Modelo de Identidad Digital para la Administración Pública

Registro Nacional de Identificación y Estado Civil
Gerencia de Registros de Certificación Digital
Sub-Gerencia de Certificación e Identidad Digital

Julio del 2017

The Internet was designed to connect machines, not people [sovrin.org]

El RENIEC

Organismo público constitucionalmente autónomo. Creado por Ley N° 26497 del 12JUL1995.

1. REGISTRO ÚNICO DE IDENTIDAD

Mantener actualizado el Registro Único de Identidad.

2. REGISTROS CIVILES

Registrar nacimientos, matrimonios, divorcios y defunciones.

3. REGISTRO ELECTORAL

Elaborar el Padrón Electoral y Verificación Domiciliaria

4. REGISTRO DE CERTIFICACIÓN DIGITAL

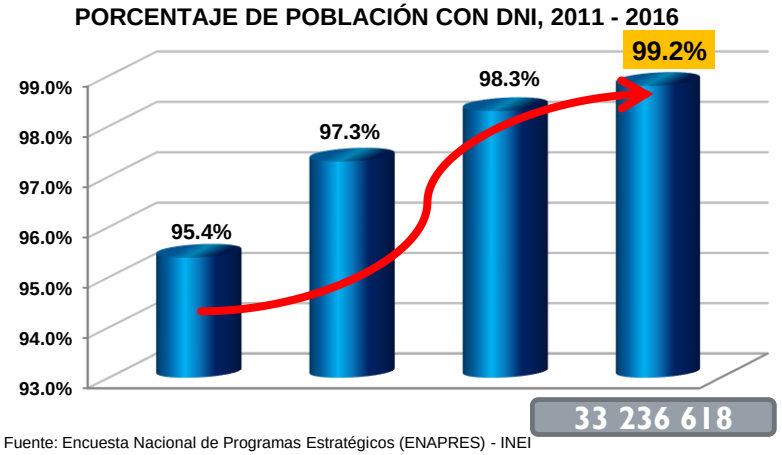
Emitir certificados digitales a personas naturales y jurídicas (Ley N° 27269, D.S. N° 052-2008-PCM)

5. REGISTRO DE VINCULADOS

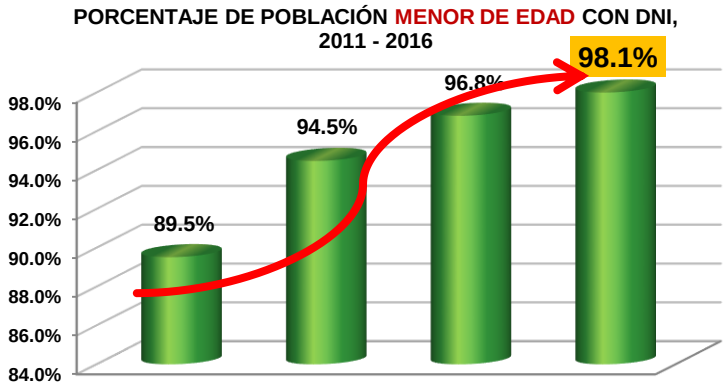
Establecer vínculos de parentesco y demás vinculaciones derivadas de las inscripciones (D.L. 1279. 27DIC2016)

El RENIEC

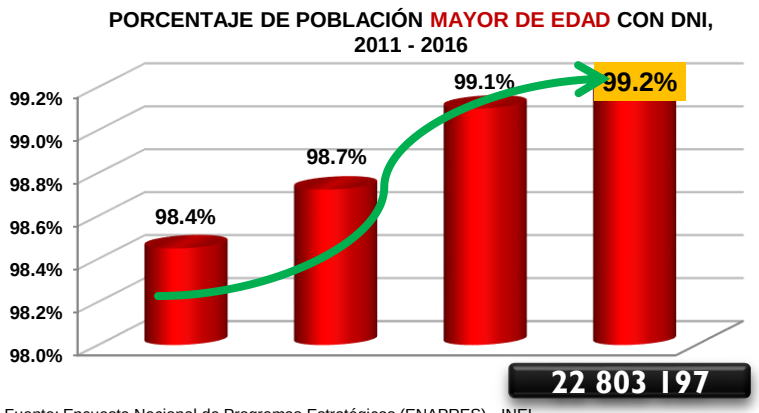
El Perú es un **país desarrollado** en materia de Identidad, alcanzando el **99%** de su población identificada



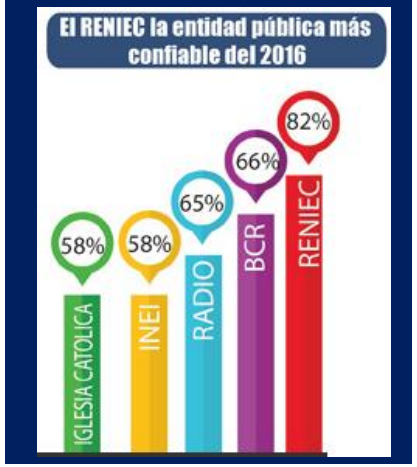
Fuente: Encuesta Nacional de Programas Estratégicos (ENAPRES) - INEI
Elaboración: Sub Gerencia de Estadística



Fuente: Encuesta Nacional de Programas Estratégicos (ENAPRES) - INEI



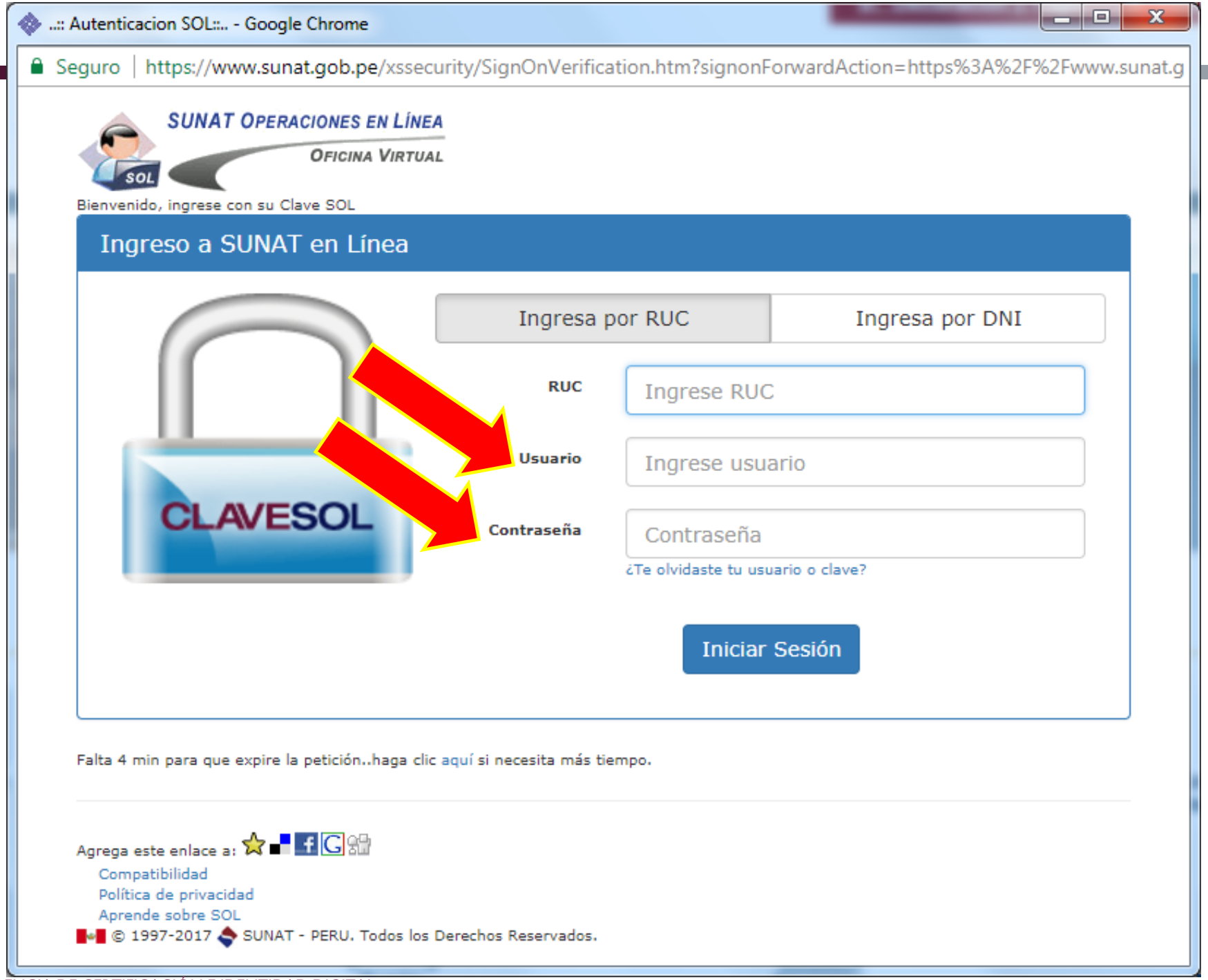
Fuente: Encuesta Nacional de Programas Estratégicos (ENAPRES) - INEI
Elaboración: Sub Gerencia de Estadística

