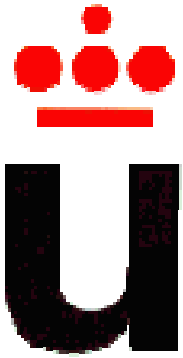


UNIVERSIDAD

REY JUAN CARLOS

ESCUELA SUPERIOR DE INGENIERÍA INFORMÁTICA

INGENIERÍA TECNICA EN INFORMÁTICA DE SISTEMAS

Curso Académico 2012/2013

Proyecto de Fin de Carrera

Hospital Virtual: Mejoras de autenticación

Autor: Nuria Fuentevilla del Haya

Tutor: César Cáceres Taladríz

Agradecimientos

Tengo que agradecer su apoyo en primer lugar a Cesar Cáceres, por habernos dirigido a lo largo de este proyecto, con los altibajos que hemos tenido durante estos años, cuando nos atascábamos en algún punto del proyecto e incluso cambiando el rumbo en alguna ocasión; gracias por tu infinita paciencia y por sacar tiempo para nosotras, incluso en fines de semana y vacaciones, debido a nuestros problemas de disponibilidad.

Por supuesto, a Laura Bermejo, mi compañera y amiga, durante la carrera y durante el proyecto fin de carrera, ha sido muy enriquecedor hacer el proyecto contigo porque nos hemos compenetrado muy bien; cuando opinamos lo mismo respecto a algún tema, es algo bueno, pero cuando discrepamos es mejor incluso, porque aprendemos mucho la una de la otra, y tener otro punto de vista en el desarrollo de este proyecto ha sido un punto muy favorable, para nosotras y para el resultado final.

A mis compañeras de la facultad, que también han estado apoyando; a medida que terminaba la carrera para ellas, seguían dándonos ánimos a nosotras, esperándonos al final del camino y dándonos fuerzas, comprendiendo las infinitas veces que hemos tenido que cancelar planes, porque teníamos que dedicarnos al proyecto.

A mi marido, que ha sabido estar a mi lado en éste periodo, sacrificando muchas cosas algunas veces, dado que en los ratos libres yo tenía que dedicarme al proyecto, y él ha sabido apoyarme y esperar con paciencia y cariño. Desde que nos conocimos hemos compaginado nuestros respectivos trabajos, en un mundo profesional muy absorbente, con poco tiempo libre disponible, estando el mío, incluso, supeditado a mi dedicación al proyecto, hemos planificado una boda y nos hemos casado desde entonces, gracias cariño por haberlo comprendido, por tu apoyo y por estar ahí.

A mi familia, que ha estado muy preocupada por la vida tan ajetreada que he tenido que llevar en los últimos años, para poder crecer profesionalmente y personalmente.

A todos, muchas gracias. Por fin, aquí está el resultado.

Resumen

En este proyecto se han estudiado distintas alternativas existentes en el mercado para mejorar la autenticación en una aplicación web, concretamente en el Hospital Virtual del Hospital Clínic de Barcelona.

Para un hospital poder gestionar las consultas médicas a través de internet resulta un gran avance, ya que facilita y mejora la vida del paciente, sobre todo si hablamos de enfermedades crónicas, que obligan al paciente a tener un control médico constante. Poder realizar el seguimiento a través de una aplicación web, mejora y facilita la calidad de vida del paciente, sin embargo, no hay que olvidar que el historial clínico del paciente es información confidencial y de alta sensibilidad, por lo que toda la información privada que un hospital almacene tanto en archivo físico como en una aplicación web debe protegerse de cualquier peligro. En el caso que nos concierne, almacenamiento web, la información de carácter confidencial almacenada en la aplicación web, deberá tener un alto nivel de protección para no estar accesible a extraños.

Índice

1. Introducción

El constante crecimiento de Internet ha mantenido y mantiene pendiente a empresarios, gente de negocios y consumidores con la promesa de cambiar el modo de trabajar e, incluso, de vida. Sin embargo, paralelo a esta nueva forma de hacer transacciones comerciales, o personales, existe una preocupación al respecto que cuestiona la seguridad de Internet, especialmente cuando se trata de información de carácter privado o sensible.[1] [2] [3]

Actualmente, en la red se maneja mucha información que no queremos dar a conocer a otras personas, como puede ser la información relativa a:

- Tarjetas de crédito.
- Números de la seguridad social.
- Correspondencia privada.
- Datos personales, médicos, bancarios…

Irónicamente, aunque la autenticación basada en nombre de usuario y contraseña es la forma más débil de autenticación, se trata, sin embargo, de la más utilizada en todo tipo de aplicaciones web.

A medida que se expande el uso de internet se incrementa más su naturaleza social e, inversamente, se hace menos segura. De hecho, respecto a la seguridad de aplicaciones web, el grupo de expertos de Web Application Security Consortium (WASC) estimaba que a principios de 2009 el 87% de todos los sitios web eran vulnerables a un ataque. [4] La seguridad, por tanto, se ha convertido en uno de los asuntos que más preocupa en nuestros días y la identificación del individuo es crucial para este propósito.

La seguridad, tanto en la informática como en otras áreas, se basa en la protección de elementos activos, entendiendo por elemento activo aquello que es tangible, como puede ser un servidor web o una base de datos con información confidencial. Cuando se vulnera la seguridad de estos datos se pone en entredicho la reputación de las

empresas a las cuales confiamos nuestros datos. La seguridad de un activo, se puede evaluar en base a tres aspectos principales: integridad, disponibilidad, confidencialidad.

- **La integridad,** se refiere a la fidelidad de los datos o recursos, y normalmente, se expresa en lo referente a prevenir la modificación no autorizada de información. La integridad incluye:
  - integridad de los datos: el volumen de la información.
  - integridad del origen: la fuente de los datos, a menudo llamada autenticación.
- **La disponibilidad,** se refiere a la habilidad de usar la información o el recurso deseado. La disponibilidad es un aspecto importante de fiabilidad, tanto como el diseño del sistema, porque un sistema que no tiene disponibilidad resulta tan poco útil como no tener sistema. El aspecto de disponibilidad que es pertinente a la seguridad es que alguien puede deliberadamente negar el acceso a los datos o a un servicio haciéndolo no disponible.
- **La confidencialidad,** es la ocultación de información o recursos. La necesidad de salvaguardar información surge al trabajar con información de carácter sensible. Los mecanismos de control de acceso garantizan una mayor protección de la información y, por lo tanto, un nivel mayor de confidencialidad. Un mecanismo de control de acceso a la información para conservar la confidencialidad es la criptografía, que cifra los datos para hacerlos incomprensibles.

Estos tres aspectos, a su vez dependen de otros tres elementos principales, que engloban los distintos controles que se pueden establecer en un sistema informático:

- **Autenticación**: los clientes de una aplicación o servicio web deben ser identificados de forma única, ya sean usuarios finales, de otros servicios o computadoras externas.
- **Autorización**: no sólo es necesario saber quiénes acceden a un sistema informático, también es necesario establecer qué es lo que pueden hacer dentro de él. Un nivel de autorización dado determina qué tipo de operaciones o transacciones puede efectuar un cliente sobre un recurso, es lo que conocemos como ROL.

- **Registro y Auditoria**: después de efectuar una operación o transacción, es importante que esta sea registrada adecuadamente y almacenada.

Todos estos conceptos son importantes en el entorno de Internet y, particularmente especiales, en aplicaciones web, dado su crecimiento en el mundo laboral; actualmente, una gran parte de los datos de las empresas se encuentra almacenado en aplicaciones web. Este proyecto nace con el deseo de mejorar la seguridad en una aplicación web ya existente, como es el Hospital Virtual. La seguridad en la que nos hemos centrado la encontramos en la fase de autenticación, cuando un usuario quiere conectarse a la aplicación web. Para ello se analizarán diversos mecanismos, estudiando la funcionalidad de cada uno de ellos, y analizando cuáles son más recomendables para cada caso. A continuación, se presenta la aplicación web.

1.1. Hospital Virtual: Sistema de Información Clínica y Telecuidado de Pacientes VIH/SIDA

El cuidado de enfermedades crónicas complejas (diabetes, EPOC, VIH/SIDA…) demanda cada vez más recursos sanitarios. En el caso del VIH/SIDA, los problemas a los que se enfrenta la persona infectada han cambiado bastante en los últimos tiempos. Con la aparición de los primeros casos de infectados, el esfuerzo se centró en la investigación y desarrollo de nuevos fármacos que lograran disminuir la tasa de mortalidad y aumentar el tiempo de vida de los pacientes; hoy en día, cada vez fallecen menos pacientes, por lo que se pretende mejorar su calidad de vida, afectada por múltiples factores (médicos, psicológicos y sociales) que acompañan a esta enfermedad. [5], [6], [7].

Este proyecto se enmarca dentro de un proyecto más amplio, el proyecto del Hospital Virtual que nace en el año 2002, desarrollado por el Grupo de Bioingeniería y Telemedicina de la Universidad Politécnica de Madrid (GBT-UPM) y el Hospital Clínic de Barcelona. La pretensión era, y es, dar una mejor calidad de vida a los pacientes con VIH estables y, para ello, se implantó un sistema de telemedicina que ofrece un seguimiento del paciente a domicilio, a través de Internet. Una vez puesto en marchar el sistema, se llevó a cabo un estudio piloto con 90 pacientes con quienes se realizó un ensayo clínico CASO-CONTROL, durante dos años, donde se evaluaba la evolución de cada paciente. Actualmente, el sistema se encuentra integrado en la rutina clínica

del centro y es usado por más de 3000 pacientes (200 de ellos desde su domicilio) y 70 profesionales.

Gracias a este sistema, el Hospital Clínic de Barcelona ofrece a sus pacientes con VIH estable un servicio de telemedicina pionero que permite atender de forma global todas sus necesidades mediante una aplicación web.

Los servicios que ofrece el Hospital Virtual son [5, 6,7]:

- Comunicación: consultas paciente-profesional de forma presencial o por videoconferencia, consultas entre pacientes a través de la comunidad virtual.
- Obtención, Gestión y Visualización de la Información: visualización de una selección de datos de la Historia Clínica Electrónica (HCE) y gestión de información sobre VIH/SIDA.
- Gestión de la Medicación: información sobre la medicación y seguimiento del cumplimiento y efectos adversos.
- Administración y Configuración: gestión y autenticación de usuarios, generación de perfiles de usuario, mantenimiento del sistema, seguridad y auditoría.

El Hospital Virtual supone una optimización del tiempo y del espacio invertido en las consultas, ya que cada una de ellas se reduce de 20 a 10 minutos, con lo que se puede realizar el doble de visitas y al paciente le permite reducir a la mitad el tiempo que invierte en desplazamientos al Hospital Clínic de Barcelona.

El Hospital Virtual ofrece distintas funciones según el tipo de usuario que sea y el grupo funcional al que pertenezca, es decir, si es un paciente, un médico, el administrador etc, el usuario tendrá acceso a los servicios propios de su perfil. En la Ilustración 1 se puede observar la página de inicio a la que acceden los pacientes.

Ilustración 1. Página principal para los pacientes del Hospital Virtual

Los usuarios acceden al sistema, un portal web, desde un navegador de Internet. Una vez cumplido el proceso de autenticación, el usuario accede a una serie de servicios específicos.

Los profesionales acceden a través de su intranet, una vez se han autenticado (usuario y contraseña) pueden entrar al Hospital Virtual, donde tienen acceso a las historias clínicas de sus pacientes. A continuación, en la Ilustración 2 se muestra la vista con los recursos de un paciente:

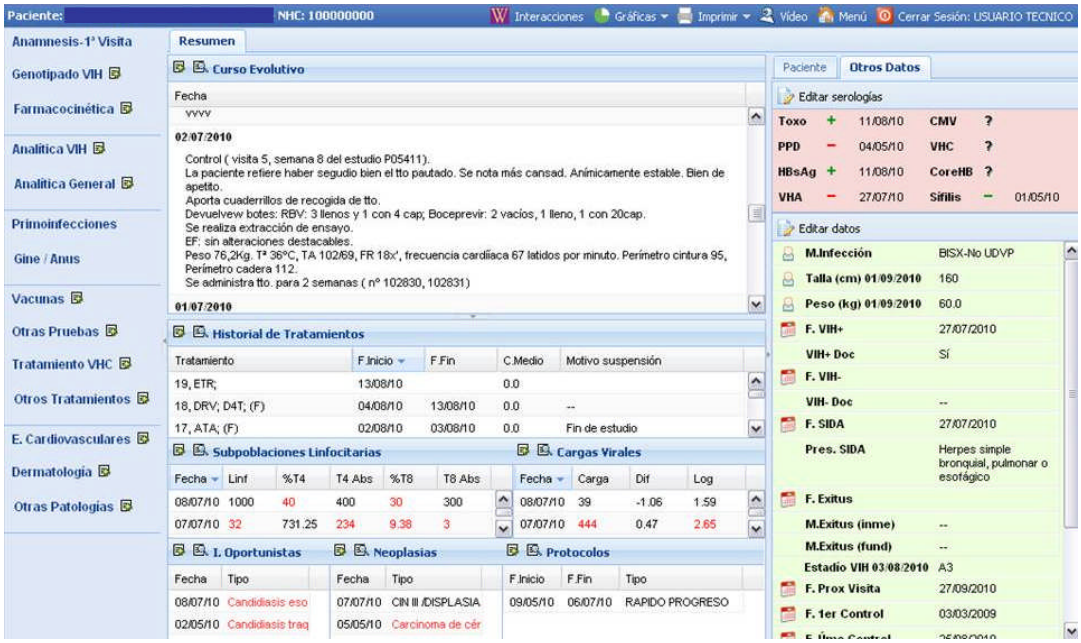


Ilustración 2. Vista de perfil profesional de un paciente concreto

En este proyecto nos vamos a centrar, precisamente en el proceso de autenticación y las medidas de seguridad empleadas en el Hospital Virtual. A continuación, se muestra la Ilustración 3 donde se observa la descripción general del sistema de telemedicina implementado:

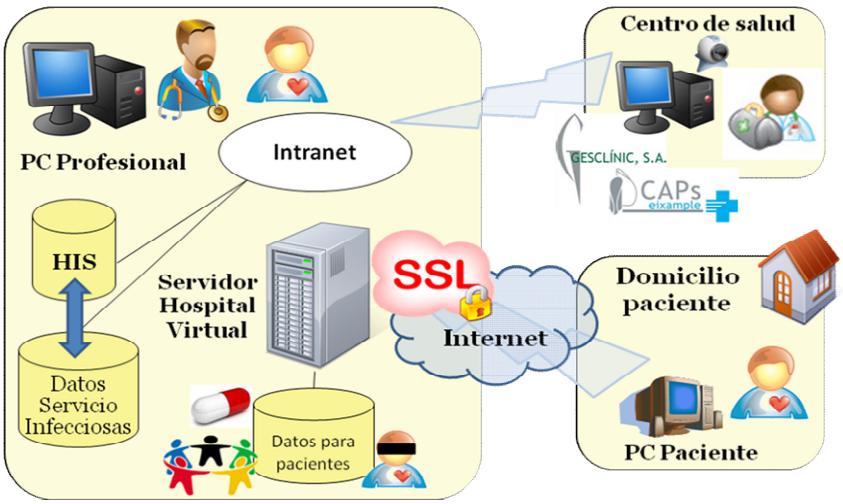


Ilustración 3. Descripción General del Sistema

Como ya se ha comentado, los profesionales se conectan desde sus propios ordenadores a través de la Intranet del Hospital Virtual; por otra parte, los pacientes se

conectan desde sus domicilios y lo hacen a través de una conexión segura de VPN basada en SSL.

La base de datos a la que acceden los pacientes está cifrada y se hacen copias de seguridad regularmente; además, no contiene ningún dato de tipo personal que pueda relacionar un registro con una persona concreta (datos anonimizados).

La conexión a la aplicación del Hospital Clínic de Barcelona se realiza mediante un proceso de autenticación dividido en dos fases. Por una parte el usuario deberá estar conectado a la VPN (Virtual Private Network, el Hospital Virtual utiliza la solución corporativa del hospital, de CISCO) y, por otra parte, una vez realizada la conexión a la VPN, se accederá a la aplicación donde se deberán introducir las credenciales de acceso (usuario-contraseña).

Por tanto, las comunicaciones se encuentran cifradas y autenticadas mediante túneles VPN, consiguiendo un acceso seguro a la información. En este proyecto nos vamos a centrar en la autenticación en la aplicación, estudiando las diferentes formas de autenticación para poder escoger la mejor en función de las necesidades.

Los profesionales utilizan el sistema Hospital Virtual para todos los pacientes del servicio de enfermedades infecciosas, tanto los que acuden a consultas presenciales como los que realizan consultas por Internet. Este sistema se comunica con varias bases de datos, además de la propia del servicio como, por ejemplo, la del Sistema de Información Hospitalaria (gestionada con SAP).

Todo acceso e interacción con el sistema queda registrado mediante un módulo de registro de eventos, con el objetivo de cumplir con la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (LOPD). Además, todos los formularios web son comprobados para evitar el uso de código malintencionado.

2. Objetivos

El objetivo principal de este proyecto es mejorar la seguridad en la autenticación del paciente al acceder al Hospital Virtual.

Para ello se van a analizar diferentes mecanismos de autenticación que existen en el mercado, teniendo en cuenta la arquitectura actual del Hospital Virtual, los riesgos existentes hoy día en Internet, así como la sensibilidad y confidencialidad de los datos que se tratan en las conexiones que se realizan para las consultas virtuales.

Para alcanzar el objetivo principal se plantean los siguientes objetivos secundarios:

- Analizar los diferentes mecanismos de autenticación, evaluando sus ventajas e inconvenientes, con la finalidad de poder determinar qué mecanismo o mecanismos podemos utilizar para mejorar la seguridad del Hospital Virtual.

- Investigar la biometría como método de autenticación, analizando todos los sistemas biométricos posibles, implementando un dispositivo biométrico para probar su funcionalidad. La biometría, hoy en día, es una de las técnicas más valoradas y, gracias al avance que se ha producido en los últimos años, encontramos un amplio abanico de posibilidades que analizaremos en este proyecto.

  Las características biométricas de un individuo se pueden dividir en dos grupos, atendiendo a las características que se analicen; éstas pueden ser anatómicas o de comportamiento.

