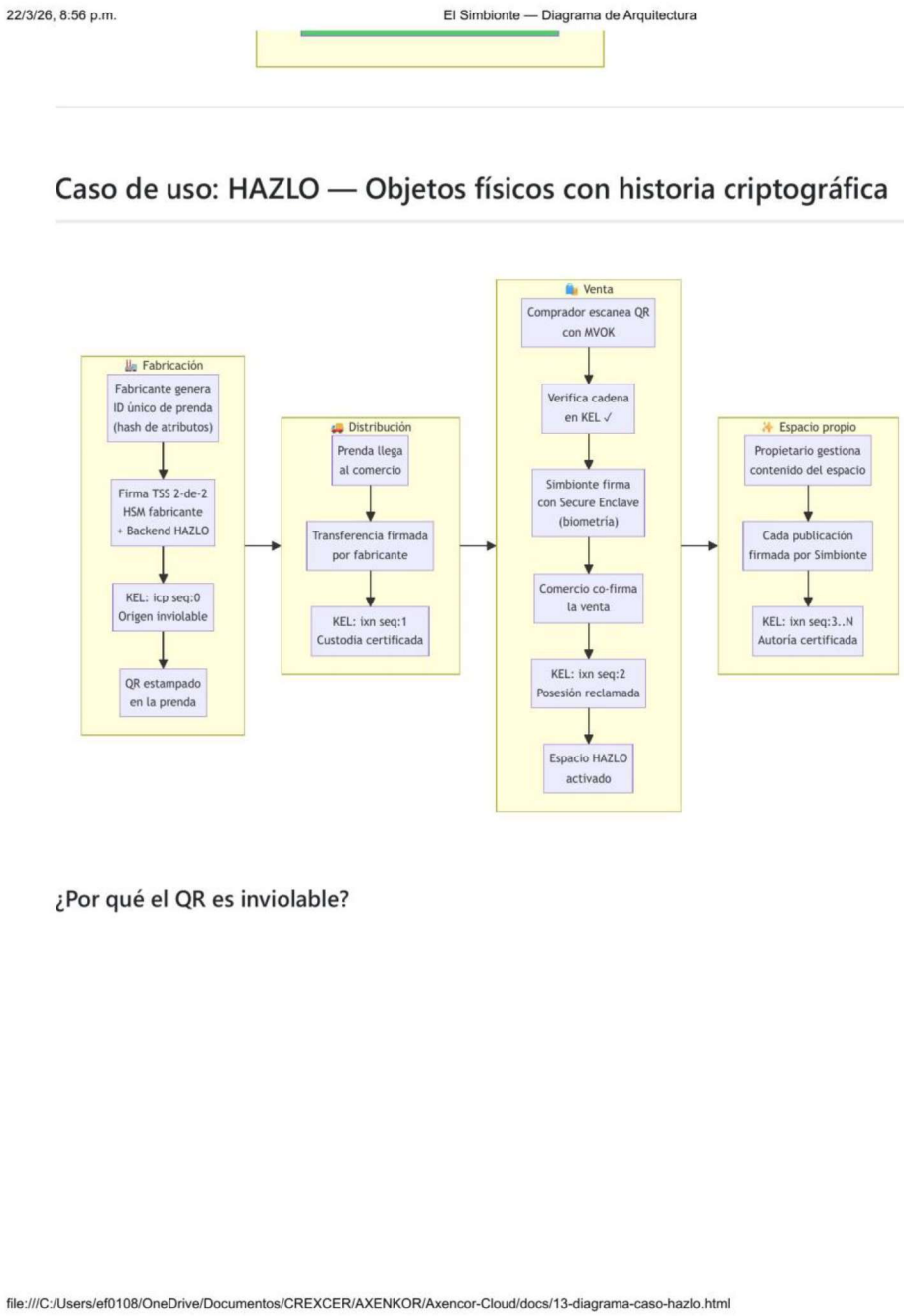


Figura 4 — El acto soberano en contexto HAZLO · Cada etapa de la vida de un objeto físico (fabricación, distribución, venta, posesión, publicación) es un acto firmado soberanamente que queda en el KEL · La cadena de custodia es irrefutable

El certificado incluye el identificador soberano del titular — no su nombre, no su RUT, no ningún dato personal. Incluye la identificación de la organización. Incluye el hash de la política o documento que fue firmado — no el documento en sí, sino una huella digital que permite verificar que no fue modificado después.

Incluye el registro en el KEL — su posición en la cadena, su hash propio, el hash del acto anterior. Incluye la firma criptográfica del billete de la firma.

E incluye las instrucciones para verificarlo: una sola línea de código, con cualquier implementación estándar de firma digital de curva elíptica, sin necesidad de OwnTrust, sin necesidad de ningún componente propietario, sin necesidad de que Axenkor exista.

Si OwnTrust desaparece mañana — si la empresa cierra, si los servidores se apagan, si el dominio expira — los certificados que emitió siguen siendo verificables. Para siempre. Por cualquiera. Con herramientas de software libre.

Eso es lo que significa que la evidencia sea autocontenida. No depende de quien la emitió. Depende solo de la matemática.

* * *

El acto soberano es, en el fondo, la respuesta a la pregunta con la que empezó este libro.

Cuando la APDP llame y pregunte qué pueden demostrar sobre el consentimiento de Juan Pérez el 15 de marzo de 2024, la respuesta con OwnTrust no es "el sistema registra que hizo clic". Es: "Aquí está el certificado. Verifica esta firma con esta llave pública. Si la verificación es exitosa, Juan Pérez firmó este documento exactamente en este momento. Nadie más pudo haberlo hecho."

Esa respuesta no requiere que el regulador confíe en la empresa. Requiere solo que confíe en la matemática.

Y la matemática no miente.

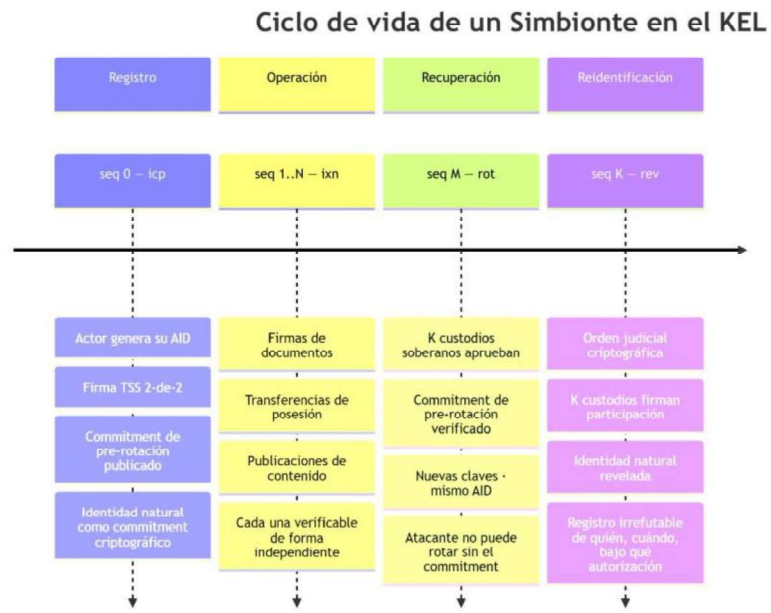
▸ Profundidad técnica — Estructura del certificado y verificación independiente

El certificado OwnTrust es un certificado digital firmado que contiene el tipo de acto, el timestamp en UTC, el AID del titular (sin datos personales), la identificación de la organización, los hashes de la política firmada y del registro en el KEL, el nivel de autenticación (secreto validado, imagen

verificada, score de presencia humana), y la firma firma digital de curva elíptica del billete de la firma con la clave pública correspondiente.

La verificación independiente requiere tres elementos: el certificado completo, la clave pública del AID del titular (incluida en el certificado), y cualquier implementación de firma digital de curva elíptica. En Python: from cryptography.hazmat.primitives.asymmetric.ed25519 import firma digital de curva elípticaPublicKey; key = firma digital de curva elípticaPublicKey.from_public_bytes(bytes.fromhex(cert["pk_aid"])); key.verify(bytes.fromhex(cert["firma"]), sha256(payload_canonico)). Si no lanza excepción, la firma es válida.

El score de presencia humana — incluido como metadata en el certificado — registra el tiempo de exposición del documento antes de la firma (en segundos), si el titular completó el scroll del documento, y el resultado de la verificación del documento de identidad si fue requerida. Este score no identifica al titular — es metadata del acto, no del actor. Pero añade una dimensión probatoria adicional que refuerza la validez del consentimiento en el contexto de la Ley 21.719.



Cada evento en el KEL está firmado con TSS 2-de-2 (ECDSA P-256 + ML-DSA Dilithium3, FIPS 204) y encadenado con SHA3-256. El Fragmento A es universal: cualquier enclave, cualquier actor, cualquier contexto. El protocolo es abierto: verificable por cualquiera con las claves públicas, sin contactar ninguna autoridad.

Figura 5 — Ciclo de vida de un Simbionte en el KEL · icp (registro) · ixn (operación) · rot (recuperación de claves) · rev (reidentificación judicial) · Cada evento firmado TSS 2-de-2 y encadenado SHA3-256

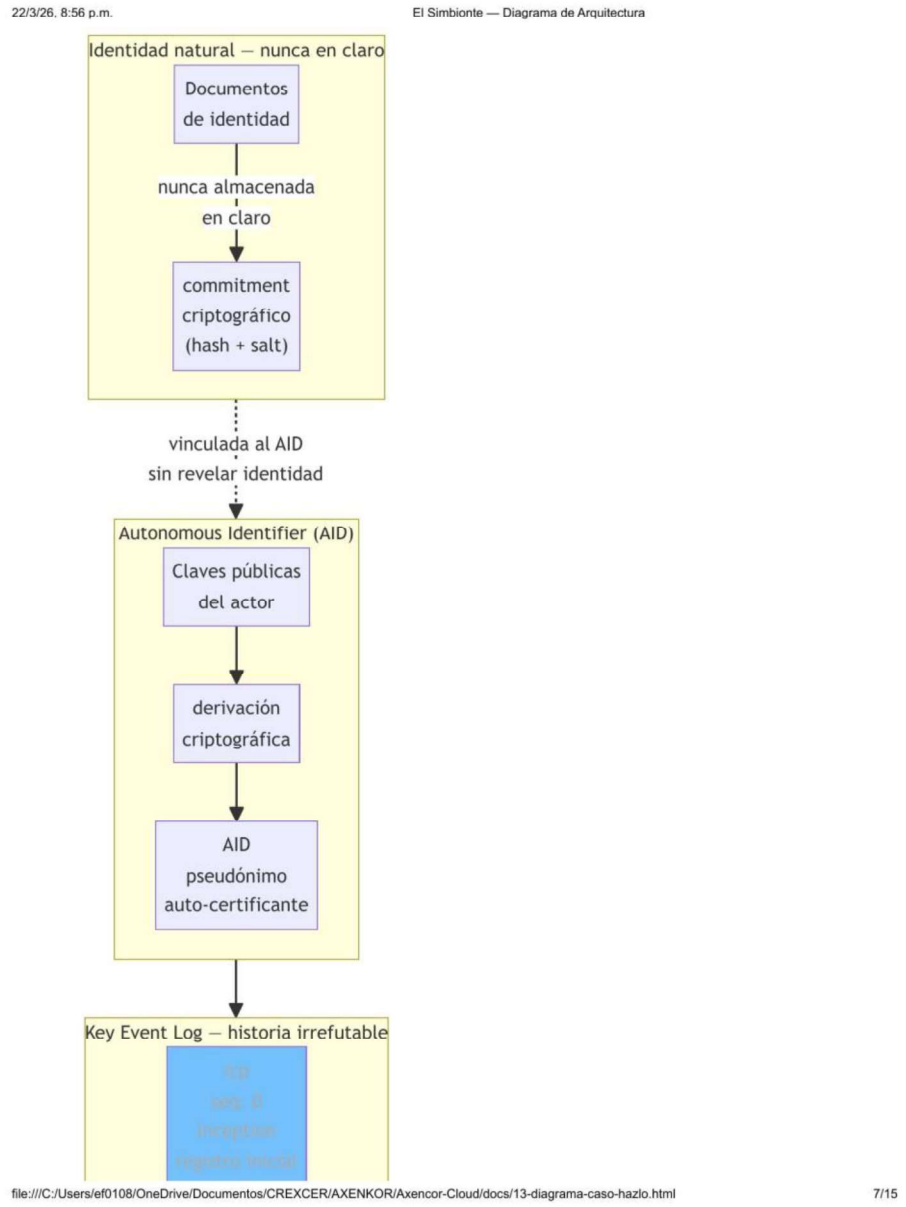


Figura 6 — La identidad soberana (AID) · La identidad natural existe solo como commitment criptográfico · El AID es pseudónimo auto-certificante derivado de las claves públicas del actor

Capítulo 10

El KEL — la cadena de verdad

El Key Event Log — el registro de eventos soberanos — es quizás el elemento más difícil de explicar del sistema, porque requiere cambiar una intuición muy arraigada sobre cómo funcionan los registros.

La intuición habitual es que un registro es el historial de una entidad. El historial de un cliente. El historial de un empleado. El historial de una cuenta. El registro existe porque la entidad existe, y el registro la describe.

El KEL invierte esa lógica completamente: el registro no describe al titular. Registra los actos. El titular aparece en el registro cuando actúa — no porque exista. El registro no es el historial del titular. Es la cadena de verdad de lo que ocurrió.

La distinción que lo cambia todo

Esta distinción — entre el registro de una entidad y el registro de un acto — tiene consecuencias profundas en la arquitectura del sistema.

Un registro de entidad necesita almacenar quién es la entidad: su nombre, su identificación, sus atributos. Para ser útil, necesita mantener esa información actualizada, coherente, accessible. Y eso significa que la entidad vive en el registro — sus datos están ahí, disponibles para quien tenga acceso.

Un registro de actos necesita almacenar solo qué ocurrió: quién firmó (identificado por el AID, no por su nombre ni RUT), qué firmó (identificado por el hash del documento, no por el contenido), cuándo (el timestamp), y la cadena que lo conecta con el acto anterior (el hash encadenado). La entidad no vive en el registro. Solo actúa en él.

