Proceso de registro e identificación sin control automático para la Universidad Nacional de Río Negro

Lugani, Carlos Fabián

Universidad Nacional de Río Negro, Sede Atlántica
Laboratorio de Informática Aplicada
clugani@unrn.edu.ar
Buerk@Springer.de

Resumen. Este trabajo describe un proceso de identificación de personas en el que en una primera etapa se realiza una autenticación en una aplicación que da como resultado una clave que es usada para registrar la identidad en un sistema, conversación, videoconferencia, plataforma, etc. Se plantea este proceso como sin comprobación en el momento de realizarse la acción de la persona y sólo de registro. El proceso ha sido diseñado para permitir la verificación de la identidad de la persona en cualquier momento posterior, brindando seguridad en la comprobación de la identidad, mediante un sistema de claves e instalación de aplicaciones en ambas partes. El sistema registra fecha y hora de la validación y funciona mediante la sincronización de las aplicaciones que intercambian registros unicamente en la instalación original de la aplicación en el cliente/persona.

Palabras clave: Blockchain, gestión de identidades, identidad digital

1 Introducción

La identidad digital es creada por una persona y es utilizada cuando se encuentra en el ciberespacio o también se puede describir como la forma en que la persona se identifica con aplicaciones o sistemas en donde le interesa que esos mismos sistemas validen que se trate de esa persona. [1] Por esto mismo, de acuerdo al tipo de sistema y el valor de las acciones que realizará el usuario en el mismo, la autenticación será mas o menos fuerte y por lo consiguiente mas o menos vulnerable. Se menciona que también pueden existir casos en donde no se puede comprobar si una persona estaba conectada, a pesar de haberlo hecho, ya que no quedan registros del suceso.

En un mundo no digital, la existencia física del documento nacional de identidad es utilizada para identificar a una persona, cuenta con parámetros propios de seguridad creados para este fin, siendo el principal factor de inviolabilidad, la falta de medios para reproducir el mismo en forma original.

Mientras que la identidad digital se compone de varios elementos como ser: nombre de un dominio de Internet, incluyendo distintos usuarios que son utilizados por una persona en redes sociales, juegos, dominios Web o sitios en los que participa, es socio o miembro, contraseñas, dirección de correo electrónico y otros factores

personales. [2] Este conjunto de publicaciones y registros en aplicaciones en las que previamente el usuario se ha registrado dan lugar a la identidad que el individuo ha definido.

Al utilizar aplicaciones informáticas, estas deben tener la funcionalidad de reconocer a los usuarios que deseen realizar acciones en la misma, normalmente este tipo de ingreso o "login" ya está determinado por la aplicación. Aun así existen casos de aplicaciones como las videoconferencias, participación en foros, servicios o aplicaciones de mensajería, archivos o documentos en formato digital; en los que no se realiza una validación de los usuarios por carecer las aplicaciones de un sistema de autenticación.

Es para estos casos en que se desea realizar una verificación de las personas, pudiendo realizar en forma posterior dicha validación de identidad y no teniendo los medios para modificar las aplicaciones que se utilizan; que se plantea este trabajo, el cual describe el proceso y los elementos que se tendrán en cuenta para su construcción.

Se evaluó como alternativa la utilización de Blockchain [3] y contratos inteligentes (Smart Contracts) para realizar la autenticación mediante certificados, pero se considera que adoptar esta metodología requeriría grandes recursos de procesamiento, establecimiento en la Universidad de una plataforma de Gestión de Identidad Digital Descentralizada (SSI) y el proceso que se presenta en este trabajo es seguro, simple y sin requerimientos de procesos o entidades intermedias especiales.

En adelante se utilizará el termino de usuarios, indicando que se refiere a los alumnos de la Universidad, así como docentes y no docentes, que utilizan los sistemas o aplicaciones tanto para realizar todo tipo de gestión como la relacionada con la cursada, inscripción a las asignaturas, utilización de la plataforma bimodal (Moodle), participación en videoconferencias, foros, redes sociales de la Universidad, etc.