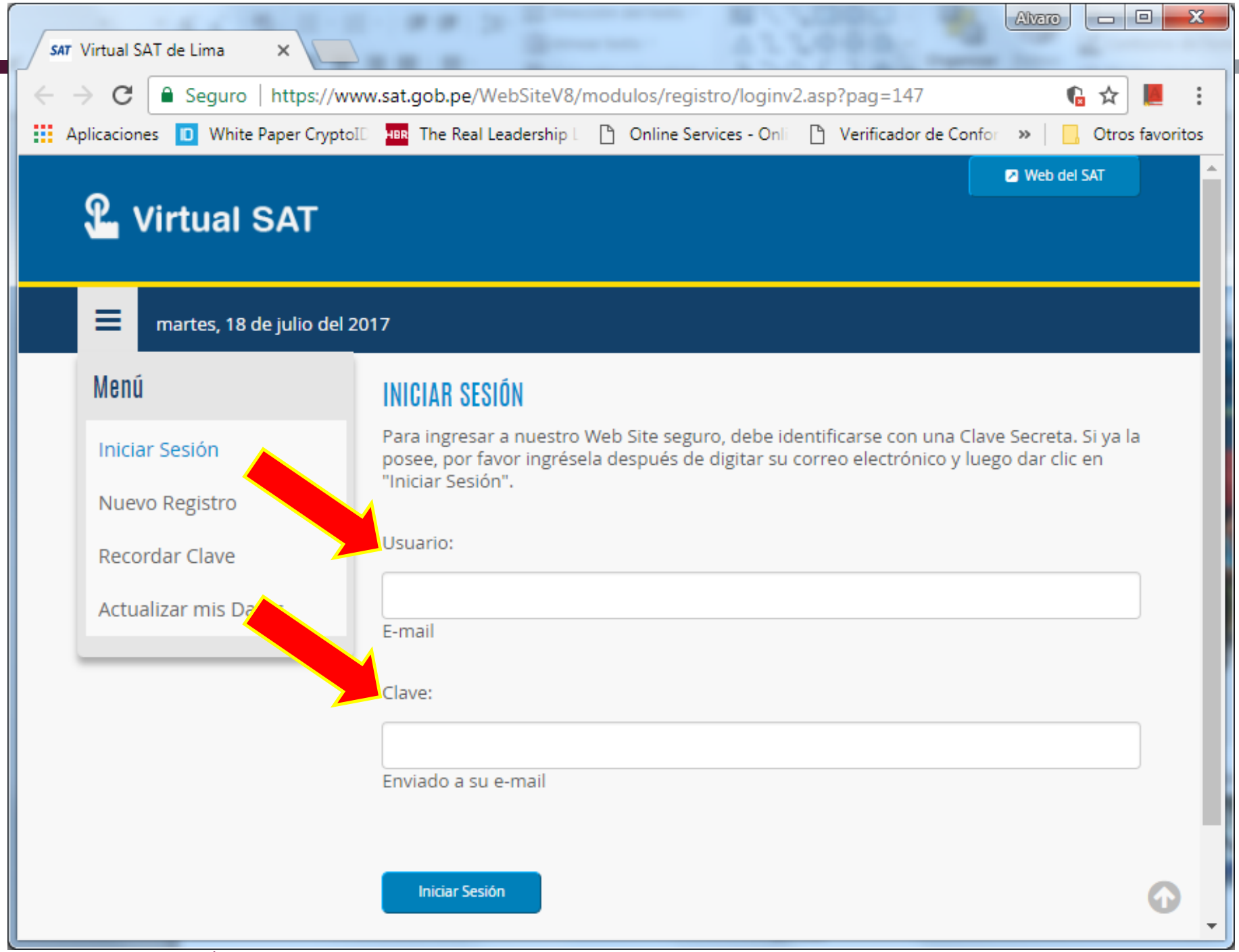


El problema en Internet

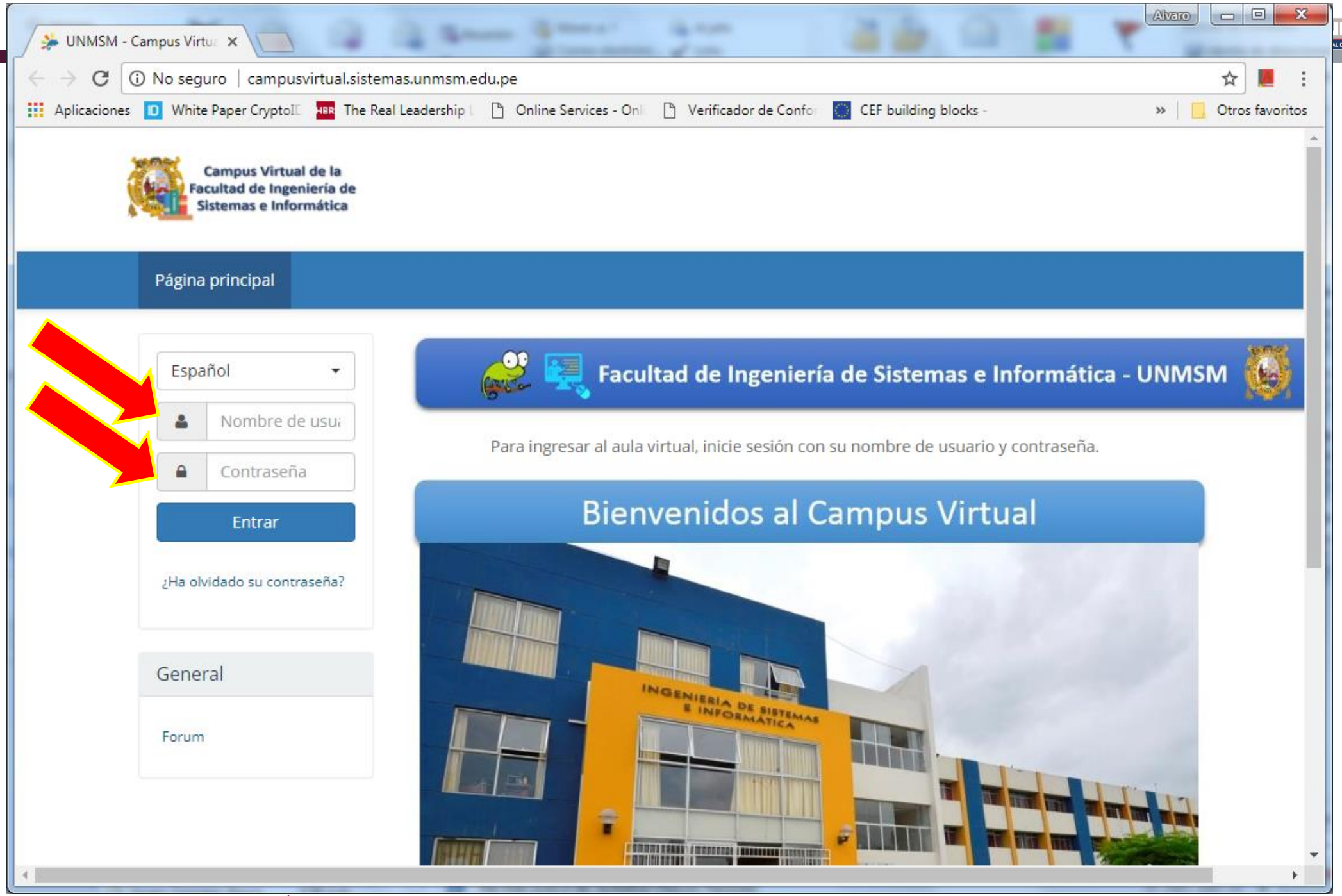
The Internet was built without a way to know who and what you are connecting to.

[Kim Cameron. The Laws of Identity, 2005.]