Esa diferencia hace posible que el KEL sea completamente público en su estructura — cualquiera puede ver que el AID identificado como "inim:did:9F2A8C1B4E7D3F0A" firmó el acto número 3 a las 14:32 del 16 de abril de 2026 — sin revelar ningún dato personal del titular. Porque el AID no es

el RUT. No es el nombre. No es ningún dato personal. Es un hash de un hash que solo el titular puede vincular a su identidad.

La cadena que no puede romperse

El KEL no es una lista de eventos. Es una cadena.

Cada evento en el KEL incluye el hash del evento anterior. Eso significa que si alguien modifica un evento — cualquier evento, en cualquier posición de la cadena — el hash del evento siguiente ya no coincide. La modificación es inmediatamente detectable.

No es necesario comparar con una copia maestra en ningún servidor central. No es necesario confiar en ninguna autoridad. La integridad de la cadena es verificable por cualquier persona que tenga acceso al registro completo y conozca el algoritmo de hash — que es una función hash criptográfica de estándar internacional, un estándar público y abierto.

Eso significa que el KEL es inmutable en la práctica. No por razones de autoridad — no porque OwnTrust lo diga. Sino porque cualquier modificación es matemáticamente detectable. Y esa detectabilidad es lo que hace que el registro tenga valor probatorio.

Un log de base de datos puede ser modificado sin que sea evidente. El KEL no puede. Esa diferencia, ante un regulador o un tribunal, es la diferencia entre evidencia y afirmación.

Lo que el titular ve — y lo que la organización ve

El KEL tiene visibilidad diferenciada por diseño.

El titular ve su KEL completo. Todos los actos que ha firmado, con todas las organizaciones, en toda la historia de su identidad soberana. Puede exportarlo como un archivo JSON verificable — sin depender de OwnTrust, sin necesitar ninguna aplicación propietaria — y guardarlo donde quiera. Es su historial. Le pertenece.

La organización ve solo sus propias entradas. El banco que usa OwnTrust puede ver los actos del titular que corresponden a esa relación — los consentimientos otorgados, las solicitudes ARCO+P ejercidas, las respuestas dadas. No puede ver los actos del titular con el hospital. No puede ver los actos del titular con la empresa de telecomunicaciones. Cada organización ve solo lo suyo.

Los terceros — reguladores, auditores, la APDP — no pueden consultar el KEL directamente. Acceden a él a través del titular, que puede compartirlo voluntariamente, o a través de un certificado específico de un acto que sea relevante para el proceso.

Esa arquitectura de visibilidad — todo para el titular, lo propio para la organización, lo necesario para el regulador — es la implementación técnica del principio de que los datos pertenecen al titular.

> *El KEL no es el historial del titular. Es la cadena de verdad de lo que ocurrió. El titular aparece cuando actúa — no porque exista.*

Los actos que el KEL registra — y los que no

El KEL registra todo lo que tiene relevancia soberana: los consentimientos otorgados, los derechos ARCO+P ejercidos, las respuestas de las organizaciones, las notificaciones recibidas, las impugnaciones realizadas, los contratos bilaterales firmados, los pagos declarados soberanamente.

El KEL no registra datos personales del titular. No registra el contenido de los documentos firmados — registra sus hashes. No registra el RUT del titular — registra su AID. No registra la IP desde la que se conectó — registra un hash de sesión que no es trazable al titular sin información adicional.

Y el KEL registra también los intentos fallidos. Si el titular intenta ejercer un derecho en una organización que no lo tiene en sus registros, el KEL registra ese intento — no como error, sino como evidencia de que ocurrió. Si la

organización no responde en el plazo legal, el KEL registra el vencimiento. Si hay una anomalía de volumen, el KEL la registra.

Todo queda. Nada se pierde. La cadena de verdad es completa — incluyendo los momentos en que la verdad no fue cómoda para alguna de las partes.

* * *

El KEL es, en el fondo, la respuesta a una pregunta que la identidad digital nunca supo responder: ¿dónde vive la evidencia de los actos de una persona en el mundo digital?

Hasta ahora vivía en los servidores de las empresas con las que esa persona interactuó. Dispersa. Fuera de su control. Dependiente de la buena voluntad de cada organización para mantenerla, compartirla, preservarla.

Con el KEL, esa evidencia le pertenece al titular. La puede ver. La puede exportar. La puede compartir con quien elija. Y nadie puede modificarla — porque la cadena de hash hace cualquier modificación matemáticamente detectable.

Por primera vez en la historia del mundo digital, el titular tiene un registro propio, independiente, irrefutable, de sus actos soberanos. No el registro que las empresas tienen sobre él. Su registro. De lo que él hizo.

Eso es soberanía digital real.

▸ Profundidad técnica — Estructura técnica del KEL y verificación de integridad

Cada entrada del KEL tiene la siguiente estructura: seq (número de secuencia), tipo (icp para génesis, rot para rotación, ixn para interacción, sys para eventos del sistema), subtipo (consentimiento_firmado, arco_cancelacion, pago_confirmado, etc.), timestamp en ISO 8601, aid del titular, hash_evento (una función hash criptográfica de estándar internacional del contenido del evento), prev_hash (hash del evento anterior — una función hash criptográfica de estándar internacional de ceros para el primero), datos (objeto con metadata del acto sin datos

personales), y firma_billete (firma firma digital de curva elíptica del billete de la firma del titular, o firma de la organización para eventos inyectados por ella).

La verificación de integridad del KEL es un proceso recursivo simple: para cada evento, calcular una función hash criptográfica de estándar internacional(contenido_del_evento) y comparar con hash_evento. Verificar que prev_hash del evento N coincide con hash_evento del evento N-1. Verificar la firma firma digital de curva elíptica de cada evento. Si todas las verificaciones son exitosas para todos los eventos de la cadena, el KEL es íntegro. Si alguna falla, existe una modificación en ese punto.

Los tipos de evento del KEL cubren el ciclo completo de la relación entre titular y organización: icp (génesis), rot (rotación por cambio de cédula o recuperación), ixn/consentimiento_firmado, ixn/arco_acceso, ixn/arco_rectificacion, ixn/arco_cancelacion, ixn/arco_oposicion, ixn/arco_portabilidad, ixn/aceptacion_respuesta, ixn/impugnacion_respuesta, ixn/notificacion_organizacion, ixn/pago_notificado, ixn/pago_confirmado, ixn/pago_disputado, ixn/firma_bilateral_parte_A y parte_B, sys/titular_no_encontrado, sys/organizacion_no_respondio, sys/notificacion_vencida, sys/anomalia_volumen, sys/titular_fallecido.

—

Fin de la Parte II

La Parte III — Las implicaciones — examina lo que este modelo cambia para cada actor.

De la hegemonía del custodio a la hegemonía objetiva

El desplazamiento que MAS produce puede nombrarse con precisión: desde la hegemonía del custodio hacia la hegemonía objetiva.
La hegemonía del custodio es el paradigma vigente: el poder pertenece a quien controla el registro. El banco sabe más sobre el titular que el titular sobre sí mismo en la relación bancaria. La plataforma conoce el historial de decisiones del usuario mejor que el propio usuario. La organización puede modificar, perder o retener información que el titular necesita pero no posee. El poder emana del acceso asimétrico a la información — y ese acceso lo tiene quien custodia los datos.
La hegemonía objetiva es el paradigma que MAS instala: el poder pertenece a los hechos matemáticamente certificados. No a quien los custodia — sino a quien los protagonizó. Un hecho certificado soberanamente no puede ser negado por quien más le conviene negarlo. No puede ser modificado por quien tiene acceso al servidor. No puede desaparecer cuando ya no le conviene a nadie que exista. Le pertenece al acto. Y el acto le pertenece al titular que lo firmó.

> *El desplazamiento desde la hegemonía del custodio hacia la hegemonía objetiva no requiere regulación, no requiere acuerdo político, y no puede ser revertido por ningún actor. Es una consecuencia directa de la arquitectura.*

Capítulo 11

La nueva distribución del poder

Cuando alguien firma un documento en papel, ambas partes se van con una copia. El contrato de arriendo tiene la firma del arrendador y la del arrendatario. Los dos tienen el mismo papel. Los dos pueden probarlo.

Cuando alguien firma un documento digital, solo una parte se va con el registro. El formulario de consentimiento existe en el servidor de la empresa. La aceptación de los términos existe en la base de datos de la plataforma. El ejercicio de un derecho existe en el sistema de la organización que debe responder a ese derecho.

Esa asimetría no es un detalle técnico. Es la fuente de casi todos los problemas que la Parte I describió. Y es lo primero que MAS corrige.

Pero corregirla no es simplemente darle al titular una copia de lo que antes solo tenía la empresa. Es algo más profundo: cambiar quién genera la evidencia. Y ese cambio redistribuye el poder entre todos los actores del sistema digital de una forma que ninguno de ellos ha experimentado antes.

El poder en el modelo actual

En el sistema digital que existe hoy, el poder tiene una fuente específica: saber cosas sobre otros que ellos no pueden fácilmente verificar ni controlar.

La organización sabe cuánto gasta el titular, con qué frecuencia, qué compra, qué abandona, qué le hace cambiar de decisión. El titular sabe que tiene una cuenta, que acumuló algunos puntos, que en algún momento aceptó unos términos cuyo contenido exacto no recuerda. La asimetría es estructural — no viene de la mala voluntad de nadie, sino de la arquitectura del sistema.

Esa asimetría produce una distribución de poder específica. La organización tiene el monopolio del relato: es quien puede decir qué pasó, cuándo, y en qué condiciones. El titular tiene, en el mejor caso, su memoria. Y la memoria no es evidencia.

El regulador depende de los registros de la organización para fiscalizarla. El juez depende de los logs de la empresa para resolver la disputa. El tribunal de arbitraje depende de los sistemas del operador para determinar los hechos. En todos los casos, la evidencia la produce quien más interés tiene en que esa evidencia sea favorable. El conflicto de interés probatorio que el Capítulo 1 describió no es una excepción del sistema — es su característica más fundamental.

Lo que MAS redistribuye

MAS no le quita poder a la organización para dárselo al titular. Eso sería un juego de suma cero que resolvería un problema creando otro.

Lo que MAS hace es cambiar la naturaleza del poder mismo.

En el modelo actual, el poder es información: quien la tiene, quien la controla, quien puede acceder a ella. En MAS, el poder es certeza: quien puede certificar que algo ocurrió, de qué forma, en qué momento, con qué consecuencias.

Y la certeza, a diferencia de la información, puede ser simétrica. Un acto ocurre entre dos partes. Las dos estuvieron presentes. Las dos pueden certificar lo que pasó. En MAS, lo hacen — literalmente. El acto soberano del titular lleva su firma. El sistema de la organización lo co-registra. Los dos tienen el mismo certificado irrefutable. Los dos pueden probarlo ante cualquier tercero sin necesitar que el otro confirme nada.

> *La asimetría que el mundo digital construyó no era inevitable. Era el resultado de una decisión de arquitectura: que la evidencia de los actos digitales viviera solo en los sistemas de quien los procesó. MAS revierte esa decisión. La evidencia vive con quien protagonizó el acto.*

Esto cambia algo más que la conveniencia técnica. Cambia la relación de fondo entre los actores del sistema. No de forma abstracta — de forma concreta, en cada transacción, en cada consentimiento, en cada ejercicio de un derecho, en cada momento donde alguien necesita probar que algo ocurrió.

Los cuatro actores cuya realidad cambia

La redistribución de poder que MAS produce no afecta a todos los actores de la misma forma. Hay cuatro cuya realidad cambia de manera suficientemente específica como para merecer examen propio.

El titular — la persona física cuyos datos se tratan, cuyos derechos se ejercen, cuyo consentimiento se solicita — pasa de ser el objeto del sistema a ser su actor principal. No porque alguien lo decida. Porque la arquitectura lo hace posible. El titular que porta sus propios certificados soberanos no necesita que ninguna

organización confirme lo que hizo. La evidencia es suya. El capítulo siguiente examina qué significa eso en la práctica.

La organización — empresa, institución, o plataforma que trata datos personales — gana algo que el modelo actual no puede darle: evidencia irrefutable de que actuó correctamente. Hoy, la organización que cumplió el proceso correcto no puede probarlo de forma que resista cualquier cuestionamiento. Con MAS, el certificado soberano del titular es la prueba. No la afirmación de la organización. La firma del titular. El capítulo 13 examina lo que ese cambio produce en la gestión operacional y en la posición legal de la organización.

El regulador — la APDP, la CMF, la UAF, cualquier autoridad de fiscalización — opera hoy dependiendo de los registros del regulado para verificar el cumplimiento del regulado. Es una contradicción estructural que MAS resuelve: cuando la evidencia proviene del titular y no del sistema de la empresa, el regulador puede verificar sin confiar. El capítulo 14 examina las implicaciones para el ejercicio de la función regulatoria.

El contrato entre particulares — el arriendo, el acuerdo de servicios, el encargo profesional — existe hoy de forma frágil en el mundo digital. Cualquier disputa sobre los términos, sobre los hechos, sobre los pagos se convierte en un enfrentamiento de afirmaciones sin árbitro neutro. Con MAS, los actos que conforman la relación contractual quedan certificados soberanamente por ambas partes. Los hechos dejan de ser disputables. El capítulo 15 examina lo que eso cambia para la economía de los contratos cotidianos.

* * *

Hay una observación que ninguno de estos cuatro capítulos dice explícitamente pero que atraviesa todos: el nuevo modelo no es más fácil de operar para ninguno de los actores.

La organización que implementa MAS tiene que hacer algo que el modelo anterior no le exigía: explicar claramente lo que pide al titular, para que el titular pueda consentir con conocimiento real. Eso es más trabajo que un banner de «Acepto todo».

El regulador que recibe certificados soberanos tiene que desarrollar la capacidad técnica de verificarlos. Eso es diferente a leer un reporte que la empresa preparó.

El titular que tiene la autoría de sus actos digitales tiene también la responsabilidad de custodiarlo. Su secreto personal no puede recuperarlo nadie más.

El nuevo modelo es más justo. También es más exigente. Exige de cada actor que asuma la parte de la responsabilidad que le corresponde — sin poder delegarla a quien tiene más poder en la relación.