1.1 Antecedente

A la fecha, existen planes de identificación de estudiantes, en el año 2021 el Consejo Interuniversitario Nacional (CIN) y el Ministerio de Educación y del Interior firmaron un convenio para implementar un software para posibilitar la garantía de identidad de los estudiantes al momento de ser evaluados a distancia en el contexto del aislamiento social por la emergencia sanitaria. El sistema se implementaría en el SIU-Quechua y permitiría la identificación de los estudiantes mediante una foto con la cual el sistema haría una consulta con el sistema del Registro Nacional de las Personas (RENAPER) lo que validaría la identidad. [4]

Se tiene en cuenta que el sistema anteriormente descrito puede ser adecuado, pero el mismo no plantea alternativas de identificación en casos de no contar las aplicaciones que se utilicen con la interfaz necesaria para realizar las comprobaciones necesarias de forma automática y en línea con los sistemas necesarios.

Este trabajo no pretende reemplazar al sistema mencionado anteriormente que se encuentra en etapa de desarrollo, sino que plantea un sistema que utiliza otras herramientas para la identificación y que puede ser una opción para un sistema que no

brinde todas las formas de identificación ante todas las circunstancias que se presenten con los alumnos o personal, así como los sistemas o procesos que requiere la Universidad Nacional de Río Negro. Por lo tanto, este trabajo pretende brindar una alternativa a un sistema en línea, siendo las características principales del presente: un sistema manual, no en línea, no automático y sin interfaz con otros sistemas.

2 Elementos del proceso

Normalmente los sistemas de gestión de identidades son utilizados por los proveedores de servicios o aplicaciones para identificar a los usuarios de los mismos en forma automática y en línea. Pero si esto no es posible, ya sea porque las aplicaciones no soportan el proceso de autenticación necesario o debería ser desarrollado un software para actuar en el proceso de acceso a la aplicación (comúnmente denominado proceso de login) y que luego interactúe con la misma aplicación para dejar registradas las acciones de los usuarios. Todo lo anterior es factible siempre que se cuente con los recursos para el desarrollo de una aplicación específica que se conecte con cada aplicación o plataforma que se desee utilizar.

En la solución que se propone, al plantear que la verificación de la identidad del usuario se puede realizar en forma posterior y no en forma automática, no es necesario desarrollar interfaz o procesos para cada aplicación a utilizar, sino incorporar un proceso manual a cualquier aplicación o plataforma, los que registrarán los principios de la identificación de usuarios propuestos.

2.1 Estructura del sistema

Se presenta el proceso de gestión de identidad que será desarrollado para la autenticación de los usuarios en la Universidad Nacional de Río Negro. Los principales aspectos que se desarrollan son los siguientes:

- El proceso gestiona la identidad de las personas con un Código (para facilitar la referencia al código que entregará la aplicación con la que un usuario es identificado se utilizará la palabra “Token” en lo sucesivo).
- Los usuarios que ingresen a una plataforma de aprendizaje, videoconferencia, etc. y en donde se requiera ser validado mediante este proceso, deberán tener una aplicación en sus celulares que les entregará un Token, el cual escribirán en la aplicación o sistema en que se encuentren participando.
- El código quedará escrito para que luego se valide, no es la intención de este proceso la validación automática, si bien puede ser realizada con los mecanismos propuestos.
- La Universidad posee la aplicación que validará la identidad de la persona, por lo que centraliza tanto la gestión de los usuarios manteniendo los registros de identidad, como la validación de los Tokens/usuarios.