  - Anatómicas: las huellas dactilares, las retinas, el iris, los patrones faciales, de venas de la mano o la geometría de la palma de la mano, representan ejemplos de características físicas.

  - Características del comportamiento se incluye la firma, el paso y el tecleo.

  - La voz se considera una mezcla de características físicas y del comportamiento, pero todos los rasgos biométricos comparten aspectos físicos y del comportamiento.

- Investigar e implementar el Vasco Digipass como mecanismo de identificación seguro. El OTP810 es un token de seguridad; existe más de una clase de token de seguridad, los que llevan claves criptográficas, firmas digitales, o los que generan contraseñas dinámicas (one time pasword, OTP); éste último es el que se va a analizar más detenidamente y a implementar para ver si constituye una solución óptima en la autenticación de usuarios en el Hospital Virtual.

3. Estado del Arte, Estudio de Alternativas

3.1. Mecanismos de Autenticación

Autenticar significa autorizar, legalizar algo; en términos informáticos hablamos de autenticación o autentificación cuando se ha de comprobar la identidad de una entidad (persona, institución…) mediante el requerimiento de unas credenciales y su posterior validación.

La autenticación es necesaria para proteger la información con la que estamos tratando. En función de lo sensible que sea la información, se deberá utilizar un mecanismo u otro de autenticación, del amplio abanico del que disponemos en el mercado.

Podemos dividir los mecanismos de autenticación en 3 grupos, basándonos en lo siguiente:

- Basados en algo conocido: contraseñas, frases de paso, etc.
- Basados en algo poseído: tarjeta de identidad, tarjeta inteligente (*smartcard*), dispositivo USB (*token*), etc.
- Basados en características físicas del usuario: verificación de voz, de escritura, de huellas, de patrones oculares, etc.

Dentro de estos grupos los sistemas más utilizados o reconocidos son:

- Autenticación basada en 1 factor: un elemento es conocido por el usuario (por ejemplo la contraseña asociada a un usuario para entrar en un portal web), algo que estamos muy acostumbrados a usar.

- Autenticación basada en 2 factores: es una combinación de dos métodos de autenticación distintos: un elemento que el usuario sabe y otro elemento que el usuario posee. Un ejemplo cada vez mas conocido y utilizado es el DNI electrónico (DNIe) que es un soporte seguro (el cual el usuario posee) que contiene un certificado que identifica de forma única a un usuario y, además, para poder autenticarse en un sistema necesitará un PIN (el cual el usuario conoce).

- Autentificación biométrica: consiste en la verificación de la identidad de un sujeto, basándose en ciertos elementos morfológicos que le son inherentes y que sólo se dan en ese sujeto. Es decir, rasgos distintivos de una persona (su voz, su huella dactilar, etc.) para, más tarde, ser capaces de comparar esa muestra con otra, y poder determinar si son iguales o no.

- Autenticación basada en *tokens*: los tokens son pequeños dispositivos hardware para la autenticación de usuarios y portabilidad de certificados. Se conectan al ordenador mediante USB, lo cual los hace compatibles con prácticamente cualquier ordenador y sistema operativo.

- Autenticación Single Sign-On (SSO): es un procedimiento de autenticación que habilita al usuario para acceder a varios sistemas con una sola instancia de identificación. Hay cinco tipos principales de SSO:

- E-SSO: Enterprise single sign-on, permite que los usuarios puedan acceder a diferentes aplicaciones con un solo conjunto de credenciales.
- WEB-SSO: WEB single sign-on, trabaja con aplicaciones y recursos accedidos vía web. Los accesos son interceptados con la ayuda de un servidor proxy o de un componente instalado en el servidor web destino. Los usuarios no autenticados que tratan de acceder son redirigidos a un servidor de autenticación y regresan sólo después de haber logrado un acceso exitoso. Se utilizan cookies, para reconocer aquellos usuarios que acceden y su estado de autenticación.
- Kerberos: usa una criptografía de claves simétricas para validar usuarios con los servicios de red, evitando así tener que enviar contraseñas a través de la red. Los usuarios se autentican en el servidor Kerberos y, una vez hayan obtenido el acceso podrán operar con el resto de aplicaciones. Al validar los usuarios para los servicios de la red por medio de Kerberos, se frustran los intentos de usuarios no autorizados que intentan interceptar contraseñas en la red.
- Identidad federada: utiliza protocolos basados en estándares para habilitar que las aplicaciones puedan identificar los clientes sin necesidad de autenticación redundante.

- OpenID: es un proceso de SSO distribuido y descentralizado, donde la identidad se compila en una url que cualquier aplicación o servidor puede verificar.

- Autenticación LDAP: (Protocolo compacto de acceso a directorios) es un protocolo estándar, de tipo cliente servidor, que permite acceder a bases de información de una red. Habitualmente almacena la información de autenticación (usuario y contraseña) y es utilizado para autenticarse, aunque es posible almacenar otra información (datos de contacto del usuario, ubicación de diversos recursos de la red, permisos, certificados, etc). En resumen, LDAP es un protocolo de acceso unificado a un conjunto de información sobre una red. No obstante, el protocolo LDAP define el método para acceder a datos en el servidor, a nivel cliente, pero no la manera en la que se almacena la información ni el modo en el que se accede. Existen otros protocolos criptográficos para autenticar identidades de forma segura, como por ejemplo: PAP (Password Authentication Protocol), CHAP (Challenge Handshake Authentication Protocol), PPP (Point-to-point Protocol), EAP (Extensible Authentication Protocol), RADIUS (Remote Authentication Dial-In User Server), TACACS (Terminal Access Controller Access Control System).

- Criptografía: Con el objeto de poder brindar los métodos más seguros de comunicación, la información es encriptada. Tenemos a nuestro alcance infinidad de algoritmos criptográficos; todos ellos se basan en que, a partir de unos datos, (información) generan unos nuevos datos encriptados. Una posible clasificación de los algoritmos criptográficos sería:

- **Criptografía de clave secreta o criptografía simétrica:** en esta división encontramos algoritmos tan conocidos como son DES, 3DES, RC2, RC4, RC5, IDEA, Blowfish y AES. En este tipo de encriptación, cada ordenador tiene una clave secreta (como si fuera una llave) que puede utilizar para encriptar un paquete de información antes de ser enviada sobre la red a otro ordenador. Las claves simétricas requieren conocer de antemano los ordenadores que van a estar hablando entre si para poder instalar la clave en cada uno de ellos. Por sí solo, este tipo de encriptación no es suficiente para desarrollar el pleno potencial de las transacciones electrónicas. No es seguro intercambiar miles o incluso millones de claves de personas por lo que para el Hospital Virtual no es aconsejable porque vulnera la seguridad del propio Hospital Clínic de Barcelona.

En el apartado de Algoritmos Criptográficos, en la siguiente sección "Mecanismos concretos de autenticación", se analizará el algoritmo DES.

- **Criptografía de clave pública** o **criptografía asimétrica**: a este grupo pertenecen Diffie-Hellman, RSA, DSA, ElGamal…Este método usa una combinación de una clave privada y una clave pública. La clave privada sólo la sabe tu ordenador, mientras que la clave pública es entregada por tu ordenador a cualquier otro ordenador con el que se quiere realizar una comunicación. Para decodificar un mensaje encriptado, un ordenador debe hacer uso de la clave pública entregada por el ordenador original, y su propia clave privada. Las dos claves funcionan conjuntamente; por ejemplo, si se quiere establecer una comunicación entre dos personas y, si una de esas dos personas le facilita a la otra su clave pública, este encriptará el texto con la clave pública facilitada y el receptor del mensaje utilizará su clave privada para revertir la encriptación del mensaje y poder obtener en claro el mensaje recibido. Si un extraño interceptara este mensaje, no podría descifrarlo porque no dispone de la clave privada del par de claves pública-privada, que es la única que puede desencriptar el mensaje que se ha encriptado con su clave pública. En el caso del Hospital Virtual, el mensaje a enviar podría ser la password del paciente para logarse en el sistema, y que dicha password se encriptase con la clave pública del servidor del hospital, de modo que al recibir la solicitud de conexión con la password encriptada, el servidor podría desencriptarla con su clave privada y ver si esa password pertenece a algún paciente que hubiese registrado en la base de datos de pacientes.

  En el apartado de Algoritmos Criptográficos, en la siguiente sección "Mecanismos concretos de autenticación" se analizará el algoritmo RSA.

- **Algoritmos HASH** o **de resumen**: SHA, MD5, Rabin-Karp, entre otros. Independientemente de lo robusto que sea el algoritmo, éste puede llegar a ser inseguro si el protocolo de capa superior muestra la información de las claves utilizadas. Alguno de los protocolos seguros más usados son: SSL, TLS, SSH, PGP.

Más adelante en el apartado de implementación, se usará el protocolo SSL y se describirá más en profundidad.

3.2. Mecanismos Concretos de Autenticación

En el mercado existen métodos de autenticación en los que podemos basarnos a la hora de analizar la mejor solución para autenticar a los pacientes en el Hospital Virtual. Algunos se han quedado obsoletos, o son poco seguros, debido a los avances tecnológicos y a los ataques de terceros que hay en la red, los cuales no hay que olvidar; otros son demasiado caros para valorar implantarlo a nivel masivo en una aplicación en la que el número de pacientes que acceden a ella puede aumentar. Por todo ello, vamos a evaluar todos los métodos de autenticación que pueden formar parte de una solución óptima para el Hospital Virtual, analizando las ventajas y desventajas que ofrecen para llegar a una conclusión final. [16]

USUARIO – PASSWORD:

Es el método de autenticación más utilizado. El usuario posee un nombre de acceso al sistema (login) y una clave (password); ambos datos generalmente se almacenan en un fichero o base de datos contra el que se validan los datos de acceso introducidos. La clave es estática, es decir, no va cambiando de forma automática, es siempre la misma y sólo cambia cuando tú lo haces o cuando el sistema detecta que ha pasado un tiempo constante y determinado para la renovación de la password, pero dependiendo de la aplicación puede que ni exista ese tiempo de expiración.

Este mecanismo de autenticación, en muchas ocasiones va acompañado de una pregunta secreta por si el usuario ha olvidado la clave, para tener la posibilidad de generar una nueva contraseña y que será enviada a la dirección de correo electrónico con la que el usuario se haya registrado.

DESVENTAJAS:

Se trata de la autenticación menos fuerte, más vulnerable. Cada persona puede manejar alrededor de 25 contraseñas, lo que hace que al final mucha gente acabe escribiéndola en un papel accesible para cualquiera o utilizando algo fácil de recordar y por lo tanto de descubrir por alguien ajeno.

Este tipo de autenticación sufre de ataques de replay, ataques man in the middle, ataque de fuerza bruta (prueba y error), phishing, etc.

Además, aquellas contraseñas que puedan ser modificadas mediante la respuesta correcta a una pregunta secreta tienen aún una mayor vulnerabilidad, pues las preguntas suelen ser de respuesta obvia.

SISTEMA DE TARJETAS DE COORDENADAS (STC):

También denominado tarjeta matricial, es utilizado como segundo factor de autenticación. Este sistema fundamentalmente es usado por aplicaciones de banca por internet.

La Tarjeta de Coordenadas es una matriz de coordenadas, organizadas en columnas y filas. Las columnas están marcadas con letras y las filas con números (o viceversa). Por ejemplo, una matriz de 90 coordenadas puede tener 9 columnas y 10 filas, cuanto mayor sea matriz mayor número de combinaciones y por lo tanto más posibles contraseñas.

Una de las posibles formas de implementación consiste en la generación de tarjetas de forma paramétrica garantizando su unicidad y almacenando los datos de las mismas encriptados. Además, se permite un número máximo de intentos, si éste es superado, la tarjeta de coordenadas quedará bloqueada y por lo tanto inutilizada.

A este sistema se le denomina un sistema de “clave dinámica” pero realmente no lo es, puesto que aunque el usuario vaya a introducir claves diferentes cada vez, éstas van a depender de las coordenadas, y el valor que hay en cada coordenada es siempre el mismo, lo único que cambia es la coordenada que le pide el sistema cada vez.

Este sistema lo suelen usar los bancos, por lo que para el usuario no tiene precio alguno, sin embargo si se quiere introducir este mecanismo en una empresa privada, en este caso en el Hospital Virtual, habría que proporcionarle las tarjetas a los pacientes que fuesen a usar el Hospital Virtual. Hay empresas que ofrecen el servicio y el coste es de 30 euros por tarjeta, no es un precio único, puesto que depende del número de tarjetas a realizar, quién realice las tareas de hosting…

DESVENTAJAS:

Se trata de un sistema vulnerable ya que, a los problemas convencionales existentes del lado del usuario con los troyanos bancarios, HTTP sniffers y otros, se une el hecho

de que las interfaces se apoyan solamente en el SSL para cifrar los datos en la transmisión, olvidando que cualquier intercepción en la capa de la aplicación no está aún cifrada por el SSL.

El sistema de tarjetas de coordenadas es un método de validación que funciona perfectamente si el usuario realiza menos de cuatro a cinco transacciones al mes. Sin embargo, si el usuario realiza por ejemplo unas 15 a 20 transacciones al mes, entonces, teóricamente, la matriz de posibilidades podría ser re-ensamblada por un atacante, aunque el usuario haya puesto todo el cuidado en que no se hayan duplicado los datos de la tarjeta de coordenadas. Para determinar el número de transacciones que pueden hacer que sea re-ensamblada hay que tener en cuenta el tamaño de la matriz.

Por último, también se ha de tener en cuenta que la tarjeta puede ser extraviada y duplicada; por esta razón se utiliza como segundo factor de autenticación.

TOKEN DE SEGURIDAD:

Un token de seguridad (también llamado token de autenticación o token criptográfico) es un dispositivo electrónico que se le da a un usuario autorizado de un servicio computarizado para facilitar el proceso de autenticación y hacerlo más seguro.

Los tokens tienen un tamaño pequeño que permiten ser cómodamente llevados en el bolsillo o la cartera, facilitando su almacenamiento y transporte.
Los tokens electrónicos se usan para almacenar claves criptográficas, como firmas digitales o datos biométricos, como las huellas digitales. Algunos diseños se hacen a prueba de alteraciones, otros pueden incluir teclados para la entrada de un PIN.

Se puede distinguir entre dos clases de token.

- Los generadores de contraseñas dinámicas OTP (one-time Password), cada contraseña únicamente sirve para una sesión y ésta caduca cada cierto tiempo predeterminado que se establezca.

- TokensUSB, permiten almacenar contraseñas y certificados, como puede ser el certificado digital de una persona física. (Éste será uno de los métodos elegidos para implementar).

Es considerado un mecanismo de autenticación fuerte porque combina la información de algo que se sabe (contraseña, pin, clave…), con algo que se tiene físicamente, (el

token). Sin uno de los dos instrumentos, la autenticación no es posible. A este modelo de autenticación se le denomina autenticación de dos factores, como habíamos visto ya anteriormente.

Estos mecanismos pueden aplicarse a todo tipo de sistemas que requieran autenticación, desde servidores de VPN hasta aplicaciones web.

DESVENTAJAS:

Los OTP son vulnerables ante la técnica llamada **man in the middle**, que consiste en la intercepción de sesiones encriptadas. El atacante se interpone entre el origen y el destino de una comunicación, para reconocer y/o modificar el contenido de los paquetes de información, sin que las víctimas lo adviertan. Actúan como un proxy entre el usuario y el dispositivo, sin que el usuario pueda apreciarlo. Esto puede ocurrir en diversos ambientes, como en correos electrónicos, navegación por Internet e, incluso, dentro de una red local.

Por otro lado, los TokensUSB que muestran una ventana emergente para que el usuario autorice el uso de una credencial, podrían ser engañados mediante una ventana similar a la real pero hecha por el atacante, obteniendo el control sobre el usuario.

Es necesario tenerlo siempre con uno mismo, sino no podrás utilizarlo siempre que quieras, tan sólo siempre que lo tengas. Además, también es necesaria una infraestructura para poder utilizarlo.

TARJETAS INTELIGENTES (SMART CARD):

También denominada tarjeta con circuito integrado (TCI), proporcionan funcionalidades de almacenamiento seguro para información sensible, como puede ser:

- claves privadas
- números de cuentas
- contraseñas
- información médica

Las encontramos en cualquier tarjeta, generalmente del tamaño de una tarjeta de crédito, que contiene un circuito integrado con microprocesador que permite ejecutar programas y almacenar datos, e incorporan ciertos mecanismos de seguridad. La energía necesaria para su funcionamiento proviene de un lector de tarjetas inteligentes.

Al igual que el token es un sistema de autenticación de dos factores, algo que se tiene y algo que se conoce.

Dependiendo de la capacidad del chip estas tarjetas pueden ser de diferentes tipos:

- **Memoria Protegida:** almacena y recupera datos que son enviados o recibidos por el chip; además, dispone de medidas de protección como, por ejemplo, un PIN para el acceso a la escritura o lectura de la misma.
- **Memoria Segura:** contiene funcionalidad criptográfica para la autenticación y cifrado de comunicaciones. Posibilita la coexistencia de varias aplicaciones en una misma tarjeta, incluyendo funcionalidades de monedero electrónico.
- **Microprocesadas**: tarjetas con una estructura análoga a la de un ordenador (procesador, memoria volátil, memoria no volátil). Albergan ficheros y aplicaciones y suelen usarse para identificación y pago con monederos electrónicos.
- **Criptográficas**: tarjetas microprocesadas avanzadas en las que hay módulos hardware para la ejecución de algoritmos de cifrado y firma digital. En estas tarjetas se puede almacenar de forma segura un certificado digital (y su clave privada) y firmar documentos o autenticarse con la tarjeta sin que el certificado salga de la tarjeta, ya que es el procesador de la propia tarjeta el que realiza la firma.

Algunos ejemplos concretos donde encontramos las tarjetas inteligentes son: tarjetas telefónicas de prepago, tarjetas SIM de móviles, DNI, carnet de conducir, monedero electrónico, tarjeta de transporte…

DESVENTAJAS:

El PIN es vulnerable ante un ataque o puede verse contagiado por un virus que inutilice el tarjeta. Además, al tratarse de un objeto físico, se puede extraviar o verse afectada por el contacto de un fluido (contacto con el agua).