Eso, en definitiva, es lo que significa redistribuir el poder. No liberarse de la responsabilidad. Asumir la que es propia.

—

PARTE III

Las implicaciones

Un cambio de arquitectura produce cambios en la distribución del poder. Esos cambios merecen ser nombrados.

— Del prólogo

Capítulo 12

Lo que cambia para el titular

María tiene cuarenta y dos años. Vive en Maipú. Compra en las tiendas de una cadena de retail habitual. Cuando quiere saber qué datos tiene el operador de retail sobre ella y para qué los usa, envía un correo a datospersonales@[empresa].cl y espera.

Espera porque la ley le otorga a la empresa treinta días para responder. Espera porque no tiene ningún mecanismo para saber si el correo llegó, si fue leído, si fue procesado. Espera porque su única evidencia de que ejerció ese derecho es una copia del correo en su bandeja de enviados — un registro que ella genera, que ella custodia, que cualquier abogado de el operador de retail puede cuestionar.

Eso es lo que cambia con OwnTrust. No para María en abstracto. Para María en concreto, con su cédula en mano, con su secreto personal, con treinta segundos disponibles.

Del objeto al actor

En todos los sistemas de gestión de datos personales que existen hoy, el titular es un objeto. Es la entidad sobre la cual se registra información. Es el destinatario de formularios, el firmante de políticas, el sujeto de los datos.

El cambio más profundo que OwnTrust produce no es técnico. Es de posición. El titular pasa de ser el objeto del proceso a ser el actor del proceso.

Cuando María ejerce su derecho de cancelación a través de OwnTrust, no envía una solicitud que el operador de retail recibirá, procesará y responderá según sus propios tiempos y criterios. María firma soberanamente el acto de ejercer ese derecho. La firma nace de su identidad — de su ADN, de su AID, de los fragmentos que derivan de su documento y que nadie más posee. el operador de retail recibe el certificado. El KEL registra que el acto ocurrió. Y si el operador de retail no responde en treinta días, el KEL registra ese incumplimiento con la misma irrefutabilidad.

María no tiene que probar que ejerció su derecho. La evidencia existe independientemente de lo que el operador de retail diga o no diga.

El registro propio

Hay algo que ningún sistema le ha dado jamás al titular: un registro propio, independiente, de sus actos soberanos en el mundo digital.

No el registro que las empresas tienen sobre él. Su registro. De lo que él hizo. Verificable sin depender de ninguna plataforma, sin necesitar que ninguna empresa confirme nada.

El KEL de María le pertenece. Puede verlo en cualquier momento. Puede exportarlo como un archivo verificable. Puede presentarlo ante la APDP, ante un tribunal, ante cualquier interlocutor que necesite saber qué hizo y cuándo.

Y ese registro sobrevive a todo. Sobrevive a que OwnTrust deje de existir. Sobrevive a que el operador de retail cambie de sistema. Sobrevive a que María cambie de dispositivo, renueve su cédula, o decida cambiar su secreto personal. El AID — derivado de su ADN, anclado en su RUT — es el hilo que une toda esa historia. Inmutable. Permanente. Suyo.

> *Por primera vez en la historia del mundo digital, el titular tiene un registro propio de sus actos soberanos. No el registro que las empresas tienen sobre él. El suyo. Irrefutable.*

El consentimiento que se entiende

Hay una dimensión del cambio para el titular que va más allá de la evidencia y el registro. Es la dimensión de la comprensión.

Cuando una empresa implementa OwnTrust, no puede presentar al titular un banner de "Acepto todo" que incluya en letra pequeña la autorización para compartir sus datos con cuarenta y siete empresas del holding. Tiene que descomponer el consentimiento en sus partes reales. Tiene que presentar cada componente de forma que el titular pueda entender qué está autorizando.

Eso no es un requisito burocrático. Es la condición para que el consentimiento sea lo que la ley dice que debe ser: libre, informado, específico e inequívoco.

Un consentimiento que el titular no entendió no es un consentimiento válido. Y OwnTrust no puede certificar lo que no es válido. Eso cambia la relación entre el titular y la organización de una forma que ningún sistema existente produce: la organización debe explicar para que el titular firme. No al revés.

El derecho a impugnar

Hay un derecho que existe en la ley y que prácticamente nadie ejerce: el derecho a impugnar un acto que el titular no reconoce.

En el mundo sin OwnTrust, impugnar requiere que el titular demuestre que no consintió algo. Esa demostración es difícil porque la evidencia del consentimiento la tiene la empresa — y la empresa dice que sí consintió.

En el mundo con OwnTrust, la impugnación es un acto soberano firmado que queda en el KEL con la misma irrefutabilidad que el acto impugnado. Si María dice que no firmó el consentimiento número 3, esa declaración queda registrada. Si la firma del consentimiento número 3 es válida, la matemática lo demuestra. Si la firma no es válida, la matemática también lo demuestra.

La impugnación deja de ser una afirmación del titular contra una afirmación de la empresa. Se convierte en un proceso verificable por cualquier tercero con acceso al certificado y conocimiento de firma digital de curva elíptica.

* * *

Hay algo más profundo en lo que cambia para el titular. Algo que no se puede medir con certificados ni con registros.

Es la experiencia de ser tratado como el actor principal de la relación — no como el objeto de ella. De que el sistema esté diseñado para que el titular entienda, para que el titular elija, para que el titular actúe.

Eso no es habitual en el mundo digital. Es, de hecho, la excepción. Y esa excepción cambia algo que va más allá de la privacidad: cambia la confianza. Cuando un titular sabe que tiene un registro propio, irrefutable, de sus actos soberanos — y que ese registro nadie puede modificar ni negar — la relación con las organizaciones que tratan sus datos deja de ser una relación de fe y se convierte en una relación de evidencia.

La fe puede defraudarse. La evidencia no.

▸ Profundidad técnica — Lo que el titular puede hacer con su KEL

El titular puede acceder a su KEL completo en cualquier momento desde la la aplicación OwnTrust. El KEL se presenta como una lista cronológica de actos soberanos, filtrable por organización, por tipo de acto, y por estado. Cada entrada muestra el tipo de acto, la organización, el timestamp, el estado actual, y el hash del certificado.

El titular puede exportar su KEL completo como un archivo JSON autocontenido. Ese archivo incluye todos los eventos, los hashes encadenados, y las firmas de cada acto. Es verificable sin OwnTrust mediante cualquier implementación de estándares criptográficos auditados por la comunidad matemática global.

El titular puede compartir un certificado específico con cualquier tercero — un regulador, un abogado, un tribunal. El certificado es autocontenido y verificable sin OwnTrust. La verificación requiere solo el certificado, la clave pública del AID incluida en él, y cualquier implementación de firma digital de curva elíptica. Una línea de código.

El titular puede impugnar cualquier acto desde su KEL. La impugnación es un acto soberano firmado que queda registrado con la misma irrefutabilidad que el acto impugnado. La organización recibe el certificado de impugnación vía notificación automática.

Capítulo 13

Lo que cambia para la organización

El Director de Protección de Datos de una aseguradora mediana recibe, en promedio, tres solicitudes ARCO+P por semana. Cada una requiere verificar que el solicitante es efectivamente el titular de los datos, localizar la información relevante en los sistemas internos, redactar una respuesta, y documentar el proceso.

El proceso completo toma, en el mejor de los casos, varios días de trabajo de al menos dos personas. Y al final de ese proceso, la evidencia que existe es un correo enviado, un registro en el sistema de gestión, y la esperanza de que si algún regulador pregunta, el expediente sea suficiente.

Eso cambia con OwnTrust. No solo el proceso — la naturaleza de la evidencia.

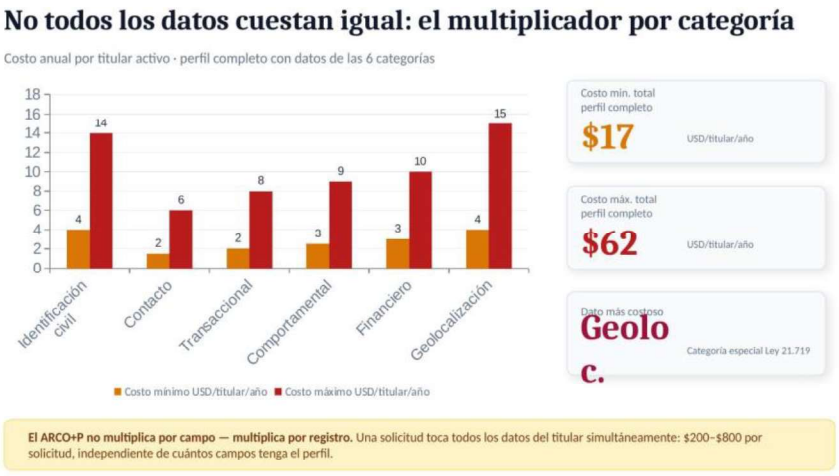


Figura 7 — Costo anual por titular según categoría de dato · El multiplicador varía de ×2 (contacto) a ×10 (geolocalización, categoría especial Ley 21.719) · Perfil completo: $17–$62 USD / titular / año

La responsabilidad que no se puede delegar

Hay una verdad incómoda que la mayoría de las organizaciones prefiere no articular: la responsabilidad sobre los datos personales de sus titulares no puede delegarse a un proveedor de tecnología.

Contratar OneTrust no exime a una organización de su responsabilidad como responsable del tratamiento. Contratar OwnTrust tampoco. Pero hay una diferencia crítica: OneTrust gestiona el proceso interno de la organización. OwnTrust produce la evidencia del acto del titular. Y la evidencia del acto del titular es exactamente lo que el regulador va a pedir cuando fiscalice.

Eso significa que la organización que implementa OwnTrust no está delegando su responsabilidad. Está equipándose con la herramienta que le permite demostrar que la asumió correctamente. No ante sí misma. Ante el regulador. Ante el tribunal. Ante el titular que disputa.

El certificado como escudo legal

El caso de uso más poderoso de OwnTrust para la organización no es el más obvio. No es la eficiencia operacional — aunque OwnTrust la produce. No es la reducción de fricción en la gestión de solicitudes ARCO+P — aunque OwnTrust la reduce.

El Simbionte Soberano y el Simbionte Derivado: identidad organizacional sin secretos

Hay una consecuencia de MAS para la organización que va más allá del cumplimiento regulatorio y de la gestión de titulares externos. Afecta la arquitectura de identidad interna de la organización misma.

Cada persona natural tiene un Simbionte Soberano — su identidad raíz permanente, anclada biométricamente, irrevocable por ninguna organización. Cuando esa persona asume un cargo, su Simbionte Soberano genera un Simbionte Derivado: una proyección funcional específica para ese rol, con capacidades delimitadas al alcance del cargo. La propiedad más importante del Simbionte Derivado es su auto-desactivación: cuando el titular sale del cargo, el Simbionte Derivado se desactiva automáticamente. Ningún administrador de TI tiene que ejecutar un proceso de deprovisioning. La organización se reconfigura sola.

En cualquier momento, el conjunto de Simbiontes Derivados activos de una organización es la lista exacta y verificable de quién la compone. No hay un directorio desactualizado. No hay una estructura de propiedad que pueda ocultarse detrás de cargos nominales. El beneficial ownership — quién controla qué posición, con qué capacidades, vinculado a qué persona natural verificada biométricamente — es una propiedad del sistema, no una declaración que puede falsificarse.

> *La cadena es directa e irrefutable: cargo → Simbionte Derivado → Simbionte Soberano → ADN → persona verificada con NFC y*

biometría. El beneficial ownership deja de ser un problema de información. Pasa a ser una propiedad de la arquitectura.

El caso de uso más poderoso es el escudo legal.

Cuando un titular reclama ante la APDP que una organización trató sus datos sin su consentimiento, la organización necesita demostrar que el consentimiento fue otorgado. El certificado OwnTrust hace esa demostración con un nivel de certeza que ningún otro sistema puede igualar: la firma criptográfica del titular, verificable matemáticamente, que prueba que ese titular específico firmó ese consentimiento específico en ese momento específico.

La APDP no necesita confiar en la organización. No necesita confiar en OwnTrust. Necesita solo verificar la firma — una operación que cualquier sistema con implementación estándar de firma digital de curva elíptica puede realizar en milisegundos.

Eso transforma la posición de la organización en cualquier proceso regulatorio. En lugar de presentar logs de base de datos que el regulador puede cuestionar, presenta certificados matemáticamente irrefutables. La diferencia, en términos de resultado del proceso, puede ser la diferencia entre una sanción de millones de dólares y una exoneración.

> *La organización que puede demostrar que el titular entendió y firmó soberanamente cada autorización no tiene nada que temer del regulador. La que solo puede mostrar que el titular hizo clic en un banner tiene todo que temer.*

El costo de la evidencia real versus el costo del riesgo

Hay un cálculo que pocas organizaciones han hecho con honestidad: el costo de la evidencia irrefutable versus el costo de no tenerla.

OwnTrust estructura su precio según el volumen de operación y la criticidad del riesgo que elimina. El principio es siempre el mismo: el costo de la evidencia irrefutable es una fracción del costo del riesgo que previene.

Una infracción grave de la Ley 21.719 — tratar datos sin consentimiento válido — puede costar el 2% de esos ingresos. Doscientos mil dólares. Por infracción.

El análisis de costo-beneficio no requiere sofisticación financiera. OwnTrust no es un gasto de compliance. Es el seguro más barato que existe contra el riesgo regulatorio más costoso que la organización enfrenta.

Y produce, además, algo que ningún seguro produce: la eliminación real del riesgo. No la transferencia del riesgo a otro actor. La eliminación: si la evidencia es irrefutable, no hay riesgo. No hay proceso. No hay sanción.

Lo que la organización no puede hacer con OwnTrust

Vale la pena ser explícitos sobre los límites del sistema desde la perspectiva de la organización. OwnTrust cambia muchas cosas. No cambia todo.

OwnTrust no puede verificar que quien ingresa los datos en el génesis es efectivamente el titular. Esa responsabilidad es de la organización. Si la organización registra en sus sistemas a una persona con un RUT que no le pertenece, OwnTrust producirá evidencia irrefutable de que esa persona incorrectamente registrada consintió. La evidencia será perfecta. El problema será de la organización.

