## CAI6. Autenticación con certificados digitales cualificados, control de acceso y subastas confiables para compras de medicamentos en Servicio de Salud

Archivos adjuntos:

AutomatizaSeparacionDeberes.pdf (251,003 KB)

Dentro del Plan de Digitalización (PD) previsto por un Servicio de Salud de un Gobierno de Europa, se ha consultado a la empresa INSEGUS sobre aspectos relacionados con la seguridad de la información y que son los siguientes:

- **AUTENTICACIÓN DE PERSONAS CON CERTIFICADOS DIGITALES CUALIFICADOS**
- **AUTENTICACIÓN DE LOS SERVIDORES WEB DEL SERVICIO DE SALUD CON CERTIFICADOS DIGITALES CUALIFICADOS**

El Servicio de Salud público nos propone **automatizar estos aspectos mediante procesos de negocio debido a los beneficios que nos han comunicado que supondrá para el mismo.** Las consultas a atender por INSEGUS son las siguientes:

### Consulta 6.1 ¿Cómo se puede generar la solicitud de los certificados digitales a las Autoridades de Certificación cualificadas para las partes interesadas del Servicio de Salud?

Se solicita a INSEGUS por parte del cliente, en primer lugar presentar, **de forma lo más visual y completa posible,** el modelo de proceso de negocio (diagrama BPMN 2.0) de elaboración de **una solicitud de un certificado digital cualificado** siguiendo la estructura especificada en el estándar X.509 a una Autoridad de Certificación mediante los ***Certificate Signing Request*** (CSR) para que pueda ser seguido por cada **una de las partes interesadas, usuarios de las aplicaciones del Servicio de Salud**. Para alcanzar la seguridad requerida en la actualidad, los certificados deben utilizar **claves de al menos 4096 bits de longitud**.

Es importante detallar **el proceso que se lleva a cabo para comprobar por la autoridad de certificación que el empleado que tiene el par de claves es realmente el que dice que es**. Puede haber varios procesos, por favor recomiende al Servicio de Salud el que considera más seguro, justificando su respuesta.

**Caso de test:** El cliente nos requiere **al menos la generación de una solicitud de certificado digital donde se lleve a cabo la implementación de dicho modelo de proceso (entre las posibles herramientas para la implementación del proceso se podrían utilizar OpenSSL y el lenguaje python o el propio lenguaje Java a través de sus correspondientes clases relacionadas con los certificados digitales**.

### ¿Cómo se puede generar la solicitud a las Autoridades de Certificación de los certificados digitales para los servidores Web de la Entidad?

Se solicita a INSEGUS por parte del cliente, presentar **de forma lo más visual y completa posible,** el proceso de elaboración de una solicitud de un certificado digital siguiendo la estructura especificada en el estándar X.509 a una Autoridad de Certificación mediante los ***Certificate Signing Request*** (CSR) para que pueda ser seguido por **los distintos empleados de dicho Servicio.**

Igual que para las partes interesadas del Servicio de Salud se pueden identificar/autenticar ante la misma y antes de poder pedir un certificado HTTPS, se debe generar también un **CSR** para los **servidores Apache de dicha entidad**. La CSR es un cuerpo de texto cifrado. Los CSR contendrán información codificada específica para el Servicio y el nombre de dominio, información que se conoce como un nombre completo o DN. El DN para la mayoría de servidores contiene los siguientes campos: País, Estado (o provincia), Localidad (o ciudad), la Organización de la Unidad

Organizacional y nombre común. Más herramientas relacionadas con la comprobación de certificados puede encontrarlas aquí.

Para que la Autoridad certificación confiable emita el certificado digital se exige muchas veces el pago de ciertas cantidades, aunque existe actualmente algunas opciones donde se puede obtener de forma gratuita **(https://letsencrypt.org/). También existen proyectos que permiten obtener certificados HTTPS sin tener que instalar software alguno y sin tener que compartir las claves privadas (https://gethttpsforfree.com**/) y que usan Let's Encrypt. Es importante detallar **el proceso que se lleva a cabo para comprobar por la autoridad de certificación que el servidor que tiene el par de claves es realmente al que se le ha firmado el certificado.**

**Caso de test:** El cliente nos requiere **al menos un caso de test donde se lleve a cabo la implementación de dicho proceso y en INSEGUS se comprobará la solicitud CSR generada para un servidor Web Apache que podría disponer el Security Team.**

### Productividad (10% más en el grado de satisfacción obtenido) ¿Cómo se puede realizar la instalación/desinstalación de los certificados digitales en los servidores Web Apache del Servicio de Salud?

Se solicita a INSEGUS por parte del cliente, el modelo de proceso de negocio(diagrama BPMN 2.0) para la **instalación y el modelo de proceso de negocio para la desinstalación de certificados digitales** en los servidores Apache del Servicio de Salud. En esta consulta se determinará un modelo de proceso donde se especifiquen las tareas a seguir en la instalación/desinstalación en los servidores Apache del Servicio.

