FIRMA DIGITAL

Claudia Dacak

Dirección de Firma Digital

Dirección General de Firma Digital y Comercio Electrónico

TETÃ MBA'E'APOPY HA ÑEMU
MOTENONDEHA
MINISTERIO DE INDUSTRIA Y COMERCIO

Dirección General de Firma Digital & Comercio Electrónico

Agenda

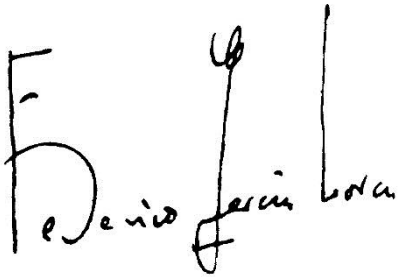
- Conceptos básicos
- Funcionamiento tecnológico de firma digital
- Autoridades de Certificación
- Certificados Digitales
- Infraestructura de Clave Pública del Paraguay
- Aplicaciones

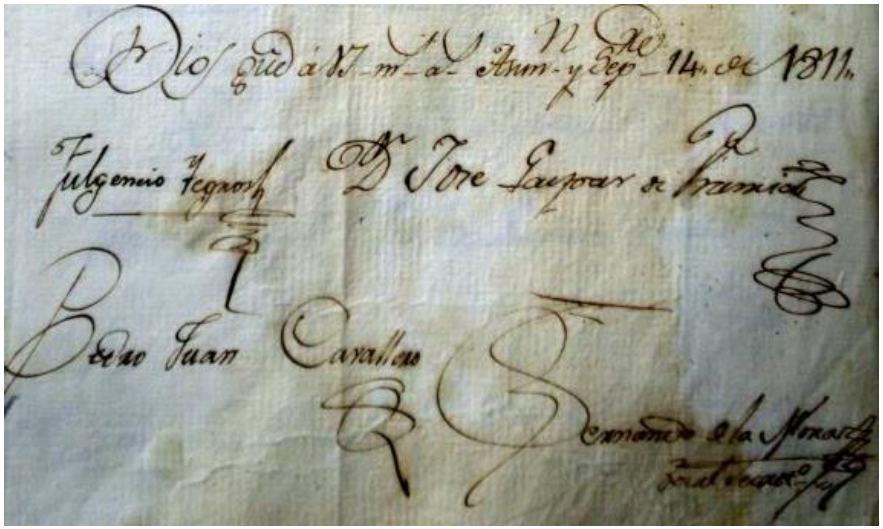
CONCEPTOS BÁSICOS

Firma

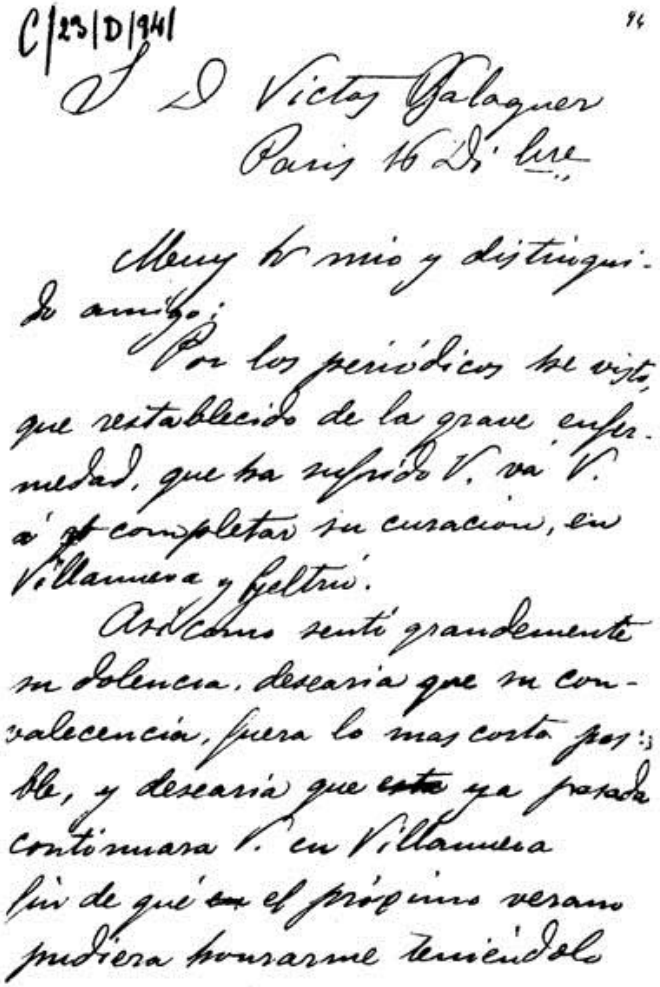
Nombre y apellido, o título, que una persona escribe de su propia mano en un documento, para darle autenticidad o para expresar que aprueba su contenido.

Real Academia Española





Así nos comunicábamos



C/23/D/941

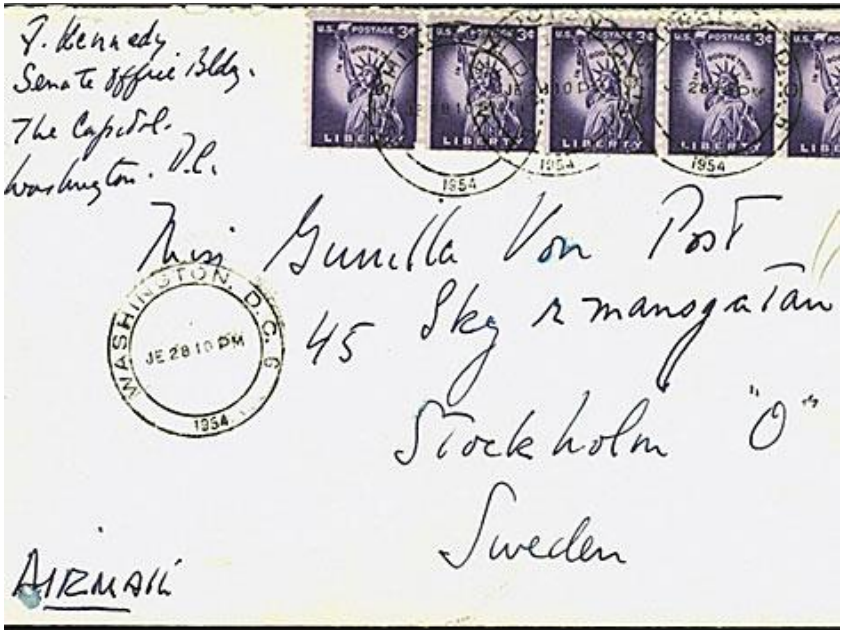
94

Sr D Victor Galaguer
Paris 16 Dr Lure

Muy Sr mio y distinguido amigo:

Por los periódicos he visto que restablecido de la grave enfermedad, que ha sufrido V. va V. a completar su curacion, en Villamuera y Geltrú.