Por último, su precio se ve encarecido al necesitar de una infraestructura para su correcto funcionamiento.

ALGORITMOS CRIPTOGRÁFICOS

Existen muchos algoritmos criptográficos cuya integridad y fortaleza han sido probadas, por lo que nos garantizan una alta fiabilidad. Los algoritmos los podemos usar para encriptar cierta información, por ejemplo, una contraseña que viaje de un ordenador a otro; en nuestro caso concreto, del ordenador del paciente al servidor donde se aloja el Hospital Virtual; el algoritmo nos permitiría verificar si la información que ha viajado es la esperada, identificando al usuario que pretende conectarse al Hospital Virtual como un paciente autorizado a la aplicación.

Entre los algoritmos más comunes que hay en el mercado podemos destacar los siguientes:

- **DES** (Data Encryption Standard)

Es un esquema de encriptación simétrico, usa una misma clave para cifrar y descifrar mensajes. Ha sido considerado un algoritmo tan robusto que, desde su creación, fue propuesto como estándar. En el documento FIPS (Federal Information Processing Standard) 46-1 del Instituto Nacional de Estándares y Tecnología (NIST) del Departamento de Comercio de Estados Unidos, publicado en 1977, se describe el DES como estándar. Es el algoritmo de cifrado simétrico más estudiado, mejor conocido y más empleado del mundo.

Se basa en un sistema monoalfabético, con un algoritmo de cifrado consistente en la aplicación sucesiva de varias permutaciones y sustituciones.

De este algoritmo cabe destacar que es el sistema más extendido del mundo, el que más máquinas usan y el más barato. Además, al ser tan usado, se puede considerar uno de los algoritmos más probados, su implementación resulta sencilla y es muy rápido en la ejecución. Desde su aparición nunca ha sido roto con un sistema práctico.

Un posible sucesor del DES es una versión conocida como Triple-DES que usa dos claves DES para encriptar tres veces, alcanzando un rendimiento equivalente a una única clave de 112 bits; obviamente, este nuevo esquema es tres veces más lento que el DES común.

DESVENTAJAS:

Por otra parte, su comercialización fuera de EEUU, tanto a nivel hardware como software, está prohibida y protegida por leyes que obligan a tener un permiso específico del Departamento de Estado para cualquier comercialización.

Además, la clave es corta, tanto que no siempre asegura una fortaleza adecuada. Hasta ahora había resultado suficiente, y nunca había sido roto el sistema pero, con la potencia de cálculo actual y futura de los ordenadores y con el trabajo en equipo por Internet, se cree que se puede violar el algoritmo.

- **RSA:** (Rivest, Shamir y Adleman)

Es un sistema criptográfico de clave pública. Como en todo sistema de clave pública, cada usuario posee dos claves de cifrado: una pública y otra privada. Cuando se quiere enviar un mensaje, el emisor busca la clave pública del receptor, cifra su mensaje con esa clave, y una vez que el mensaje cifrado llega al receptor, este se ocupa de descifrarlo usando su clave privada. El uso generalizado de RSA facilita el intercambio de firmas digitales.

RSA es el algoritmo más conocido y usado de los sistemas de clave pública y también el más rápido de todos ellos. Presenta todas las ventajas de los sistemas asimétricos, incluyendo la firma digital, aunque resulta más útil a la hora de implementar la confidencialidad el uso de sistemas simétricos, por ser más rápidos. Se suele usar también en los sistemas mixtos para encriptar y enviar la clave simétrica que se usará posteriormente en la comunicación cifrada.

El algoritmo tiene 3 partes definidas

Generación de claves, Cifrado y Descifrado.

DESVENTAJAS:

RSA, al ser tan complejo, es mucho más lento que DES y que otros criptosistemas simétricos.

Como en todos los cifrados, es importante como se distribuyan las claves públicas del RSA; La distribución de la clave debe ser segura contra un atacante que se disponga a espiar el canal para hacer un ataque.

- **RSA y DES:**

Finalmente pasamos a analizar ambos algoritmos de manera complementaria, ya que RSA es más un complemento que un sustituto de la encriptación DES. Ambos sistemas poseen ventajas de las que el otro carece.

DES es un sistema rápido de encriptación que funciona bien en encriptaciones de gran tamaño. Mientras que RSA es bueno para encriptar mensajes pequeños, DES es una mejor elección con mensajes más grandes debido a su velocidad. Además, RSA ofrece firmas digitales y un intercambio seguro de claves sin necesidad de intercambio previo de códigos secretos.

Combinar los dos sistemas de encriptación es como enviar un mensaje codificado en una envoltura segura. Una transacción típica con envoltura digital RSA con otra parte, podría realizarse de la siguiente manera:

1. Encripta el mensaje con una clave DES aleatoria.
2. Encripta la clave DES con RSA
3. Envía por Internet el documento encriptado mediante la combinación DES/RSA

CERTIFICADOS DIGITALES

Antes de hablar de los certificados digitales es importante hablar de lo que son las autoridades de certificación; éstas son organismos reconocidos por la comunidad internauta sobre los que descansa toda la seguridad de este proceso de certificación, el símil habitual es el de los notarios.

El certificado digital es un documento digital emitido por un tercero confiable, en general una autoridad de certificación (CA: Certification Authority), que garantiza la vinculación entre la identidad de un sujeto o entidad y su clave pública, es decir, la autoridad de certificación entrega un certificado digital personalizado a un individuo que le permitirá identificarse ante terceros. Más adelante trabajaremos con certificados digitales, en la implantación de uno de los dispositivos, objeto de estudio de este proyecto.

El certificado digital permite autentificar y garantizar la confidencialidad de las comunicaciones entre personas, empresas o instituciones públicas a través de las

redes abiertas de comunicación. El certificado es personal y, gracias al grado de confidencialidad, evita suplantaciones.

La base de esta tecnología reside en los códigos secretos o encriptación. La encriptación garantiza la confidencialidad, la integridad y la autenticidad de la información que se desea transmitir y que tiene vital importancia para la persona o empresa.

En esta tecnología, cada usuario y, por lo tanto, cada certificado, posee una clave privada que se mantiene secreta y una pública que pasan a formar parte de un certificado digital. También permiten detectar si una transacción ha sido alterada durante la transmisión a través de la red, consiguiendo de este modo garantizar el objetivo esencial de aseverar la integridad de un mensaje.

El certificado es emitido para ser almacenado en el ordenador personal del solicitante (en nuestro caso seria el paciente el que almacenaría el certificado en su ordenador), pero se puede instalar en varios a la vez, aunque no es recomendable instalarlo en sitios públicos, porque si no se desinstala al finalizar, el certificado puede quedar al alcance de terceras personas. El propietario del certificado podrá realizar diferentes operaciones a través de la red identificándose igual que si lo hiciese físicamente.

DESVENTAJAS:

El certificado digital se ha de solicitar personalmente; para ello se deberá poner a punto el ordenador y acudir personalmente al sitio indicado por la CA, para que una persona física dé fe que la persona que ha solicitado el certificado digital es quien dice ser. Se ha de tener cuidado porque si alguien se apodera de él (olvido en un ordenador público, en un pen drive perdido, etc.) puede sufrir suplantación de identidad y realizar todo tipo de operaciones en nombre del certificado que posea.

3.3. Dispositivos Biométricos para la Identificación de Usuarios [20, 21]

La biometría estudia medios para verificar una identidad o identificar unívocamente a las personas, basándose en características anatómicas o físicas, como puede ser la identificación por huellas dactilares, las retinas, el iris, los patrones faciales, de venas de la mano o la geometría de la palma de la mano, o en rasgos del comportamiento, como son el ritmo del tecleo, la firma, el patrón de la voz o

el reconocimiento por ADN. La voz se considera una mezcla de características físicas y del comportamiento.

Los dispositivos que se sirven de la biometría tienen una gran ventaja: no necesitan que el usuario dependa de su memoria para recordar contraseñas, o llevar dispositivos encima, ya que identifican biológicamente al instante al usuario, sin necesidad de un elemento externo; ésto puede resultar muy útil para algunas personas que tengan problemas de memoria

3.3.1. Características Físicas

- Identificación por huellas dactilares [22, 23, 24, 25, 26, 27]

Las huellas dactilares son los pliegues o formas caprichosas que adopta la piel que cubre las yemas de los dedos; de manera más específica podemos definir estos pliegues por su forma de dos maneras: las salientes se denominan crestas papilares y las depresiones surcos interpapilares.

En las crestas se encuentran las glándulas sudoríparas. El sudor que éstas producen contiene aceite, que se retiene en los surcos de la huella, de tal manera que cuando el dedo hace contacto con una superficie queda un residuo de ésta, la huella dactilar.

Las huellas dactilares son únicas e irrepetibles, aún en gemelos idénticos, debido a que su diseño no está determinado estrictamente por el código genético, sino por pequeñas variables en las concentraciones del factor del crecimiento y en las hormonas localizadas dentro de los tejidos. Incluso, en un mismo individuo, la huella de cada uno de sus dedos es diferente. La ciencia que estudia el reconocimiento de las personas mediante la impresión o reproducción física de los dibujos formados por las crestas papilares en las yemas de los dedos se llama dactiloscopia; es una rama de la papiloscopia, técnica basada en principios científicos debidamente comprobados que tienen como objeto establecer de manera categórica e indudable la identidad física humana, a través del estudio de los calcos, impresiones o estampas de las crestas papilares, ya sean palmares o plantares.

La base para la identificación de huellas dactilares está constituida por dos axiomas:

Las huellas dactilares son únicas.

Las huellas dactilares no cambian a lo largo de la vida.

La base de las prácticas de identificación dactilar es el hecho de que la unicidad de las impresiones dactilares se expresa en las crestas papilares, que muestran los rasgos de un carácter principal que mantiene sus propiedades, incluso en condiciones adversas. La situación, la dirección y las relaciones de las crestas se mantienen idénticas cuando se imprimen a presión, cuando se estira la piel flexible, e incluso cuando se distorsiona, hasta un nivel relativamente elevado.

Tras años de investigación y la experiencia adquirida en los mismos, se ha demostrado que los aspectos principales de los detalles de las crestas no cambian con el crecimiento; desde que naces hasta tiempo después de la muerte conservamos las formas y detalles de las crestas papilares. Como los detalles están incrustados en la dermis o capa profunda de la piel, recuperan su forma original cuando la piel descansa después de un daño temporal de la epidermis o capa exterior de la piel, como pueden ser las quemaduras, ampollas, abrasiones o incluso callosidades. Sólo cuando de un daño exterior, por ejemplo, una herida profunda, afecte la dermis la piel desarrollará un tejido de cicatrización que modificará los detalles papilares. Sin embargo, después de cierto tiempo esto podrá transformarse en una característica permanente, y dar a ese pedazo de piel un aspecto aún más inconfundible.

La huella digital ha tenido diferentes usos a lo largo de la historia de la humanidad. Según B.C. Bridgest, ilustre experto en investigación y especialista en la materia, la huella digital comenzó a utilizarse en antiguas civilizaciones. Algunos de lo primeros usos prácticos de la identificación, mediante la impresión de huella digital, se le acreditan a los chinos, quienes la aplicaban diariamente en sus negocios y empresas legales; además, en la cultura china se establecía que, para divorciarse de la esposa, el esposo debía dar un documento que expusiera siete razones para hacerlo en el cual todas las letras deberían estar escritas con su propia mano y signar el documento con sus huellas dactilares. También, desde el siglo XIX es utilizada en investigaciones criminalísticas.

En México, artículo 1834 del Código Federal Civil, [29] como en otros países del mundo, las huellas digitales son reconocidas legalmente como sustituto de la firma escrita, indispensable para validar un contrato o documento, en los casos en que la persona involucrada no pueda o no sepa firmar.

Tecnológicamente, es posible que la huella dactilar nos identifique en tareas diarias, como pueden ser abonar la cuenta de un restaurante [19] o el control de presencia en el trabajo, ya que existen muchas empresas que ofrecen la implantación de sistemas de identificación y pago mediante huella dactilar.

Algunos ejemplos concretos de pago en comercios con huella dactilar los encontramos en varios comercios de Barcelona, uno de ellos es una ferretería. El usuario se registra una primera vez y, desde entonces, su huella queda grabada y vinculada a su tarjeta de crédito. Cabe destacar que el sistema toma en consideración las huellas de dos dedos, en vez de uno, y que detecta con absoluta precisión que los dedos sean reales y vivos, descartada, por tanto, la posibilidad de usar un dedo cortado, como hemos visto en las películas.

La ley de protección de datos de carácter personal (LOPD) 15/1999 del 13 de diciembre, los datos de huella dactilar que almacena nuestro sistema de control de presencia se consideran de bajo nivel; no se consideran de nivel alto, ya que no puede obtenerse a partir de ellos datos sobre orientación sexual, sexo, raza, etc... ni tampoco se consideran de nivel medio, ya que tampoco podríamos obtener datos de los gustos, aficiones, habilidades, etc... del propietario de la huella.

Según la LOPD, un dato de carácter personal de nivel bajo, que es usado solamente para el control interno del personal de la empresa, no requiere de autorización de los empleados, ya que se entiende que son datos necesarios para la gestión interna. Tan solo sería necesario publicar en el tablón de anuncios una nota informativa comunicando la implantación de un sistema de control de presencia por huella dactilar, por lo que se tomarán muestras de las huellas dactilares de todos los empleados. Además, se advertirá de que el sistema cumple con la legalidad vigente; al respecto el artículo 5 de dicha ley dice que si bien no será preciso el consentimiento del interesado, si deberá advertirse al mismo de los extremos contenidos en ese precepto y, especialmente, de las consecuencias disciplinarias que podría acarrear su negativa a que la huella sea tratada.

Puntos característicos de la huella dactilar

La comparación directa entre la imagen de la huella que se pretende identificar y el resto de huellas almacenadas en la base de datos no sería un medio fiable, debido a la alta probabilidad de errores, tales como, ruidos en la imagen, áreas de huella

dañadas, posición diferente en la postura del dedo en el momento de tomar la imagen, etc... La solución a este problema consiste en la extracción de una serie de puntos característicos a partir de la imagen de la huella y comparar después éste conjunto de puntos característicos con los almacenados en la base de datos pertenecientes a otras huellas dactilares; el sistema, por lo tanto, acota la búsqueda centrándose en un grupo. Para sacar la imagen de la huella y poder comparar los puntos característicos de la misma con los almacenados en la base de datos usamos sensores biométricos de huella dactilar; hay varios tipos de sensores en el mercado.

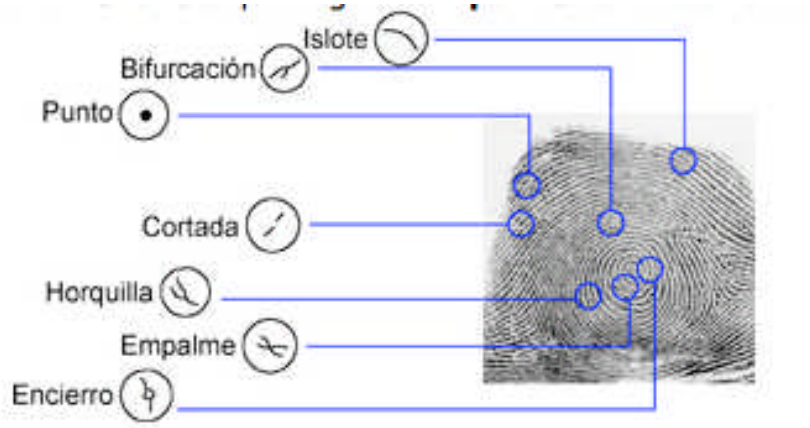


Ilustración 4. Diferentes puntos característicos [30]

La imagen muestra los siete puntos característicos que hay en un dedo; éstos se repiten indistintamente para formar entre 60 y 120 puntos característicos.

Tipos de sensores

En el mercado actual existen muchos tipos de sensores biométricos de huella, lectores capaces de convertir una huella en una imagen procesable por un algoritmo.

- **Lectores ópticos**

Es, probablemente, el tipo de sensor más extendido hoy en día. Los sensores ópticos se basan en una extracción de puntos de la imagen que se genera de la huella, poseen velocidad en la captura y resolución de la imagen variable dependiendo en gran parte de la calidad del aparato. Este tipo de sensor es el más utilizado por su bajo coste y por su facilidad de uso. Funciona con un dispositivo CCD (Charged Coupled Device), como el usado en las cámaras digitales, que tienen un array de diodos sensibles a la luz que generan una señal eléctrica en respuesta a fotones de luz. Cada diodo graba un pixel, un pequeño punto que representa la luz que le es reflejada.

Cuando terminamos de pasar el dedo por el lector, se recuperan todos los pixeles situándolos en su posición correcta y formando así la imagen. Hay que tener en cuenta que obtendremos una imagen invertida del dedo, con áreas más oscuras que representan más luz reflejada (las crestas del dedo) y áreas más claras que representan menos luz reflejada (los valles entre las crestas).

En el mercado existen muchos modelos y marcas de sensores ópticos, se ha tenido la oportunidad de probar el funcionamiento del BioShield, ésto lo veremos más adelante en el apartado de implementación; sin embargo, hay mucha oferta en este tipo de lectores. Por ejemplo, el ZK7000 es un lector de huellas digitales USB, diseñado para su uso con aplicaciones de software empresarial ZKSoftware.

Ilustración 5. ZK7000

Donde simplemente coloca su huella digital en la ventana del lector brillante y el lector, de forma rápida y automáticamente, escanea la huella dactilar. Los componentes electrónicos incorporados calibran el lector y cifran los datos explorados antes de enviarlos a través de los productos. El precio es de unos 700€, algo elevado para el propósito de este proyecto.

- **Lectores LE:Es (Light Emitting)**

Se trata de una nueva tecnología que supera las otras tecnologías de lectura de huella dactilar existentes (óptica, térmica...); se basa en un polímero que reacciona al contacto con la huella emitiendo luminiscencia; de esta forma, al ser tan sólo la parte que contacta con el sensor la que emite luz, las crestas de la huella forman un patrón, ésto hace que genere una imagen exacta de la huella, aunque ésta esté sucia o incluso pintada. Muy fiable porque evita falsos rechazos. [41]

Ilustración 6 sensor LE

- **Lectores capacitivos**

El método capacitivo genera una imagen de las crestas y valles de la huella en la superficie de un circuito integrado de silicona. Es el tipo de sensor más caro y, también, de los más delicados. No admite instalación en el exterior y ha sido tradicionalmente muy utilizado en sistemas de control de acceso.