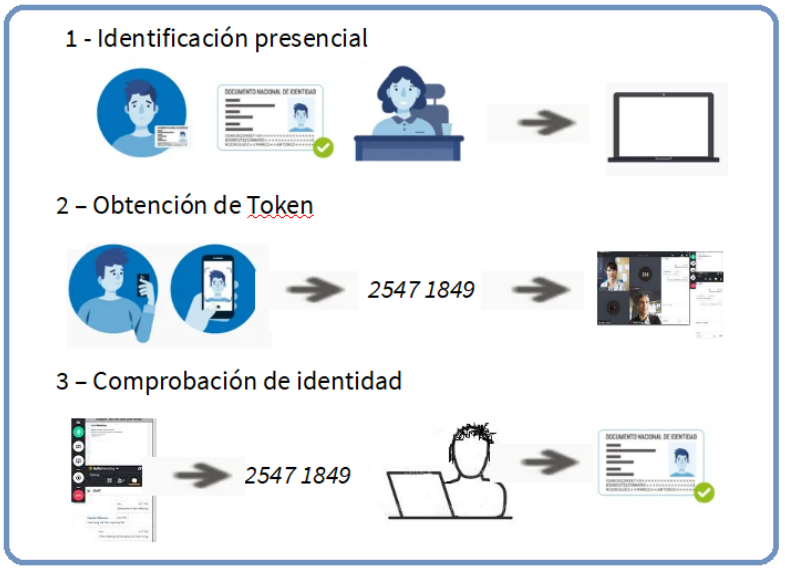
2.2 Esquema general

A forma de ejemplo, esta aplicación puede responder la siguiente situación:

Registro de fecha 19/7/2022
[Javier Grazzia
8:51
Buenos días. Aprobado 9361 8459]

Datos a ingresar en la aplicación: 19/7/2022 8:51 Javier Grazzia 9361 8459
Salida de la aplicación de validación: Verificado / No verificado
---

Se presenta en la Fig. 1 la forma esquemática el proceso de verificación



2.3 Aplicación móvil

La primer acción que realiza el usuario consiste en la verificación de la identidad en forma presencial. Una vez cargado los datos en el sistema y comprobada la identidad de la persona, se le brindará un código de acceso por única vez que sirve para la instalación de la aplicación móvil.

La aplicación se instala en el teléfono celular del usuario, se utiliza el código entregado y descrito anteriormente y requiere autenticación fuerte para habilitar la

entrega del Token. Al habilitar el nuevo usuario se produce un intercambio de contraseñas entre la aplicación central y la aplicación de usuario que es propia de esa la instalación y que es utilizada luego en el algoritmo del código. Entendiendo por autenticación fuerte, la huella dactilar para activar la aplicación o el reconocimiento facial. Se destaca que es necesaria esta autenticación biométrica ya que es considerada la más adecuada y segura para la identificación inequívoca del usuario. [5] [6] Luego de la autenticación, la aplicación entrega un Token que consiste en un numero de 8 cifras que es utilizado por la persona para copiar en forma manual en la aplicación o plataforma en que se encuentra participando.

2.4 Generación del Token

Las características del Token a generar son: número de 8 cifras, el cual es un resultado de un algoritmo, debido a que el tiempo es una variable de entrada del algoritmo, el Token cambia cada minuto (cambiando la entrada del tiempo en minutos) y por lo tanto no se repite la secuencia ya que es producto de un cálculo matemático. Lo que resulta en que el numero de ocho cifras está asociado a tres elementos:

- tiempo (día, hora, minuto)
- usuario
- clave del sistema generada en la instalación de la aplicación del usuario

El algoritmo tiene la capacidad de generar un Token a partir de los tres elementos mencionados, por lo tanto en la comprobación de identidad la aplicación centralizada tiene la capacidad de ingresar los mismos tres elementos y comparar el Token generado, si el mismo es igual, se dá por verificada la identidad. Asimismo, en caso que exista una diferencia, que podría deberse a la tardanza en que el usuario escribe el código, la aplicación central también puede calcular el Token anterior y si se comprueba que es correcto también verificar como correcto.