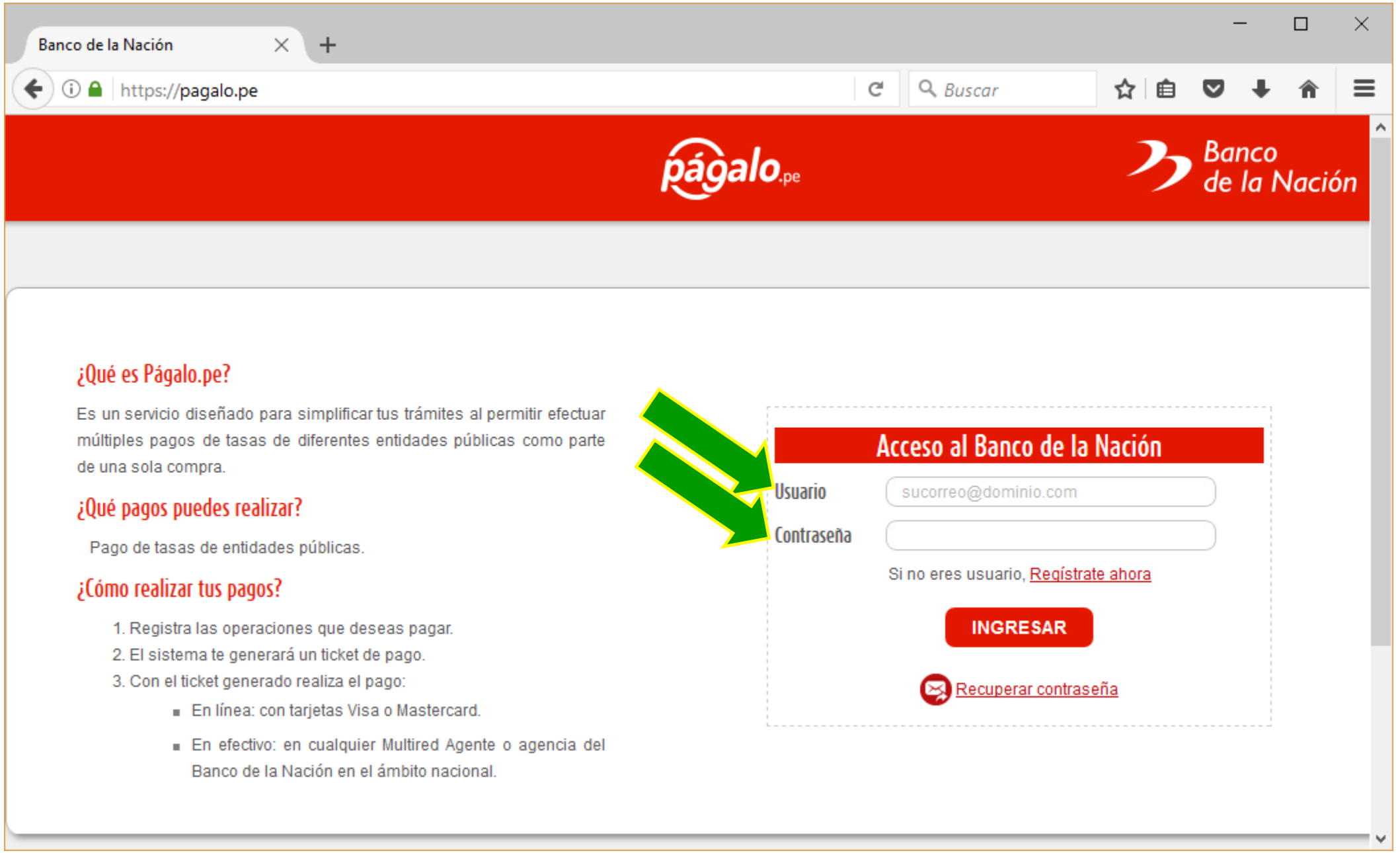

..:: Autenticacion SOL::.. - Google Chrome
Seguro | https://www.sunat.gob.pe/xssecurity/SignOnVerification.htm?signonForwardAction=https%3A%2F%2Fwww.sunat.g
SUNAT OPERACIONES EN LÍNEA
OFICINA VIRTUAL
Bienvenido, ingrese con su Clave SOL
Ingreso a SUNAT en Línea
CLAVESOL
Ingresa por RUC
Ingresa por DNI
RUC
Ingrese RUC
Usuario
Ingrese usuario
Contraseña
Contraseña
¿Te olvidaste tu usuario o clave?
Iniciar Sesión
Falta 4 min para que expire la petición..haga clic aquí si necesita más tiempo.
Agrega este enlace a:
Compatibilidad
Política de privacidad
Aprende sobre SOL
© 1997-2017 SUNAT - PERU. Todos los Derechos Reservados.


Virtual SAT de Lima
Seguro | https://www.sat.gob.pe/WebSiteV8/modulos/registro/loginv2.asp?pag=147
Aplicaciones
White Paper CryptoID
The Real Leadership
Online Services - Onl
Verificador de Confor
Otros favoritos
Web del SAT
Virtual SAT
martes, 18 de julio del 2017
Menú
Iniciar Sesión
Nuevo Registro
Recordar Clave
Actualizar mis Da
INICIAR SESIÓN
Para ingresar a nuestro Web Site seguro, debe identificarse con una Clave Secreta. Si ya la posee, por favor ingrésela después de digitar su correo electrónico y luego dar clic en "Iniciar Sesión".
Usuario:
E-mail
Clave:
Enviado a su e-mail
Iniciar Sesión


Directorio Nacional de In
Seguro | https://dina.concytec.gob.pe/appDirectorioCTI/
Aplicaciones
White Paper CryptoID
The Real Leadership
Online Services - Onl
Otros favoritos
INICIO
GEOCONCYTEC
GUÍA CALIFICACIÓN
REGINA
Manual de uso
Iniciar sesión
DINA
Directorio Nacional de Investigadores e Innovadores
Usuario (Nro documento de identidad)
Contraseña
Ingresar
Olvidé mi contraseña
Buscar investigadores
¿Aún no te has registrado?
Regístrate ahora
https://dina.concytec.gob.pe/appDirectorioCTI/#

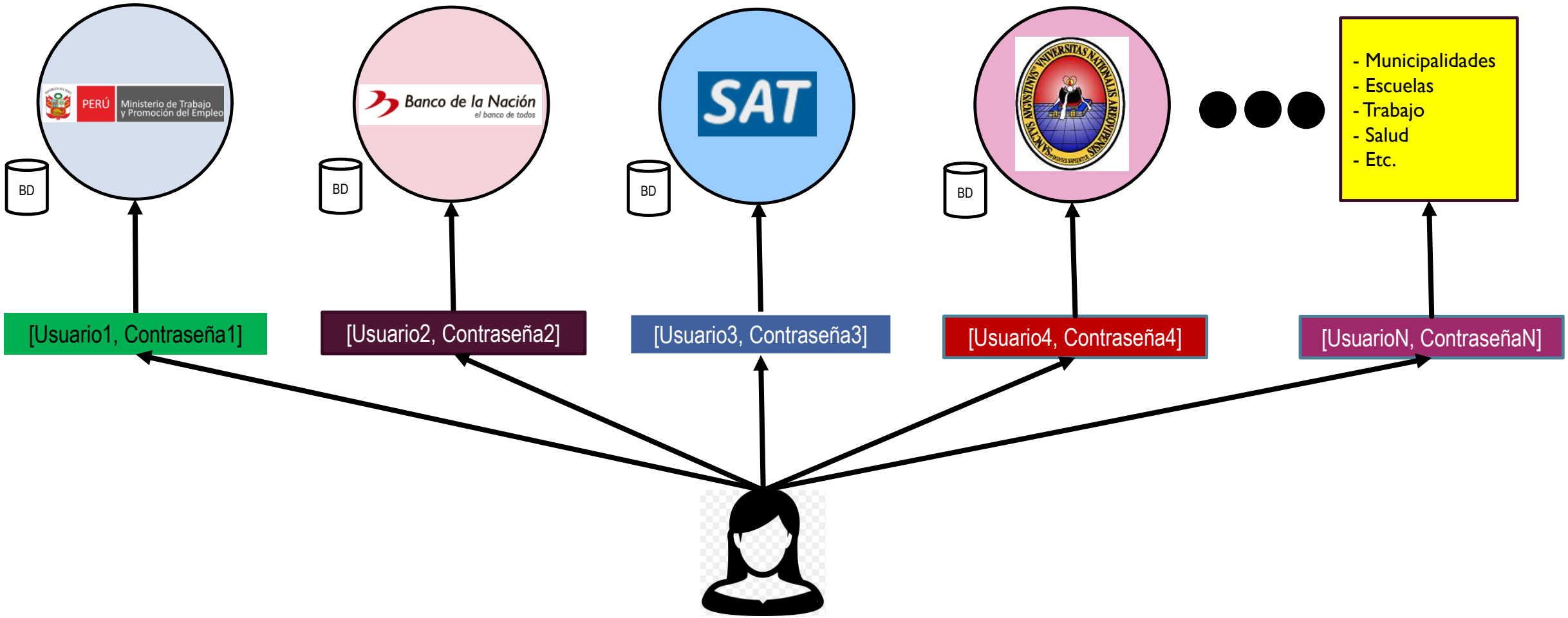

UNMSM - Campus Virtua
Alvaro
No seguro
campusvirtual.sistemas.unmsm.edu.pe
Aplicaciones
White Paper CryptoID
The Real Leadership
Online Services - Onl
Verificador de Confo
CEF building blocks -
Otros favoritos
Campus Virtual de la Facultad de Ingeniería de Sistemas e Informática
Página principal
Español
Nombre de usu
Contraseña
Entrar
¿Ha olvidado su contraseña?
General
Forum
Facultad de Ingeniería de Sistemas e Informática - UNMSM
Para ingresar al aula virtual, inicie sesión con su nombre de usuario y contraseña.
Bienvenidos al Campus Virtual
INGENIERÍA DE SISTEMAS E INFORMÁTICA