Ilustración 7. Sensor capacitivo

- **Lectores térmicos**

El sensor térmico utiliza un sistema único para reproducir la imagen del dedo completo, “deslizándolo” sobre sensor. Durante este movimiento se realizan tomas sucesivas de temperatura y se pone en marcha un software especial que reconstruye la imagen del dedo, gracias a las diferencias de temperatura entre las crestas y los valles de los surcos que forman los pliegues de la huella. Los lectores de tecnología térmica son especialmente indicados para soluciones de control de acceso y admiten su instalación en el exterior. Dado el reducido tamaño del sensor, son sistemas que cada vez más se están incorporando en ordenadores portátiles para funciones de control de acceso lógico. Tienen cierta dificultad de uso por lo que es necesario un cierto aprendizaje.

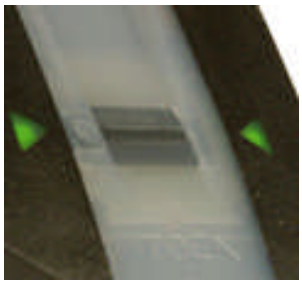


Ilustración 8. Sensor térmico

o Biometría ocular [31, 32, 33]

La vista es un sentido muy apreciado por el ser humano y el ojo es su herramienta. La biometría se ha interesado en el estudio oftalmológico como herramienta de identificación unívoca de los seres humanos.

Hay dos formas de escanear los ojos:

- **El escáner de iris:** se realiza utilizando una videocámara y examinando los patrones de color únicos, que se encuentran en los surcos de la parte coloreada de nuestros ojos. También, están empezando a utilizarse en los aeropuertos y, en algunos, se está probando esta tecnología como sustituta de los mostradores de facturación; en este caso, nuestro ojo sería nuestro billete.
- **El escáner de retina:** mide el patrón de venas en el fondo del ojo y se obtiene proyectando una luz infrarroja a través de la pupila. Esta luz es bastante invasiva y es, por lo tanto, un mecanismo menos habitual, pero se sigue utilizando para restringir el acceso a instalaciones militares, laboratorios de investigación y otras áreas de alta seguridad.

Tanto el escáner de retina como el de iris son los sistemas biométricos considerados como los sistemas más seguros, pero no siempre funcionan. El escáner de retina no funciona en personas ciegas o con cataratas, mientras que la precisión de los escáneres de iris varía en función de la luz ambiente y del ángulo en que se coloque la cabeza.

Otros factores externos que también afectan a estos escáneres son la raza y el color de los ojos; cuanto más oscuros, más le cuesta al escáner distinguir dónde acaba la pupila y empieza el iris.

Este tipo de biometría, por lo tanto, pertenece a una tecnología altamente segura, hoy en día bastante cara, por lo que es apropiada para emplazamientos de muy alta seguridad.

Dispositivos de biometría ocular por USB

La firma de seguridad biométrica *Hoyos Group* ha desarrollado una tecnología de escaneo de iris vía USB, para conseguir seguridad en el PC.

El Grupo Hoyos ha nombrado a su innovadora tecnología "*Eye-Lock*". El escáner portátil de iris es aproximadamente del tamaño de una tarjeta estándar y muy liviano.

Ilustración 9. Eye Lock

El dispositivo tiene que estar conectado con un ordenador a través del puerto USB. Al leer el iris de la persona, ésta es identificada y puede utilizar esta verificación de identidad en cualquier sitio on-line, ya sea para correo electrónico, PayPal, una cuenta bancaria o el Hospital Virtual.

Gracias a la tecnología biométrica, es posible que no sea necesario tener que recordar y escribir la contraseña de las cuentas importantes on-line. Sólo un contacto visual con el dispositivo y automáticamente, se desbloquean las cuentas protegidas por contraseña en la pantalla del ordenador.

El dispositivo lee el iris de un usuario y crea una clave numérica única, que cambiará cada vez que uno entra a su cuenta. Eso significa que no hay posibilidad de que a la contraseña se le de un mal uso.

- Reconocimiento facial [35, 36, 37, 38]

En el rostro existe abundante información para reconocer el estado mental y humor de un individuo. En todas las caras existen, al menos, dos ojos, dos cejas, la nariz, la boca y la barbilla. La distancia entre los ojos, la sombra de las cejas, la nariz y la barbilla son diferentes para cada individuo. Al igual que cambia el tamaño, los ángulos o la expresión de la cara, varían también las imágenes de la cara. La relación de la

posición de las distintas partes de la cara, así como sus sombras y tamaños, ha contribuido a la clasificación de los rostros y a la posibilidad de reconocer a una persona. Una de las principales ventajas del reconocimiento facial es que se trata de un método no intrusivo, ya que los datos pueden ser adquiridos, incluso sin que el sujeto se percate de ello.

En la actualidad pueden distinguirse dos tipos de datos faciales, basándonos en el aspecto externo:

- **Las imágenes de intensidad**, donde se representa la textura de la cara.
- **Los datos tridimensionales**, que recogen la estructura geométrica facial. La información tridimensional puede representarse de dos modos diferentes:
    - mediante una imagen de rango: se trata de una imagen en niveles de gris, donde la intensidad de cada píxel representa la profundidad del objeto en ese punto.
    - mediante una nube de puntos en el espacio, habitualmente aproximados a una superficie mediante un conjunto de polígonos.

La principal limitación de los sistemas de imágenes de intensidad basados en una representación facial de textura es su dependencia de las condiciones de iluminación y de la posición de la cara.

Por el contrario, la representación 3D, por su propia definición, no depende de la iluminación y, además, permite la normalización de la cara en posición.

Las imágenes de textura aportan información determinante de áreas de la cara donde no existe una gran variación en la estructura geométrica, como puede ser la frente, las cejas y las áreas con vello facial.

En el caso de los datos 3D, la información aportada es más relevante en las áreas donde no existe una gran diferencia entre el aspecto de la textura, pero sí en la forma facial, como puede ser la mandíbula, la barbilla o las mejillas.

Reconocimiento facial en los teléfonos de última generación [13]

Existen aplicaciones para los teléfonos de última generación, que permiten utilizar la biometría para proteger el dispositivo, puesto que hoy día los teléfonos son mucho mas parecidos a ordenadores personales que a teléfonos, en ellos almacenamos gran cantidad de información sensible que necesita ser protegida.

- **Para iPhone**: El **RecognizeMe** es una aplicación para que utiliza la cámara frontal del dispositivo para realizar un desbloqueo del teléfono mediante reconocimiento facial.

  Su funcionamiento es muy sencillo. Tras ser instalada la aplicación en el iPhone, se añade un botón adicional en la pantalla de bloqueo del teléfono y basta con tocarlo para que el iPhone utilice su cámara frontal para analizar el rostro de la persona que tiene justo delante. En caso de que la persona se encuentre en su base de datos y la reconozca, el iPhone queda desbloqueado de forma sencilla pero, si no es así, de nuevo devuelve al dispositivo a la pantalla de desbloqueo.

- **Para Android:** la aplicación se llama **Visidon AppLock**, nos permite configurar un complejo sistema de reconocimiento facial y así limitar el acceso a nuestra Tablet o teléfono. El funcionamiento de Visidon AppLock es sencillo. Una vez instalada la aplicación seleccionaremos las aplicaciones que deseamos proteger con el sistema de reconocimiento facial. Una vez escogidas las aplicaciones a proteger, introducimos una cara, o varias, que realicen la función de contraseña.

Estos sistemas sólo funcionan con dispositivos que tienen cámara frontal.

o Palma de la mano [39, 28, 14]

Los sistemas biométricos basados en las manos están teniendo un uso creciente en la seguridad de instalaciones como aeropuertos, plantas nucleares y estadios olímpicos. Son ideales para un uso masivo, ya que tienen una buena relación entre el tiempo de uso y el tiempo de análisis. Además, no presentan reticencias ni incomodidades por parte del usuario como pueden presentar los sistemas basados en reconocimiento de la retina.

Muchas de las características biométricas relacionadas con la mano son relativamente invariantes y peculiares, aunque no únicas. Son medidas geométricas tales como: longitud, anchura y altura de la mano y dedos. Ésto hace que los sistemas biométricos basados en manos sean normalmente utilizados para tareas de verificación y no de identificación.

Los sistemas de la geometría de la mano usan una cámara óptica para capturar dos imágenes ortogonales bidimensionales de la palma y lados de la mano, ofreciendo un equilibrio de fiabilidad y facilidad de su uso. Recogen normalmente más de 90 medidas dimensionales, incluyendo el ancho, la altura, y longitud digital; las distancias entre las juntas y formas del nudillo.

La adquisición de las imágenes se realiza en entornos controlados, que constan de una plataforma formada por unos pivotes para fijar la posición de la mano/dedos y un espejo para poder obtener también el dorso de la mano. Los principales inconvenientes de estos sistemas son el mantenimiento que requieren, debido al desgaste y suciedad de la plataforma y espejos.

El reconocimiento palmar inherentemente implementa muchas de las características de emparejamiento que han permitido que el reconocimiento por huella dactilar sea uno de los más conocidos y el más publicitado método biométrico. Tanto la huella palmar como la huella dactilar son representadas a través de la información de la impresión de surcos de fricción. Esta información combina el flujo de surcos, las características de los surcos y la estructura de los surcos de la porción de la epidermis expuesta.

La información representada por estos surcos de fricción permite determinar si áreas correspondientes de fricción de surcos han sido originadas por la misma fuente, o bien, si es imposible que hayan sido originadas por la misma fuente.

- **Venas de la mano**

Una variante en la biometría que se basa en las palmas de la mano, es la que estudia las venas de la palma de la mano. La forma de los conductos sanguíneos es única en cada individuo, al igual que las huellas dactilares, por lo que cada “mapa sanguíneo” corresponde a una persona en concreto. [17]

El sistema de reconocimiento biométrico de la palma de la mano es muy amplio y entre sus diferentes posibles estudios encontramos el de las venas de la palma de la mano. Éstas investigaciones demuestran que el patrón de las venas es único para cada individuo y, al estar 3 milímetros por debajo de la epidermis es más difícil de falsificar.

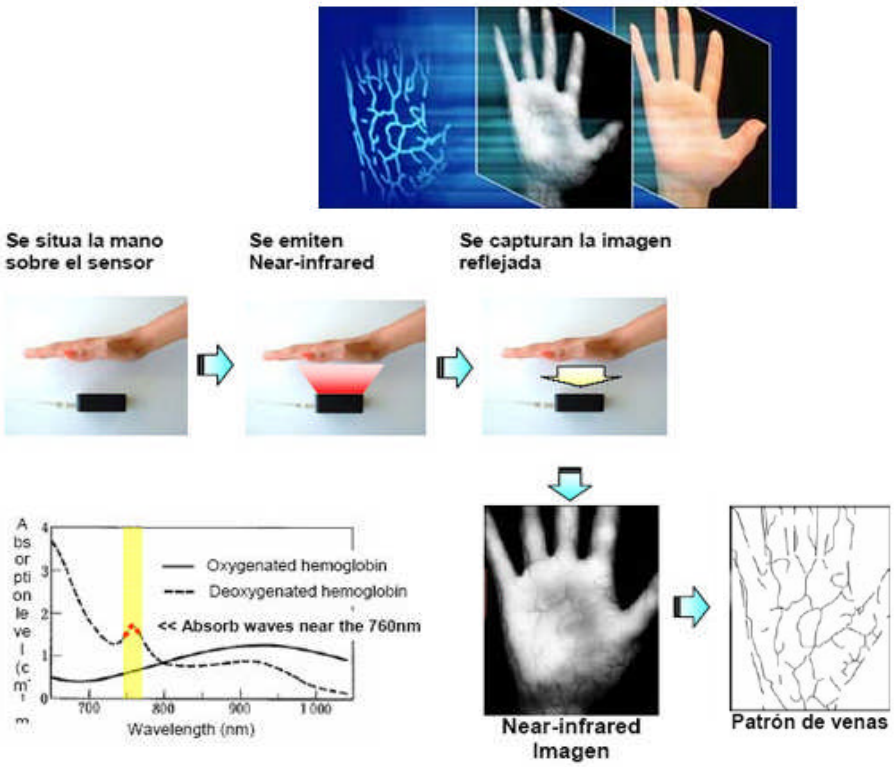


Ilustración 10. Patrón de venas

En España, La Caixa está realizando una prueba piloto con este sistema de seguridad biométrica. [17]

3.3.2. Características de Comportamiento

A pesar de lo que se pueda pensar, los indicadores biométricos de comportamiento son también una buena opción para establecer la identidad de una persona.

- Ritmo de tecleo

La biometría de tecleo es el proceso en el que se analiza la manera en que un usuario teclea en un terminal, mediante una monitorización del número de golpes que se le dan a un teclado por segundo, para así identificar patrones de ritmo.

Desde hace ya un tiempo se ha demostrado que el ritmo de tecleo es una buena señal de identidad; además, se trata de uno de los sistemas de análisis biométricos más económicos, ya que lo único que se necesita es un teclado.

Los ritmos de golpes de teclas de un usuario son medidos y registrados por un algoritmo para desarrollar una plantilla biométrica de patrones de escritura de usuarios, para autenticaciones futuras.

La aplicación del ritmo de tecleo al acceso computarizado es relativamente nueva y ha habido poco trabajo en dicha área.

Una técnica de verificación de tecleo puede clasificarse como estática o continúa. En el caso de los métodos estáticos se hace un análisis en un periodo específico de tiempo, como por ejemplo, mientras alguien teclea una clave corta. Los métodos estáticos aportan un mayor control que una contraseña por sí misma, pero no dan seguridad continúa, puesto que no pueden detectar la sustitución de un individuo después de la verificación inicial. Por otro lado, la verificación continúa permite monitorizar el comportamiento de tecleo de un usuario durante periodos más largos.

DESVENTAJAS:

Entre las desventajas, cabe citar el paso del tiempo, ya que con el tiempo perdemos velocidad en los dedos. Además, en caso de tener un accidente que inmovilice un dedo o una mano, el ritmo del tecleo cambia considerablemente.

- Firma

Las posibilidades de uso de los datos biométricos en la firma electrónica no se quedan en la simple identificación de la persona, como en el caso del control de acceso. Mediante una contraseña podemos obtener acceso o accionar un proceso; sin embargo, apoyándonos en rasgos dinámicos y biométricos, como la firma escrita y la voz, logramos también documentar un acto de voluntad del individuo, un acto que es inseparable de la persona y que no puede darse por error.

Al contrario que en el caso del número secreto, nuestros rasgos distintivos garantizan que somos la persona autorizada, pues estos rasgos no podrán ser ni espiados, ni robados, ni transferidos a otra persona.

La firma electrónica a partir de la captación de la firma escrita está, por las características señaladas, predestinada para ser usada en la firma de contratos, documentos, recibos y protocolos.

El aspecto dinámico de la firma escrita es muy importante, no solo porque constituye la forma perfecta de documentar un acto voluntario, sino porque permite identificar al autor, es decir, permite unir cada firma electrónica a una única persona en concreto.

La firma electrónica está dividida en datos estáticos y datos dinámicos. Los datos estáticos se desprenden del trazado de la firma en dos dimensiones, y pueden revelan al grafólogo ciertos rasgos inequívocos. Los datos dinámicos de la firma electrónica son mucho más fáciles de analizar que los datos dinámicos de la firma sobre el papel, pues los datos en soporte electrónico son exactos. Sólo los datos dinámicos, la presión, la dirección, la velocidad y los cambios en la velocidad de la firma, son capaces de ofrecer una seguridad máxima en el momento de identificar una firma.

Cualquiera puede, tras cierto tiempo practicando, imitar el trazado de la firma escrita de otro y no es difícil adquirir una muestra de la firma de cualquier persona. Pero algo que el falsificador no puede conocer y, aunque conociera, no podría imitar, son los rasgos dinámicos de la firma.

Así, la firma escrita se convierte en la mejor y más segura opción para aquellos que deseen utilizar la firma electrónica.

3.4. Otros Tipos de Biometría

La tecnología ha ido más allá y está incorporando características como el olor corporal y las ondas cerebrales para identificar a las personas. [18]

Se está buscando hasta el más insólito de nuestros rasgos y características físicas para poder realizar su estudio biométrico, para probar que uno es, efectivamente, uno mismo.

Teniendo en cuenta el éxito que han tenido experiencias como la lectura de la huella digital, el iris del ojo, o los trazados faciales, ahora hay nuevas iniciativas que se basan en otros rasgos menos obvios, como el olor corporal, la oreja, las ondas cerebrales, las venas y hasta el mismísimo ADN.

Ninguna persona huele igual a otra, por muchos perfumes o jabones que uno se aplique. Por eso, la empresa Mastiff Electronic Systems está desarrollando y probando

un novedoso sensor electrónico extremadamente sensible que imita el sentido del olfato humano para detectar partículas de olor liberadas por cada individuo.

En la misma línea existen proyectos para descifrar las ondas cerebrales. Los especialistas apuestan por sistemas biométricos que midan las ondas electromagnéticas emitidas por el cerebro humano. En vez de aproximarse y acostar la cabeza sobre un sensor, esta tecnología conseguiría medir los pulsos provenientes del cerebro sin que el usuario necesite mover un solo músculo.

ACTUALIDAD EN BIOMETRIA [34, 36,12]

Entre las herramientas que las fuerzas armadas norteamericanas tenían a su disposición para asegurarse de que poseían la identidad correcta de Osama bin Laden después de haberlo eliminado, estaban los escáneres biométricos como el de reconocimiento facial, según un artículo de Wired.

La herramienta específica empleada por el personal militar, para asegurarse de que tenían a la persona correcta, fue una versión actualizada de Secure Electronic Enrolment Kit (SEEK II), un dispositivo biométrico móvil que obtiene escaneado de iris, huellas digitales o escaneados faciales, y autentifica identidades mediante la comparación de esa información, por vía inalámbrica, con una base de datos del FBI.