Aunque sentí grandemente su dolencia, desearia que su convalecencia, fuera lo mas corta posible, y desearia que esta ya pasada continuara V. en Villamuera hasta de que en el próximo verano pudiera honrarme teniéndole



J. Kennedy
Senate Office Bldg.
The Capitol.
Washington. D.C.

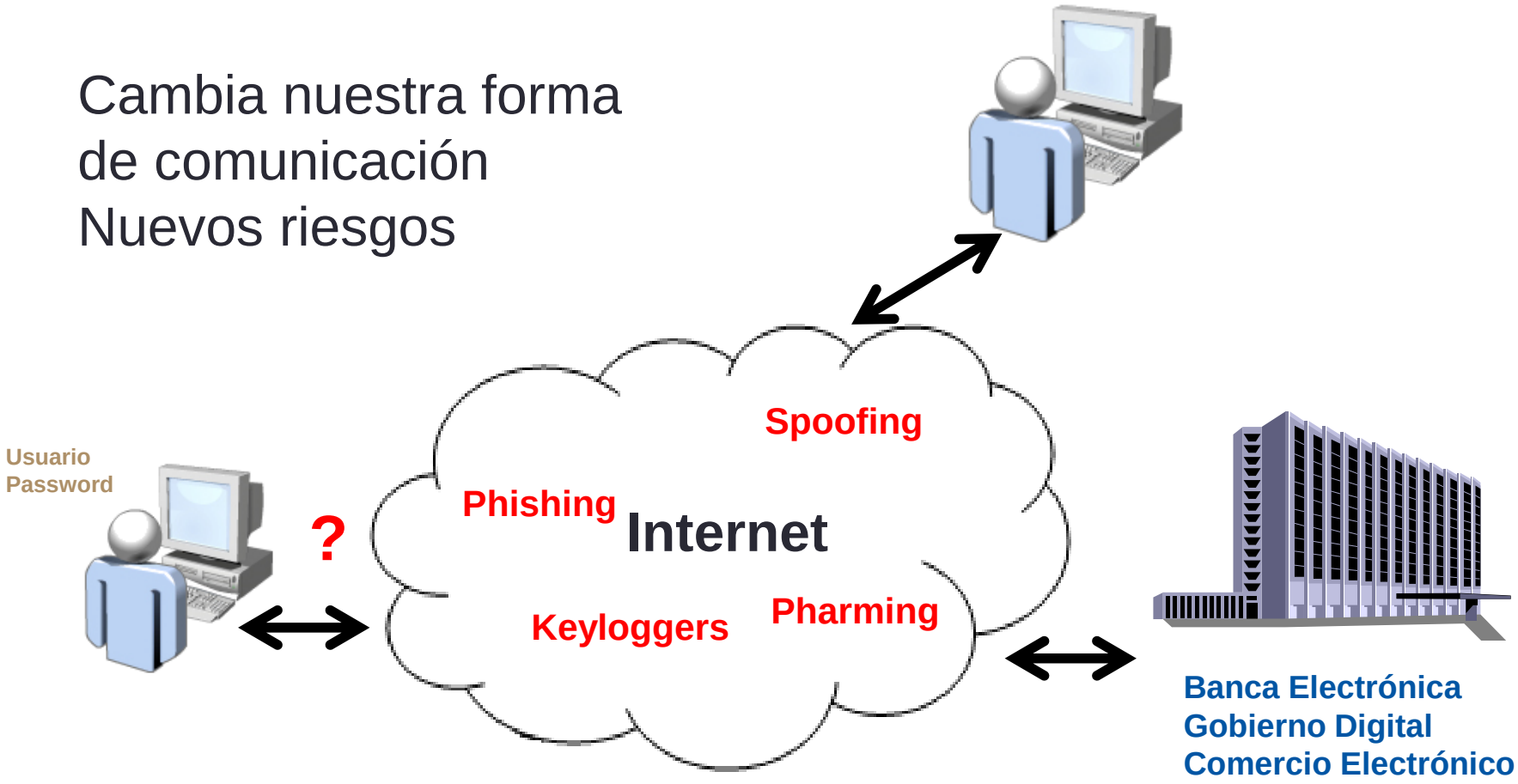
WASHINGTON, D.C.
JE 28 10 PM
1954

Miss Gunilla Von Post
45 Sköldungatan
Stockholm "O"
Sweden

AIRMAIL

Hasta que llegó Internet

Cambia nuestra forma
de comunicación
Nuevos riesgos



Situación

- No es posible determinar con certeza el emisor
- Un documento puede ser fácilmente alterable
- Puede ser objeto de repudio