OwnTrust no puede garantizar que el titular entendió lo que consintió — solo que lo leyó y lo firmó. La comprensión real depende de cómo la organización presente el contenido. OwnTrust exige que la presentación sea descompuesta en componentes específicos. No puede verificar que esa presentación sea suficientemente clara para cada titular individual.

OwnTrust no es un sistema de gestión de datos personales. Es un sistema de certificación de actos soberanos. La organización sigue necesitando los procesos internos para gestionar, tratar y proteger los datos. OwnTrust certifica que el titular autorizó ese tratamiento. No gestiona el tratamiento en sí.

* * *

Hay una consecuencia del cambio para la organización que es más difícil de articular pero igualmente real.

Cuando la evidencia del consentimiento proviene del titular — cuando es él quien firma, con su identidad soberana, lo que está autorizando — la organización ya no puede pretender que obtuvo más de lo que el titular firmó. El certificado dice exactamente qué autorizó. No más. No menos.

Eso requiere que la organización diseñe sus procesos de consentimiento con honestidad. No con el objetivo de maximizar los opt-ins, sino con el objetivo de obtener autorizaciones válidas para los usos que realmente necesita.

Es un cambio de incentivos estructural. Y produce, como consecuencia, una relación más honesta entre la organización y sus titulares. Una relación donde ambas partes saben exactamente cuál es el acuerdo. Sin ambigüedades. Sin letra pequeña. Sin banners diseñados para maximizar clics.

Eso no es solo un beneficio ético. Es un beneficio comercial. La confianza del titular es el activo de privacidad más valioso que una organización puede tener. Y OwnTrust es el único sistema que la produce de forma verificable.

▸ Profundidad técnica — La integración desde la perspectiva de la organización

La organización se integra con OwnTrust a través de dos modalidades. El SDK programático — para organizaciones con capacidad técnica — permite invocar OwnTrust desde cualquier sistema, recibir certificados vía notificación automática, consultar el estado de los actos del titular, e inyectar notificaciones firmadas con la clave institucional de firma de la organización. El tiempo de implementación típico es de una a dos semanas.

El el portal de gestión — para organizaciones sin capacidad técnica — provee un portal web que permite gestionar manualmente los actos ARCO+P, descargar los certificados, y consultar el historial de cada titular. Sin código. Sin infraestructura. Configuración en cuarenta y ocho horas.

En ambos casos, la organización gestiona dos pares de llaves criptográficas: las claves criptográficas institucionales para firmar sus respuestas y notificaciones. Estas claves son generadas y custodiadas por la propia organización.

El sistema entrega el certificado a la dirección configurada por la organización con tres reintentos automáticos con intervalos crecientes.

Capítulo 14

Lo que cambia para el regulador

La Agencia de Protección de Datos Personales de Chile inicia operaciones con un mandato claro y un desafío igualmente claro: hacer cumplir la Ley 21.719 en un país donde la cultura del dato personal — tanto en las organizaciones que los tratan como en los titulares que los generan — está en formación.

El primer desafío no es de voluntad ni de recursos. Es de estándar probatorio. ¿Qué tipo de evidencia es suficiente para determinar que una organización trató datos sin consentimiento válido? ¿Un log de base de datos? ¿Un correo? ¿Una pantalla de formulario web?

Esa pregunta no tiene una respuesta técnica establecida en Chile. Tendrá que construirse — caso a caso, proceso a proceso — en los primeros años de funcionamiento de la APDP.

OwnTrust introduce en esa construcción un estándar que ningún otro sistema puede proveer: la firma criptográfica del titular como evidencia del acto.

La evidencia matemáticamente verificable

Existe una diferencia fundamental entre dos tipos de evidencia que el regulador puede examinar.

El primero es la evidencia testimonial: alguien — la empresa, el sistema de gestión — dice que algo ocurrió. Puede estar apoyada por logs, por pantallas, por registros de auditoría. Pero en última instancia depende de que alguien lo afirme y de que el regulador le crea.

El segundo es la evidencia matemática: la verificación de una firma criptográfica que demuestra que cierta llave privada firmó cierto contenido en cierto momento. Esa verificación no depende de que nadie le crea nada. Depende solo de la matemática — que no tiene interés en el resultado del proceso.

El certificado OwnTrust es evidencia del segundo tipo. Cualquier funcionario de la APDP con acceso al certificado y a una implementación estándar

de firma digital de curva elíptica puede verificar en milisegundos que la firma es válida — o que no lo es. Sin necesidad de peritos. Sin necesidad de que la empresa explique su sistema. Sin necesidad de que OwnTrust confirme nada.

Esa independencia de la evidencia respecto de quien la emite es el principio más poderoso del sistema desde la perspectiva del regulador. La evidencia habla por sí misma.

El nuevo estándar probatorio que emerge

Cuando el regulador comience a recibir certificados OwnTrust como evidencia en los procesos de fiscalización, algo importante ocurrirá: el estándar implícito de evidencia para el consentimiento comenzará a elevarse.

Hoy la APDP acepta como evidencia de consentimiento lo que las organizaciones presenten — logs, pantallas, reportes de sus sistemas de gestión. Mañana, cuando una organización presente un certificado con firma firma digital de curva elíptica del titular y otra presente un log de base de datos, el contraste será inevitable.

El regulador no necesitará dictar una norma técnica específica sobre qué tipo de evidencia es suficiente. El mercado lo definirá solo: las organizaciones que pueden demostrar el consentimiento con firma criptográfica del titular tendrán una ventaja regulatoria tan clara que las demás tendrán incentivos para adoptar el mismo estándar.

Ese proceso de elevación del estándar es gradual pero inexorable. Y cada caso donde un certificado OwnTrust sea determinante en el resultado de un proceso regulatorio acelera esa elevación.

> *La APDP no necesita definir qué es evidencia suficiente. Solo necesita comparar lo que distintas organizaciones presentan. La diferencia entre una firma matemática y un log de base de datos se explica sola.*

Lo que el regulador puede hacer que antes no podía

Hay capacidades regulatorias que OwnTrust habilita y que no existen con los sistemas actuales.

La primera es la verificación independiente. El regulador puede verificar cualquier certificado OwnTrust sin necesidad de peritos externos ni de acceso a los sistemas de la organización. La verificación es instantánea, determinista, y reproducible. No hay espacio para la discrepancia de opiniones expertas.

La segunda es la detección de patrones. Cuando el KEL registra que una organización no respondió a múltiples solicitudes ARCO+P dentro del plazo legal, ese patrón es visible y verificable. No requiere que los titulares afectados presenten reclamos individuales. El registro sistemático del incumplimiento existe independientemente de si algún titular decidió actuar.

La tercera es la protección del titular en tiempo real. Cuando el sistema detecta un volumen anormal de transacciones — potencialmente indicativo de consentimientos masivos obtenidos de forma irregular — los certificados se marcan automáticamente. El titular puede impugnar. El regulador puede investigar. La evidencia ya existe.

La cuarta — y más importante — es la posibilidad de actuar sobre evidencia irrefutable. En el sistema actual, muchos casos de vulneración de privacidad no se persiguen porque la evidencia es insuficiente o disputada. Con OwnTrust, cuando el certificado dice que el titular no consintió algo que la organización dice que sí consintió, la matemática resuelve la disputa. El regulador puede actuar con certeza.

* * *

Hay una dimensión política del cambio para el regulador que vale la pena nombrar.

La APDP es una institución nueva. Su credibilidad se construirá en los primeros años — con los primeros casos, las primeras sanciones, las primeras

exoneraciones. Esa credibilidad depende en parte de la calidad del estándar probatorio que aplique.

Un regulador que acepta como evidencia suficiente los logs de base de datos de las empresas que fiscaliza está, implícitamente, aceptando la palabra de quien tiene interés en el resultado. Un regulador que exige o valora la firma criptográfica del titular — evidencia que no puede ser generada por la organización — está construyendo su credibilidad sobre un estándar que ningún interés puede corromper.

OwnTrust no le dice a la APDP cómo debe regular. Le provee el instrumento para hacerlo con el estándar más alto disponible.

▸ Profundidad técnica — La verificación desde la perspectiva del regulador

El regulador recibe un certificado OwnTrust en formato JSON. La verificación requiere tres pasos: extraer la clave pública pk_aid del campo firma_soberana, calcular SHA256 del payload canónico del certificado, y ejecutar firma digital de curva elíptica.verify(pk_aid, sha256_payload, firma). Si el resultado es True, la firma es válida — el titular identificado por ese AID firmó ese contenido en ese momento. Si es False, la firma no es válida.

Esta verificación es reproducible infinitamente, produce siempre el mismo resultado, y no requiere acceso a OwnTrust ni a ningún sistema propietario. Cualquier implementación estándar de firma digital de curva elíptica — en Python, en JavaScript, en Go, en cualquier lenguaje — produce el mismo resultado.

El regulador puede adicionalmente verificar la integridad del KEL: calcular una función hash criptográfica de estándar internacional de cada evento y comparar con el hash almacenado, verificar que el prev_hash de cada evento coincide con el hash_evento del anterior. Si la cadena es íntegra, el registro no fue modificado. Si algún hash no coincide, existe una modificación en ese punto específico de la cadena.

Capítulo 15

Lo que cambia para los contratos

Ariel es arrendador. Tiene un departamento en Ñuñoa que arrienda por cuatrocientos cincuenta mil pesos al mes. Su arrendataria es Carolina, profesora, treinta y ocho años. Llevan dos años en la misma relación sin mayores problemas.

El mes pasado Carolina le transfirió el arriendo con dos días de retraso. Ariel dice que no llegó. Carolina dice que sí transfirió. Tienen los registros de sus propios bancos — que cada uno interpreta a su favor. No tienen ninguna evidencia que un tercero pueda verificar independientemente.

Ese conflicto no es inusual. Es la norma en cualquier relación contractual entre particulares donde la evidencia la genera y custodia cada parte por separado. Y es exactamente el tipo de conflicto que OwnTrust puede eliminar.

El acto bilateral soberano

Un contrato entre dos partes tiene un problema estructural similar al del consentimiento corporativo: la evidencia de que ambas partes acordaron algo generalmente la custodia una de ellas, o un tercero al que ambas deben confiarle algo.

El notario resuelve ese problema para los actos que lo requieren por ley — escrituras, poderes, declaraciones juradas. Pero para la inmensa mayoría de los actos contractuales cotidianos — contratos de arriendo, acuerdos de servicio, préstamos entre particulares — el notario es demasiado costoso, demasiado lento, demasiado inconveniente.

Lo que existe para esos actos es la buena fe. O el papel firmado. O el correo aceptado. O el mensaje de WhatsApp. Ninguno de los cuales produce evidencia irrefutable.

El acto bilateral soberano de OwnTrust produce lo que ninguno de esos mecanismos puede producir: la firma criptográfica de ambas partes sobre el mismo contenido, en el mismo momento, con la misma irrefutabilidad. El

contrato de arriendo de Ariel y Carolina, firmado con OwnTrust, no puede ser disputado. Ambas partes firmaron soberanamente. El KEL lo registra. El certificado lo demuestra.

Los pagos recurrentes certificados

El caso de Ariel y Carolina va más allá del contrato inicial. El conflicto real está en los pagos mensuales — en si Carolina transfirió o no, en si Ariel recibió o no.

OwnTrust introduce en este contexto un concepto que no existe en el derecho contractual actual: la declaración soberana de pago.

Cuando Carolina transfiere el arriendo, puede declarar soberanamente en OwnTrust que realizó el pago — la fecha, el monto, el concepto. Esa declaración queda firmada en el KEL con su identidad soberana. Cuando Ariel confirma que recibió el pago, también lo declara soberanamente. Las dos declaraciones — de quien paga y de quien recibe — quedan encadenadas en el KEL. El pago está doblemente certificado.

Si hay disputa — si Ariel dice que no recibió lo que Carolina dice que transfirió — el KEL registra la discrepancia. Ninguna de las dos partes puede negar lo que declaró. El árbitro — sea un mediador, un juez de policía local, o un tribunal — tiene evidencia irrefutable de lo que cada parte afirmó en qué momento.

Eso no resuelve todos los conflictos. Un pago declarado soberanamente no es un pago bancario verificado. Pero produce algo que no existía antes: un registro firmado, irrefutable, de lo que cada parte dijo que hizo. Y ese registro tiene un valor probatorio que ningún mensaje de WhatsApp puede igualar.

> *OwnTrust no reemplaza al notario. Produce para los actos cotidianos lo que el notario produce para los actos solemnes: evidencia de que algo ocurrió, firmada por quien lo hizo, verificable por quien necesite saberlo.*

Lo que cambia en la relación contractual

La implicación más profunda para el mundo de los contratos no es técnica. Es relacional.

Los contratos existen para resolver conflictos que podrían ocurrir. Cuando la evidencia de lo que las partes acordaron es clara, irrefutable, y verificable por terceros, los conflictos que dependen de la ambigüedad sobre lo acordado desaparecen. Las partes saben exactamente cuál es el acuerdo. Saben que cualquier disputa será resuelta por la evidencia — no por quien recuerde mejor, no por quien tenga mejor abogado, no por quien tenga acceso a los registros relevantes.

Eso produce algo que va más allá de la eficiencia: produce confianza. La confianza no de que la otra parte es buena persona — sino de que si algo sale mal, la verdad del acuerdo existe y puede probarse.

En las relaciones comerciales de largo plazo — un arriendo de años, un contrato de servicios recurrente, una relación laboral — esa confianza tiene un valor económico real. Reduce los costos de transacción. Reduce los costos de conflicto. Reduce la necesidad de intermediarios que custodien la evidencia.

El notario es caro no porque sea ineficiente. Es caro porque produce algo valioso: evidencia irrefutable. OwnTrust produce el mismo resultado para los actos cotidianos — a una fracción del costo, en treinta segundos, sin salir de casa.

Los límites actuales — y cómo evolucionan

Es importante ser honestos sobre lo que OwnTrust puede hacer hoy en el contexto contractual — y lo que no puede.

Hoy OwnTrust requiere que exista una organización como intermediario de la relación. El contrato de arriendo entre Ariel y Carolina necesita que el sitio de corretaje — o cualquier organización que actúe como facilitador — sea el que crea el acto bilateral en OwnTrust. Los particulares no pueden crear actos directamente entre sí sin un intermediario institucional.