**Caso de test:** El cliente nos requiere **al menos un caso de test donde se lleve a cabo la implementación de dicho modelo de proceso en un servidor Apache. La correcta implementación se comprobará en INSEGUS usando una herramienta para testeo del certificado del Servicio de Salud como confiable.**

## Consulta 6.2 Verificación Automática de la Política de Control de Acceso teniendo en cuenta conflictos de intereses, separación/segregación de deberes dinámica y binding de deberes para elaborar compras de medicamentos en el Servicio de Salud

Para la resolución de esta consulta debe consultar el documento AutomatizaSeparacionDeberes que se adjunta en esta consultoría.

### Productividad (20% más en el grado de satisfacción obtenido) ¿Cómo se puede realizar el despliegue del control de acceso dinámico en el BPMS de Bonita BPM?

Se solicita a INSEGUS por parte del cliente, la posibilidad de desplegar el control de acceso dinámico en la herramienta de Bonita BPM, de tal forma que se haga dicho control de forma automática a través de dicha herramienta.

**CAI6. Seguridad en el desarrollo y despliegue de software en tecnologías emergentes. Blockchain**

## CONSULTA 3 del CAI6. CONSULTORÍA SOBRE SEGURIDAD DE LAS COMPRAS DE MEDICAMENTOS DE UN SERVICIO DE SALUD PÚBLICO

En el Servicio de Salud Público nos ha consultado sobre el desarrollo y despliegue de un software sobre cómo podrían ser las subastas de segundo precio (tipo Vickrey-Premio Nóbel de Economía 1996) para la **compra de una determinada cantidad de medicamentos a los proveedores autorizados por dicho Servicio.** Se muestra abajo un ejemplo, donde hay tres proveedores apostantes para realizar ofertas para proveer una determinada cantidad de un determinado medicamento al Servicio de Salud, que tras ver sus ofertas (2750,2500,3020) resulta que el Proveedor B es el ganador de la apuesta y el Servicio de Salud le pagará cuando le entregue los medicamentos una cantidad de 2750€ y no lo que había ofertado. Esto facilita que se hagan ofertas a la baja para el Servicio de Salud por parte de todos los proveedores

👨‍💼 **Proveedor A oferta 2750€** 👩‍💼 **Proveedor B oferta 2500€**
👨‍💻 **Proveedor oferta 3020€**

Hay que tener en cuenta que todos los que participan en la subasta **deben pagar un porcentaje de al menos el 10% lo que pujan**, por si cuando se le asigna el encargo de proporcionar los medicamentos y realmente no lo proporcionan en una fecha dada, perderán dicha cantidad. **Las apuestas deben permanecer confidenciales hasta que finalice la subasta.**

- Las pujas que se admiten deberían tener un valor positivo entero mayor de cero, toda puja que no cumpla esto no será considerada.
- También hay un valor máximo que determina el Servicio de Salud, por encima del cuál no se admiten pujas. Esto evita que se tenga que pagar un valor superior al que tiene estimado el Servicio de Salud que vale el suministro de medicamentos.
- Los pujantes no pueden pujar dos veces, por tanto hay que controlarlo.
- Puede haber hasta 30 pujadores en la subasta, una vez cubierto se cierra la subasta
- La subasta se abre con una fecha determinada al crear el Smart contract
- La subasta se cierra cuando hay 30 pujas o se llega al deadline o fecha límite. Cualquier apuesta después del deadline no está admitida.
- Gana la subasta el que presenta la puja más baja al Servicio de Salud, pero se le pagará lo que haya pujado el segundo más alto. En caso que no haya dos pujadores o más, se le pagará lo que él ha pujado.
- Se paga al hacer la puja al menos el 10% de lo pujado, en caso que sean ganadores de la subasta, se le devolverá sumando al costo del suministro dicha cantidad, en caso que sea ganador y no suministre el material, no se le devolverá. A todos los pujadores se le devolverá la cantidad entregada una vez finalizada la subasta.
- Es necesario que los pujadores puedan conocer al ganador cuando finalice la subasta.

## Desarrollo de smart contract seguros

El Servicio de Salud nos solicita el **desarrollo de los correspondientes Smart Contract, tenga en cuenta que el código debe recoger que los participantes en la subasta deben entregar una cantidad de Ethereum cuando hacen una puja, y se le deben devolver a cada uno cuando finalice todo el proceso de subasta, excepto al ganador si no proporcionase la cantidad de medicamento estipulado.**

**El precio de las cantidades que apuestan los proveedores debe ser siempre inferior al precio de mercado en el momento de comienzo de la subasta y aparecerá reflejado en el Smart contract. Igualmente debe aparecer cuando se finalizará la subasta de medicamentos y las cantidades aportadas por los proveedores no ganadores de la subasta se deben devolver una vez finalizada la subasta.** El precio de las cantidades que apuestan los proveedores debe ser siempre inferior al precio de mercado en el momento de comienzo de la subasta y será necesario determinarlo al crear el Smart contract. Una vez entregado los medicamentos se debe hacer efectivo la cantidad de acuerdo a la subasta Vickrey al proveedor o proveedores que han proporcionado los medicamentos al Servicio de Salud.