NO HAY CONFIANZA EN LA COMUNICACIÓN

Es necesaria confianza de las partes

En la identidad de todas las entidades

Autenticación

En que los datos no sean modificados

Integridad

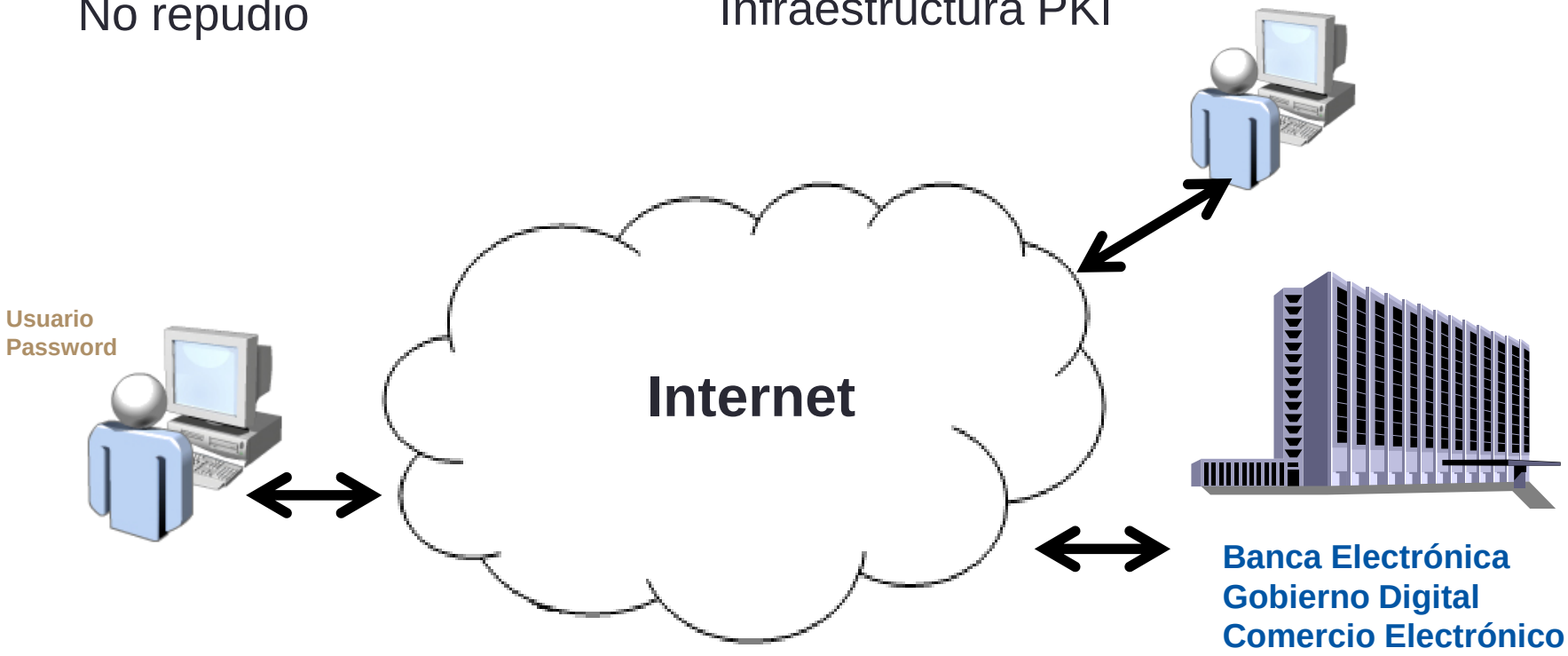
En que las partes no se desdigan

No Repudio

La solución

Autenticación
Integridad
No repudio

Firma Digital
Certificados Digitales
Infraestructura PKI



Que no es una firma digital

- Una firma digitalizada
- Una contraseña
- Un documento encriptado
- Un registro biométrico
- Una cadena de caracteres única para cada persona

Firma Digital

La firma digital es un conjunto de datos generados mediante un algoritmo matemático y basado en técnicas criptográficas (de generación de claves) que se añade al documento que se quiere enviar por Internet y que permite no solo vincular ese documento a una determinada persona o entidad, sino impedir que dicho documento sea modificado por el camino.

Es un proceso tecnológico

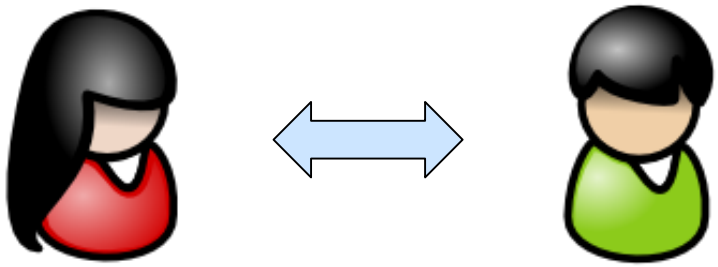
Requiere de un marco legal para su implementación y aplicación

FUNCIONAMIENTO

Criptografía

- Criptografía simétrica

  Los sistemas de cifrado que emplean la misma clave para el cifrado y el descifrado son conocidos como algoritmos de clave simétrica, se utilizan para la criptografía simétrica



Alicia y Roberto acuerdan la clave por algún medio de comunicación.

Roberto

Criptografía

- Criptografía simétrica

  Seguridad radica en mantener secreta la clave

  - La clave se puede deducir
  - Se deben definir canales seguros para distribuir la clave
  - Riesgos de Ingeniería Social

Criptografía

- Criptografía asimétrica

Los sistemas de cifrado que emplean un par de claves para el cifrado y el descifrado son conocidos como algoritmos de clave pública o asimétrica

Clave Privada: es utilizada por su titular para el cifrado del mensaje, es secreta y mantenida por ese titular bajo su exclusiva responsabilidad

Clave Pública: es utilizada por el receptor de un mensaje cifrado para verificar la integridad y la autenticidad

Cifrado Asimétrico

Supongamos la existencia de candados especiales que utilizan dos llaves.