El dispositivo SEEK II, conocido también como Crossmatch, es una versión más rápida y robusta de los sistemas biométricos BATS y HIIDE que el personal militar empleó con anterioridad en el Medio Oriente para recoger la mayor cantidad de información posible, con el fin de diferenciar mejor entre los ciudadanos comunes y aquellos que tienen vínculos con el terrorismo.

El SEEK II tiene varias actualizaciones importantes con respecto a sus predecesores en términos de su acceso a base de datos, así como su habilidad para comunicarse por vía inalámbrica, gracias a sus múltiples capacidades de comunicación, así como su acceso a bases de datos más allá de las disponibles en el país en que está siendo utilizado.

Pese a la utilización del reconocimiento facial, los funcionarios de Defensa sostienen que la biometría de huellas digitales sigue siendo la modalidad biométrica más útil y confiable para los cuerpos militares. Sin embargo, por esa misma razón, algunos

piensan que esos procedimientos modernos utilizados en operaciones militares le dan cierto sentido de labor policíaca cuando el personal militar busca evidencias para enviarlas al FBI para su análisis.

El uso de la biometría en hospitales [9, 10, 11]

La biometría se introduce poco a poco también en el sector hospitalario; existen unas soluciones ya estudiadas y presentadas por empresas del sector de la biometría, que abarcan, desde el control de presencia y asistencia del personal del hospital, hasta las áreas restringidas por cada usuario, dependiendo de su identidad, permitiéndole o denegándole el acceso a puntos del hospital sobre los que se requiera un control mayor, tales como quirófanos, laboratorios, etc...

La solución completa consta de un sistema de impresora de tarjetas, que imprime, codifica y personaliza la tarjeta que recibe el usuario como método de identificación para personal medico o incluso pacientes; el sistema de acceso es colocado en las puertas o torniquetes del hospital, el coste podría aumentar si hubiese que instalar los sistemas de acceso.

En algunos hospitales se han usado soluciones biométricas para la identificación de pacientes, con el objetivo de ser más minuciosos con los historiales médicos y evitar así el cruce de historiales. En centros médicos de Nueva York se usan dispositivos biométricos del Iris.

4. Metodología Empleada

La metodología empleada durante la elaboración del proyecto ha sido el modelo de desarrollo en espiral, que consta de cuatro fases cíclicas. No hay un número definido de iteraciones, éstas las decide el equipo de proyecto, hasta que se hayan conseguido todos los objetivos propuestos en el apartado de Objetivos.

En cada vuelta o iteración hay que tener en cuenta los objetivos y las alternativas. La idea principal es decidir qué problema vamos a resolver, estudiar todas las alternativas, escoger una, desarrollarla y comprobar su buen funcionamiento antes de afrontar la siguiente etapa (vuelta de la espiral).

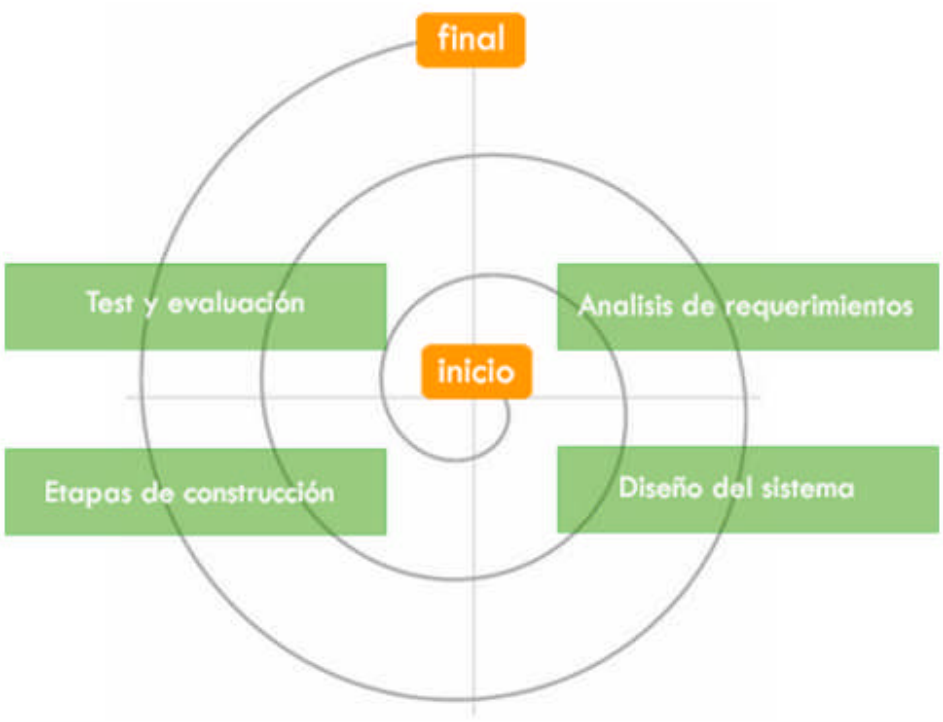


Ilustración 11: Desarrollo espiral [8]

- **Análisis de requerimientos:** Basándonos en los objetivos del proyecto, cada iteración tiene en cuenta las tareas y los hitos del objetivo que se aborda en esa iteración.

- **Diseño del sistema:** Con los requisitos definidos ya en la etapa anterior se realiza el diseño a seguir en esta fase para conseguir el hito propuesto en esta vuelta de la espiral.

- **Construcción:** Esta fase se realiza de manera diferente en dependencia del objetivo a tratar en ese momento y de la etapa del proyecto en la que nos encontrábamos.

  - Así, para objetivos parciales que constaban de análisis e investigación de metodología y documentación se cumplían los objetivos documentales marcados.

  - Y para objetivos parciales de implementación se estudiaba la mejor manera de realizar el desarrollo y se elaboraba un diseño óptimo para su posterior ejecución.

- **Test y evaluación**: Las pruebas de implementación se han realizado posteriormente a la etapa de construcción, no obstante, para objetivos parciales en los que la documentación era nuestro pilar, la fase de pruebas la hemos realizado corrigiendo y mejorando la información recabada.

5. Especificación, Diseño e Implementación

De todos los métodos de autenticación que se han estudiado en este proyecto, se han implementado dos de ellos para analizar su funcionalidad más en profundidad, estos dispositivos son un token de seguridad y un lector de huella dactilar.

Inicialmente se analizó un token USB llamado WebIdentity [40] una llave de acceso seguro a través de internet

Ilustración 12. Token USB Webidentity

Con este dispositivo no se llegó a conseguir la conexión por diversos problemas con la interpretación del código, ya que usaba funciones de las que no se tenía ninguna información como era el caso de INITDONGLE. Con el WebIdentity se aprendió a manejar el fichero global.asa, también se estudió asp, visualbasic script y java script. Todo esto, al menos, ha servido de base para la implementación posterior del token de seguridad Digipass.

El WebIdentity permitiría a los usuarios del Hospital Virtual logarse introduciendo únicamente el usuario, se creó una base de datos donde todos los usuarios se encontraban almacenados, con los datos USER y el PIN, el token calculaba el pin (con algoritmos de encriptación 3DES) y comparaba en plano el pin generado por el WebIdentity y el almacenado.

5.1. Token: Implementación de un Sistema de Autenticación Digipass

Mientras se iban analizando otros métodos de autenticación, se ha nombrado ya el token de seguridad, comentando que iba a ser uno de los mecanismos a estudiar más

en profundidad procediendo, además, a su implementación. Se ha elegido la opción del token USB, que permite almacenar certificados digitales, como ya se ha visto éstos ya conllevan una garantía de seguridad en sí mismos, en un dispositivo USB que además es fácil de transportar.

Ilustración 13: Token Digipass

- Análisis de requisitos

En el inicio del proyecto se pidió alguna implementación de los mecanismos investigados, el token de seguridad era uno de los mecanismos más interesantes para poder analizar más en profundidad y existía la opción de conseguir uno para el estudio, el token que se ha implantado es el Vasco Digipass, Eutron se lo ha proporcionado a la universidad y ésto ha facilitado, por tanto, el proceso de elección del dispositivo.

Además se ha visto que funciona de manera parecida a otros token de seguridad existentes en el mercado, por lo que no existía inconveniente a la hora de implementar el Vasco Digipass en lugar de otros.

- Tecnología empleada

Actualmente hay bastante variedad de tecnologías para acometer los desarrollos que surgieron, a continuación se identifican los lenguajes de programación y los entornos de desarrollo empleados.

- Los lenguajes de programación

Java Script - Es un lenguaje script (el más usado hoy) orientado a objetos. Está basado en acciones, poco restrictivo y generalmente incrustado como una pequeña funcionalidad dentro de una aplicación web. Es multiplataforma y es interpretado directamente por el navegador. Lo hemos usado para poder acceder a los archivos locales (el token) del paciente que se quiere conectar al Hospital Virtual.

C++: es un lenguaje de programación diseñado a mediados de los años 80 por Bjarne Stroustrup. La intención de su creación fue el extender al exitoso lenguaje de programación C con mecanismos que permitieran la manipulación de objetos. En ese

sentido, desde el punto de vista de los lenguajes orientados a objetos, el C++ es un lenguaje híbrido. Posteriormente se añadieron facilidades de programación genérica, que se sumó a los otros dos paradigmas que ya estaban admitidos (programación estructurada y la programación orientada a objetos). Por esto se suele decir que el C++ es un lenguaje de programación multiparadigma. Lo hemos usado para desarrollar la lógica del servidor, hemos creado una DLL propia con este lenguaje de programación.

ASP (Active Server Pages): es un lenguaje de programación de servidores para generar páginas web dinámica. Lo hemos utilizado para crear una página web intermedia en HTML que lleva etiquetas incrustadas que dan información personalizada.

HTML: HyperText Markup Language, lenguaje de marcado predominante para la elaboración de páginas web que se utiliza para describir y traducir la estructura y la información en forma de texto, así como para complementar el texto con objetos tales como imágenes. El HTML se escribe en forma de «etiquetas», rodeadas por corchetes angulares (<,>). HTML también puede describir, hasta un cierto punto, la apariencia de un documento, y puede incluir un script (por ejemplo, JavaScript), el cual puede afectar el comportamiento de navegadores web y otros procesadores de HTML. Se ha usado para la página intermedia.

- Entorno de desarrollo empleado

Visual Estudio 2008: es un entorno de desarrollo integrado (IDE, por sus siglas en inglés) para sistemas operativos Windows. Soporta varios lenguajes de programación tales como Visual C++, Visual C#, Visual J#, y Visual Basic .NET, al igual que entornos de desarrollo web como ASP.NET. Aunque actualmente se han desarrollado las extensiones necesarias para muchos otros. Lo hemos usado para los desarrollos en Java Script, C++, ASP y HTML.

Visual Studio permite a los desarrolladores crear aplicaciones, sitios y aplicaciones web, así como servicios web en cualquier entorno que soporte la plataforma .NET (a partir de la versión .NET 2002). Así se pueden crear aplicaciones que se intercomuniquen entre estaciones de trabajo, páginas web y dispositivos móviles.

Servidor IIS: Servidor Web y un conjunto de servicios para el Sistema Operativo Microsoft Windows. Ofrece servicios de FTP, SMTP, NNTP; HHTP y HTTPS. La versión de ISS utilizada es la 7.0. Integrado en el Windows vista.

Lo hemos utilizado para poder crear un servidor

- Introducción al Digipass

Vasco es empresa líder en la provisión de soluciones de autenticación, cuenta con proyectos destacados, entre ellos nos encontramos Paypal Security Key. Entre sus productos se encuentra el token Vasco Digipass, que es su producto estrella. Para su desarrollo Vasco ha contado con la tecnología Eutron.

El Digipass es un dispositivo de pequeño tamaño que permite autenticarse con seguridad en aplicaciones y sitios web.

Para este proyecto el token fue facilitado por la empresa distribuidora Abox al tutor, con un precio en el mercado que ronda los 35 euros para menos de 100 unidades, o 30 euros para más de 100.

La instalación del token no nos ha llevado muchos problemas, se pueden ver en los pasos que hemos seguido en el Anexo I.

Entre la versatilidad que ofrece el Digipass en este proyecto nos hemos centrado en la autenticación con certificado electrónico, aunque hemos estudiado más funcionalidades del token.

Instalado el token, empezamos a trabajar con él y ver las opciones que ofrece el dispositivo. El objetivo perseguido era implementar el token en el Hospital Virtual para obtener una autenticación más segura por lo que se estudiaron todas las acciones que podía llevar a cabo el dispositivo

- Autenticar con la contraseña de una sola vez (OTP): el token facilita un número en su display, ese número podría ser utilizado como contraseña de acceso.
- Realizar operaciones criptográficas. Una vez introducido el token se puede cifrar y descifrar texto con la ayuda de un certificado digital y el par de claves pública y privada
- Firmar digitalmente: mediante un certificado digital almacenado en el token se puede firmar un documento dándole validez oficial.

Aunque nos centraremos en el uso del token con certificados, hemos probado el **cifrado y descifrado** de datos, para ello inicialmente se desarrolló un proyecto en C++ utilizando la consola como salida. Se puede ver más en detalle en el Anexo II.

Finalmente se descartó esta opción porque, aunque se consiguió cifrar y descifrar, no conseguíamos el objetivo principal, que es, mejorar la autenticación. Por lo que se volvió a realizar un estudió de las posibilidades del token y nos decantamos por la utilización de certificados digitales.

Con los certificados se ha trabajado el cifrado y descifrado para ello se instalaron varios certificados digitales, con diferente extensión (.pfx, .p12, .crt, .cert), en el dispositivo; este método garantizaría al Hospital Virtual un mayor nivel de seguridad.

Para poder utilizar el certificado, este deberá estar instalado en el navegador en "Certificados Personales" en formato .pfx o .p12, cuando una aplicación lo necesite lo reconocerá automáticamente.

Los certificados digitales los encontramos con diferente extensión, los contemplados en este proyecto han sido:

- .pfx: es la copia de seguridad con clave privada de un certificado (exportado desde Internet Explorer).
- .p12: es la copia de seguridad con clave privada de un certificado (exportado desde Firefox).
- .cer y .crt: son formatos de exportación de clave pública de certificados.

La CA propia del Hospital Clínic de Barcelona deberá crear un certificado con formato estándar X509 (como son los .pfx y .cer) e instalarlo en cada token antes de dárselo a los pacientes. La web del Hospital Virtual, será accesible sólo si se reconoce este certificado.

5.1.1 Implementación del protocolo de autenticación para el Token Vasco Digipass 860 con C++ y JavaScript

Con el objetivo de autenticar el servidor se ha creado una CA, con la que se ha generado un certificado para el servidor (.cer). La CA se ha creado apoyándonos en

los servicios que ofrece OpenSSL, una vez hemos obtenido un certificado lo hemos agregado al servidor Microsoft IIS donde realizamos las pruebas del sitio web.

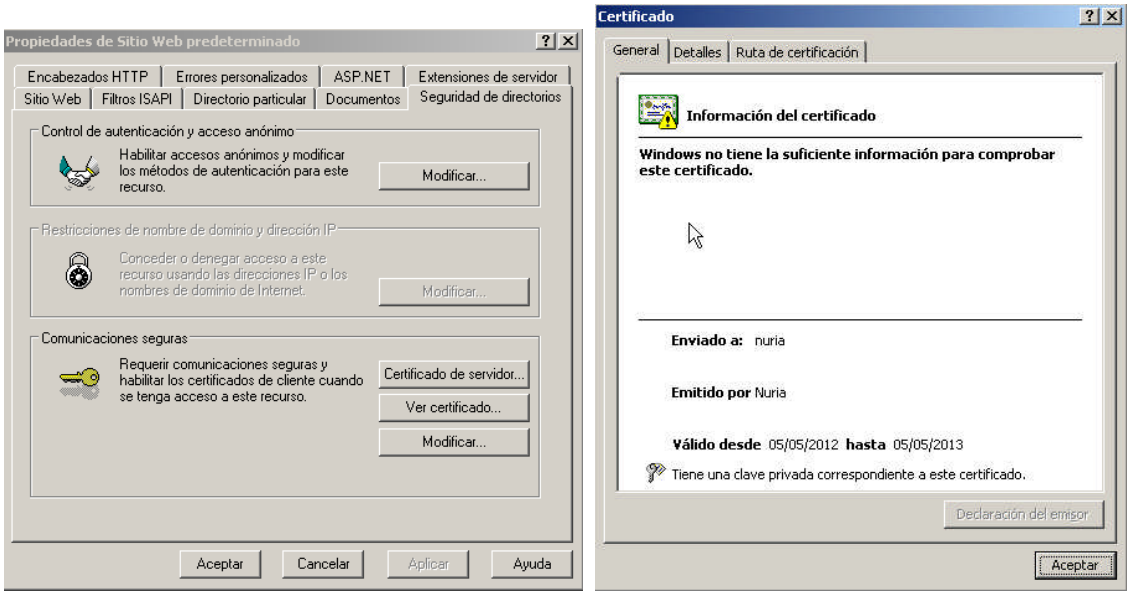


Ilustración 14. Información del Certificado

Éste certificado, una vez instalado en el servidor, nos da la opción de establecer un canal seguro para simular una comunicación SSL.

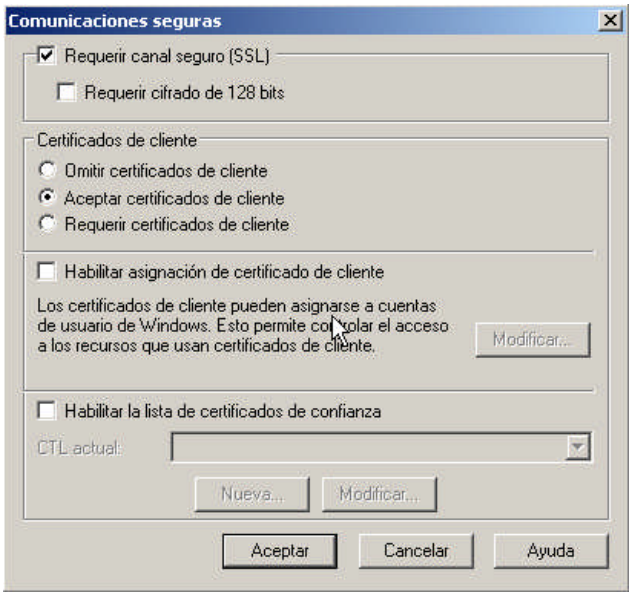


Ilustración 15. Canal Seguro

Se ha creado un proyecto de tipo WebApplication en Visual Estudio, con servidor de IIS, (el servidor es configurable en las propiedades de la aplicación web), ya que el

servidor ASP que nos proporciona el entorno de desarrollo no permitía el uso de SSL y por lo tanto no era posible establecer una conexión segura.

