Autenticación de Registros Digitales

CONTEXTO

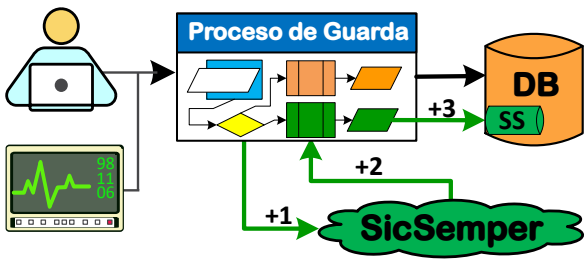
La mayor parte de las organizaciones genera sus registros de procesos de negocio en formato digital. Esto involucra tanto a los procesos internos como a las interacciones con sus proveedores y clientes.
Para los prestadores de servicios, los registros de interacciones con los clientes ven especialmente aumentada su criticidad y, en muchos casos, su volumen.
Estos registros han pasado de textos simples a documentos con formato, imágenes, audio y vídeo; a partir de lo cual, la opción de resguardar un ejemplar hológrafo o un impreso firmado desaparece.

PROBLEMA

Ante una controversia, la validez y confiabilidad de los registros no son condición suficiente para su resolución, ya que a partir de ellas no podemos demostrar su autenticidad.
Más allá de que el registro cuestionado persista incorrupto, existen escenarios en los que se hace necesario dotarlos de mayor autoridad.
Esto se debe a que la autenticidad introduce un concepto adicional que es la preservación, definida como un conjunto de acciones tendientes a proteger el registro de cualquier tipo de alteración, incluso intencional.

SOLUCION

SicSemper es la solución que permite demostrar fehacientemente la autenticidad del contenido de los registros digitales ya sea en línea con el proceso de guarda, como en procesos posteriores de digitalización y consolidación.
Incluye tanto el servicio de autenticación como la preservación de esta evidencia (sin copias) y la posibilidad de validarla a lo largo del tiempo.



SicSemper · Detalles del Servicio

SicSemper es un servicio de autenticación que aumenta el valor probatorio de los registros digitales. Estos registros pueden consistir en cadenas de texto sin formato, estructuras XML, documentos, imágenes, videos, sonidos, etc. que durante la autenticación se combinan con datos complementarios como la fecha y la hora de generación, el originante y, de manera opcional, un destinatario específico.

SicSemper se estructura como SaaS (Software como Servicio), conlleva una muy sencilla implementación y se encuentra alojado en la nube, sobre infraestructura Microsoft Azure, bajo los mayores estándares de redundancia, accesibilidad y continuidad de negocio.

¿Cómo se resguarda la confidencialidad de los registros autenticados?

El servicio no almacena el contenido de los registros recibidos sino un conjunto de digestos tipo "hash" que permiten validar su autenticidad y los datos complementarios; pero no reconstruir la información original del registro. Toda la información recibida se descarta una vez procesada.

En los casos en los que las condiciones de confidencialidad del suscriptor para con sus clientes lo hicieran necesario, el contenido a autenticar puede ser encriptado antes de ser enviado, ya que no hay ningún requerimiento de que el servicio "comprenda" la información recibida.

¿Qué se recibe como resultado del proceso de autenticación?

Al finalizar la autenticación, se recibe un mensaje que contiene el resultado de la operación, un identificador o token y la fecha y hora de procesamiento. Estos datos serán conservados para permitir la validación de autenticidad del registro correspondiente.

¿Cómo se implementa SicSemper?

SicSemper es accesible como servicio web en sentido estricto, por lo que puede ser consumido desde cualquier plataforma informática capaz de invocar este tipo de servicios a través de Internet.

La interfaz de datos expone los "verbos" que permiten Acreditar la suscripción, enviar el contenido a Autenticar y posteriormente, Validar su autenticidad.