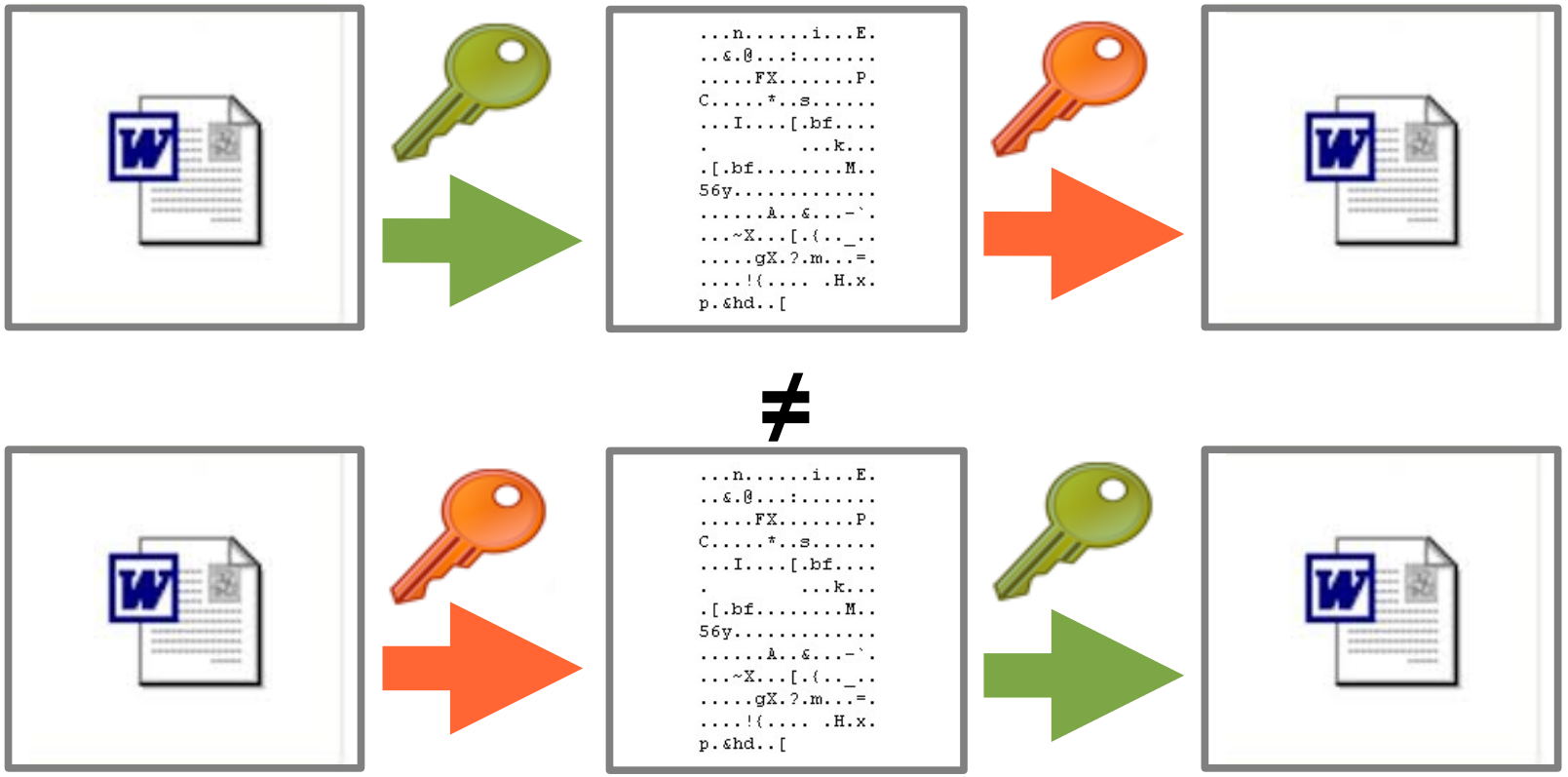
Si una llave de ellas se utiliza para cerrarlos, solamente la llave correspondiente podrá ser usada para abrirlos.

Llave Privada
(Cerrar)

Llave Pública
(Abrir)

La Llave Privada debe mantenerse secreta, mientras que la Llave Pública puede ser distribuida.

Cifrado Asimétrico - Características

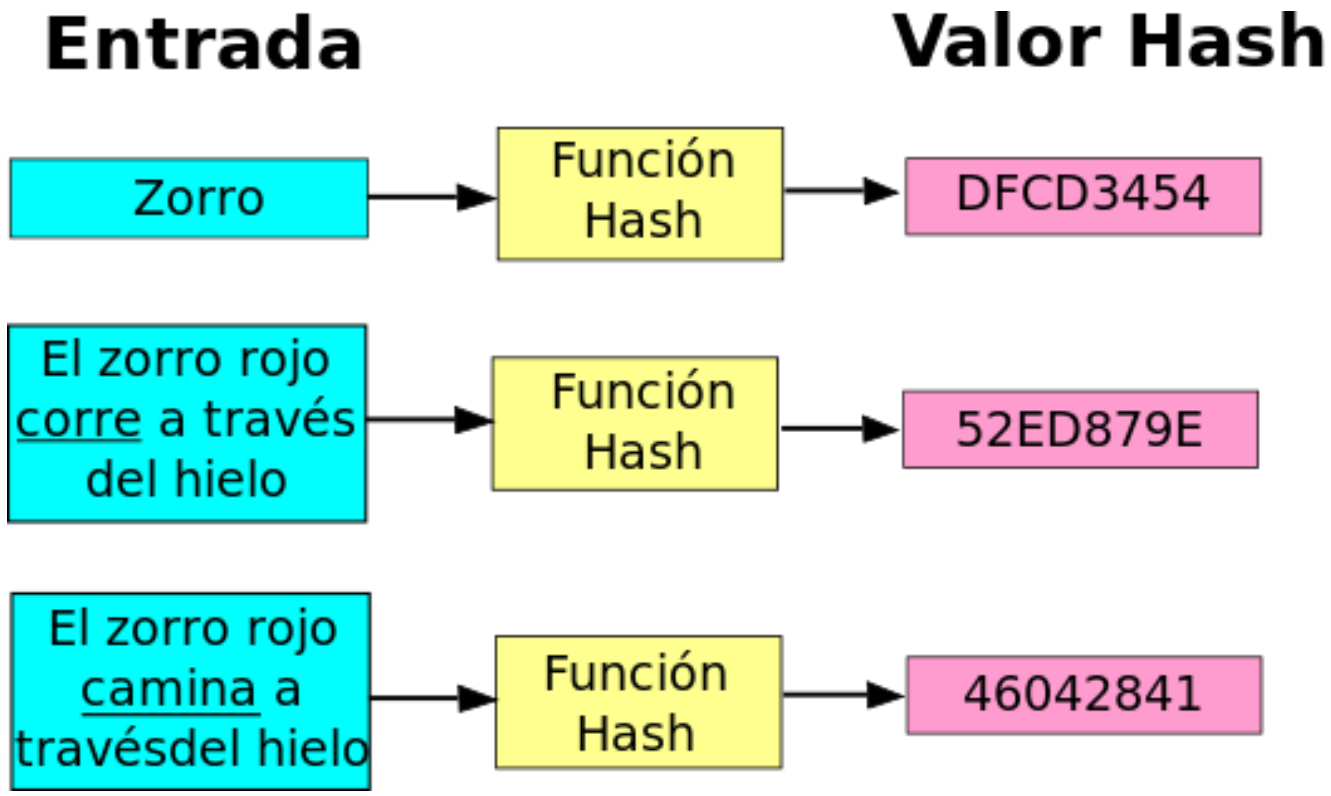


Huella Digital, Resumen o Hash

Función Hash: Es un procedimiento matemático que toma un mensaje de datos y devuelve un resumen o huella digital con las siguientes características

- El tamaño de la huella se mantiene fijo, no depende del tamaño del mensaje
- La menor alteración al mensaje de entrada genera una huella distinta
- No se puede deducir el mensaje original a partir del resumen
- La probabilidad de que una huella digital sea igual para dos mensajes distintos es ínfima