Con la instalación del certificado en el servidor, junto con la creación de un directorio virtual en la configuración del servidor web de IIS, queda preparada la estructura lógica para una comunicación segura entre hospital y paciente, a través de SSL.

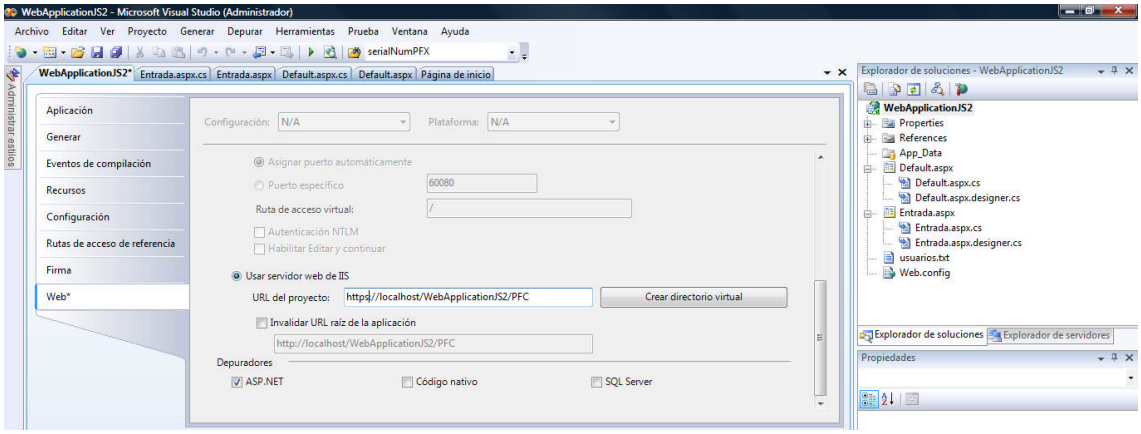


Ilustración 16. Configuración Directorio Virtual para Conexión Segura

Las propiedades del servidor son independientes en cada proyecto. La programación de la aplicación web ha sido realizada en C++ (para controlar la lógica del servidor) y JavaScript.

La página web está implementada en HTML, contiene, además, código JavaScript para controlar el formulario de acceso e interactuar con una DLL construida en C++, necesaria para que el servidor, como veremos mas adelante, pueda recuperar datos del paciente y permitirle o denegarle el acceso al Hospital Virtual.

Los datos de los usuarios acreditados por el Hospital Virtual para acceder a la aplicación se han almacenado en un fichero plano donde se guarda su código de usuario (nombre del paciente) y el número de serie del token facilitado a cada paciente.

Una aplicación web no tiene acceso a los recursos locales de un pc ni a ningún almacenamiento externo a su servidor. Para poder acceder al token, se ha decidido usar una DLL desarrollada en C++ incluida en el proyecto de Visual Studio la cual podemos utilizar mediante instrucciones JavaScript.

Para poder acceder a la DLL se declara una variable de tipo ActiveXObject:

var x = new ActiveXObject("ANamespace.BClass");

Después de esta llamada ya podemos usar la DLL invocando sus funciones en nuestro código C++.

Para incluir la DLL ha sido necesario compilarla y registrarla en el servidor. [15]

Para compilarla se introduce esta instrucción en la consola de comandos de MS-DOS:

csc /t:library BClass.cs

Para registrarla en nuestro servidor IIS se ejecuta esta otra instrucción:

regasm BClass.DLL /tlb /codebase

El objetivo de esta DLL es determinar si el número de serie del token, empleado para intentar acceder al Hospital Virtual, obtenido del certificado que se encuentra instalado dentro del token, es válido.

Se ha establecido un control de errores, de modo que la aplicación devuelve error si no se puede leer el fichero o si no es un certificado válido.

Para leer el certificado, salta un popup de control de ActiveX al que debemos permitir el acceso, esto sucede una vez por sesión.

Para realizar las pruebas se ha creado una web de acceso propia ya que no teníamos la posibilidad de acceder al entorno de prueba del Hospital Virtual. En ésta web se da la opción de usar certificados de tipo .cer o de tipo .pfx al desconocer que tipo de certificados usaría el hospital, por lo que se puede utilizar cualquiera de los dos. (se puede presentar solo con uno dependiendo de que tipo de certificados vaya a ofrecer el hospital a sus pacientes, si ellos mismos los emiten, los certificados tendrán que ser .cer si los encargan a una CA reconocida podrán ser .pfx).

- **Caso éxito**

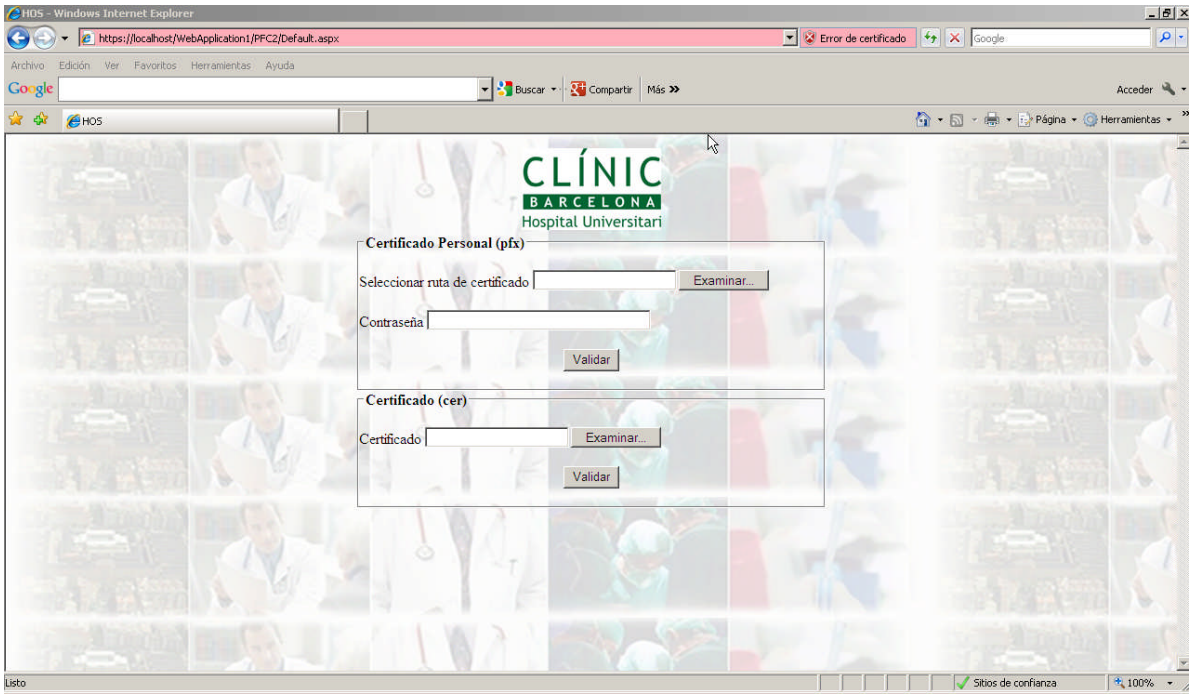


Ilustración 17. Acceso al Hospital Virtual

Una vez el usuario introduce los datos, si no ha habido problemas en la conexión y el certificado es reconocido por el servidor, para saber que todo ha ido bien, se le da la bienvenida desde una página intermedia y, se redirecciona a la web del Hospital Clínic de Barcelona.

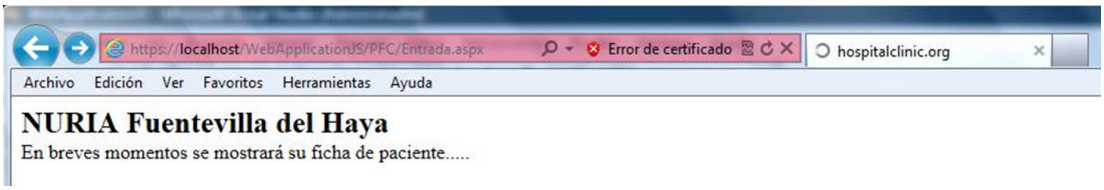


Ilustración 18. Página intermedia con datos de acceso

Ilustración 19. Página principal Hospital Virtual

- **Caso fracaso**

Si el certificado no se reconoce, se muestra un pop up en el que se indica que algo ha fallado, con el mensaje “usuario desconocido”.

Ilustración 20. Pop Up usuario desconocido

- **Ventajas de la autenticación con token de seguridad**

Es transportable gracias a su tamaño reducido.

Se puede generar una comunicación segura con el Hospital Virtual desde cualquier lugar.

- **Inconvenientes de la autenticación con token de seguridad**

Hay que gestionar la creación de los certificados, ya sea actuando el Hospital como CA o encargando los certificados a una CA existente como por ejemplo la Fabrica Nacional de la Moneda y Timbre (FNMT).

Hay que hacer un trabajo extra para poder usarlo, requiriendo el proceso de instalación del certificado en el token antes de proporcionárselos a los pacientes.

5.1.2 Implementación del protocolo de autenticación para el Token Vasco Digipass 860 con certificados digitales

Con el objetivo de usar los certificados personales del usuario (.pfx) como par de clave pública y privada, es decir, con la clave privada encripto y con la pública desencripto, se ha creado el siguiente procedimiento. Para ello como punto de partida se ha tomado el proyecto inicial.

La finalidad de esta nueva implementación es que cuando el usuario se conecte reciba un identificador que deberá devolver al servidor cifrado con su clave privada. El servidor recibirá el identificador cifrado y deberá descifrarlo con la clave pública del certificado de usuario. Para terminar compara el valor enviado inicialmente con el obtenido del descifrado y si se corresponde se permite el acceso, en caso contrario, se deniega.

Después de analizar los diferentes algoritmos de cifrado asimétricos existentes y las implementaciones que nos proporciona el lenguaje de programación C++ se decidió utilizar el protocolo RSA por su adaptabilidad al proceso. Para ello en la DLL, se le han incluido dos métodos nuevos Cifrado y Descifrado, que utilizan la funcionalidad de los namespaces System.Security.Cryptography y System.Security.Cryptography.x509certificates:

using System.Security.Cryptography;

using System.Security.Cryptography.X509Certificates;

Por otra parte, en el código principal del servidor se ha incluido la funcionalidad el envío del identificador y la recepción del mismo. También se utilizan las mismas primitivas de la DLL para realizar el Descifrado.

Esta implementación no ha sido finalizada por los obstáculos encontrados. Estos son:

1. Cifrado y Descifrado con clave privada.

- Se ha intentado recuperar el valor de la propiedad *keyexchangealgorithm* del certificado, obteniendo como resultado un valor *undefined.* Mientras que esa misma propiedad usada en la clave pública devuelve RSA-PKCS1-KeyEx
- Por otra parte, la propiedad *Signaturealgorithm*, perteneciente al algoritmo de firmado de la clave privada si devuelve el valor RSA-sha1.

Esta incongruencia nos hace plantearnos si el problema radica en la estructura del certificado o en las primitivas del lenguaje de programación.

Por lo que la función de cifrado genera una excepción al no poder hacer el casting para adaptarlo a la clase de cifrado RSA que es la que definida para nuestro algoritmo.

2. El servidor necesita conocer o bien la clave pública o bien tener acceso al certificado para poder extraerla (sólo el algoritmo de la clave). Nosotros disponíamos del certificado pero no se ha conseguido facilitar al servidor la clave pública. Ante esta situación se ha intentado acceder al certificado a través de la DLL utilizando nuevas primitivas de cifrado y descifrado específicas para el servidor:

   string Cifrado(string cert, string pass, string str);

   string Cifrado2(string cert, string pass, string str);

   string Descifrado(string cert, string pass, string str);

   string Descifrado2(string cert, string pass, string str);

   No se ha encontrado la manera de comunicar al servidor con esta DLL y obtener el acceso a las primitivas de la misma. También se ha intentado implementar el mismo mecanismo que el explicado en el ANEXO II.

5.2. Biometría

o Análisis de requisitos

Como se ha visto en el apartado de “Estado del Arte, Estudio de Alternativas”, en el espacio dedicado a la biometría, los sensores ópticos son los mecanismos de autenticación más extendidos para identificar una huella dactilar. El tutor del proyecto me facilitó el dispositivo biométrico BioShield, con el fin de realizar un estudio detallado, probando toda su funcionalidad. El BioShield es un dispositivo externo que se conecta al pc mediante puerto USB.

Ilustración 21. Biologon

El sensor óptico lleva instalado un software específico que le permite analizar un conjunto de puntos característicos, con ellos el software biométrico de huella digital genera un modelo en dos dimensiones, que se almacena en una base de datos, indicando además datos de la persona que ha sido objeto del estudio, un código de usuario por ejemplo. La ubicación de cada punto característico se representa mediante una combinación de números (x.y) dentro de un plano cartesiano, los cuales sirven como base para crear un conjunto de vectores que se obtienen al unir dichos puntos entre sí.

Para llevar a cabo el proceso inverso, la verificación dactilar, y así poder identificar a un usuario mediante su huella, se comparan estos mismos vectores, no la imagen en sí, para ello se utiliza un algoritmo que permite asociar la huella que se desea identificar con otras almacenadas en la base de datos.

Éste procedimiento lo vemos representado gráficamente con el siguiente conjunto de imágenes:




Ilustración 22 Ilustración 23 Ilustración 24 Ilustración 25

En este proceso, el dedo es leído por un lector de huellas (Ilustración 22), se codifica mediante los puntos característicos (Ilustración 23), entonces una plantilla matemática de vectores que unen los puntos característicos se genera (Ilustración 24), ésta

imagen se almacena y reconoce un conjunto de números que sólo podrán ser reconocidos en una plantilla (Ilustración 25), éstos son los vectores que usa el dispositivo para comparar con otros almacenados en la base de datos e identificar a un usuario concreto.

El lector óptico BioShield se ha instalado mediante un proceso relativamente sencillo. Estudiando sus manuales de uso se han conocido las diferentes funcionalidades que tiene el lector, éstas son:

- Identificar a un usuario en un ordenador que tiene varios usuarios registrados y, así, **iniciar la sesión** asociada a ese usuario.
- Identificar a un usuario con permisos para **abrir una aplicación** concreta, la cual se ha protegido con contraseña.
- Identificar a un usuario que tiene permisos para **abrir un documento** protegido con contraseña.

A continuación se muestra un ejemplo concreto de cada funcionalidad estudiada.

- Inicio de sesión

Para hacer esta prueba se crearon varios usuarios en el sistema operativo Windows, y posteriormente la cuenta a configurar fue protegida con contraseña.

Desde el Gestor de usuarios en “Seguridad de Biologon”, nos metemos a la cuenta que queremos modificar y entramos en la opción de “Cambiar las propiedades de Biometrics”.

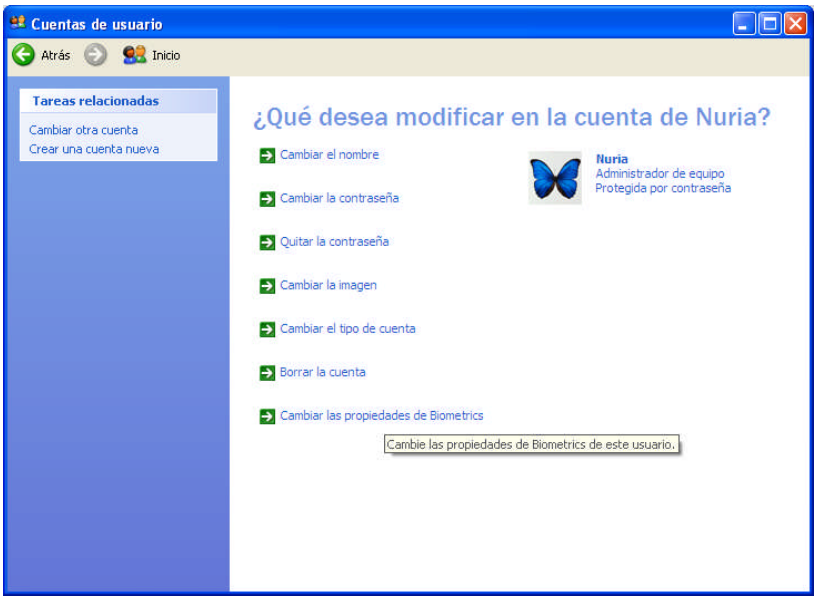


Ilustración 26

Sale un asistente de configuración de huella digital, elegimos la opción de contraseña o biometría. Registramos la huella digital, y la asociamos a la contraseña de usuario.

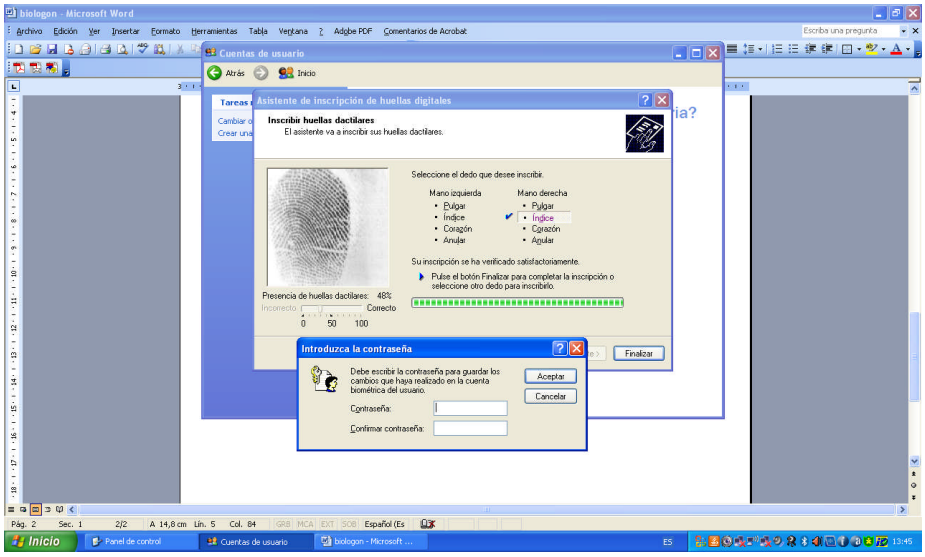


Ilustración 27

A partir de este momento, si queremos acceder a la cuenta que hemos configurado, podremos hacerlo introduciendo la huella, o metiendo la contraseña.