Eso cambia con la versión 2 del protocolo, cuando la validación NFC del documento haga posible una verificación de identidad sin Agente IA externo. En ese punto, dos particulares podrán crear actos bilaterales directamente — sin intermediario — con la misma irrefutabilidad que los actos mediados por una organización.

Esa evolución transformará el mercado de contratos entre particulares de una forma que ningún sistema existente ha logrado: pondrá la evidencia irrefutable al alcance de cualquier persona, para cualquier acuerdo, en cualquier contexto. Sin notario. Sin intermediario. Sin costo prohibitivo.

* * *

Volvamos a Ariel y Carolina.

En el mundo con OwnTrust, cuando Carolina transfiere el arriendo, declara soberanamente que lo hizo. Cuando Ariel recibe, declara soberanamente que lo recibió. Las dos declaraciones quedan en el KEL — irrefutables, encadenadas, firmadas con sus identidades soberanas.

Si algún mes hay un conflicto, no hay discusión sobre qué declaró cada uno. La declaración existe. Es verificable. Nadie puede decir que dijo algo diferente de lo que el KEL registra.

Eso no elimina todos los conflictos. Pero elimina los conflictos sobre los hechos. Lo que queda — si queda algo — son conflictos sobre la interpretación de los hechos. Y esos conflictos son mucho más fáciles de resolver cuando todos están de acuerdo en cuáles son los hechos.

> *El secreto bancario como categoría protege información que, en MAS, el banco no tiene. La identidad natural del titular nunca vive en el servidor de la institución: lo que existe son hechos certificados bilateralmente. El banco no puede revelar quién es el titular porque por diseño no lo sabe. Lo que protege al titular no es el silencio del banco — es la soberanía sobre qué hechos decide presentar y a quién.*

▸ Profundidad técnica — El flujo del contrato bilateral en OwnTrust

El contrato bilateral requiere que ambas partes estén registradas como titulares en la organización que actúa como facilitadora. La organización crea el acto bilateral con tipo ixn/firma_bilateral. El sistema presenta el documento a la Parte A para su firma soberana — con secreto personal y, si la organización lo requiere, con imagen de la cédula. El KEL registra firma_bilateral_parte_A.

El sistema luego presenta el mismo documento a la Parte B para su firma. El KEL registra firma_bilateral_parte_B. El certificado bilateral se emite cuando ambas partes han firmado. El certificado incluye las firmas de ambos AIDs — verificables independientemente.

Los pagos recurrentes se implementan como actos de tipo ixn/pago_notificado — firmado por quien declara haber cobrado — e ixn/pago_confirmado — firmado por quien declara haber pagado. La combinación de ambas declaraciones en el KEL produce evidencia de pago doblemente certificada. Si hay disputa — ixn/pago_disputado — el KEL registra la discrepancia y la organización facilita la mediación.

—

Fin de la Parte III

La Parte IV examina el futuro — el camino hacia la soberanía total.

Capítulo 16

Lo que cambia para el sistema financiero

Miguel revisa cinco mil solicitudes de crédito al mes. Las empresas medianas que quieren financiar su capital de trabajo, los profesionales independientes que quieren una hipoteca, las startups que necesitan una línea operacional. Para cada una, el proceso es el mismo: la empresa o persona presenta sus estados de cuenta de los últimos seis meses, su declaración de renta, su carpeta tributaria.

Miguel sabe que algunos de esos documentos están alterados. Lo sabe por la experiencia acumulada de ver miles de carpetas — hay patrones que no cuadran, redondeos que no existen en transacciones reales, totales que no coinciden con lo que el cliente declara en la conversación. Pero no puede probarlo. El PDF que tiene en pantalla es el único documento que existe. No hay nada con qué verificarlo.

Aprueba o rechaza créditos basándose en documentos que podrían ser ficción. A veces financia a quien no debería. A veces rechaza a quien sí podría pagar. El costo de esa incertidumbre lo pagan todos: los que pagan tasas más altas porque el riesgo sistémico es más alto, los que son rechazados aunque sean solventes, los bancos que asumen pérdidas por créditos mal evaluados.

El problema no es Miguel. El problema es que el sistema financiero construyó sus mecanismos de evaluación sobre datos declarados — no sobre hechos certificados.

Eso es lo que MAS cambia.

El secreto bancario como respuesta a la arquitectura equivocada

El secreto bancario —en Chile regulado por la Ley General de Bancos— existe para proteger a las personas de un riesgo específico: que las instituciones financieras compartan información sobre ellas sin su consentimiento.

Ese riesgo es real. Y la protección que el secreto bancario ofrece es legítima dentro de la arquitectura que describe: aquella donde el banco acumula información sobre el titular y la custodia.

Pero esa arquitectura asume algo que en MAS no existe: que el banco sabe cosas sobre el titular que el titular no puede controlar.

En MAS, el banco no sabe cosas sobre el titular en el sentido clásico. El banco certifica hechos en los que ambos participaron. Cada transacción es un acto que ocurrió entre el titular y la institución — un hecho que los dos presenciaron, que los dos co-produjeron, que los dos tienen registrado de forma idéntica en el KEL compartido. No hay asimetría de información. No hay nada que el banco sepa que el titular no sepa ya.

> *El secreto bancario protegía al titular de que el banco compartiera lo que sabía. En MAS, el banco no sabe nada que el titular no sepa. Lo que existe son hechos certificados que pertenecen a ambas partes por igual. La categoría que necesita protección cambia: ya no es el secreto del banco sobre el titular. Es la soberanía del titular sobre qué hechos presenta y a quién.*

Eso no elimina la necesidad de privacidad financiera. La transforma. En lugar de depender de que el banco guarde silencio, el titular controla directamente qué hechos certificados decide presentar, a quién, con qué granularidad y por cuánto tiempo. La privacidad deja de ser una restricción sobre el banco. Pasa a ser un atributo soberano del titular.

El crédito sin revelar datos

El problema de Miguel tiene una solución que el sistema financiero actual no puede implementar: evaluar el crédito sin que el solicitante revele sus transacciones.

Parece contradictorio. Si el banco no sabe cuánto gana y cuánto gasta el solicitante, ¿cómo evalúa si puede pagar? La respuesta está en la distinción entre conocer los datos y verificar una propiedad de esos datos.

Lo que Miguel necesita saber para aprobar una hipoteca no es el detalle de cada transacción del solicitante. Necesita saber si sus ingresos mensuales están por encima de cierto umbral. Si su nivel de endeudamiento está por debajo de cierto límite. Si su historial de pagos en los últimos veinticuatro meses cumple ciertos criterios.

En MAS, esas propiedades pueden ser certificadas sin revelar los datos subyacentes.

El banco del solicitante — que participó en sus transacciones, que co-firmó cada uno de sus actos financieros — puede emitir un atributo certificado: «Los ingresos promedio mensuales de este titular durante los últimos doce meses están en el rango de X a Y.» El solicitante presenta ese atributo a Miguel. Miguel verifica la firma del banco emisor. Confirma que el atributo es auténtico. Evalúa el crédito.

Miguel no vio una sola transacción. No sabe en qué gasta el solicitante, con quién trabaja, qué comprró el martes pasado. Solo sabe lo que necesita saber para tomar la decisión crediticia.

Eso es lo que en criptografía se llama una prueba de conocimiento cero aplicada a datos financieros: demostrar que una propiedad es verdadera sin revelar la información que la fundamenta. En MAS, el banco del solicitante es el garante criptográfico de esa propiedad. La firma del banco sobre el atributo es matemáticamente verificable. No puede ser alterada. No puede ser fabricada.

Para el solicitante, es más privacidad. Para Miguel, es más certeza. Para el sistema, es menos riesgo. Los tres ganan sin que nadie pierda.

El lavado de dinero que se auto-certifica

La intuición al escuchar que el titular controla sus propios hechos certificados es que eso crea un escudo para el crimen financiero. La intuición es incorrecta.

El lavado de dinero funciona hoy por tres razones estructurales que MAS elimina.

La primera es la identidad falsa. El sistema bancario actual hace KYC una vez, con documentos que pueden ser falsificados. Un operador del crimen organizado puede abrir cuentas bajo identidades de testaferros con documentación alterada. En MAS no hay identidad declarada. Hay identidad derivada matemáticamente de la biometría del titular real. El ADN es el resultado de una función criptográfica aplicada a características faciales verificadas contra el chip del Registro Civil. No existe un ADN para una persona que no estuvo físicamente presente en el génesis. No existe la posibilidad de abrir una cuenta MAS bajo una identidad que no sea la propia.

La segunda es la alteración de registros. Hoy, un empleado bancario con acceso suficiente puede modificar o eliminar transacciones. Los registros son bases de datos administradas por la institución. En MAS, cada acto financiero produce un certificado que va a la Bóveda D con encadenamiento hash. Modificar un certificado rompe la cadena. Cualquier auditor puede detectar la alteración en milisegundos. No hay insider que pueda borrar un hecho certificado — porque el hecho existe en el KEL de ambas partes.

La tercera es la denegación plausible. Hoy, un imputado puede argumentar que no autorizó una transacción, que sus credenciales fueron comprometidas, que el registro del banco está equivocado. En MAS, la firma soberana del titular está en cada acto. Esa firma deriva de su ADN, que deriva de su biometría. La única forma de que la firma sea válida es que el titular estuvo presente y la generó. La denegación plausible desaparece: si el acto lleva tu firma soberana, lo hiciste.

> *El crimen financiero que opera en MAS no se esconde detrás de identidades falsas, registros alterables o denegaciones plausibles. Opera con su identidad real, deja huellas inmutables, y produce evidencia*

> *matemáticamente irrefutable de cada uno de sus actos. Nunca antes el sistema financiero había sido tan inhóspito para el lavado de dinero.*

El operador del crimen organizado que usa MAS está creando, en cada transacción, un registro perfecto y atribuible de su propia actividad criminal. Irónicamente, el sistema que más protege la privacidad del ciudadano honesto es el que más expone al delincuente financiero.

La investigación que cambia sin perder poder

Si las instituciones no acumulan perfiles sobre sus titulares, ¿cómo investigan los reguladores y los fiscales? La respuesta es que el mecanismo cambia — el poder investigativo no disminuye.

En el modelo actual, el tribunal ordena al banco revelar sus registros sobre el titular. El banco presenta lo que tiene. La defensa cuestiona si esos registros fueron manipulados. El proceso se extiende. Las respuestas son inciertas.

En MAS, el tribunal ordena a la institución certificar los hechos en los que participó. La institución estuvo presente en cada transacción. Puede ser compelida a certificar los hechos que co-firmó. Esa certificación es matemáticamente irrefutable — ninguna defensa puede argumentar que fue fabricada.

Más importante aún: la Bóveda D contiene hechos certificados sin PII. El patrón de esos hechos — frecuencia inusual, montos atípicos, contrapartes recurrentes — es visible para reguladores con acceso apropiado sin necesitar revelar la identidad del titular. La Unidad de Análisis Financiero puede detectar patrones sospechosos antes de saber a quién pertenecen. Cuando el patrón justifica la investigación, el mandato judicial conecta el patrón al ADN. La identidad se revela solo cuando hay causa suficiente.

Eso es más parecido a una investigación bien construida que a la vigilancia masiva que caracteriza el sistema actual. Y produce evidencia que soporta mejor el escrutinio judicial.

Open Finance redefinido

La Ley 21.521 — la Ley Fintec chilena de 2023 — establece un marco de portabilidad de datos financieros. Su lógica es simple: si el cliente autoriza, las instituciones deben compartir sus datos con terceros — otras fintechs, aseguradoras, empresas que ofrecen mejores condiciones.

Es una conquista real. Y está construida sobre el modelo equivocado.

El Open Finance de la Ley 21.521 asume que los datos del titular viven en las instituciones y que la portabilidad consiste en permitir que esas instituciones los compartan con otras instituciones. El titular da permiso. Las instituciones transfieren datos. El titular no ve lo que se transfiere, no puede verificar que sea exacto, y no puede revocar el acceso en tiempo real sin pasar por los procesos de cada institución.

En MAS, el Open Finance tiene una arquitectura diferente. El titular no da permiso para que su banco comparta sus datos. El titular decide qué hechos certificados presenta directamente a qué actores. No hay transferencia entre instituciones. Hay presentación soberana de hechos que le pertenecen al titular.

La fintech que quiere ofrecer mejores condiciones crediticias no pide al banco del titular acceso a su cuenta. Le pide al titular que presente los atributos certificados relevantes. El titular decide cuáles presentar, por cuánto tiempo, y revoca ese acceso en tiempo real si cambia de opinión.

Es más poder para el titular. Más competencia en el mercado financiero. Y menos concentración de datos en instituciones que se convierten en objetivos de ataques.

* * *

El sistema financiero es el lugar donde la tensión entre privacidad y transparencia es más visible y más difícil de resolver. Cualquier arquitectura que lo olvide produce, inevitablemente, uno de dos fracasos: o protege tanto la privacidad que habilita el crimen financiero, o produce tanta transparencia que destruye la privacidad.

MAS resuelve esa tensión de una forma que ningún sistema anterior había logrado. Protege más la privacidad del ciudadano honesto — porque nadie acumula su perfil financiero completo — y hace más difícil el crimen financiero — porque ningún acto puede negarse, alterarse ni atribuirse a una identidad falsa.

La clave está en la distinción entre datos y hechos. Los datos son acumulables, perfilables, revelables sin consentimiento. Los hechos certificados son soberanos, irrefutables y presentados únicamente cuando el titular lo decide.

Miguel puede evaluar créditos con certeza sin ver las transacciones del solicitante. La UAF puede detectar patrones de lavado sin necesitar acceso masivo a todos los registros financieros. El regulador puede exigir evidencia irrefutable sin tener que confiar en los propios registros del regulado.

Ese es el sistema financiero que MAS habilita. No como un proyecto futuro. Como la consecuencia directa de aplicar la arquitectura de memoria cero a los actos financieros.

▸ **Profundidad técnica — Prueba de conocimiento cero de atributos financieros en MAS**

La prueba de conocimiento cero (ZKP) aplicada a atributos financieros en MAS opera mediante compromisos criptográficos sobre los hechos del KEL. El banco del titular calcula un commitment C = Hash(valor_atributo || nonce_secreto) y lo firma soberanamente. El titular puede presentar ese commitment junto con una prueba de rango — una ZKP que demuestra que el valor real está en un rango R sin revelar el valor exacto.