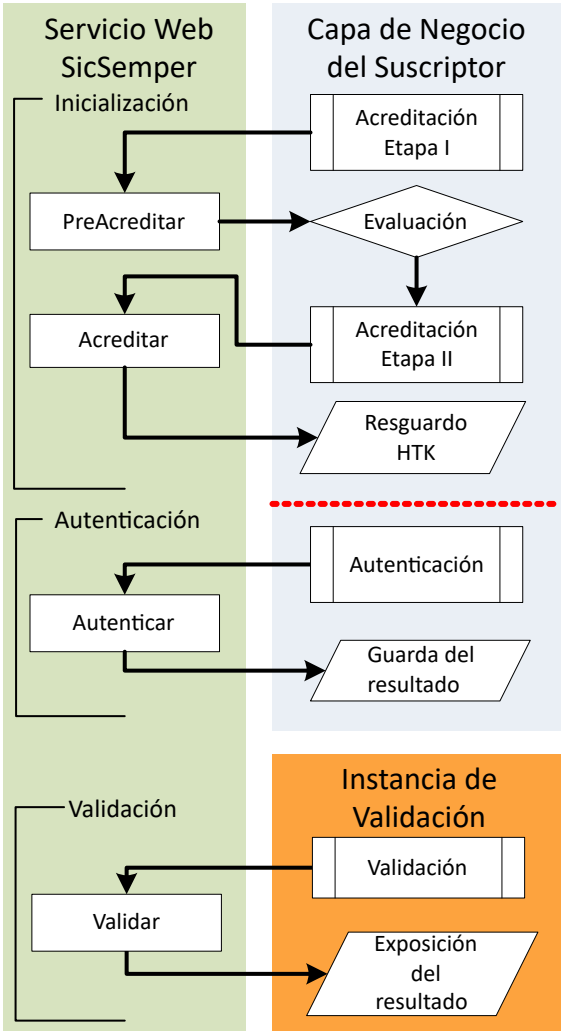
¿Cómo se contrata SicSemper?

SicSemper se contrata como una suscripción por el término mínimo de 6 meses para los cuales se establece un volumen mensual de transacciones, un tamaño máximo de registro y un tiempo límite de retención. Por ejemplo una suscripción puede pactarse para cien mil transacciones de registros de hasta 100KiBs, con retención por 10 años.
A partir de 2016, se podrán combinar lotes de registros de diferente tamaño dentro de una misma suscripción, manteniendo el mismo lapso de preservación.

SicSemper · Funcionamiento

El servicio de SicSemper, expone 4 métodos o verbos funcionales: PreAcreditar, Acreditar, Autenticar y Validar.

Los dos primeros verbos corresponden a la inicialización del servicio y podrán funcionar bajo requerimiento, ya que el lapso de acreditación puede pactarse por hasta 24hs, permitiendo efectuar múltiples autenticaciones a partir de una única inicialización. Esto es posible gracias a la implementación de una secuencia de hipertokens (HTK) parcialmente renovados en cada transacción, que permiten asegurar la vigencia de la acreditación.



El verbo PreAcreditar recibe un mensaje con la identificación de la suscripción (convenio) y el suscriptor.

El método verifica los datos y habilita el siguiente paso, solicitando elementos específicos para la acreditación, como por ejemplo, valores determinados de una tarjeta CMC (conjunto Mayor de Coordenadas) y provee un primer hipertoken (HTK) que le permitirá continuar la secuencia lógica.

Al Acreditar, el subscriptor envía un mensaje con el HTK recibido y los datos (coordenadas) solicitados.

El método verifica los datos y en caso positivo responde con un nuevo HTK que le permitirá continuar la secuencia lógica (más detalles en "Implementación").

Para Autenticar, el subscriptor envía el último HTK recibido y el contenido o registro codificado base64 (más detalles en "Implementación").

El método evalúa la información recibida y combina la información del registro con detalles de la subscripción, la fecha-hora y el servidor que efectúa el procesamiento.

Concluye el proceso con la devolución de un identificador de la transacción y la fecha-hora utilizada por el servidor y un nuevo HTK que le permitirá autenticaciones adicionales.

En condiciones típicas, la invocación del verbo Validar se produce de manera esporádica e independiente del proceso de autenticación y podrá requerir o no, de acreditación previa (según lo haya dispuesto el suscriptor).

En esta instancia de validación, el llamado a Validar utiliza un mensaje que incluye el identificador del convenio, el de la autenticación en sí, el del usuario que la produjo, la fecha-hora y el contenido, tal como originalmente fuera enviado para su autenticación.