- Aplicación protegida

Las pruebas se han hecho con la aplicación Word.

Se crea un documento de Word, y de abre la aplicación de BioShield, nos muestra la siguiente barra de herramientas.

Ilustración 28

Tiene varias opciones, la que se ha de usar en este caso es la tercera, “Protección de aplicaciones”, se pincha sobre el icono, y se arrastra el ratón hasta el marco superior del documento WORD, entonces sale una ventana.

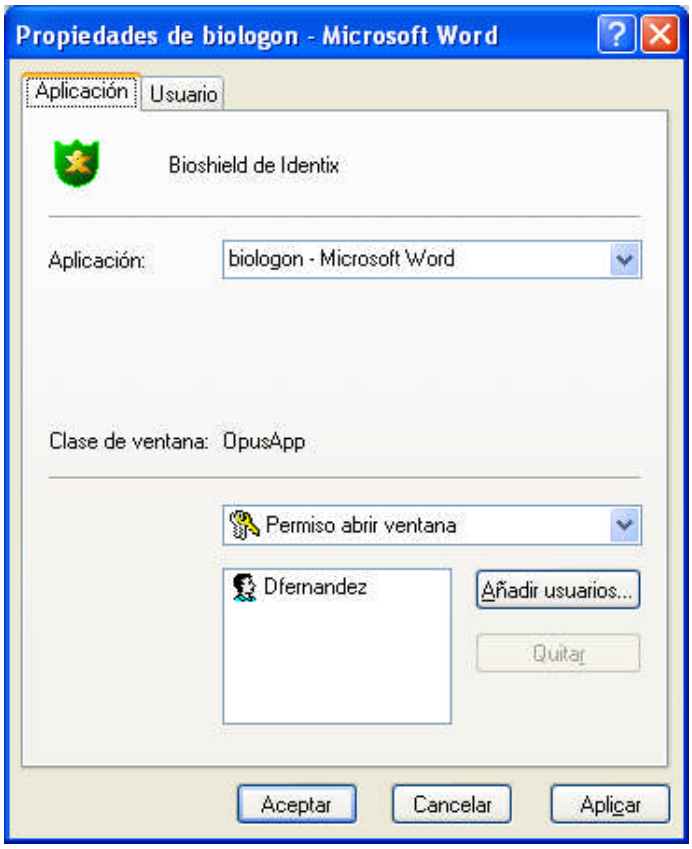


Ilustración 29

Se pueden añadir los usuarios que se quieran siempre y cuando estén ya registrados en el dispositivo Bioshield todos ellos podrán tener acceso a la aplicación.

A partir de este momento cuando se vuelva a abrir la aplicación protegida con la tecnología de Biologon, saldrá una ventana de acceso, pidiendo identificación y autenticación como uno de los usuarios registrados en el sistema para poder usar la aplicación.

Basta con poner la huella de uno de los usuarios registrados, y la aplicación se abrirá.

- Documento concreto protegido

Las pruebas se han hecho con un documento concreto creado desde la aplicación Excel.

Se crea un documento de Excel, y se protege para la apertura, con las opciones de seguridad que el propio office te proporciona:

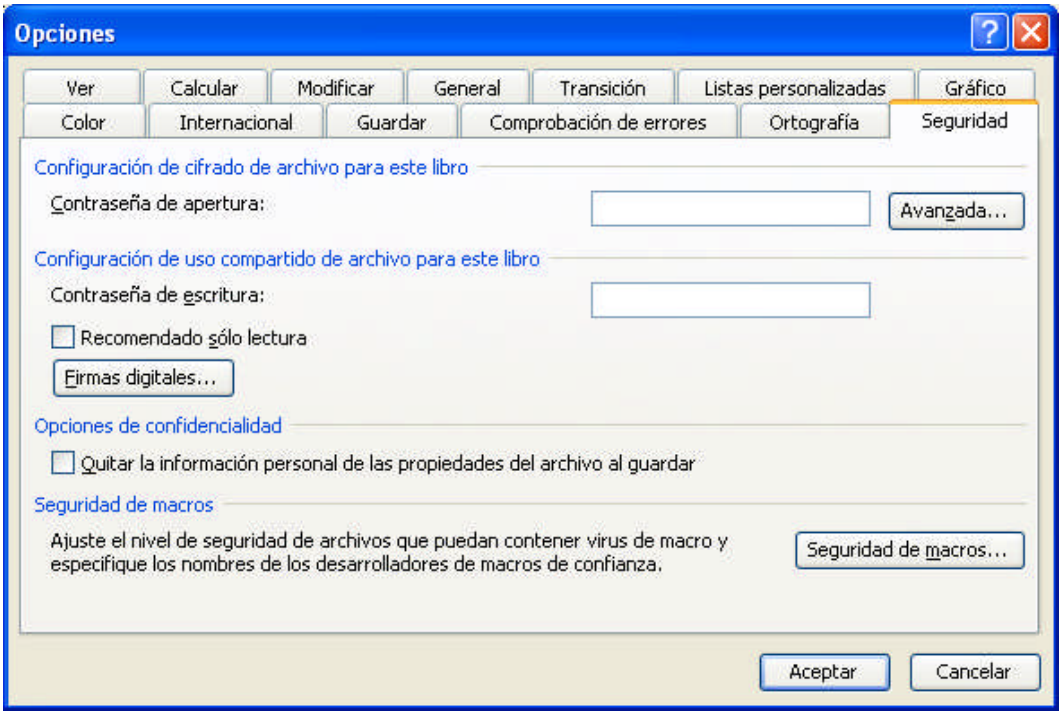


Ilustración 30

La contraseña de apertura debe ser la misma que una de las que tenga registrado el Biologon con un usuario. Al intentar abrir el documento de nuevo, cuando nos pida la contraseña de apertura, abrimos el BioShield.

Ilustración 28

De todas las herramientas que tenemos la que debemos usar en esta ocasión es la primera “Banco de contraseñas”, se pincha sobre el icono, y se arrastra el ratón hasta la ventana donde nos pide la contraseña. A partir de ahora, cuando queramos entrar, nos pedirá directamente la huella.

Ilustración 31

Si no diferenciamos usuario, y sólo hay uno por huella, al meter la huella directamente lo identificará, si hay más de un usuario por huella, nos pedirá que diferenciemos el usuario que queremos. Indistintamente, si la huella introducida es la que corresponde en el banco de contraseñas del Biologon a la contraseña del documento, éste se abrirá sin problemas.

- Otras utilidades del BioShield

Aún queda una funcionalidad más del BioShield por mostrar, es el "acelerador de acciones" (segundo botón del menú herramientas) funciona igual que el banco de contraseñas, pero esta vez lo que protege son distintas funciones dentro de una aplicación, si queremos proteger el menú herramientas, o el botón de imprimir… se realizará con esta opción.

- **Ventajas de la autenticación con un lector de huella óptico**

No te pueden suplantar. No hay que memorizar la contraseña asociada a un usuario, por lo que se pueden poner contraseñas muy complejas, y que el software del dispositivo la introduzca en el sistema al introducir el usuario su huella. Es por lo tanto más seguro que el mecanismo de autenticación de usuario-password en sí mismo.

- **Inconvenientes de la autenticación con un lector de huella óptico**

Al sufrir heridas, quemaduras en el dedo con el que se haya identificado al usuario en el software, la imagen de la huella se ve alterada y el sistema no lo reconoce aunque el usuario que pretende logarse sea quien dice ser.

6. Conclusiones y Trabajos Futuros

Se han cumplido los objetivos que se marcaron al inicio de este proyecto, el objetivo principal consistía en mejorar la seguridad en la autenticación del paciente al acceder al Hospital Virtual. Para mejorarla, se habían definido objetivos parciales que se han ido cumpliendo respectivamente. Se han analizado los diferentes mecanismos de autenticación, evaluando sus ventajas e inconvenientes, con la finalidad de poder determinar qué mecanismo o mecanismos podemos utilizar para mejorar la seguridad del Hospital Virtual.

Se han estudiado más en profundidad dos dispositivos que se han implementado y ambos tienen mecanismos muy diferentes a la hora de tratar el login de un usuario, uno de ellos pertenece al campo de la biometría, el BioShield, se trata de un lector óptico de huella digital y el otro es un token de seguridad, OTP810, que utiliza certificados digitales como base para identificar y autenticar un usuario en un sistema.

Después de analizar todos los mecanismos de autenticación existentes en el mercado, de haber tenido la oportunidad de analizar e implementar algunos de ellos con la finalidad de comprender su funcionamiento y determinar si comprendía un equilibrio entre funcionalidad, seguridad e integridad sin olvidarnos de factores claves como son la economía y la facilidad de uso, se pueden aconsejar cualquiera de los dos dispositivos implementados en este proyecto.

El lector óptico de huella digital hoy día es un método de autenticación muy fácil de instalar, sin elevar demasiado el coste que supondría el mantenimiento aunque limita al paciente al uso de un pc en el cual tenga instalado el lector.

El token eleva algo el precio y lleva un manual de instalación que quizá es algo más complicado. Además hay que crear los certificados para lo que el Hospital Clínic de Barcelona debería hacerse CA o encargarlos a la FNMT.

Como trabajos futuros se propone crear una base de datos para almacenar la relación entre usuario y certificado en vez de utilizar un fichero plano. Además se podría modificar el desarrollo para que el paciente se pudiera conectar al Hospital Virtual con cualquier navegador.

Se recomienda continuar con las tareas iniciadas en el apartado 5.1.2, para completar la autenticación del paciente al Hospital Virtual mediante certificados digitales instalados en el token.

También se plantea la ampliación del proyecto para que el servidor pueda leer todos los tipos de certificados.

Y se recomienda probar otros métodos de autenticación que se están extendiendo mucho últimamente, ya que éste es un campo que crece cada día, y se considera podrían ser una buena alternativa a implementar en el Hospital Virtual, como pueden ser los sms al móvil de un paciente indicándole un código de acceso temporal cada vez que intente conectarse al Hospital Virtual.

Por último, como trabajo futuro se plantea la puesta en marcha de lo estudiado en el Hospital Virtual, integrándolo por completo.

7. Bibliografía

[1] http://dspace.ups.edu.ec/ Capitulo 1 “Seguridad informática” Premisas básicas en seguridad

[2] S. Amador Donado, M.A. Niño Zambrano, A. Flechas. Seguridad computacional. Libro de consulta para administradores y usuarios. Primera Edición http://www.govannom.org/seguridad/seg_general/seg_com.pdf. (Capitulo 5 introducción a la criptografía para RSA y DES)

[3] http://www.monografias.com/ Seguridad en desarrollo sobre aplicaciones web

[4] http://www.linux-party.com/ Artículo: Seguridad de aplicaciones web: Pruebas de vulnerabilidades

[5] León A, Cáceres C, Fernández E, Chausa P and Martin M, *A New Multidisciplinary Home Care Telemedicine System to Monitor Stable Chronic Human Immunodeficiency Virus-Infected.* Revista: PLoS ONE. **Índice de Impacto (JCR): 4,351 (2009).** Año 2011

[6] P. Chausa Fernández, C. Cáceres Taladriz, F.J. García Peces, Hospital Virtual: Sistema de información clínica y telecuidado de pacientes VIH/SIDA basado en tecnologías web 2.0. Congreso: XXVIII Congreso Anual de la Sociedad Española de Ingeniería Biomédica (CASEIB 2010). Madrid, 2010.

[7] Caceres C, Sistema de telemedicina para la atención a pacientes con VIH/SIDA en su domicilio. Revista: JANO Medicina y Humanidades. Madrid, 2008.

[8] http://www.acertasoftware.com/mspiral.html

[9] http://www.kimaldi.com/sectores/geriatricos_y_centros_sanitarios/accesos_a_hospitales

[10] http://www.videos-it.com/videos/469/biometria/uso-de-biometria-para-identificacion-de-pacientes-a-traves-del-iris-en-centros-medicos-de-nueva-york/biometria

[11] http://www.sintel.com.mx/Hospitales.html

[12] http://www.sistemasbiometricos.cl/WEB/2011/05/22/gobierno-argentino-estudia-la-biometria/

[13] http://convergenciadigital.com/

[14] http://www.terra.es “Biometría en la palma de la mano”

[15] http://dotnetslackers.com/articles/csharp/WritingAnActiveXControlInCSharp.aspx

[16] https://zonatic.usatudni.es/es/aprendizaje/aprende-sobre-el-dnie/57-aspectos-tecnicos/208-sistemas-actuales-de-autenticacion-y-firma.html

[17] http://www.20minutos.es/noticia/245928

[18] www.sistemasbiometricos.cl artículo: se estudian nuevos métodos de biometría

[19] http://www.elnuevodia.com/huelladigitalparapagarlascompras-1295468.html

[20] TECNOLOGÍAS BIOMÉTRICAS APLICADAS A LA SEGURIDAD Tapiador Mateos, Merino; Sigüenza, Juan A., (aut.) Ra-Ma, Librería y Editorial Microinformática

[21] Sánchez-Reillo, R., Sánchez-Avila, C. and González-Marcos, A. (2000) "Biometric Identification through Hand Geometry Measurements", IEEE Trans. On Pattern Analysis and Machine Intelligence, 22(10), pp. 1168-1171.

[22] http://www.xatakaciencia.com

[23] http://www.disbio.com

[24] http://es.wikipedia.org/

[25] http://www.monografias.com/trabajos11/crida/crida.shtml

[26] http://arantxa.ii.uam.es/~jortega/RecHuella_ASAL.pdf

[27] Harry Soderman y John O'Connell. "Métodos Modernos de Investigación Policíaca"

[28] http://www.cea-ifac.es. Prototipo biométrico de manos basado en su disposición natural. Antonio Adán, Andrés S Vazquez, Fernando Molina y Gloria Bueno

[29] http://info4.juridicas.unam.mx/ijure/fed/1/1848.htm?s=

[30] http://www.aplicacionestecnologicas.com/Biometria/Huella_Digital/index.html

[31] http://snooecuador.com/ Articulo biometría ocular de 24 de Agosto de 2010

[32] http://www.sistemasbiometricos.cl. Artículo Eye Lock:Seguridad para su PC por USB

[33] Ecografia y biometría ocular, cap 11: Talevi, Tallano. 2007 primera edición

[34] http://www.sistemasbiometricos.cl articulo Militares emplearon biometría para confirmar la identidad de Bin Laden del 10 de Mayo.

[35] http://www.frav.es/pdf/2009/opa2009.pdf

[36] http://www.sistemasbiometricos.cl. Artículo: Android con Biometría facial

[37] http://www.sistemasbiometricos.cl. Artículo: RecognizeMe, reconocimiento facial para el iPhone

[38] http://www.sistemasbiometricos.cl. Artículo: Australia, inicia piloto con Biometría Facial para vigilancia.

[39] Sánchez-Reillo, R., Sánchez-Avila, C. and González-Marcos, A. (2000) "Biometric Identification through Hand Geometry: Measurements", IEEE Trans. On Pattern Analysis and Machine Intelligence, VOL. 22 No10

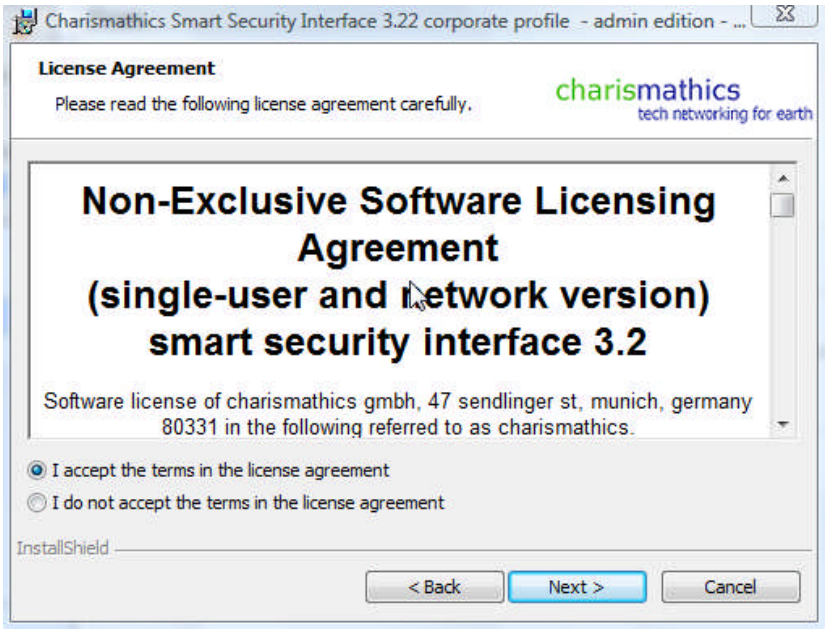
[40] http://www.abox.com/productos.asp?pid=156