El verificador (la fintech, Miguel, la aseguradora) verifica: (1) que la firma del banco sobre el commitment es válida; (2) que la prueba de rango es matemáticamente correcta para el commitment presentado. Sin ninguna de estas dos verificaciones acceder al valor subyacente.

En la implementación de MAS, el banco emisor del atributo firma el commitment con su clave soberana institucional — que también tiene un KEL. El verificador puede comprobar que el banco emisor es una

institución acreditada y que su firma no ha sido revocada. La cadena de confianza es: titular → banco → atributo certificado → prueba de conocimiento cero → verificador.

Esto elimina la necesidad de que el titular comparta sus estados de cuenta, el historial de transacciones o cualquier dato de cuenta. Solo el atributo certificado — «mis ingresos están en el rango X-Y» — con la prueba de que eso es verdad, verificable sin revelar la base.

—

Capítulo 16 (bis)

Lo que cambia para la fidelización

Hay una industria entera que no está en el debate sobre privacidad digital — y debería estar. Es la industria de la fidelización.

Los programas de puntos, los cupones personalizados, los esquemas de retención basados en el comportamiento de compra representan una de las inversiones más grandes que las organizaciones hacen en su relación con los clientes. Y están construidos sobre el mismo defecto de origen que los sistemas de gestión de consentimiento: la asimetría de información entre la organización y el titular.

La organización sabe cuánto gasta el cliente, qué compra, cuándo, con qué frecuencia, qué abandona en el carrito, qué le hace cambiar de tienda. El cliente sabe que tiene ciertos puntos acumulados y que con ellos puede obtener un descuento. La relación es fundamentalmente desigual. Y esa desigualdad — durante décadas — fue la base del negocio.

Lo que los datos dicen — y nadie presenta en el board

La investigación sobre programas de fidelización ha acumulado, en los últimos años, un conjunto de hallazgos que el sector prefiere no discutir abiertamente.

McKinsey & Company publicó en 2021 que solo el 13% de los miembros de programas de lealtad cambia realmente su comportamiento de compra como resultado del programa. El 87% restante habría gastado lo mismo sin él. Lo que

la organización atribuye al programa es, en su mayor parte, el comportamiento natural de sus clientes más comprometidos — que se habrían inscrito de todos modos porque ya son clientes frecuentes.

Bond Brand Loyalty documentó en su reporte 2023 que el usuario promedio está inscrito en 14.8 programas de fidelización pero solo participa activamente en 6.4. El resto son cuentas dormidas, puntos que no se redimirán, datos que la organización acumula sobre personas que no están en la relación que creen que están.

Javelin Strategy & Research estimó en 2020 que el fraude anual en programas de lealtad globalmente supera los tres mil millones de dólares. El fraude no ocurre a pesar de la sofisticación del sistema — ocurre precisamente porque el sistema está construido sobre identidades no verificadas que acumulan valor sin que nadie certifique que pertenecen a quien dice ser su titular.

Bain & Company publicó en 2022 que entre el 25 y el 35 por ciento del incremento observado en el gasto de los miembros leales es genuinamente incremental — atribuible causalmente al programa. El resto es selección: los clientes más leales se inscriben porque ya eran leales, no porque el programa los hizo así.

Hallazgo	Fuente	Implicación
Solo 13% cambia comportamiento real	McKinsey, 2021	87% del costo del programa no produce efecto incremental
14.8 programas inscritos / 6.4 activos	Bond Brand Loyalty, 2023	El 57% de las inscripciones son datos muertos que se acumulan
$3.1B fraude anual en loyalty	Javelin Strategy, 2020	La identidad no verificada es el principal vector de ataque
25-35% del lift es genuinamente incremental	Bain & Company, 2022	El 65-75% del lift observado es sesgo de selección, no causalidad

Lo que estos números revelan no es que los programas de lealtad sean inútiles. Revelan que están midiendo lo que les conviene medir, atribuyéndose lo que es conveniente atribuirse, y evitando la pregunta que ningún dashboard interno

hace: ¿cuánto de lo que llamamos lealtad es preferencia real, y cuánto es simplemente la inercia de no haberse tomado el tiempo de salirse?

La jaula de oro

El programa de fidelización bien diseñado produce un efecto específico: hace costoso salirse. No porque el cliente no quiera salirse. Sino porque ha acumulado puntos que perdería, porque se ha acostumbrado a beneficios que el competidor no ofrece, porque el sistema de datos que la organización tiene sobre él le permite personalizar la oferta de una forma que un competidor nuevo no podría replicar desde cero.

Eso se llama, en la literatura de marketing, lock-in. Y durante mucho tiempo fue sinónimo de éxito.

El problema es que el lock-in que funciona en una relación asimétrica de información empieza a fallar cuando el cliente tiene acceso a más información. Cuando puede comparar. Cuando puede saber exactamente qué está cediendo a cambio de esos puntos. Cuando la fricción de salirse ya no compensa la incomodidad de quedarse en una relación que no eligió soberanamente.

> *El cliente que se queda porque no puede irse no es un activo — es un pasivo con fecha de vencimiento.*

Lo que el titular realmente quiere

Hay una confusión persistente en la industria de la fidelización: entre retención y preferencia.

La retención es que el cliente siga comprando. La preferencia es que el cliente quiera seguir comprando. La primera puede lograrse con fricción suficiente. La segunda solo puede ganarse.

Lo que el titular realmente quiere — y esto aparece consistentemente en cualquier estudio serio sobre comportamiento del consumidor en la era digital — no es

acumular puntos. Es tener relaciones con organizaciones que lo tratan como adulto. Que le explican para qué usan sus datos. Que le dan la opción real de decidir qué comparte y qué no. Que respetan sus decisiones cuando las toma.

Un cliente que eligió el programa de beneficios porque lo entendió y lo valoró es un cliente completamente diferente al que lo tiene porque nunca entendió cómo darse de baja.

Lo que OwnTrust cambia en este contexto

OwnTrust no elimina los programas de fidelización. Cambia la base sobre la que están construidos.

Cuando una organización implementa OwnTrust, el titular puede ver exactamente qué autorizó — componente por componente. Puede ver que autorizó el uso de sus datos de compra para personalizar ofertas dentro de esa organización. Y puede ver que no autorizó compartir esos datos con otras empresas del holding, ni usarlos para perfilamiento demográfico, ni cederlos a terceros para publicidad.

Esa granularidad cambia la relación. El titular que sabe exactamente qué autorizó y por qué — que entiende que está cediendo algo a cambio de algo que valora — es un titular que eligió soberanamente participar en el programa. Su participación no es inercial. Es activa. Y eso tiene un valor comercial que ningún sistema de puntos puede generar por sí solo.

Además, cuando el titular puede revocar cualquier autorización en treinta segundos con su firma soberana, la organización recibe una señal de mercado enormemente valiosa: sabe qué partes de su propuesta el titular valora suficientemente como para mantener, y qué partes no. Esa información — obtenida a través de la decisión soberana del titular, no a través de inferencias estadísticas — es la señal de mercado más honesta que existe.

El nuevo modelo de fidelización — basado en merecer

El programa de fidelización del futuro no se basa en hacer costoso salirse. Se basa en hacer valioso quedarse.

La diferencia parece sutil. No lo es.

Una organización que hace valioso quedarse tiene que preguntarse constantemente: ¿qué le estamos ofreciendo al titular que él elija valorar? ¿Qué hace que un titular con plena libertad de decisión, con información completa sobre lo que está cediendo, prefiera seguir en esta relación?

Esa pregunta es infinitamente más difícil de responder que «¿cómo diseñamos el sistema de puntos para que salirse sea complicado?». Pero producir la respuesta genera un activo que ningún programa de puntos puede generar: confianza genuina.

La confianza genuina no puede copiarse por un competidor. No puede comprarse con un presupuesto de marketing. No puede forzarse con un diseño de interfaz optimizado para maximizar aceptaciones. Solo puede ganarse — a través de la experiencia del titular de que esta organización lo trata como lo que es: un adulto con derechos soberanos sobre sus propios datos.

* * *

Hay una ironía en todo esto que vale la pena nombrar.

Las organizaciones que adopten OwnTrust van a obtener algo que sus sistemas actuales no pueden darles: datos de preferencia real. No datos de comportamiento sesgados por los incentivos del programa. No inferencias estadísticas sobre lo que el titular probablemente quiere. Datos de lo que el titular explícitamente eligió compartir, en qué condiciones, para qué propósito.

Esos datos son más valiosos. Más honestos. Más útiles para construir una propuesta de valor que el titular realmente quiera.

La soberanía del titular no es el fin del conocimiento del cliente. Es el comienzo del conocimiento honesto. Y el conocimiento honesto — el que viene de la

decisión soberana del titular, no de la asimetría de información — es la base más sólida que existe para construir una relación comercial de largo plazo.

> *La jaula de oro retiene. La soberanía de la elección fideliza. No son sinónimos. Y la diferencia entre los dos es la diferencia entre un cliente que espera poder irse y un cliente que no quiere irse.*

—

PARTE IV

El futuro

El camino hacia la soberanía total no es una predicción. Es una trayectoria.

«La soberanía no es el destino del viaje. Es la condición para que el viaje valga.»

Capítulo 17

De la cédula a la biometría

Carmen tiene sesenta y cuatro años. Tiene también tres cédulas de identidad distintas — la que usó durante su matrimonio, la que obtuvo cuando recuperó su nombre de soltera, y la que renovó el año pasado cuando la segunda venció. En cada una de esas transiciones, algo de su historia digital se fragmentó. Los sistemas de salud que la conocían por un nombre aprendieron un nombre nuevo. Los sistemas financieros actualizaron sus registros. Las plataformas donde tenía cuentas le pidieron que volviera a verificar su identidad.

En OwnTrust, ninguna de esas transiciones cambió nada.

Cuando Carmen renovó su cédula el año pasado, su historial de actos soberanos permaneció intacto. Las organizaciones que la conocen a través de OwnTrust no recibieron ninguna notificación, no necesitaron actualizar ningún campo, no tuvieron que pedirle que se registrara de nuevo. El hilo que conecta todos sus actos digitales sobrevivió a la renovación del documento porque no está anclado en el número del documento. Está anclado en el RUT. Y el RUT de Carmen no cambia.

Ese es el primer nivel de la arquitectura de identidad soberana. Suficiente para construir OwnTrust. Insuficiente para lo que viene.

El límite del RUT

El RUT funciona como ancla de identidad por una razón específica: en Chile, es un identificador permanente, único, asociado inequívocamente a una persona física. El Registro Civil lo administra con criterios robustos. El sistema legal lo reconoce como referencia primaria.

Pero el RUT tiene límites que la arquitectura honesta no puede ignorar.

El primero es geográfico: el protocolo diseñado sobre el RUT no exporta directamente a jurisdicciones donde ese identificador no existe o no tiene el mismo valor legal. Un sistema de identidad soberana verdaderamente portable necesita un ancla que no dependa de la decisión institucional de ningún Estado específico.

El segundo es de seguridad: los cuatro datos del documento — RUT, número de documento, fecha de nacimiento, fecha de vencimiento — son datos que en teoría solo el titular y el Registro Civil conocen, pero que en la práctica pueden ser conocidos por quien haya tenido acceso al documento físico, por quien haya procesado copias del documento, por quien tenga acceso a ciertos registros administrativos. No son datos secretos en el sentido fuerte del término.

El tercero, el más sutil, es filosófico: una identidad anclada en un número asignado por el Estado depende del Estado. Si el Estado decide asignar un nuevo número, si el Estado desaparece o se transforma radicalmente, si los sistemas de registro pierden consistencia — el ancla se debilita. Para una arquitectura que aspira a la soberanía real, eso es un límite que el diseño debe reconocer explícitamente.

OwnTrust lo reconoce. Por eso la especificación técnica de la arquitectura — la especificación técnica de la arquitectura — diseña el sistema en tres niveles, con la posibilidad de migración entre niveles sin ruptura del historial de actos soberanos del titular.

El chip como verificador criptográfico

La cédula de identidad chilena emitida desde 2013 contiene algo que la mayoría de sus portadores desconoce: un chip de comunicación de campo cercano con datos biométricos firmados criptográficamente por el Registro Civil de Chile.

El ecosistema de presencia: wearables como endpoints del Simbionte

La cédula es la llave del génesis. El Secure Enclave del teléfono es el hogar del Fragmento A. Pero el titular no porta solo un dispositivo. Porta un ecosistema: reloj, anillo, lentes, teléfono. En el horizonte próximo: bolígrafo, ropa, entorno físico instrumentado.
Cada uno de esos dispositivos tiene capacidad de lectura biométrica. Cada uno puede, potencialmente, ser un nodo de autenticación del Simbionte Soberano. La identidad biométrica ambiental — la visión de que el Simbionte se expresa no desde un único dispositivo sino desde el ecosistema completo de presencia física del titular — no es una extensión de la arquitectura actual. Es su evolución natural, para la que el protocolo base está diseñado desde el origen.
Los wearables con sensores fisiológicos — variabilidad cardíaca, conductancia galvánica, temperatura — extienden la capacidad de detección de coerción: la coerción que dura minutos deja huella fisiológica en el baseline continuo que una autenticación puntual no puede capturar. En ese modelo, la autenticación no es un acto — es un estado. El titular está autenticado mientras su ecosistema confirme que es él. Cualquier inconsistencia entre sensores es una señal de anomalía.

El titular del futuro no se autentica. Está autenticado.

No con una firma digital cualquiera. Con la firma de la la autoridad certificadora del Estado que Chile mantiene bajo los estándares de la Organización de Aviación Civil Internacional, los mismos estándares que usan los pasaportes en todo el mundo. El chip contiene, entre otros datos, la fotografía tomada por el Registro Civil en el momento de la emisión. Esa fotografía está firmada de forma tal que cualquier actor con acceso al certificado raíz de la la autoridad certificadora del Estado puede verificar que es auténtica — que proviene realmente del Registro Civil, que no fue alterada, que corresponde a ese documento específico.