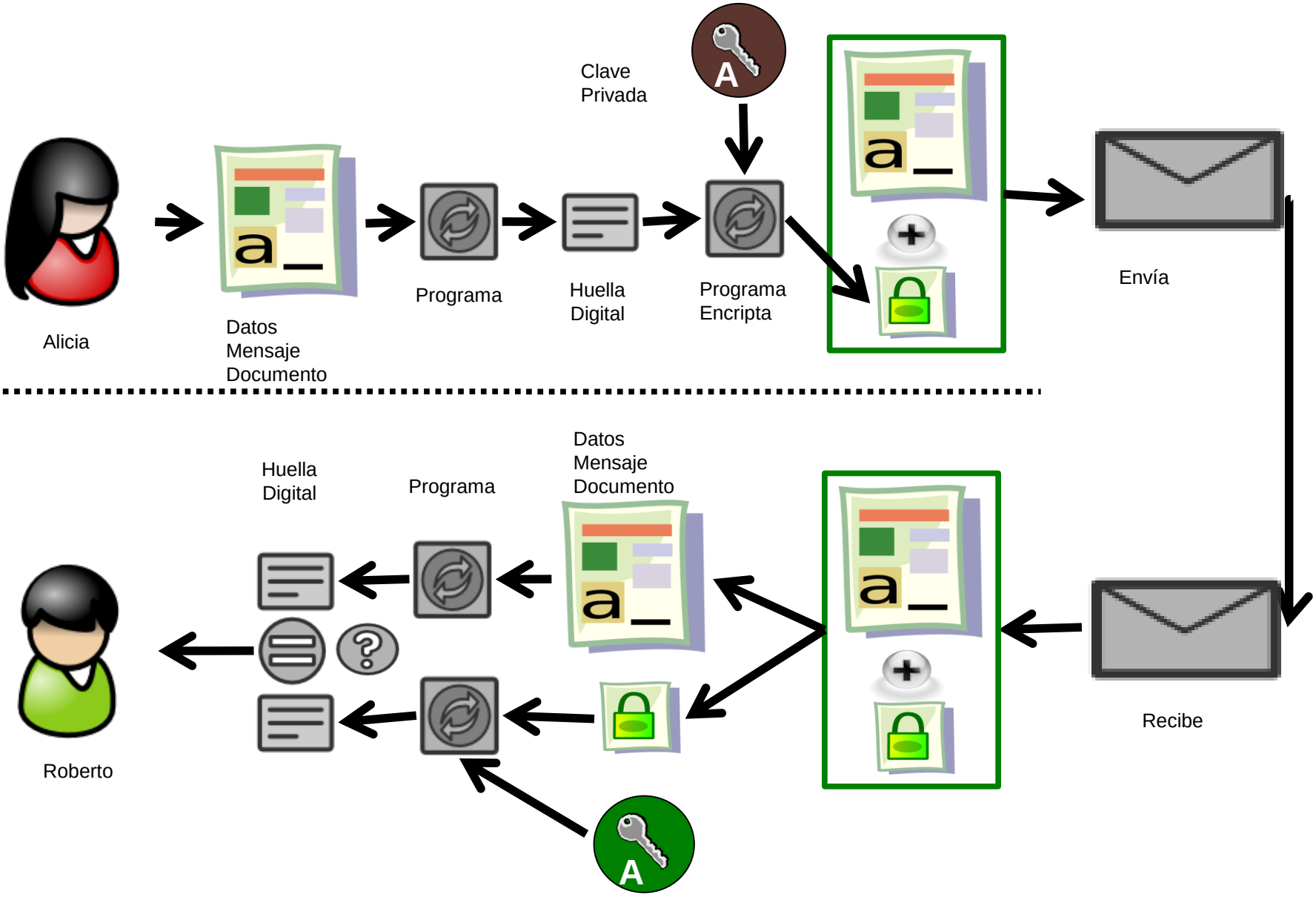
Huella Digital, Hash o Resumen



Firma Digital

- Podemos decir que técnicamente la Firma Digital es la **huella digital del mensaje, cifrada asimétricamente mediante la clave privada,** que se anexa al documento original.

- Pero falta algo mas…


Clave
Privada
A
Alicia
Datos
Mensaje
Documento
Programa
Huella
Digital
Programa
Encripta
Envía
Huella
Digital
Programa
Datos
Mensaje
Documento
Recibe
Roberto
A