2.5 Aplicación de validación

La aplicación que gestiona la verificación de los Tokens e identidad de las personas es diseñada como una interfaz de usuario de simple uso soportada en una plataforma Web, la interacción con los usuarios está dada por las siguientes acciones:

- Ingreso de un nuevo usuario con datos validados por una persona que comprueba la identidad de la otra persona. Esta será la única interacción personal con el sistema que se planea.
- Ingreso de un Token y datos para la verificación de la persona por parte del personal habilitado a la aplicación de validación.

3 Conclusión

Con este trabajo se intenta brindar una herramienta que pueda solucionar la identificación de usuarios para situaciones específicas en donde no se pueden verificar los mismos en el momento de su participación y que se pueda hacerlo en forma posterior con un nivel de seguridad adecuado. Se tuvieron en cuenta las siguientes premisas:

- Oportunidad: se ha detectado el problema de la verificación de usuarios y si bien existen soluciones para procesos de autenticación en línea, no se han presentado soluciones para la autenticación y verificación no es línea mediante un método simple como del descrito, siendo este proceso una alternativa que soluciona este aspecto.
- Solución: el proceso se considera factible de realizar y se comenzará a desarrollar la aplicación, el nivel de complejidad no es alto y por lo tanto con normales requerimientos de hardware, software, comunicaciones y almacenamiento.
- Innovación: si bien el proceso en sí no es innovador, si lo es la utilización de un código que surge de un algoritmo cuyos ingresos son el tiempo y el usuario, además de contraseñas similares a una infraestructura de claves. Lo cual brinda seguridad en la comprobación ya que se realiza una autenticación biométrica y en especial lo inédito es la capacidad de realizar la verificación en forma posterior en el tiempo, sin importar cuando tiempo haya pasado y sin sobrecargar bases de datos con registros de Tokens.
- Beneficiarios y factibilidad de reproducción: este trabajo se presenta para solucionar un requerimiento de verificación real, se desarrollará y en un futuro trabajo se presentarán los resultados de la implementación en la Universidad Nacional de Río Negro, la reproducción de este proceso es de transferencia simple con las pautas presentadas, por lo mismo se destaca la facilidad con la que este proceso se puede reproducir en otras organizaciones.

Referencias

1. Clare Sullivan, Digital citizenship and the right to digital identity under international law, Computer Law & Security Review, Volume 32, Issue 3 (2016) 474-481, ISSN 0267-3649, https://doi.org/10.1016/j.clsr.2016.02.001.
2. Vidal Martínez, A. A., y Camarena Gómez, B. O. (2015). Evolución y análisis de una experiencia de utilización de videoconferencia de sala y de escritorio. Píxel-Bit, Revista de Medios y Educación, (47), 59-71.
3. Martínez, Marcos Gestión de Identidad Digital Descaentralizada (SSI) con Blockchain Recuperado de http://bibliotecadigital.econ.uba.ar/download/tpos/1502-1906_MartinezMH.pdf [Consultado 2 Jun. 2022]

4. CIN Consejo Interuniversitario Nacional. (2021) Recuperado de https://www.cin.edu.ar/siu-quechua-para-la-identificacion-digital-de-estudiantes-de-instituciones-universitarias-publicas/ [Consultado 2 Jun. 2022]
5. Alvez, C. E., Benedetto, M. G., Etchart, G. R., Luna, L. J., Leal, C. R., Fernández, M. A. Loggio, S. R. (2014). PID 7035 Identificación de personas mediante Sistemas Biométricos. Estudio de factibilidad y su implementación en organismos estatales. Ciencia, Docencia y Tecnología Suplemento, 4 (2014) Recuperado de https://pcient.uner.edu.ar/index.php/Scdyt/article/view/7 [Consultado 2 Jun. 2022]
6. Gámez, F. D. G., y Agapito, J. B. Autenticación facial como soporte extra en los entornos virtuales de aprendizaje para evitar el fraude académico. Revista Tecnología, Ciencia y Educación. (2016) Recuperado de https://www.revistasocitec.org/index.php/TCE/article/view/[Consultado 2 Jun. 2022]