Lo que el génesis de segunda generación de OwnTrust hace con ese chip es precisamente eso: usarlo para establecer una cadena de confianza que llega hasta el Estado.

El proceso es el siguiente. El titular acerca su cédula al dispositivo. El dispositivo lee el chip mediante el protocolo NFC estándar. Extrae los datos personales y la

fotografía biométrica. Verifica la firma del Registro Civil contra el certificado la autoridad certificadora del Estado incluido en la aplicación. Si la verificación es exitosa, el documento es auténtico — matemáticamente, no por declaración de nadie.

Luego, el dispositivo activa la cámara frontal. Un modelo de reconocimiento facial — un motor de reconocimiento facial que corre completamente en el dispositivo, sin enviar ninguna imagen a ningún servidor, — compara la cara del titular en vivo con la fotografía del chip. Si la similitud supera el umbral, la persona es el titular del documento.

Y entonces — esto es lo más importante — tanto la fotografía del chip como la imagen en vivo se destruyen. No se envían a ningún servidor. No se almacenan en ninguna base de datos. No contribuyen a ningún perfil biométrico. Existen en memoria por segundos. El sistema recibe solo el resultado: el titular es quien dice ser, con el respaldo criptográfico del Registro Civil de Chile.

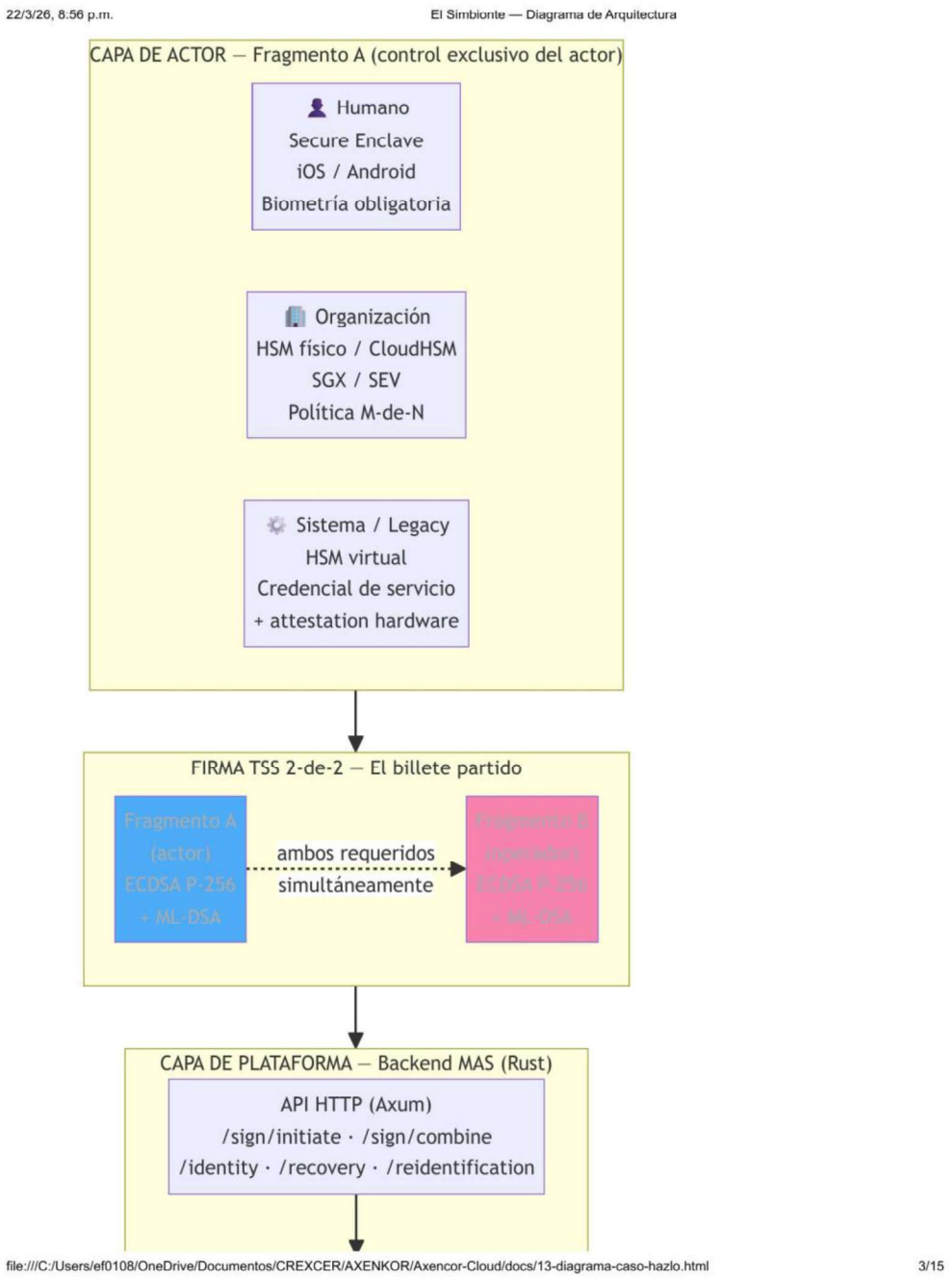


Figura 8 — Arquitectura en tres capas del Motor de Autoría Soberana (MAS) · Capa de Plataforma (Backend Rust / el motor del servidor backend) · Capa de Actor (Fragmento A, hardware) · Capa de Aplicación (MVOK, SDK B2B, HAZLO) · TSS 2-de-2: ECDSA P-256 + ML-DSA FIPS 204

Eso produce algo que ninguna verificación manual puede producir: una cadena de confianza que no depende de la declaración de ninguna empresa privada. OwnTrust no dice que Carmen es Carmen. El Registro Civil firmó la fotografía de Carmen. La matemática verificó que Carmen y la fotografía coinciden. OwnTrust solo registra el resultado de esa verificación.

El ADN biométrico

El chip NFC resuelve el problema de autenticidad del documento. Pero todavía depende del documento físico. Que el titular lo tenga. Que esté vigente. Que el chip funcione. Que el Estado que lo emitió siga operando con los mismos estándares.

La arquitectura de MAS — el Motor de Autoría Soberana, del cual OwnTrust es la primera implementación — diseña un tercer nivel que trasciende el documento por completo.

El ADN biométrico no se calcula a partir de ningún identificador asignado por ninguna institución. Se calcula a partir de características de la geometría facial del titular — proporciones derivadas de la estructura ósea que permanecen estables a lo largo de décadas, que no dependen de ningún documento, que ningún registro civil puede revocar, que ningún sistema puede alterar.

Este ADN no es una fotografía ni un template biométrico de los que usan los sistemas de reconocimiento facial actuales — que almacenan el template y lo usan para comparar. Es una función matemática aplicada a características geométricas que produce un identificador estable, calculado completamente en el dispositivo, sin que ningún dato biométrico crudo salga nunca del hardware del titular.

El titular se convierte en su propia llave maestra. No porque alguien lo decidió. Porque la matemática lo permite.

* * *

Hay algo que vale nombrar sobre el arco completo de esta evolución.

El movimiento de la cédula a la biometría no es un movimiento técnico. Es un movimiento sobre la naturaleza de la identidad. La respuesta a la pregunta — ¿quién soy yo, en el mundo digital? — cambia radicalmente según cuál sea el ancla.

> *Si el ancla es un número asignado por el Estado, la identidad digital depende del Estado. Si el ancla es un documento físico, depende de tener ese documento. Si el ancla es la geometría facial del titular, depende únicamente de él — de que siga siendo la persona que es.*

OwnTrust comienza con el RUT porque es el ancla más robusta disponible hoy en Chile, la que el sistema legal reconoce, la que permite construir la primera implementación con la máxima legitimidad institucional posible. Pero diseña desde el principio para migrar sin ruptura hacia anclas más fundamentales. El titular que genera su identidad soberana hoy no pierde su historial cuando la biometría esté disponible. Su registro de actos soberanos migra con él.

Eso es lo que hace que la arquitectura sea verdaderamente soberana: no solo en el momento presente, sino a través del tiempo.

▸ **Profundidad técnica — El génesis NFC en la especificación técnica**

El proceso técnico del génesis de segunda generación opera en cuatro fases secuenciales:

Primera fase — lectura MRZ: La aplicación usa la cámara para leer la la zona de datos legibles del documento de la cédula. Extrae el número de documento, la fecha de nacimiento y la fecha de vencimiento. Estos tres datos constituyen la contraseña el mecanismo de control de acceso al chip que el estándar los estándares internacionales de documentos de identidad requiere para establecer una sesión autenticada con el chip.

Segunda fase — handshake NFC: Con la contraseña BAC, la aplicación establece la sesión autenticada. Lee el el grupo de datos personales del chip (datos del documento), el el grupo de datos biométricos del chip (fotografía biométrica en formato formato de imagen) y el el objeto de seguridad del documento, que contiene los hashes firmados de todos los Data Groups).

Tercera fase — verificación de autenticidad: La aplicación verifica que los hashes del SOD coinciden con los datos leídos, y que la firma del SOD es válida contra el la autoridad certificadora del Estado de Chile incluido en la aplicación. Sin conexión a internet. Sin consulta al Registro Civil. Completamente offline. Si ambas verificaciones pasan, el documento es auténtico con certeza criptográfica.

Cuarta fase — matching biométrico on-device: La cámara frontal captura la imagen del titular. un motor de reconocimiento facial on-device extrae embeddings faciales de la imagen en vivo y de la fotografía del chip. Calcula la similitud biométrica. Si supera el umbral configurado, la persona es el titular. La fotografía del chip y la imagen en vivo se destruyen inmediatamente. El ADN se calcula con los datos del

chip — más robusto que el ingreso manual. El IS permanece igual, garantizando la continuidad del historial.

La migración de un titular con génesis v1 a génesis v2 es transparente: el IS no cambia, el AID del próximo acto incorpora el respaldo NFC, el historial anterior permanece intacto.

—

Capítulo 18

MAS — el protocolo completo

Imagine un contrato firmado por una entidad que no es una persona humana. No una empresa representada por un apoderado — sino un agente autónomo de software que actúa en nombre de una persona, ejecutando instrucciones que esa persona definió previamente, en un momento en que la persona no está disponible para firmar.

La pregunta que ese contrato plantea no es nueva. El derecho lleva siglos respondiendo preguntas sobre mandatos, representaciones y poderes legales. Pero la respuesta que el derecho ha construido depende de intermediarios verificables: notarios, registros, sellos institucionales. Intermediarios que existen porque, en su ausencia, no hay forma de verificar que el agente realmente tiene la autoridad que afirma tener.

MAS resuelve ese problema sin intermediarios. Con matemática.

De la persona al protocolo

OwnTrust implementa la identidad soberana para un caso de uso específico: una persona humana que interactúa con una organización. El titular llega con su cédula. El sistema genera el ADN, el AID, la firma soberana. El acto queda registrado de forma irrefutable. La organización recibe el certificado.

Ese es el primer perímetro del problema de identidad digital. Importante. Urgente. Resoluble con la arquitectura que los capítulos anteriores describieron.

Pero el problema de identidad digital tiene un perímetro más amplio. Uno que la próxima década va a volver urgente de una forma que hoy apenas se intuye.

¿Qué pasa cuando el actor que necesita demostrar su identidad no es una persona, sino un agente autónomo? ¿Qué pasa cuando una empresa no está compuesta de personas tomando decisiones en tiempo real, sino de agentes de inteligencia artificial coordinando entre sí, ejecutando contratos, transfiriendo valor, actuando en mercados? ¿Qué pasa cuando la identidad de una organización necesita ser verificable no por un humano en una oficina, sino por otro sistema en un milisegundo?

Estas preguntas no son hipotéticas. Son el horizonte próximo de la economía digital. Y ningún sistema de identidad digital diseñado para el mundo de hoy tiene respuesta para ellas.

MAS la tiene.

El Simbionte

El Simbionte es la entidad de identidad soberana en MAS. No es una cuenta. No es un certificado. Es una entidad viva — con origen, historia y capacidad de delegación.

El Simbionte de una persona tiene un AID derivado de su ADN, un historial de actos soberanos registrado en su KEL, y la capacidad de generar sub-identidades — identidades contextuales que se vinculan al Simbionte principal mediante una relación de delegación verificable en el propio KEL.

Cuando una persona le da instrucciones a un agente autónomo — le dice «actúa en mi nombre para este propósito específico, dentro de estos límites» — esas instrucciones se registran en el KEL como un acto soberano. El agente recibe un fragmento de autoridad derivada, verificable matemáticamente. Quien interactúa con ese agente puede verificar, sin contactar a la persona ni a ningún intermediario, que el agente tiene la autoridad que afirma tener.

No porque el agente lo dice. Porque el KEL del titular lo registra, con la firma soberana del titular, en el momento en que la autoridad fue delegada.

La empresa agéntica

La empresa agéntica es aquella cuyos procesos más críticos los ejecutan agentes autónomos coordinados por un sistema de identidad verificable.

No es ciencia ficción. Las empresas ya operan con procesos automatizados que toman decisiones sin intervención humana en tiempo real. Lo que les falta es la infraestructura de identidad que permita que esos procesos sean verificables externamente — que quien interactúa con uno de esos agentes pueda saber que el agente tiene la autoridad que afirma tener, que la delegación fue otorgada por un humano con identidad soberana verificable, que los límites de esa delegación son los que el agente dice que son.

MAS provee esa infraestructura. No como un producto de software. Como un protocolo abierto sobre el cual cualquier implementación puede construirse.

Una empresa que opera sobre MAS puede tener agentes que firman contratos, que procesan solicitudes, que transfieren valor — y cada uno de esos actos queda registrado en el KEL del agente, vinculado al KEL del humano que delegó la autoridad, verificable por cualquier contraparte sin necesitar contactar a ningún intermediario.

> *La empresa agéntica no es una metáfora. Es la consecuencia natural de tener un protocolo donde cualquier actor puede actuar con identidad verificable — y donde la responsabilidad siempre remonta, matemáticamente, al titular humano que otorgó la delegación.*

La portabilidad entre protocolos

Hay una consecuencia del diseño de MAS que no es obvia hasta que se examina en detalle: la portabilidad entre protocolos.