AUTORIDADES DE CERTIFICACION

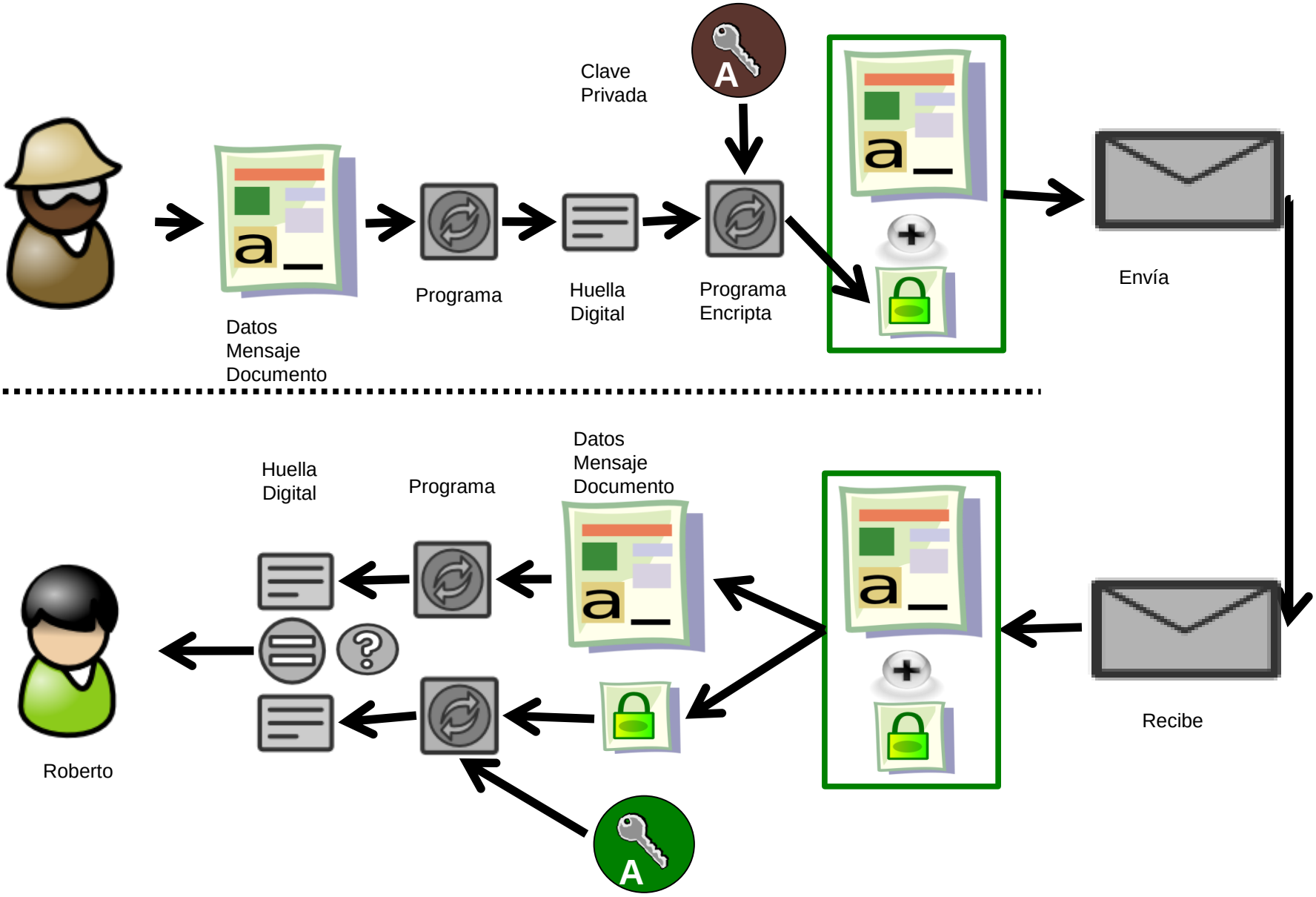
Confianza

- Quien garantiza la identidad de las partes?

- Cualquiera puede generar un par de claves y decir que son de Alicia.

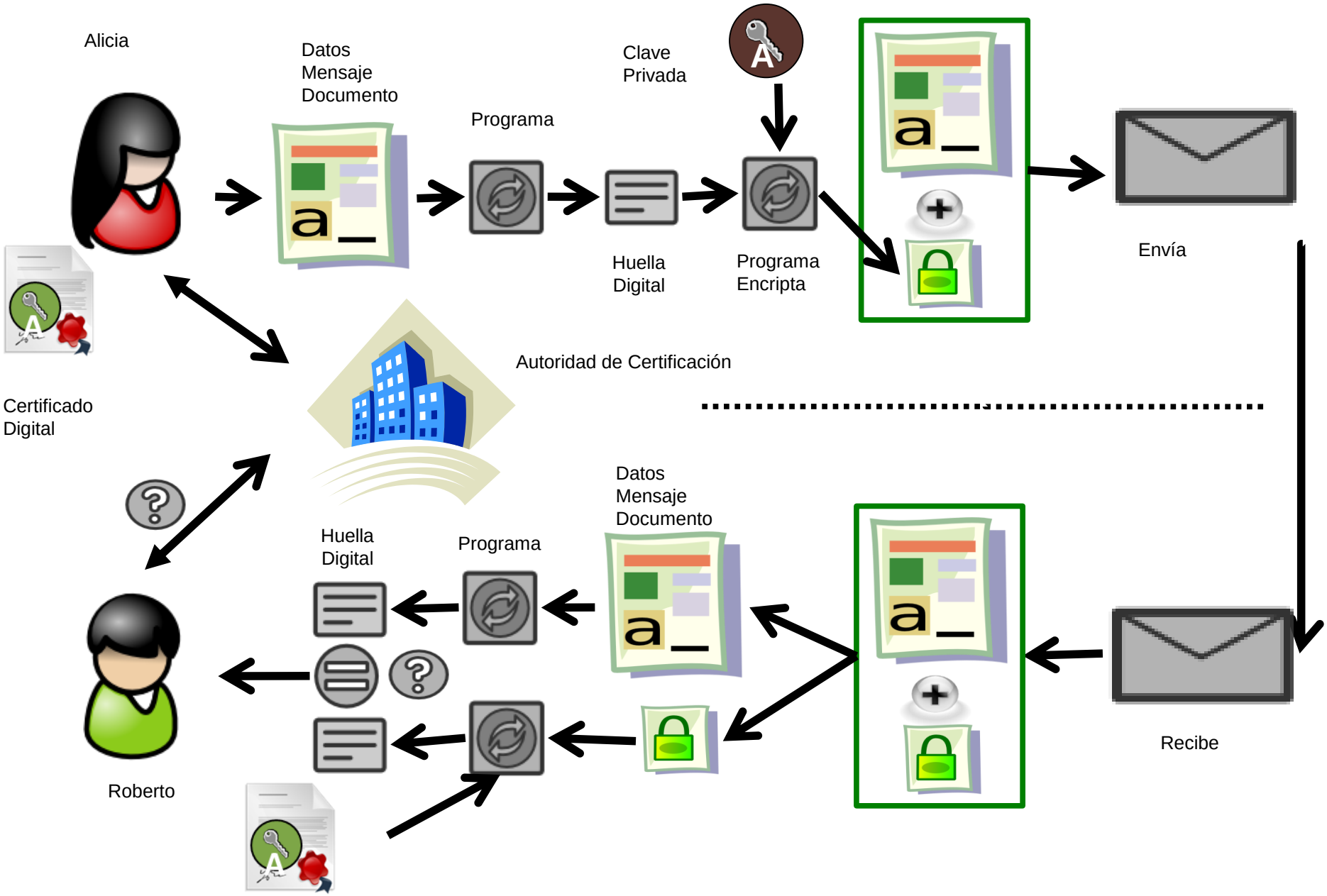
- Es necesario un tercero en confianza.

.


Clave
Privada
A
Datos
Mensaje
Documento
Programa
Huella
Digital
Programa
Encripta
Envía
Huella
Digital
Programa
Datos
Mensaje
Documento
Recibe
Roberto
A

Confianza

- Quien garantiza la identidad de las partes?
- Cualquiera puede generar un par de claves y decir que son de Alicia.
- Es necesario un tercero en confianza.
- Una Autoridad de Certificación autentica que la clave pública corresponde a Alicia.