https://casillas.pj.gob.pe/sinoe/login.x
SINOE - Sistema de Notifica...
Archivo Edición Ver Favoritos Herramientas Ayuda
PODER JUDICIAL DEL PERÚ
Justicia Honorable, País Respetable
SINOE
Sistema de Notificaciones Electrónicas V.2.0.29
Bienvenidos al sistema de SERVICIOS EN LÍNEA mediante la cual usted podrá realizar diversos procedimientos judiciales en tiempo real, así reducir el tiempo y mejorar la seguridad en todo el proceso.
Los servicios en línea que ofrece el Poder Judicial son los siguientes:
SINOE Sistema de Notificaciones Electrónica
MPE Sistema de Mesa de Partes Electrónica
Usuario
Contraseña
¿Olvidó sus Datos de Casilla?
VPR5L
Ingrese Captcha
Ingresar
SOLICITAR REGISTRO DE CASILLA
INSTRUCTIVO
INSTRUCTIVO
VIDEO PROMOCIONAL


Banco de la Nación
https://pagalo.pe
Buscar
págalo.pe
Banco de la Nación
¿Qué es Págalo.pe?
Es un servicio diseñado para simplificar tus trámites al permitir efectuar múltiples pagos de tasas de diferentes entidades públicas como parte de una sola compra.
¿Qué pagos puedes realizar?
Pago de tasas de entidades públicas.
¿Cómo realizar tus pagos?
1. Registra las operaciones que deseas pagar.
2. El sistema te generará un ticket de pago.
3. Con el ticket generado realiza el pago:
En línea: con tarjetas Visa o Mastercard.
En efectivo: en cualquier Multired Agente o agencia del Banco de la Nación en el ámbito nacional.
Acceso al Banco de la Nación
Usuario
sucorreo@dominio.com
Contraseña
Si no eres usuario, Regístrate ahora
INGRESAR
Recuperar contraseña

El problema en Internet

Ciudadano con múltiples credenciales de identidad electrónica



El problema: implicancias

Ciudadano con múltiples credenciales de identidad electrónica

ENTIDADES PÚBLICAS

- Implementación de servicios electrónicos no focalizada en el servicio propiamente dicho
- Inversión alta: gestionar credenciales
- Seguridad y privacidad discutible

CIUDADANOS

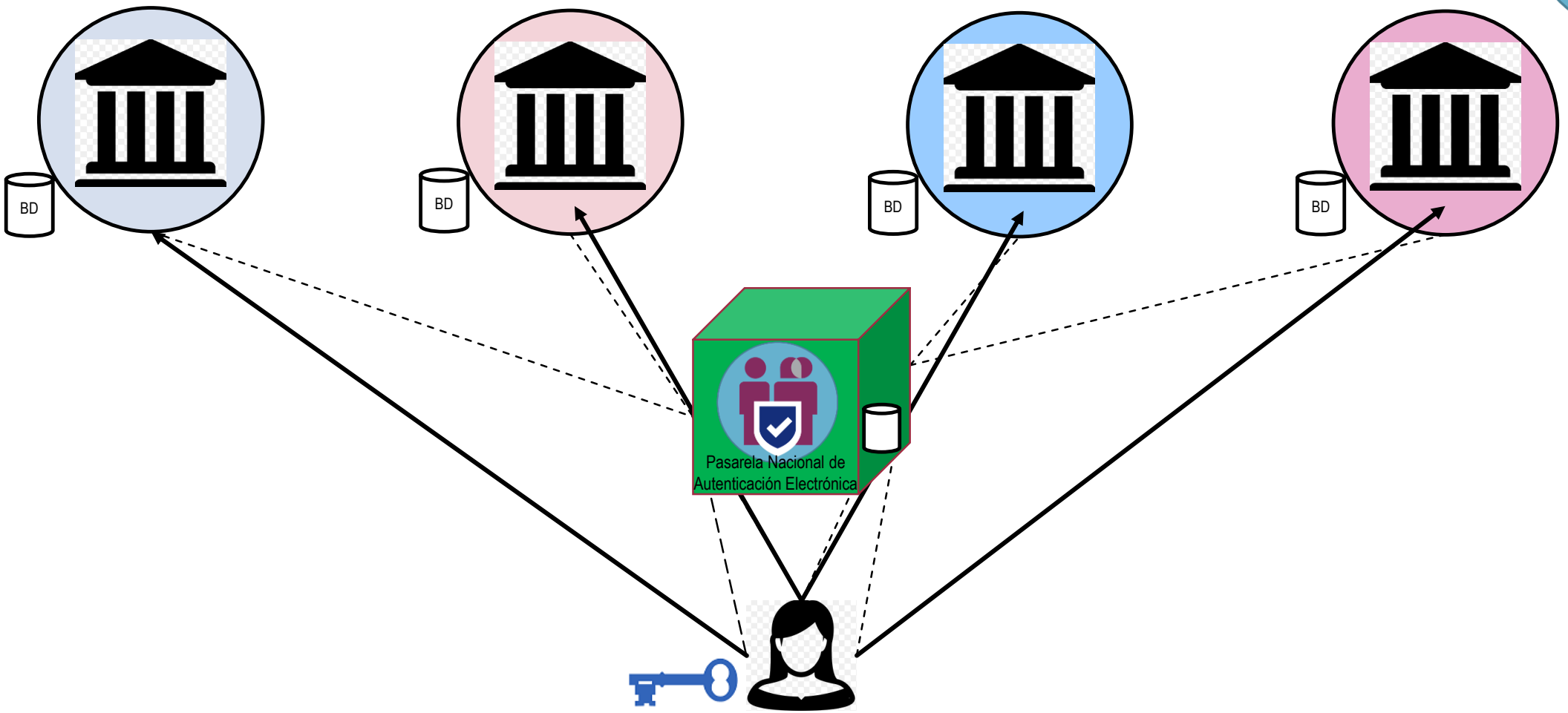
- Una credencial (usuario/contraseña) por cada Entidad Pública
- Pésima experiencia del usuario
- Seguridad en riesgo
- Privacidad discutible