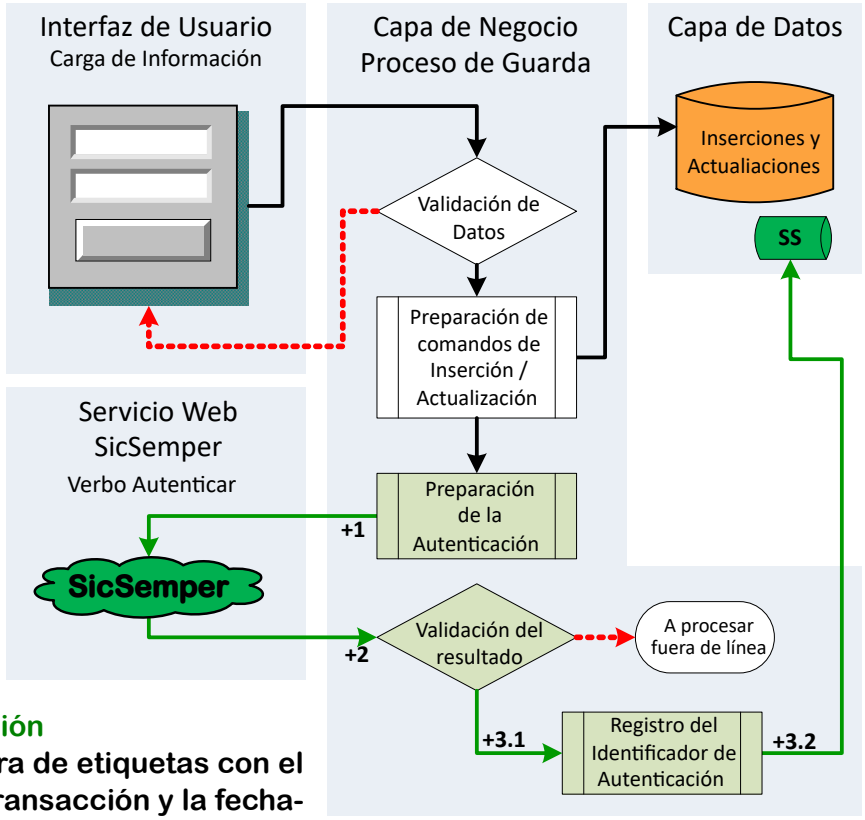
El método verifica los datos de identificación y, en caso positivo, aplica al contenido a validar el mismo tratamiento utilizado durante la autenticación y determina la autenticidad del mismo.

SicSemper · Implementación

La implementación del servicio de autenticación puede realizarse en línea con el proceso de guarda de registros o posteriormente, mediante el procesamiento por lotes.

La autenticación en línea puede implementarse fácilmente agregando 3 simples pasos posteriores a la guarda de datos y una tabla adicional para el registro del resultado de la autenticación.

En el esquema presentado a la derecha (simplificación de un caso tipo) se observan 3 subprocesos remarcados con fondo verde claro:



Preparación de la autenticación

Realiza la composición del mensaje a enviar a SicSemper.
El mensaje es una simple estructura de etiquetas en la que se organizan los identificadores de la suscripción, el HiperTokens recibido previamente y el contenido a autenticar codificado Base64. Finaliza con la invocación del verbo Autenticar de SicSemper.

Validación del resultado

Evalúa si la autenticación resultó positiva o no.

Registro del Identificador de Autenticación

La autenticación devuelve una estructura de etiquetas con el resultado, un identificador único de la transacción y la fecha-hora de registro.

Los dos últimos valores deberán ser registrados en una nueva tabla, accesoria al modelo de datos original, estableciendo una relación unívoca con el registro autenticado. Adicionalmente se recomienda contar con un campo entero adicional que identifique el "protocolo" utilizado en la preparación del contenido para su autenticación: el usuario activo, cuáles campos y en qué orden se incluyeron, su codificación y, cuando corresponda, su encriptación.

La autenticación fuera de línea puede utilizarse tanto por política prestablecida como para dar tratamiento a los registros cuya autenticación en línea fue intencionalmente omitida (P.e. hora pico, el tipo de registro conlleva requerimientos especiales, etc.) o hubiera fallado (p.e. no disponibilidad de conexión a internet).

El procedimiento de invocación del verbo autenticar fuera de línea es exactamente el mismo: Preparación - Validación - Registro, resultando el mecanismo más sencillo para su implementación, el rastreo de registros de las tablas principales que no poseen contrapartida en la tabla adicional que resguarda los identificadores de autenticación.

En todos los casos debe tenerse en cuenta que, para la posterior validación de autenticidad, deberá enviarse exactamente el mismo contenido que se utilizó en la autenticación junto con los identificadores de convenio, usuario autenticador, transacción de autenticación y la fecha-hora de procesamiento.