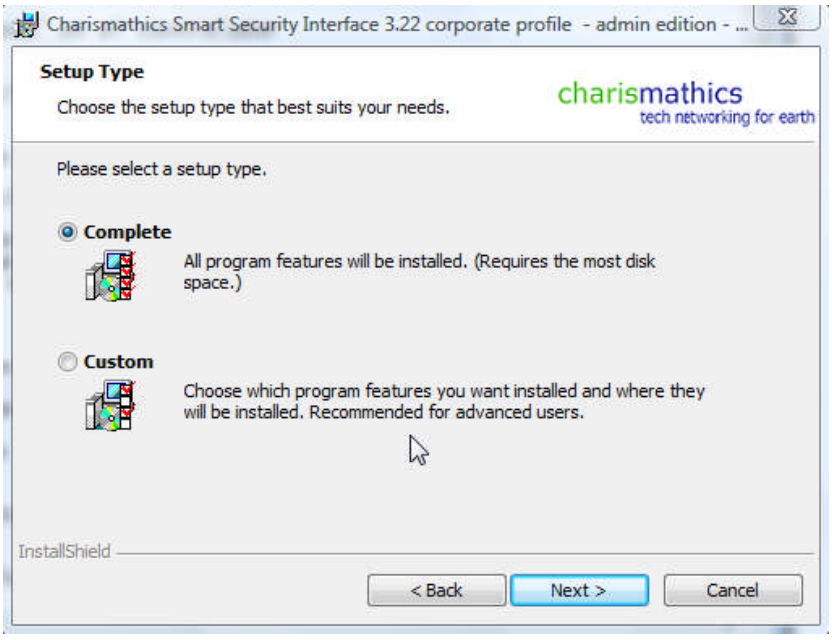
[41] http://www.trazablog.com/?p=208

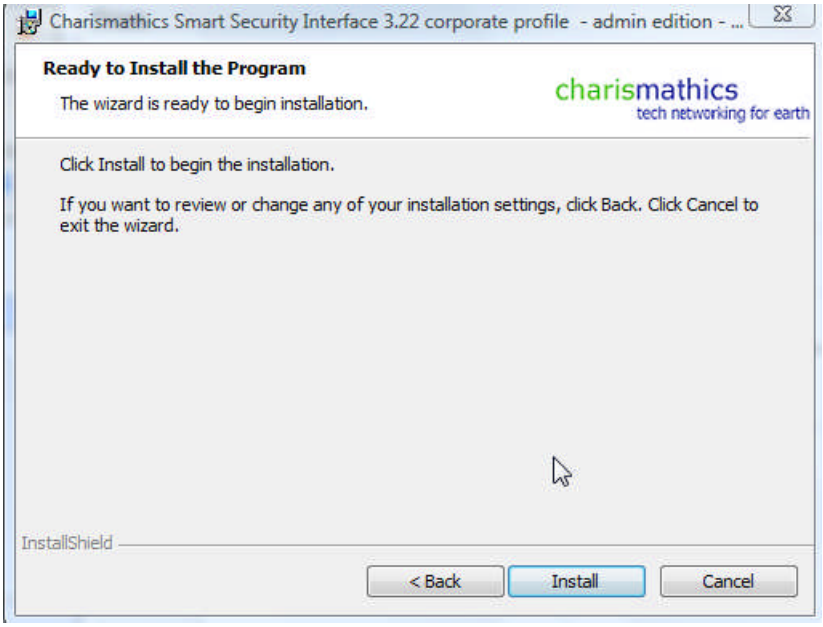
Anexo I

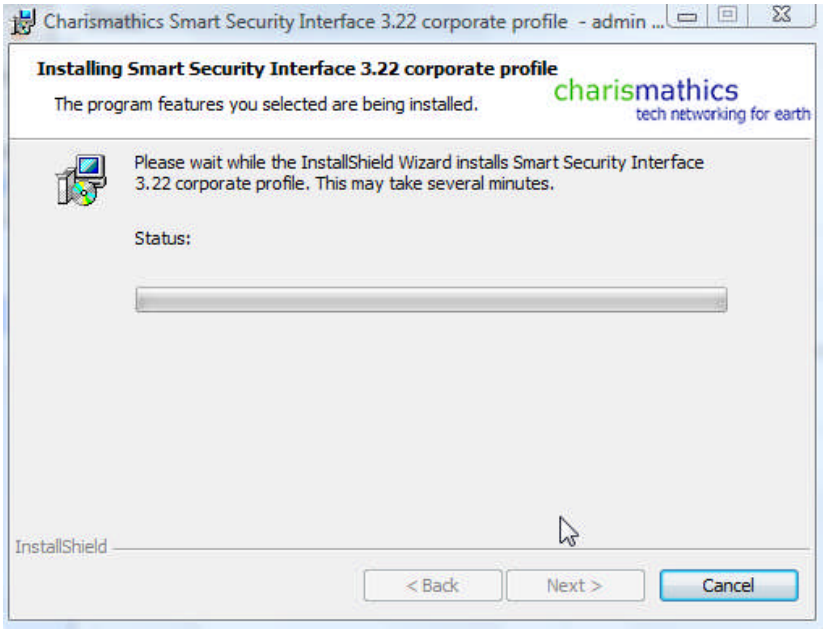
Instalación del Vasco Digipass

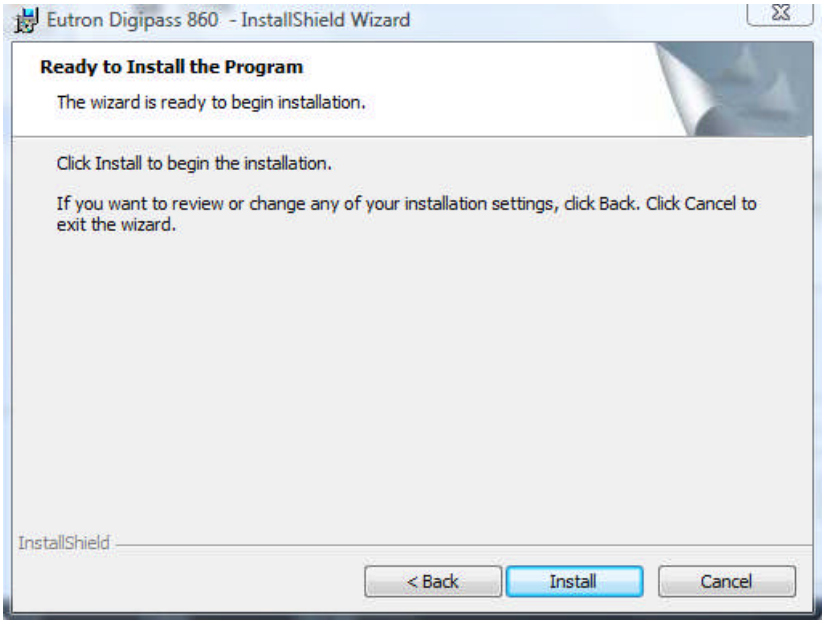
La instalación del dispositivo consta de los siguientes pasos:

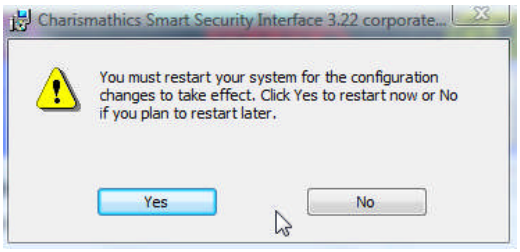




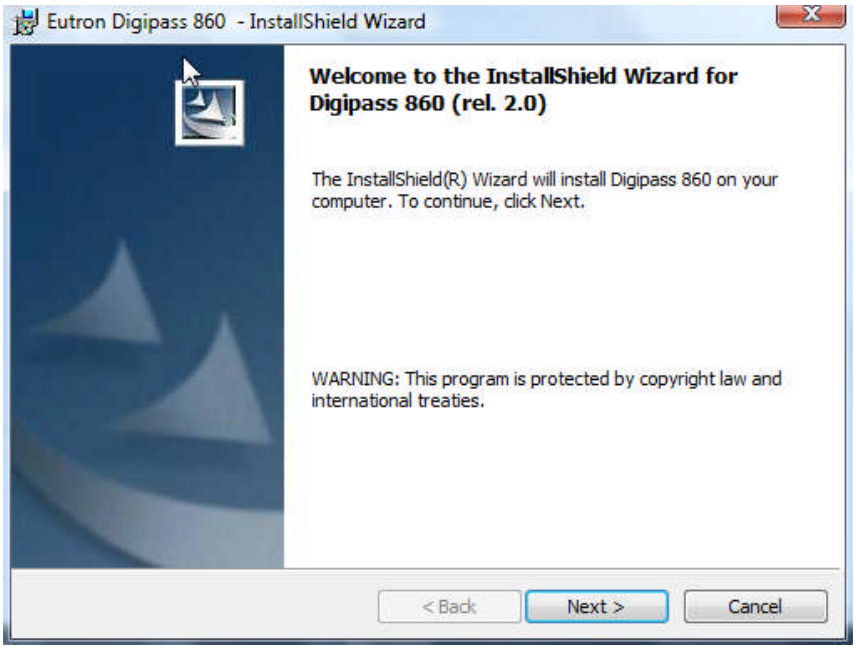

Charismathics Smart Security Interface 3.22 corporate profile - admin edition - ...
Ready to Install the Program
The wizard is ready to begin installation.
charismathics
tech networking for earth
Click Install to begin the installation.
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
InstallShield
< Back
Install
Cancel

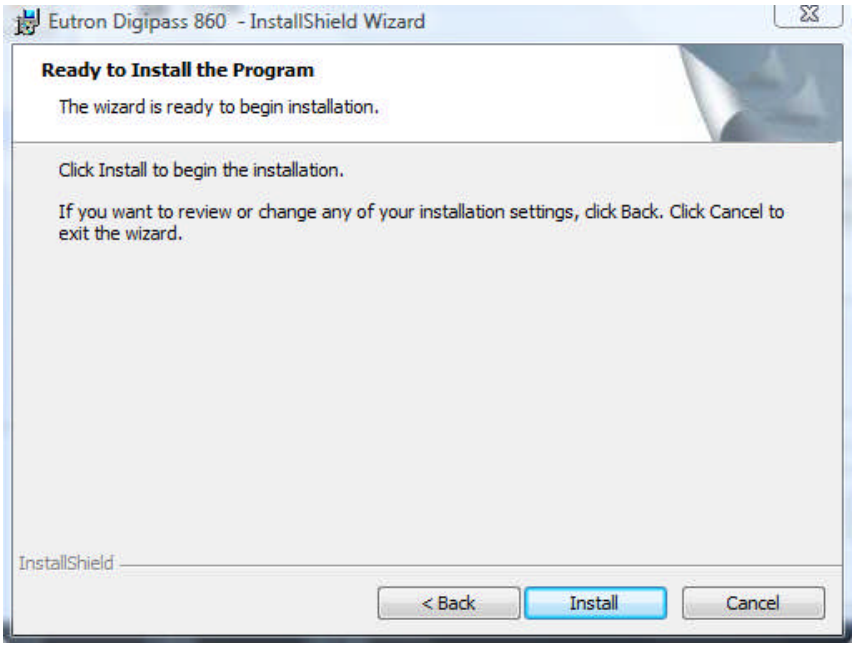

Charismathics Smart Security Interface 3.22 corporate profile - admin ...
Installing Smart Security Interface 3.22 corporate profile
The program features you selected are being installed.
charismathics
tech networking for earth
Please wait while the InstallShield Wizard installs Smart Security Interface 3.22 corporate profile. This may take several minutes.
Status:
InstallShield
< Back
Next >
Cancel

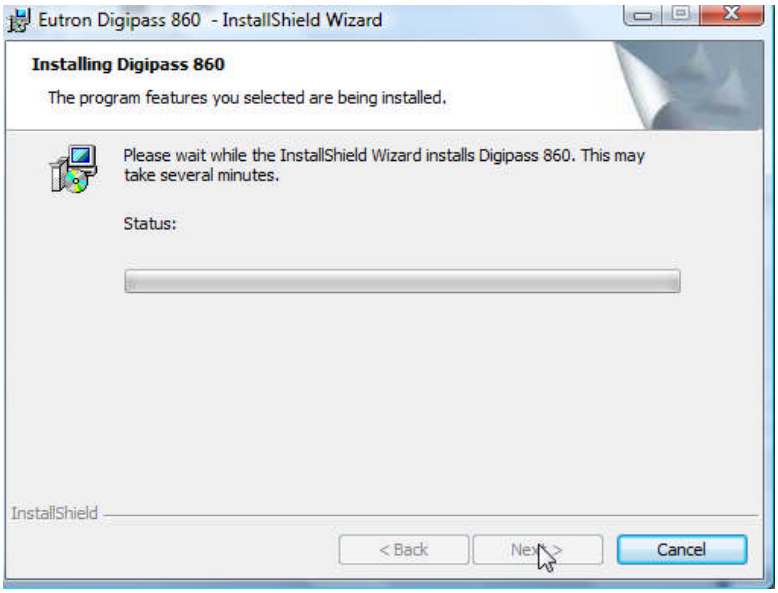


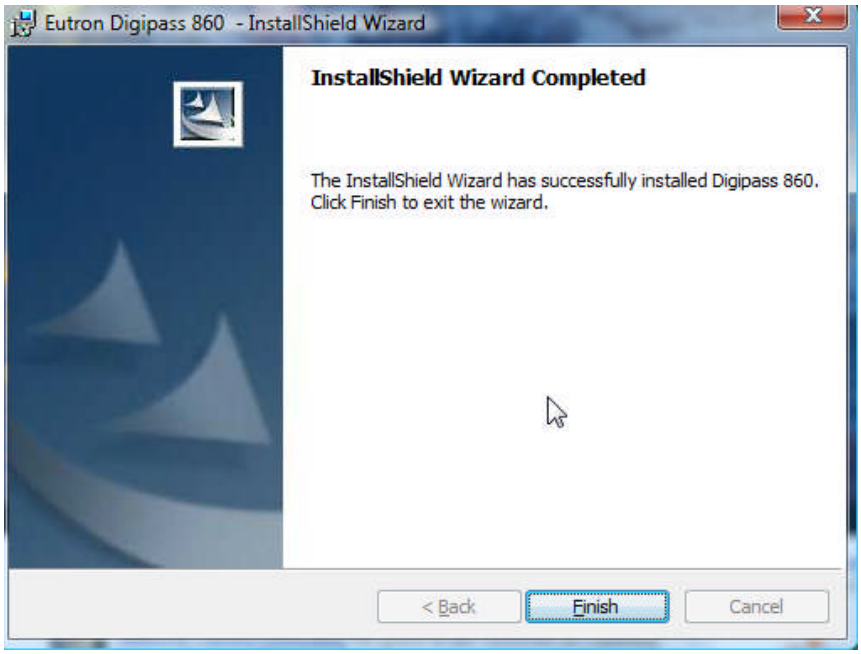


Se reinicia el equipo y se continúa con la instalación:


Eutron Digipass 860 - InstallShield Wizard
Welcome to the InstallShield Wizard for Digipass 860 (rel. 2.0)
The InstallShield(R) Wizard will install Digipass 860 on your computer. To continue, click Next.
WARNING: This program is protected by copyright law and international treaties.
< Back
Next >
Cancel


Eutron Digipass 860 - InstallShield Wizard
Ready to Install the Program
The wizard is ready to begin installation.
Click Install to begin the installation.
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
InstallShield
< Back
Install
Cancel





Finalizado el proceso de instalación, en el escritorio encontraremos el icono de acceso al token:

Anexo II

Cifrado y descifrado de datos mediante una API

Buscando información de las APIs que el propio token podría facilitarnos encontramos unas librerías (.DLL) que ya tenía implementadas OTP para el manejo y uso de su token. La gran dificultad nos la encontramos en este punto, a la hora de usar estas librerías, puesto que no sabíamos los procedimientos o funciones que debíamos usar en cada caso ni como acceder a ellas. Usamos documentación funcional del PKCS#11 para explotar el manejo de la DLL que finalmente utilizamos.

Se creó una API para poder realizar las llamadas a las funciones implementadas dentro de la DLL.

A continuación, vamos a ver unos ejemplos de algunas de las funciones que se han definido en la API para el cifrado y descifrado, explicando su estructura dentro de la misma.

- Función que determina si hay un token conectado a un puerto USB del pc, e identificar dónde esta el token, y si hay mas de uno el número de ellos.

Definición de tipos:

```
typedef UINT (CALLBACK* LPFNDLLFUNC2)
(CK_BBOOL,          /* only slots with tokens? */
 CK_SLOT_ID_PTR,    /* receives array of slot IDs */
 CK_ULONG_PTR);     /* receives number of slots */
```

Variable de tipo tipo función de la función:

```
LPFNDLLFUNC2 lpfnDLLFunc2;    // GetSlotList
```

Comando para el precompilador:

```
lpfnDLLFunc2 = (LPFNDLLFUNC2)GetProcAddress(hDLL, "C_GetSlotList");
```

- Función para cifrado de datos.

Definición de tipos:

typedef CK_RV (CALLBACK LPFNDLLFUNC21)(CK_SESSION_HANDLE, CK_BYTE_PTR,CK_ULONG,CK_BYTE_PTR,CK_ULONG_PTR);*

Estos tipos se corresponden con:

CK_SESSION_HANDLE - Identificador de session
CK_BYTE_PTR - Texto a encriptar
CK_ULONG - Longitud de los datos
CK_BYTE_PTR - Texto encriptado
CK_ULONG_PTR - Longitud del texto encriptado

Variable de tipo tipo función:

LPFNDLLFUNC21 lpfnDLLFunc21; // Cifrado de datos

El comando para el precompilador, vincula la llamada con la función dentro de la DLL.

lpfnDLLFunc21 = (LPFNDLLFUNC21)GetProcAddress(hDLL, "C_Encrypt");

En este momento tenemos definidas las funciones para poder utilizarlas desde el programa principal. Para poder usarlas tienen que ser preprocesadas.

El programa comienza después de que se han cargado todas las funciones que vamos a usar en él y que tenemos disponibles en la DLL. Lo primero que hay que hacer es cargar la DLL.

hDLL = LoadLibrary("C:/temp/cmP11.DLL");

Lo siguiente es comprobar si existe un token pinchado en el pc, la llamada a la función es la siguiente, (Esta función corresponde con el primer ejemplo mostrado).

uReturnVal = lpfnDLLFunc2(CK_FALSE, pSlotList, &v_nslots);

Después de comprobar que tenemos un token pinchado, y dónde se encuentra, se abre una sesión con ese token. Hacemos un login al token con usuario y pin. Si existe conexión, se genera una clave de sesión con un objeto de tipo clave. Con esa clave de sesión se inicializa el mecanismo de cifrado.

Se pide por pantalla un texto a cifrar, el cual se almacena y se cifra con la función mostrada como segundo ejemplo. En paralelo se inicializa el mecanismo de descifrado y ese mismo texto que ya está cifrado entra a la función de descifrado como parámetro de entrada para ser procesado y descifrado. El resultado es el mensaje en claro que inicialmente se introdujo por pantalla.

De este modo se comprobó que funcionaban correctamente las funciones de cifrado y descifrado de la DLL.

Para finalizar el programa se libera sesión, el slot donde esta pinchado el token, y finalizamos los procesos de cifrado y descifrado, además hay que señalar que en todo momento introdujimos un control de errores para optimizar el programa.