OwnTrust es una implementación de MAS. Pero no la única posible. El protocolo está diseñado para que múltiples implementaciones puedan interoperar — que el AID de un titular en OwnTrust pueda ser verificado por un sistema construido sobre otra implementación de MAS, en otra jurisdicción, por otro operador.

Eso es lo que convierte MAS en infraestructura en el sentido verdadero del término. No un producto que un actor controla. Un protocolo que cualquier actor puede implementar y con el que cualquier implementación puede interoperar.

El efecto de red que esto produce es diferente al efecto de red de las plataformas tradicionales — donde el valor está en la centralización, en que todos usen el mismo sistema. El efecto de red de MAS está en la descentralización: cada nueva implementación amplía el perímetro de actores que pueden interactuar con verificación soberana, sin que ninguno de ellos dependa de los demás.

* * *

OwnTrust no es el destino. Es el primer paso.

La arquitectura que este libro describió — el ADN, el AID, el KEL, las Bóvedas, el principio de memoria cero — es la implementación de MAS para el caso de uso más inmediato: la persona que necesita demostrar que consintió, que ejerció un derecho, que firmó un acto soberano, en el mundo digital de hoy.

El protocolo completo va más lejos. No porque sea más complejo — sino porque el problema que resuelve es más amplio. El mundo donde agentes autónomos necesitan identidades verificables, donde empresas necesitan demostrar que sus procesos automatizados actúan dentro de los límites autorizados por humanos reales, donde jurisdicciones diferentes necesitan interoperar sin crear nuevos intermediarios de confianza — ese mundo es el que MAS tiene diseñado para habitar.

Y está llegando más rápido de lo que la mayoría de las organizaciones se están preparando para él.

▸ **Profundidad técnica — Delegación soberana en MAS**

La delegación en MAS opera mediante un evento de tipo ixn/delegación en el KEL. Este evento contiene: el AID del delegante (el titular humano), el AID del agente delegado, el alcance de la delegación (descripción estructurada de propósitos y límites), la vigencia de la delegación, y la firma soberana del delegante.

El agente recibe, junto con su propio AID, una referencia verificable al evento de delegación en el KEL del titular. Cuando el agente actúa, incluye esa referencia en el certificado del acto. La contraparte puede verificar que el evento de delegación existe en el KEL del titular, que la firma es válida, y que el acto del agente cae dentro del alcance delegado.

La cadena de verificación es: acto del agente → delegación en KEL del titular → firma soberana del titular → ADN del titular. En ningún punto de esa cadena interviene OwnTrust como garante. La matemática es garante.

Los eventos de delegación pueden ser revocados por el titular mediante un evento rot/revocación en su propio KEL. La revocación es inmediata. Cualquier acto posterior del agente que no incluya una delegación vigente es matemáticamente inválido.

—

Capítulo 19

La soberanía como derecho

En el siglo XIII, los comunes en Inglaterra eran tierras de uso compartido. Bosques donde las comunidades cazaban, pastizales donde los pequeños agricultores llevaban sus animales, aguas de donde sacaban el alimento que no podían cultivar. Nadie los poseía. Todos los usaban. La lógica de su existencia era la misma que la lógica del aire: algo que estaba ahí porque lo necesitaban todos.

El movimiento de cercamientos — entre los siglos XV y XIX — los convirtió en propiedad privada. No de golpe. No con una decisión única. Sino con la acumulación de actos individuales de registro, de vallado, de exclusión. Cada uno de esos actos parecía local, específico, razonable en su contexto. El resultado agregado fue que los comunes desaparecieron — y con ellos, la posibilidad de subsistencia autónoma para millones de personas que pasaron a depender del trabajo en tierras de otros.

Estamos viviendo el equivalente digital de ese proceso. Sin que nadie lo haya decidido explícitamente. Sin que nadie lo esté nombrando con la claridad que merece.

El cercamiento digital

Los datos de identidad — quién eres, qué hiciste, con quién interactuaste, qué consintiste, qué decidiste — son el equivalente digital de los comunes. Durante milenios de historia humana, esa información era conocida por quien la protagonizaba, por su comunidad inmediata, y por nadie más. Era, en términos prácticos, soberana.

La infraestructura digital la cercó. No con mala intención. Con la lógica de quien construye un sistema que necesita identificar a sus usuarios, que necesita recordar sus preferencias, que necesita gestionar sus transacciones. Cada decisión de diseño fue local y razonable. El resultado agregado fue que los datos de lo que millones de personas hacen, deciden, consienten y desisten quedaron en servidores de organizaciones que no son esas personas.

Y a diferencia de los comunes del siglo XIII, este cercamiento ocurrió sin que la mayoría de los afectados siquiera lo notara. Porque los cercadores no vallaron tierras visibles. Cercaron algo mucho más difícil de ver: la evidencia de los propios actos.

La regulación que no llega a la raíz

Las leyes de datos personales — en todas sus versiones, en todas las jurisdicciones — parten de un supuesto que nunca cuestionan. Asumen que los datos existen en servidores de terceros y que la tarea de la norma es regularlos en beneficio de quien los protagonizó.

Es una concesión enorme, disfrazada de protección.

El RGPD europeo, la Ley 21.719 chilena, la LGPD brasileña, la CCPA californiana — todas ellas construyen sobre la misma premisa: los datos del titular están en

poder de organizaciones, y el titular tiene derechos sobre esos datos. Derechos de acceso, de rectificación, de cancelación, de oposición, de portabilidad.

Esos derechos son conquistas reales. Han cambiado la forma en que las organizaciones gestionan los datos. Han dado a los titulares herramientas que antes no tenían. Merecen el reconocimiento que tienen.

Y son insuficientes.

Son insuficientes porque regulan la custodia de algo que debería pertenecer al titular desde el origen. Son insuficientes porque los derechos que otorgan son peticiones: el titular pide al custodio que le muestre, corrija o elimine lo que debió ser suyo desde el principio. No es soberanía. Es dependencia con procedimiento. Son insuficientes porque no responden la pregunta fundamental: ¿quién tiene derecho a generar la evidencia de un acto?

Esa pregunta es diferente a «¿quién es dueño de los datos?». Es más profunda. Porque los datos son consecuencia. La evidencia es el acto mismo. Y el acto ocurrió en el titular, con el titular, por el titular. La pregunta es por qué la evidencia de ese acto le es ajena desde el momento en que existe.

El derecho que falta

Lo que los sistemas legales no han reconocido todavía — y lo que este libro argumenta que deben reconocer — es el derecho a generar irrefutablemente la evidencia de los propios actos.

No como un derecho derivado de la privacidad. No como un aspecto de la protección de datos personales. Como un derecho autónomo, con su propio fundamento y sus propias implicaciones.

> *El derecho a la soberanía digital sobre los propios actos. Con tres componentes concretos: el derecho a una identidad digital que no dependa de ninguna plataforma para existir; el derecho a generar evidencia de los propios actos verificable por cualquier tercero sin intermediarios; y el*

> *derecho a que los actos pasados permanezcan como fueron registrados en el momento en que ocurrieron.*

Lo que los Estados deben hacer

Los Estados tienen una tarea concreta que hacer con esta arquitectura — una tarea que va más allá de regular el comportamiento de las empresas.

Deben tratar la infraestructura de identidad soberana como tratan cualquier otra infraestructura crítica: como un bien público que requiere estándares abiertos, interoperabilidad obligatoria y protección frente a la captura por actores privados.

Cuando los Estados estandarizaron las tomas eléctricas, no lo hicieron para favorecer a ningún fabricante de electrodomésticos. Lo hicieron porque una infraestructura básica sin estándares es una infraestructura que beneficia a quien la controla y perjudica a quien depende de ella. La identidad digital soberana es hoy exactamente eso: una infraestructura básica sin estándares, que beneficia a las plataformas que la controlan.

Además, los Estados deben reconocer legalmente la evidencia soberana — el certificado criptográfico firmado por el titular — como evidencia de primera clase en los procesos administrativos y judiciales. No como un sucedáneo de los medios de prueba tradicionales. Como la forma más robusta de evidencia digital que existe, superior a los logs de base de datos, superior a los correos electrónicos, superior a cualquier registro que dependa de la honestidad del custodio.

Lo que las empresas deben aceptar

Las empresas que han construido sus modelos de negocio sobre la asimetría de información con sus clientes deben aceptar una verdad que resulta incómoda: esa asimetría no fue una conquista. Fue una concesión temporal de personas que no tenían alternativa.

La alternativa ahora existe.

Las organizaciones que implementen identidad soberana no están cediendo poder. Están reconociendo que el poder que tenían sobre los datos de sus clientes era prestado. Y que devolver ese poder — construir la relación sobre evidencia soberana en lugar de asimetría informacional — produce algo que ningún programa de puntos puede producir: una relación que el titular elige porque la entiende, porque la valora, porque sabe exactamente lo que está cediendo y por qué.

Esa relación es más difícil de construir. Es también la única que no tiene fecha de vencimiento.

Lo que los titulares pueden exigir

Los titulares — las personas — pueden exigir algo que hasta hace muy poco no era técnicamente posible: la autoría soberana de su historia digital.

No como un privilegio reservado a quienes entienden de criptografía. Como una condición básica de participación en la economía digital, tan natural como la posibilidad de firmar un contrato en papel.

Pueden exigir que las organizaciones con las que interactúan les permitan generar evidencia de sus propios actos. Que les devuelvan la autoría de lo que consintieron. Que les muestren exactamente qué autorizaron, cuándo y para qué — no en términos de política de privacidad, sino en términos de actos específicos con firmas verificables.

Esa exigencia no requiere legislación específica para cada tecnología. Requiere que el derecho reconozca el principio y que la arquitectura técnica lo haga operativo.

El principio ya está siendo reconocido, con diferentes grados de claridad, en las legislaciones de datos más avanzadas del mundo. La arquitectura técnica que lo hace operativo ya existe.

Lo que queda es la voluntad de las organizaciones de adoptarla — no porque la ley las obligue, sino porque es lo correcto para el tiempo que vivimos.

* * *

Hay una razón por la que este argumento importa más allá del debate técnico sobre identidad digital.

Las democracias del siglo XXI enfrentan una tensión estructural entre dos realidades: la creciente capacidad de los sistemas digitales de conocer, predecir y modelar el comportamiento humano, y la necesidad de que las personas sean actores autónomos — con la capacidad real de elegir, de disentir, de actuar de formas que los sistemas no predijeron.

Un titular cuya identidad digital depende completamente de organizaciones que no controla no es un actor autónomo en el sentido pleno. Es un actor dentro de un sistema diseñado por otros, con las reglas que esos otros definieron, con la información que esos otros decidieron que necesita tener.

> *La soberanía digital no es un tema técnico. Es una condición política. Y la arquitectura para habilitarla ya existe.*

—

EPÍLOGO

La Agencia de Protección de Datos Personales llama.

No es la misma persona que llamó en el prólogo de este libro. Es una analista diferente, en una jurisdicción diferente, con una reclamación diferente. Pero la pregunta es la misma que lleva años siendo la misma pregunta: ¿puede demostrar que el titular consintió?

Esta vez, la persona al otro lado del teléfono no busca en logs de base de datos. No redacta correos a su equipo legal pidiendo que reconstruyan el expediente. No cruza los dedos esperando que el sistema de gestión haya registrado correctamente lo que ocurrió hace dieciséis meses.

Abre el panel de OwnTrust. Busca el nombre del titular. Genera el certificado del acto de consentimiento. Es un código QR. Lo comparte con la analista de la APDP.

La analista lo escanea con el verificador estándar. El sistema ejecuta la verificación en milisegundos. Calcula el hash del certificado. Verifica la firma contra la clave pública del AID del titular. Confirma que el encadenamiento del KEL es íntegro. Devuelve el resultado.

Válido.

No «la empresa dice que es válido». No «el sistema registra que ocurrió». La matemática dice que este titular específico, con esta clave específica derivada de esta identidad soberana, firmó este consentimiento específico el día y hora registrados.

La analista de la APDP no tiene que confiar en la empresa. No tiene que confiar en OwnTrust. Tiene que confiar únicamente en estándares criptográficos auditados por la comunidad matemática global — los estándares criptográficos que decenas de miles de matemáticos y criptógrafos han examinado durante décadas y que ningún actor, en ningún lugar del mundo, ha logrado comprometer.

La llamada termina en doce minutos.

* * *

Este libro comenzó con una pregunta: ¿qué les muestra?

La pregunta parecía ser sobre compliance, sobre regulación, sobre los treinta días que la ley otorga para responder a una fiscalización. Pero nunca fue esa la pregunta real.

La pregunta real era sobre la naturaleza de la evidencia. Sobre quién tiene el derecho de generarla. Sobre por qué en el mundo digital — el mundo donde ocurre una fracción creciente de los actos más importantes de la vida de las personas — la evidencia de esos actos existe en servidores ajenos, bajo el control de organizaciones con interés en el resultado.

OwnTrust no es la respuesta definitiva a esa pregunta. Es la primera respuesta práctica, implementable hoy, con la infraestructura legal e institucional que Chile tiene disponible. La respuesta definitiva es MAS — el protocolo completo que hace la soberanía portable, interoperable, independiente de cualquier Estado o cualquier empresa.

Pero las respuestas definitivas siempre llegan después de las primeras respuestas prácticas. El ferrocarril llegó antes que la autopista. La autopista llegó antes que el avión. La primera implementación práctica de una idea correcta es lo que demuestra que la idea es correcta — y lo que abre el camino para las implementaciones que la llevarán más lejos.

La idea que este libro defiende es esta:

> *La evidencia de los actos de una persona le pertenece a esa persona. No como metáfora. No como aspiración. Como consecuencia matemática de una arquitectura donde la firma soberana del titular es el origen de la evidencia — y donde ningún actor puede generar esa evidencia en nombre del titular sin su participación activa.*

Cuando esa idea sea obvia — cuando parezca tan natural como que un contrato requiera la firma de ambas partes, como que una escritura pública requiera un notario, como que una sentencia requiera un juez ajeno a la disputa — nadie recordará que hubo un tiempo en que no lo era.

Por ahora, todavía lo recordamos.

Y ese recuerdo es la razón por la que vale la pena construir.

—

Fin de MEMORIA CERO

Identidad soberana, acto irrefutable

AXENKOR SpA · Primera edición, 2026