RENIEC

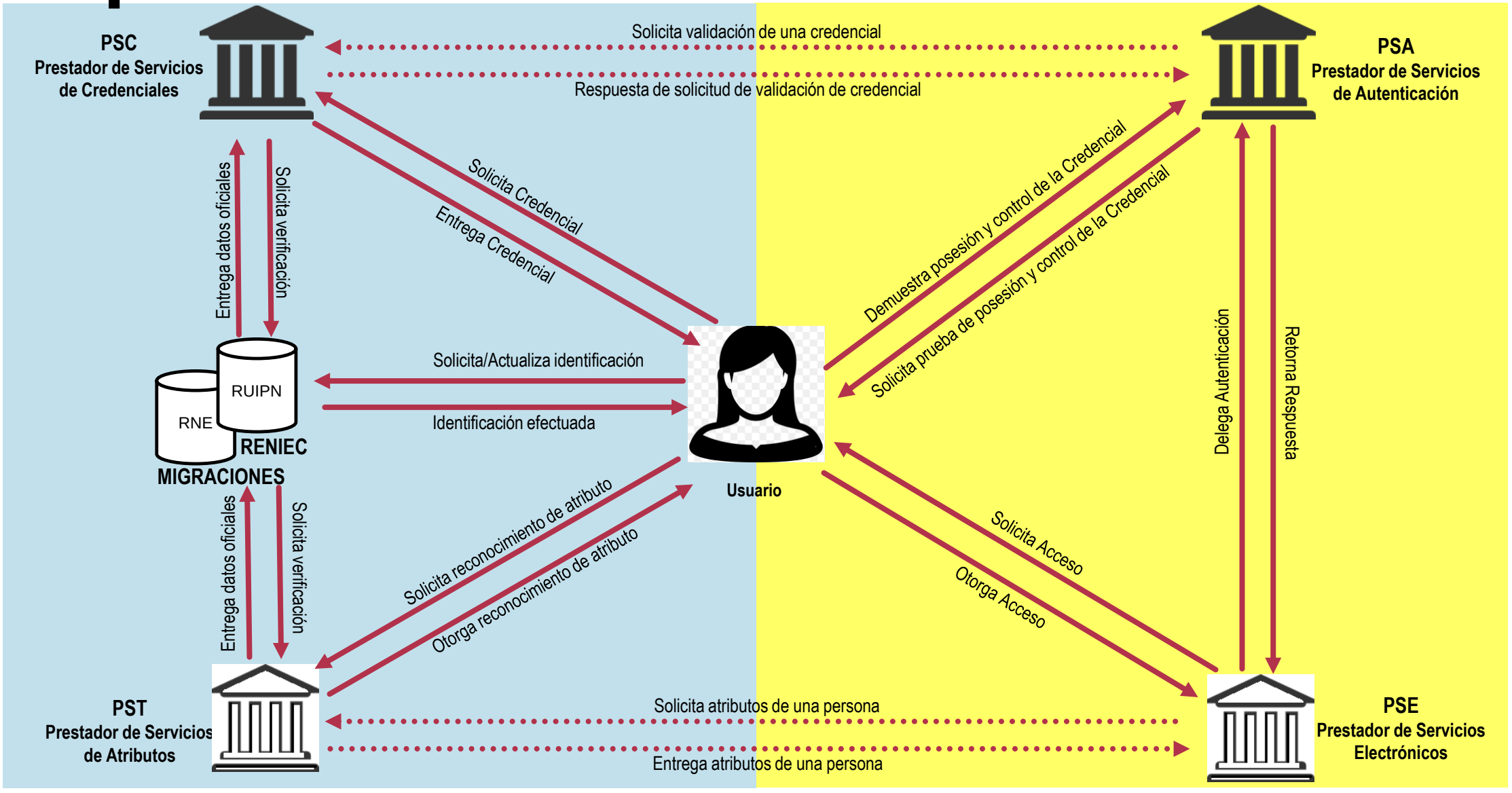
- Las mismas implicancias que cualquier entidad pública

Propuesta de solución

Pasarela Nacional de Autenticación Electrónica: uso de **"credenciales" oficiales**



Propuesta de solución

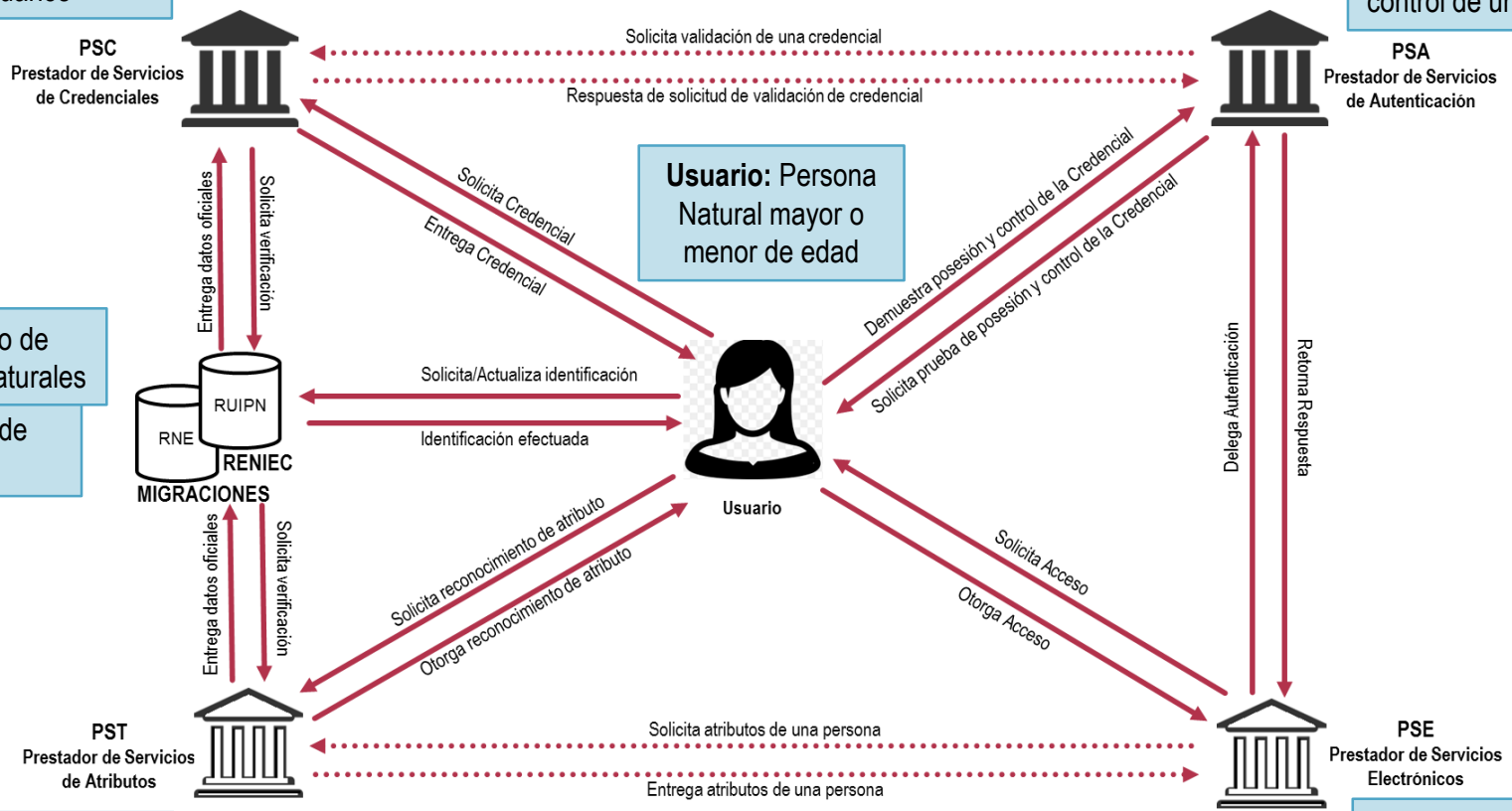


Propuesta de solución

Modelo de Identidad Digital para la Administración Pública

Prestador de Servicios de Credenciales
Entidad de Confianza que administra credenciales vinculadas a los usuarios

Prestador de Servicios de Autenticación
Entidad de confianza que verifica la identidad de un usuario por medio de la verificación de la posesión y control de una credencial emitida por un PSC.



RUIPN: Registro Único de Identidad de Personas Naturales

RNE: Registro Nacional de Extranjeros

Prestador de Servicios de Atributos
Entidad que administra atributos de usuarios que pueden ser consultados por un PSE.

Prestador de Servicios Electrónicos
Entidad que, para dar acceso a un usuario a los recursos de un sistema de información o para procesar una transacción, confía en las respuestas de un PSA. El PSE puede solicitar también atributos del usuario a un PST.