Alicia
Datos
Mensaje
Documento
Programa
Clave
Privada
Huella
Digital
Programa
Encripta
Envía
Certificado
Digital
Autoridad de Certificación
Datos
Mensaje
Documento
Huella
Digital
Programa
Recibe
Roberto

CERTIFICADO DIGITAL

Certificado Digital

El Certificado Digital es un documento electrónico, asignado por una Autoridad Certificadora, que relaciona una identidad con una Clave Pública.

Sus componentes principales son:

- Emisor
- Titular
- Un identificador único
- Fecha de emisión
- Fecha de caducidad
- Clave Pública del Titular
- La Firma Digital del emisor

Certificado Digital

Visor de certificados: mail.google.com

General | Detalles

Este certificado se ha verificado para los siguientes usos:

Certificado de servidor SSL

Enviado a

Nombre común (CN)	mail.google.com
Organización (O)	Google Inc
Unidad organizativa (OU)	<No incluido en el certificado>
Número de serie	5E:D7:18:6A:C4:ED:3D:A1

Emitido por

Nombre común (CN)	Google Internet Authority G2
Organización (O)	Google Inc
Unidad organizativa (OU)	<No incluido en el certificado>

Período de validez

Emitido el	09/10/13
Vencimiento el	09/10/14

Huellas digitales

Huella digital SHA-256	DC 34 46 71 69 E4 6E 46 96 94 A3 32 43 7E 5F FD 0C F9 C9 60 7B A3 0C 20 F2 24 DD 9C 43 F4 E5 34
Huella digital SHA-1	12 11 31 73 B3 29 AB C5 10 66 DB 4B 14 EE 2D 1F 48 D1 05 2C

Usos de Certificados

- Firma Digital
- Autenticación
- Cifrado

Ciclo de vida de Certificados

- Emisión
  - Inicio de su vigencia
- Expiración
  - Finalización del periodo de validez
  - Renovación del certificado
- Revocación del Certificado
  - Si la clave privada está comprometida
  - Cambio de datos del Certificado
  - CRLs Listas de Certificados revocados
- Suspensión
  - Revocación temporal

Proceso de Validación de Firma

- Conseguir el Certificado del signatario
- Verificar la validez del Certificado
  - Dentro del periodo de validez
  - Certificado no revocado
  - Firma digital de CA correcta
  - Verificar cadena de confianza
- Verificar la firma digital del hash del mensaje con la clave pública del emisor

INFRAESTRUCTURA DE CLAVE PÚBLICA

Infraestructura de Clave Pública

- Para gestionar el ciclo de vida del certificado se necesitan:
  - Tecnología
  - Personas
  - Políticas
  - Procedimientos
  - Marco Legal

Infraestructura de Clave Pública (PKI)

Es el *conjunto de normas jurídicas, hardware, software, bases* de datos, redes, estándares tecnológicos, personal calificado y procedimientos de seguridad que permiten que distintas entidades (individuos u organizaciones), mediante el uso de certificados digitales como herramienta, se identifiquen entre sí de manera segura al realizar transacciones en redes, especialmente Internet, permitiendo además dotar de autoría e integridad a los documentos digitales.

Objetivo de PKI

Asegurar las comunicaciones en redes de comunicación abiertas mediante el uso de criptografía de clave pública, equivalente al empleo de la firma manuscrita, ensobrado y sellado de documentos en el mundo físico.

Confianza!!

Infraestructura de Clave Pública

- Hay cuatro actores principales:
  - Quien firma
    - Suscriptor
  - Quien necesita verificar la firma
    - Parte que confía
  - Quien certifica que la firma corresponde a una cierta persona
    - Autoridad Certificadora
  - Quien controla el sistema
    - Autoridad de Aplicación

Infraestructura de Clave Pública

- Autoridad de Aplicación (AA)
- Autoridad de Certificación (CA, PSC)
- Titular del Certificado
- Repositorio
- Parte Utilizadora, parte que confía
- Autoridad de Registro (AR)

Autoridad de Aplicación

PKI - Paraguay

Autoridad de Aplicación (AA)
La institución designada en la Ley de Firma Digital es el Ministerio de Industria y Comercio.
Ente regulador

Autoridad de Certificación Raíz (CA Raíz)
Es la base de la cadena de confianza. Encargada de emitir y revocar certificados de Autoridad de Certificación.
Tiene un certificado autofirmado.

.

PKI - Paraguay

Autoridades de Certificación (CA) Prestadores de Servicios de Certificación (PSC)
Encargadas de emitir y revocar certificados. Son terceras partes confiables que dan fe de la veracidad de la información incluida en el certificado.
Firman digitalmente los Certificados de Personas Físicas o Jurídicas.

Autoridad de Registro (AR)
Es la encargada de verificar el enlace entre el certificado y la identidad del titular.
No esta legislado. En Paraguay esta responsabilidad es de las Autoridades Certificadoras

PKI - Paraguay

Autoridad de Validación (AV)
Encargada de comprobar, la validez de los certificados
No está legislado. En Paraguay esta tarea la realizan las Autoridades de Certificación.