**El Servicio de Salud nos solicita el desarrollo del correspondiente Smart Contract y que tenga en cuenta que el código debe recoger que los participantes en la subasta deben entregar una cantidad de Ethereum cuando hacen una puja, y se le deben devolver a cada uno cuando finalice todo el proceso de subasta, excepto al ganador o ganadores (en el caso que la puja final sea igual para varios a la vez) por si no proporcionase la cantidad de medicamento estipulado. Por tanto, en el informe solamente se solicita por el cliente el fichero con el código correspondiente al smart contract.**

## Testing de seguridad mediante analizadores estáticos para los smart contract desarrollados

**Los Security Team de INSEGUS deben procurar que los Smart contract implementados no tengan vulnerabilidades de seguridad antes de desplegarse en una blockchain real. La existencia de vulnerabilidades de seguridad en la tecnología blockchain ha provocado que durante el año 2021 que los cibercriminales hayan robado $3.300.000.000 en criptoactivos y en el año 2022 se han producido $3.800.000.000 de robos según un reciente informe.**

**Por todo ello se hace necesario usar las herramientas adecuadas para mitigar dichas vulnerabilidades y evitar estos problemas económicos. Dada la importancia del tema se han desarrollado innumerables herramientas de depuración del código de los smart contract, entre ellas podemos destacar DSol-decompile, Ethersolve, Evmdis, Osiris, Oyente, Panoramix, Rattle, Securify2, Slither, Smartcheck, Vandal, etc... Hay que tener cuidado con el uso de las herramientas pues muchas veces dan un elevado número de falsos positivos que deberían descartarse de forma manual.**

**El cliente nos solicita un informe detallado de las pruebas realizadas y los resultados de las mismas tras llevar a cabo el testing de seguridad de los smart contract desarrollados por el Security Team.**

Esta consulta sería para la productividad (hasta 15% añadido al grado de satisfacción obtenido en el CAI)

## Despliegue y testing dinámico en una red de pruebas de Ethereum de los smart contracts desplegados

Ethereum es una de las plataforma más usada en el mundo para el despliegue de smart contracts.Los factores claves detrás de esta popularidad son su escalabilidad y capacidad para gestionar un alto número de transacciones, no obstante debido a las tasas GAS usar Ethereum puede resultar demasiado costoso. Por ello, en vez de usar directamente la red Ethereum, para el despliegue de los smart contract y DApps antes de ponerlos en producción podemos usar entornos simulados que son conocidos como **Ethereum Testnets. En cualquier** Ethereum TestNet, los Ether no tienen valor real y además no hay marketplace para comprar Ether para una TestNet. Pero para realizar cualquier operación en la TestNet se necesitarán Ether. Para ello se pueden usar los conocidos como **TestNet Faucet. Un faucet es simplemente una herramienta basada en la Web**

**que facilita a los usuarios de la Testnet los tokens que necesita para realizar las operaciones de los smart contracts.**
Existen una amplia variedad de Ethereum TestNets disponibles para que los desarrolladores de smart contract o DApps puedan escoger las más convenientes dependiendo de los requisitos del proyecto de desarrollo. Entre las Ethereum Testnet más usadas podemos citar a **Goerli y Sepolia**, aunque la operatividad de estas redes de pruebas están sujetas a bastantes cambios.
Para conectarse a una de estas Testnet existen muchas herramientas disponibles. Entre ellas se encuentra **Metamask**, que es una herramienta que fácilmente puede descargarse como una extensión del navegador (disponible para Firefox, Chrome y Brave). Metamask permite a los desarrolladores comunicarse con la Ethereum Testnet.
El Servicio de Salud **nos solicita en esta consulta grupal que le indiquemos el proceso que el Security Team ha llevado a cabo para desplegar los smart contract en la Ethereum Testnet y cómo proponen que se conecten los usuarios del Servicio de Salud a dicha Tesnet para ejecutar las diferentes operaciones de los smart contracts. Nos solicita también que le detallemos la justificación técnica de la propuesta que realiza el Security Team sobre lo que nos requiere el Servicio de Salud.**
**El Servicio de Salud nos requiere que dada la dirección de un smart contract ya desplegado en la Ethereum Testnet, llevemos a cabo sobre dicho smart contract:**

- **Plan de pruebas de la correcta ejecución de todas operaciones que pueden invocar los usuarios del Servicio de Salud y los proveedores del mismo.**
- **Resultado de las pruebas realizadas y especificación de las posibles vulnerabilidades de seguridad que presenta el smart contract desplegado por otro Security Team.**
- **Informar sobre posibles soluciones tecnológicas para mitigar o evitar dichas vulnerabilidades.**

**SE ADJUNTAN DOS FICHEROS EJEMPLOS EN SOLIDITY Y QUE SE REFIEREN A CÓDIGOS (QUE PUEDEN CONTENER ERRORES) RELACIONADOS CON EL OBJETO DE ESTA CONSULTORÍA**

**En esta página Web puede encontrar ejemplos de smart contract relacionados con subastas (Simple Auction y Blind Auction)**