Propuesta de solución

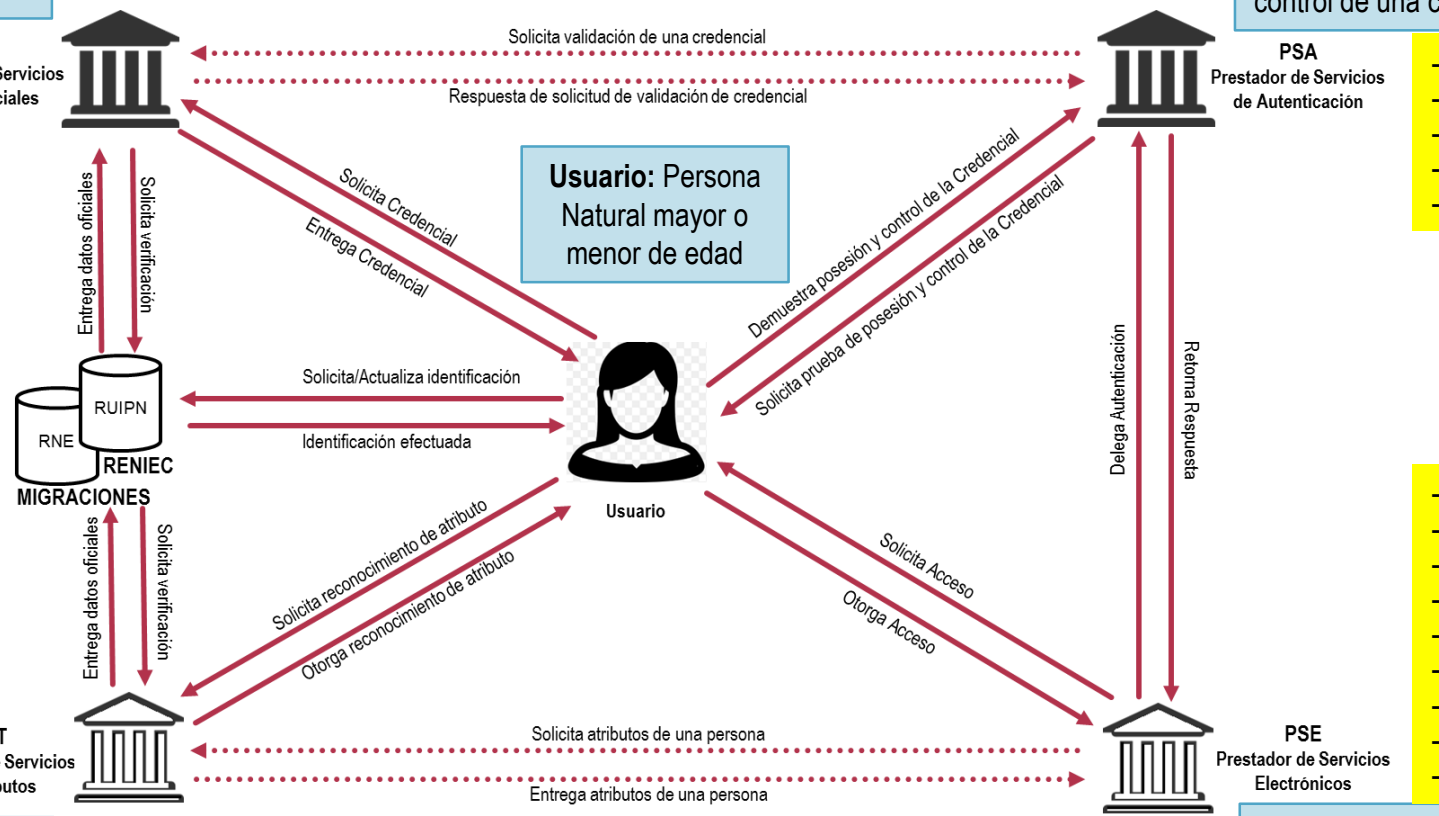
Modelo de Identidad Digital para la Administración Pública

Prestador de Servicios de Credenciales
Entidad de Confianza que administra credenciales vinculadas a los usuarios

- RENIEC (DNIe, Clave nacional)
- Sunat (clave SOL)
- BCP (Token RSA)
- Movistar (Smartphone)
- Etc.

Prestador de Servicios de Autenticación
Entidad de confianza que verifica la identidad de un usuario por medio de la verificación de la posesión y control de una credencial emitida por un PSC.

- RENIEC
- Sunat
- BCP/ASBANC
- Movistar
- Etc.



- Colegios Profesionales (habilitación)
- CONADIS (discapacitados)
- ONPE (omisos)
- CONCYTEC (investigador)
- MINEDU (estudiante)
- RENIEC (estado civil, vinculados, etc.)
- Etc.

Prestador de Servicios de Atributos
Entidad que administra atributos de usuarios que pueden ser consultados por un PSE.

- Municipalidades
- Universidades
- Hospitales
- Ministerios
- Organismos autónomos
- PNP
- Fuerzas armadas
- Empresas públicas
- Etc.

Prestador de Servicios Electrónicos
Entidad que, para dar acceso a un usuario a los recursos de un sistema de información o para procesar una transacción, confía en las respuestas de un PSA. El PSE puede solicitar también atributos del usuario a un PST.

Propuesta de solución: beneficios

Pasarela Nacional de Autenticación Electrónica: **una única "credencial" oficial**

ENTIDADES PÚBLICAS

- Facilita la implementación de servicios electrónicos. Foco en sus procesos misionales y no en procesos de identidad.
- Reduce la inversión
- Facilita el acceso fluido de los usuarios a sus servicios
- Gestiona el **nivel de riesgo**

CIUDADANOS

- Administra una credencial oficial
- Experiencia del usuario mejorada
- Acceso simplificado
- Protege la privacidad
- Mejora la seguridad

RENIEC

- Identidad como servicio
- Prestación del servicio a entidades públicas y privadas
- Proveedor Oficial de Identidad Digital para el Estado Peruano

Propuesta de solución: beneficios

Pasarela Nacional de Autenticación Electrónica: **una única "credencial" oficial**

ENTIDADES PÚBLICAS

- Facilita la implementación de servicios electrónicos. Foco en sus procesos misionales y no en procesos de identidad.
- Reduce la inversión
- Facilita el acceso fluido de los usuarios a sus servicios
- Gestiona el **nivel de riesgo**

CIUDADANOS

- Administra una credencial oficial
- Experiencia del usuario mejorada
- Acceso simplificado
- Protege la privacidad
- Mejora la seguridad

RENIEC

- Identidad como servicio
- Prestación del servicio a entidades públicas y privadas
- Proveedor Oficial de Identidad Digital para el Estado Peruano
- Protagonismo tanto en el mundo físico como en el electrónico

Proyectos similares

CONNECT.GOV USA

FranceConnect

GOV.UK VERIFY

DIACC Canada

clave España

Claveúnica tu acceso digital Chile

Sistema de clave única

Uruguay Digital

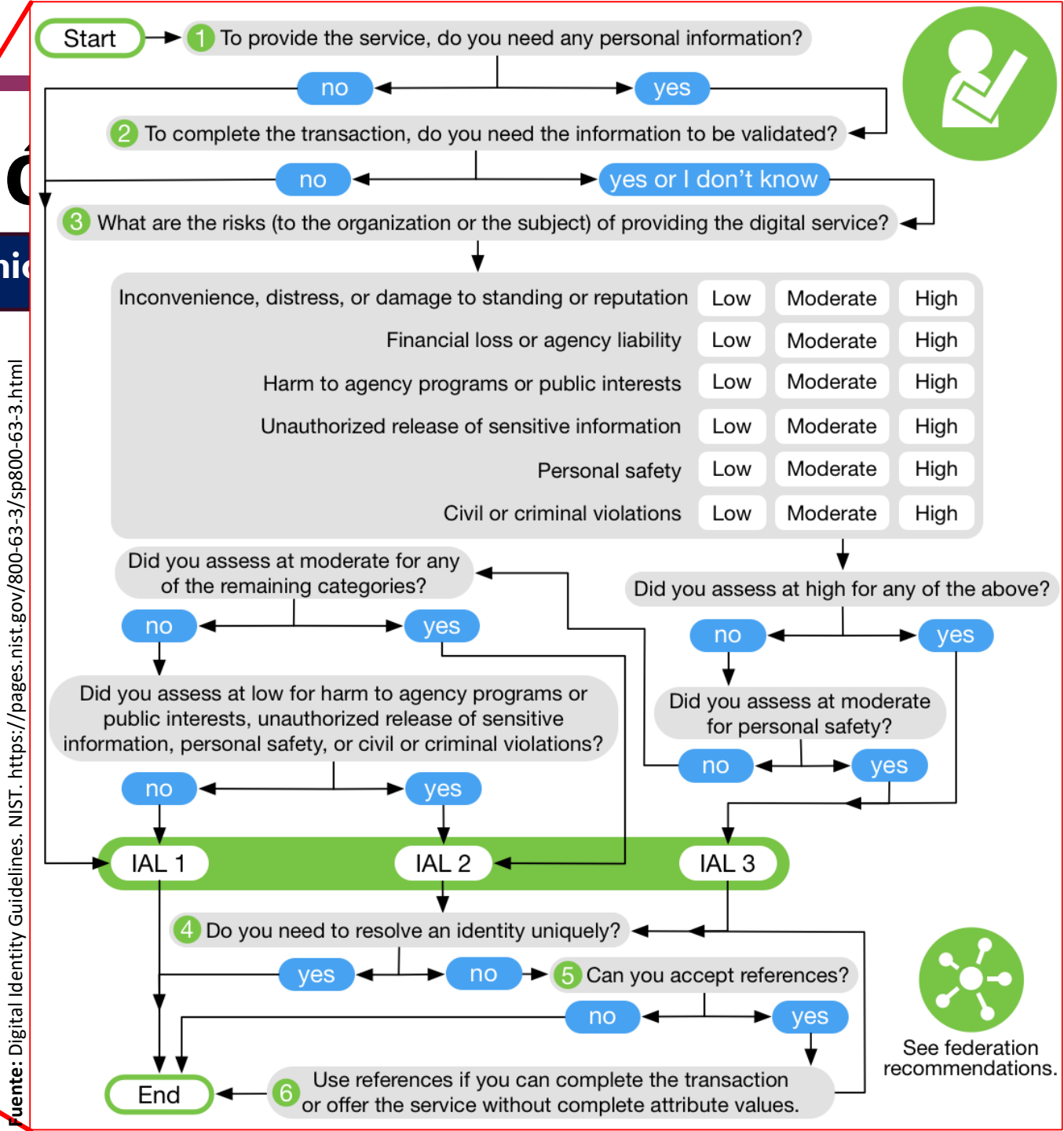
Propuesta de soluci

Pasarela Nacional de Autenticación Electrónica: una úni

ENTIDADES PÚBLICAS

- Facilita la implementación de servicios electrónicos. Foco en sus procesos misionales y no en procesos de identidad.
- Reduce la inversión
- Facilita el acceso fluido de los usuarios a sus servicios
- Gestiona el **nivel de riesgo**