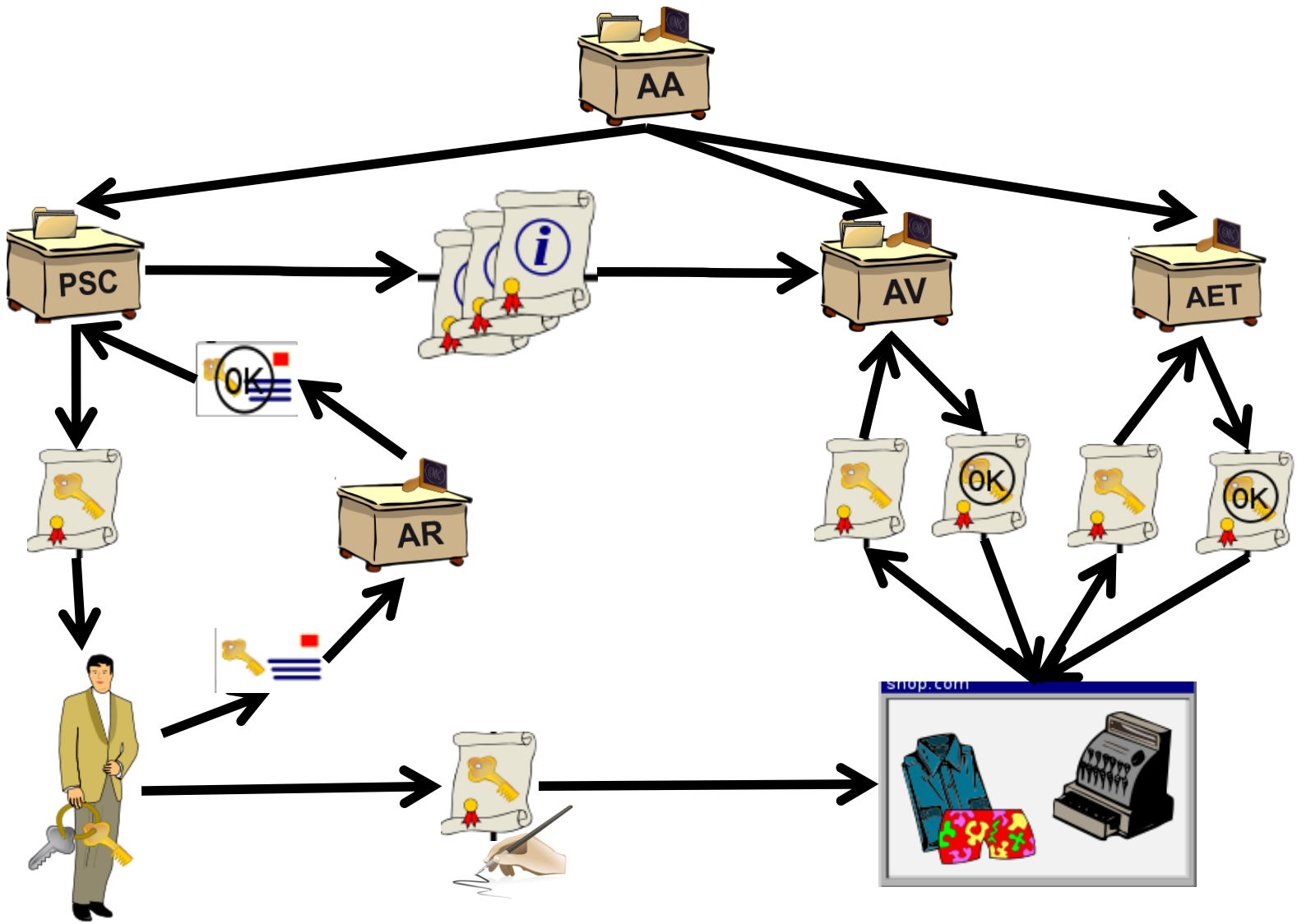
Autoridad de Estampado de Tiempo (AET)
Encargada de firmar documentos con la finalidad de probar que existían en un determinado instante de tiempo
No esta legislado.

PKI - Paraguay

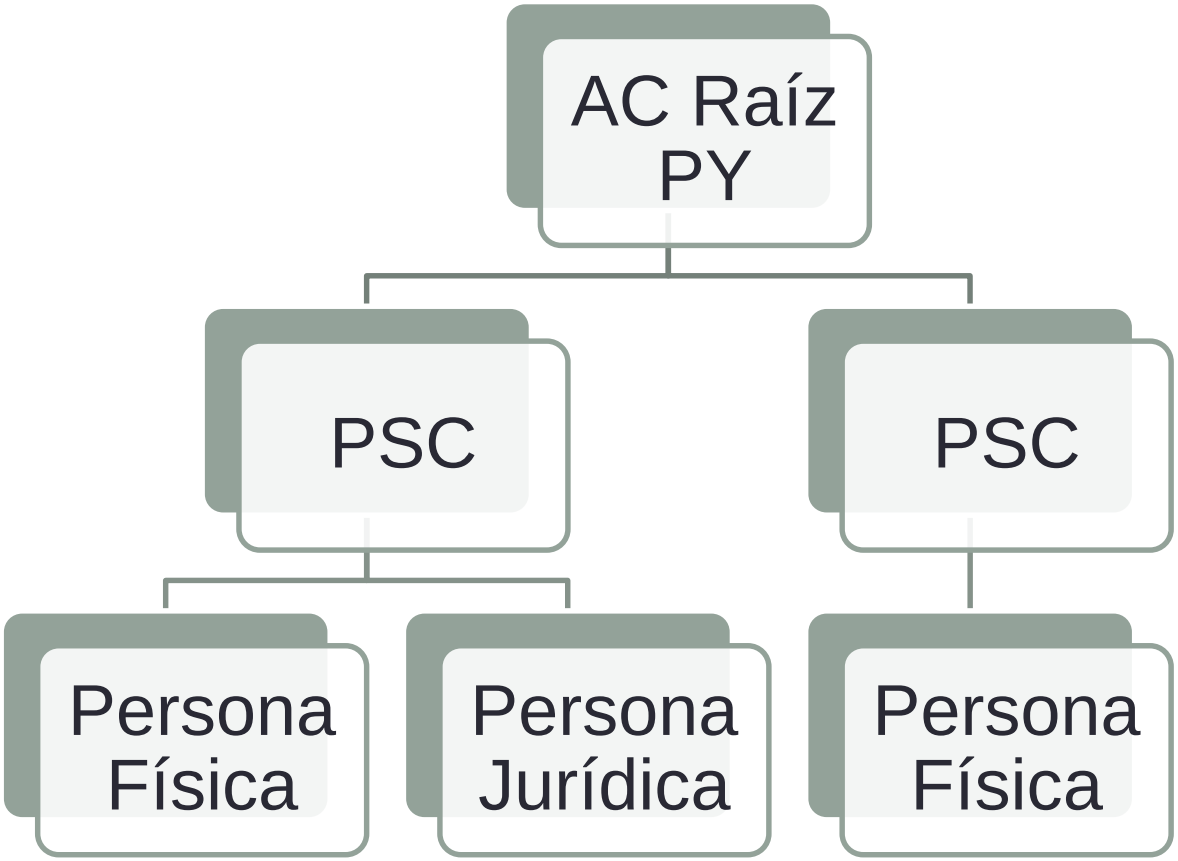
Lista de certificados revocados

Es una lista que incluye los certificados que por algún motivo no tienen validez

Tarea recae en el PSC


AA
PSC
AV
AET
AR
OK
OK
OK
OK
shop.com

PKI - Paraguay



APLICACIONES

Aplicaciones

Digitalización de documentos

Tramitación de expedientes

Trámites bancarios

Certificados Médicos

Autenticación en la Web.

Comercio Electrónico para el pago seguro

Certificados de exportación electrónicos

MUCHAS GRACIAS !!!!

Consultas: cdacak@mic.gov.py
cpdacak@yahoo.com

616 3056 / 214 279

www.acraiz.gov.py