Cada organización determina el nivel de confianza de la [credencial, autenticación, respuesta] de acuerdo al **nivel de riesgo** de su transacción electrónica



Fuente: Digital Identity Guidelines. NIST. https://pages.nist.gov/800-63-3/sp800-63-3.html

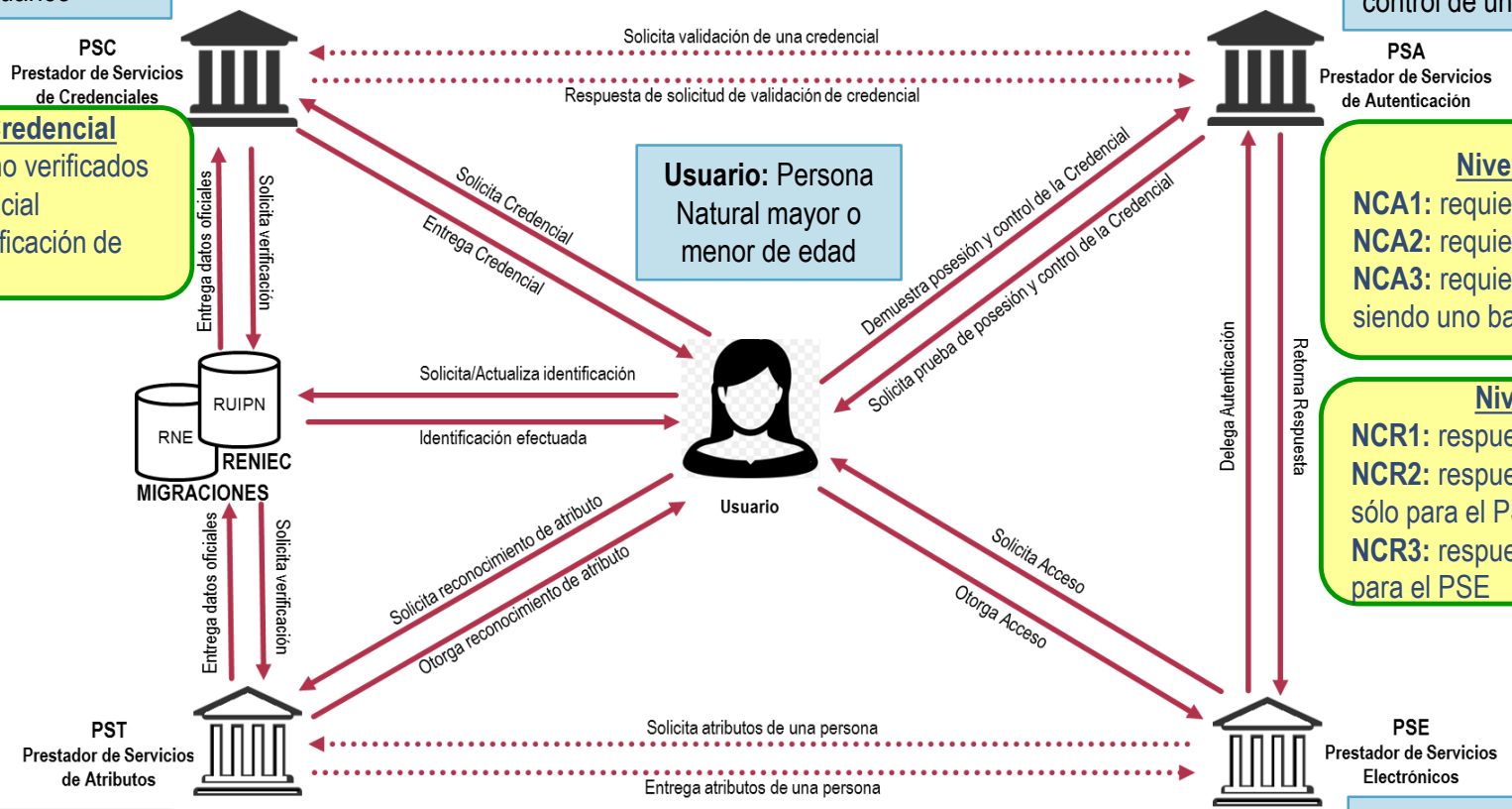
Propuesta de solución

Modelo de Identidad Digital para la Administración Pública

Prestador de Servicios de Credenciales
Entidad de Confianza que administra credenciales vinculadas a los usuarios

Prestador de Servicios de Autenticación
Entidad de confianza que verifica la identidad de un usuario por medio de la verificación de la posesión y control de una credencial emitida por un PSC.

Niveles de Confianza de la Credencial
NCC1: atributos autodeclarados, no verificados
NCC2: validación remota o presencial
NCC3: validación presencial y verificación de documentos



Niveles de Confianza de la Autenticación
NCA1: requiere un factor de autenticación
NCA2: requiere dos factores de autenticación diferentes
NCA3: requiere dos factores de autenticación diferentes, siendo uno basado en llaves criptográficas y HW

Niveles de Confianza de la Respuesta
NCR1: respuesta de portador, firmada por el PSA
NCR2: respuesta de portador, firmada por el PSA y cifrada sólo para el PSE
NCR3: respuesta de suscriptor, firmada por el PSA y cifrada para el PSE

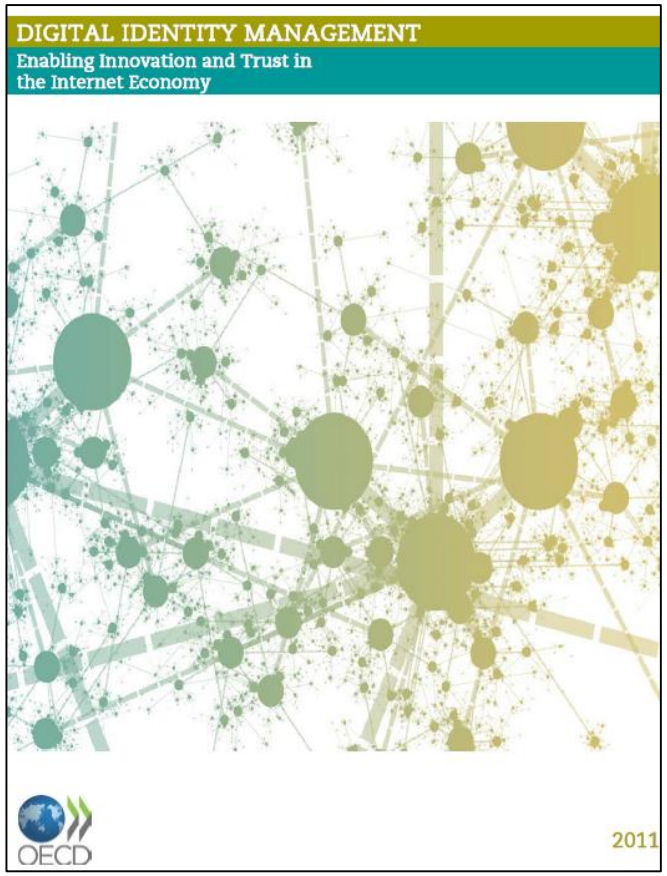
Prestador de Servicios de Atributos
Entidad que administra atributos de usuarios que pueden ser consultados por un PSE.

Prestador de Servicios Electrónicos
Entidad que, para dar acceso a un usuario a los recursos de un sistema de información o para procesar una transacción, confía en las respuestas de un PSA. El PSE puede solicitar también atributos del usuario a un PST.

OECD y la Identidad Digital

Recomendaciones para los gobiernos

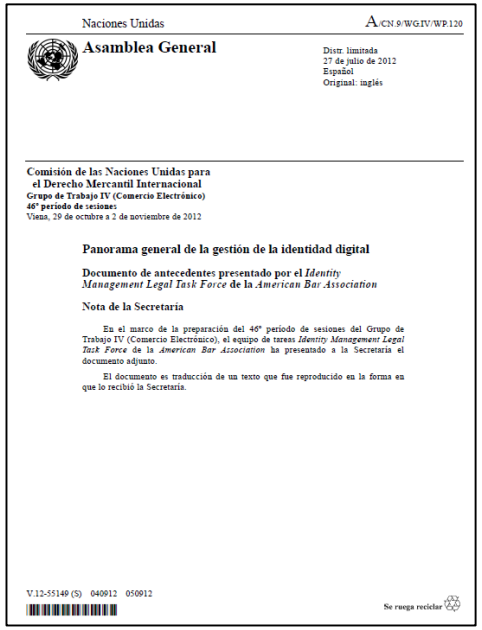
1. Adoptar una estrategia clara para la gestión de las identidades digitales.
2. No perder de vista los potenciales beneficios a largo plazo de una economía basada en el Internet.
3. Los procedimientos de gestión de la identidad actualmente llevados a cabo de manera *offline* pueden ser un punto de partida natural para desplegar procedimientos de gestión de identidades de manera *online*.
4. Las actividades relacionadas al gobierno electrónico de alcance nacional deben ser alineadas con la estrategia de gestión de identidades, por ser esta de carácter transversal.
5. La política de credenciales digitales debe balancear las ventajas y desventajas del uso de múltiples credenciales frente al uso de una única credencial; lo que implica considerar el equilibrio entre privacidad y usabilidad.
6. Las políticas de gestión de identidades digitales deben garantizar el respeto a las regulaciones sobre la privacidad y seguridad.
7. Los países miembros deben trabajar de forma coordinada a fin de facilitar el gobierno y comercio electrónico transfronterizo.



Fuente: *DIGITAL IDENTITY MANAGEMENT. Enabling Innovation and Trust in the Internet Economy. OECD, 2011. http://www.oecd.org/sti/ieconomy/digitalidentitymanagementandelectronicauthentication.htm*

Identidad Digital …

UNCITRAL, eIDAS, NIST, etc.



Naciones Unidas A/CN.9/WG.IV/WP.120

Asamblea General

Distr. limitada
27 de julio de 2012
Español
Original: inglés

Comisión de las Naciones Unidas para el Derecho Mercantil Internacional
Grupo de Trabajo IV (Comercio Electrónico)
46º período de sesiones
Viena, 29 de octubre a 2 de noviembre de 2012

Panorama general de la gestión de la identidad digital

Documento de antecedentes presentado por el *Identity Management Legal Task Force* de la *American Bar Association*

Nota de la Secretaría

En el marco de la preparación del 46º período de sesiones del Grupo de Trabajo IV (Comercio Electrónico), el equipo de tareas *Identity Management Legal Task Force* de la *American Bar Association* ha presentado a la Secretaría el documento adjunto.

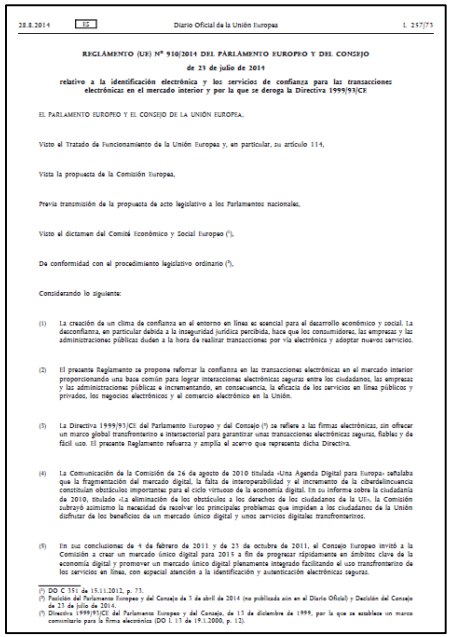
El documento es traducción de un texto que fue reproducido en la forma en que lo recibió la Secretaría.

V.12-55149 (S) 040912 050912

Se ruega reciclar

El presente documento ofrece una visión general de la gestión de la identidad digital, su función en el comercio electrónico, las cuestiones jurídicas que plantea y las barreras legales que plantea. Se basa en la labor que adelanta el grupo de tareas *Identity Management Legal Task Force* de la *American Bar Association* (ABA), y se presenta como material de antecedentes para informar al Grupo de Trabajo de cuestiones pertinentes.

Fuente: *Panorama general de la gestión de la identidad digital. UNCITRAL, 2012.*
Fuente: https://documents-dds-ny.un.org/doc/UNDOC/LTD/V12/551/49/PDF/V1255149.pdf?OpenElement



28.8.2014 ES Diario Oficial de la Unión Europea L 257/73

REGLAMENTO (UE) Nº 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO
de 23 de julio de 2014
relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE

EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea y, en particular, su artículo 114,

Vista la propuesta de la Comisión Europea,

Previa transmisión de la propuesta de acto legislativo a los Parlamentos nacionales,

Visto el dictamen del Comité Económico y Social Europeo (1),

De conformidad con el procedimiento legislativo ordinario (2),

Considerando lo siguiente:

(1) La creación de un clima de confianza en el entorno en línea es esencial para el desarrollo económico y social. La desconfianza, en particular debida a la inseguridad jurídica percibida, hace que los consumidores, las empresas y las administraciones públicas duden a la hora de realizar transacciones por vía electrónica y adoptar nuevos servicios.

(2) El presente Reglamento se propone reforzar la confianza en las transacciones electrónicas en el mercado interior proporcionando una base común para lograr interacciones electrónicas seguras entre los ciudadanos, las empresas y las administraciones públicas e incrementando, en consecuencia, la eficacia de los servicios en línea públicos y privados, los negocios electrónicos y el comercio electrónico en la Unión.

(3) La Directiva 1999/93/CE del Parlamento Europeo y del Consejo (3) se refiere a las firmas electrónicas, sin ofrecer un marco global transfronterizo e intersectorial para garantizar unas transacciones electrónicas seguras, fiables y de fácil uso. El presente Reglamento refuerza y amplía el acervo que representa dicha Directiva.

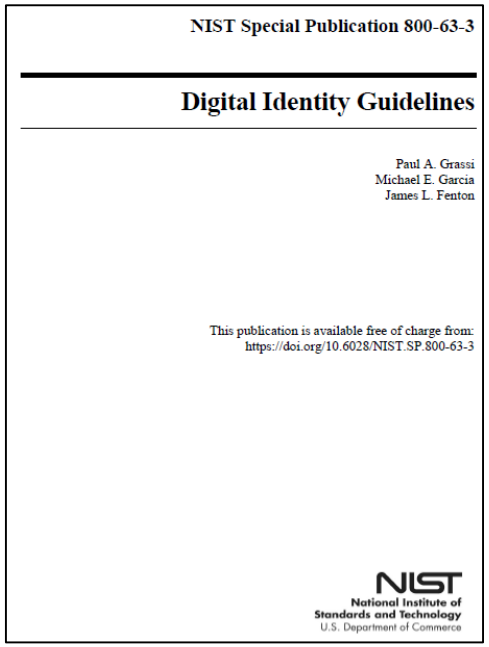
(4) La Comunicación de la Comisión de 26 de agosto de 2010 titulada «Una Agenda Digital para Europa» señalaba que la fragmentación del mercado digital, la falta de interoperabilidad y el incremento de la ciberdelincuencia constituían obstáculos importantes para el ciclo virtuoso de la economía digital. En su informe sobre la ciudadanía de 2010, titulado «La eliminación de los obstáculos a los derechos de los ciudadanos de la UE», la Comisión subrayó asimismo la necesidad de resolver los principales problemas que impiden a los ciudadanos de la Unión disfrutar de los beneficios de un mercado único digital y unos servicios digitales transfronterizos.

(5) En sus conclusiones de 4 de febrero de 2011 y de 23 de octubre de 2011, el Consejo Europeo invitó a la Comisión a crear un mercado único digital para 2015 a fin de progresar rápidamente en ámbitos clave de la economía digital y promover un mercado único digital plenamente integrado facilitando el uso transfronterizo de los servicios en línea, con especial atención a la identificación y autenticación electrónicas seguras.

(1) DO C 351 de 15.11.2012, p. 73.
(2) Posición del Parlamento Europeo y del Consejo de 3 de abril de 2014 (no publicada aún en el Diario Oficial) y Decisión del Consejo de 23 de julio de 2014.
(3) Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica (DO L 13 de 19.1.2000, p. 12).

REGLAMENTO (UE) N o 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.

Fuente: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.SPA



NIST Special Publication 800-63-3

Digital Identity Guidelines

Paul A. Grassi
Michael E. Garcia
James L. Fenton

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-63-3

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

These guidelines provide technical requirements for federal agencies implementing digital identity services and are not intended to constrain the development or use of standards outside of this purpose. The guidelines cover identity proofing and authentication of users (such as employees, contractors, or private individuals) interacting with government IT systems over open networks. They define technical requirements in each of the areas of identity proofing, registration, authenticators, management processes, authentication protocols, federation, and related assertions. This publication supersedes NIST Special Publication 800-63-2.

Fuente: https://pages.nist.gov/800-63-3/