Tilsor

Pilar de la seguridad del gobierno electrónico

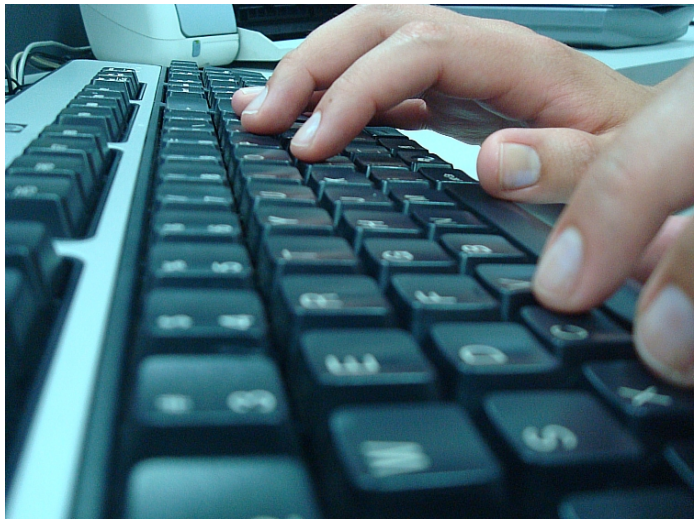
Ing. Eduardo Giménez, PhD

JIAP 2011

Tilsor

- Contexto y marco legal
- ¿Qué es la Firma Electrónica Avanzada?
- Propiedades de seguridad de la FIE
- Soluciones de gobierno electrónico

Tilsor



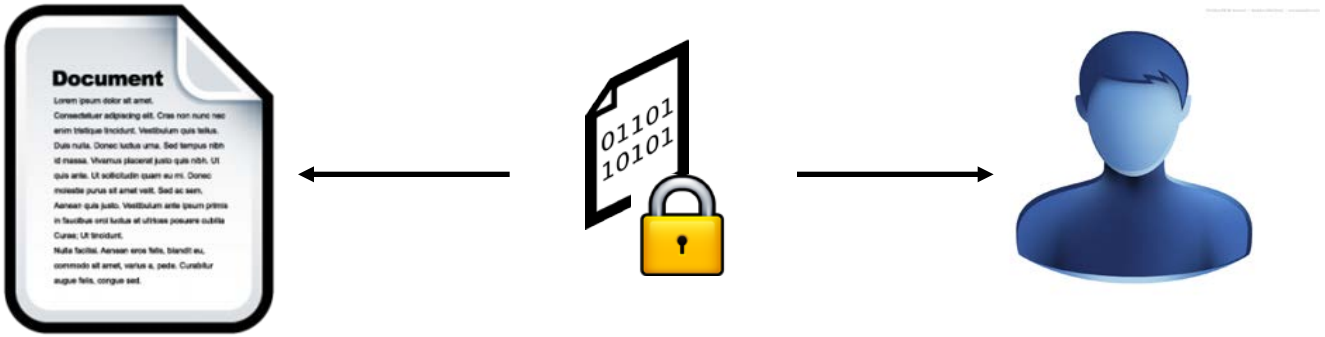
- Menos papel.
- Más servicios públicos remotos.
- Transacciones electrónicas rápidas y seguras.

Tilsor

- Ley 18.600 del 5/11/2009: documento electrónico y firma electrónica
- Reconocen su validez y eficacia jurídica
- Introduce dos conceptos:
  - Firma electrónica
  - Firma electrónica avanzada

Tilsor

- “Los datos en forma electrónica anexos a un documento electrónico o asociados de manera lógica con el mismo, utilizados por el firmante como medio de identificación.”



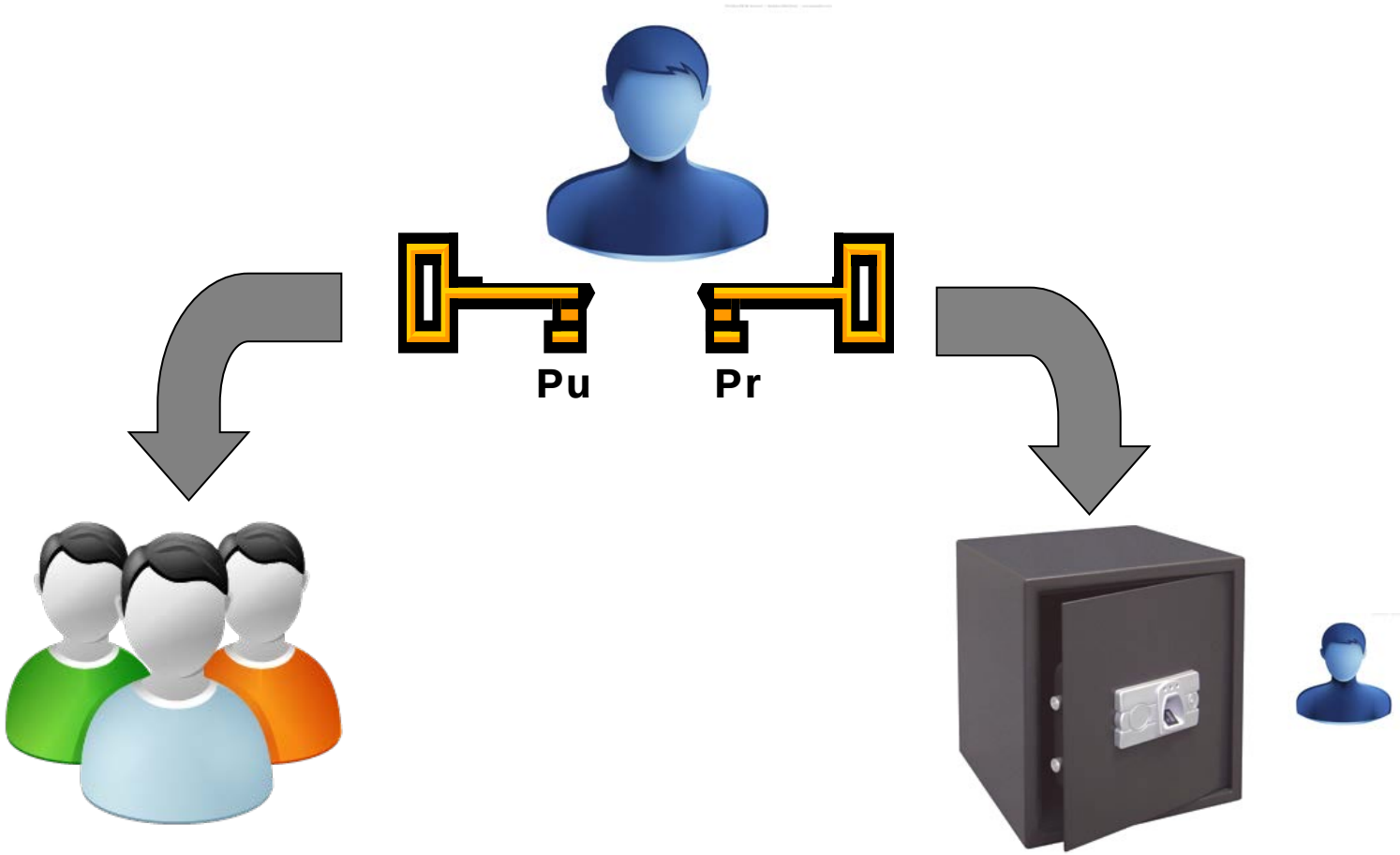
Firma digital

Tilsor

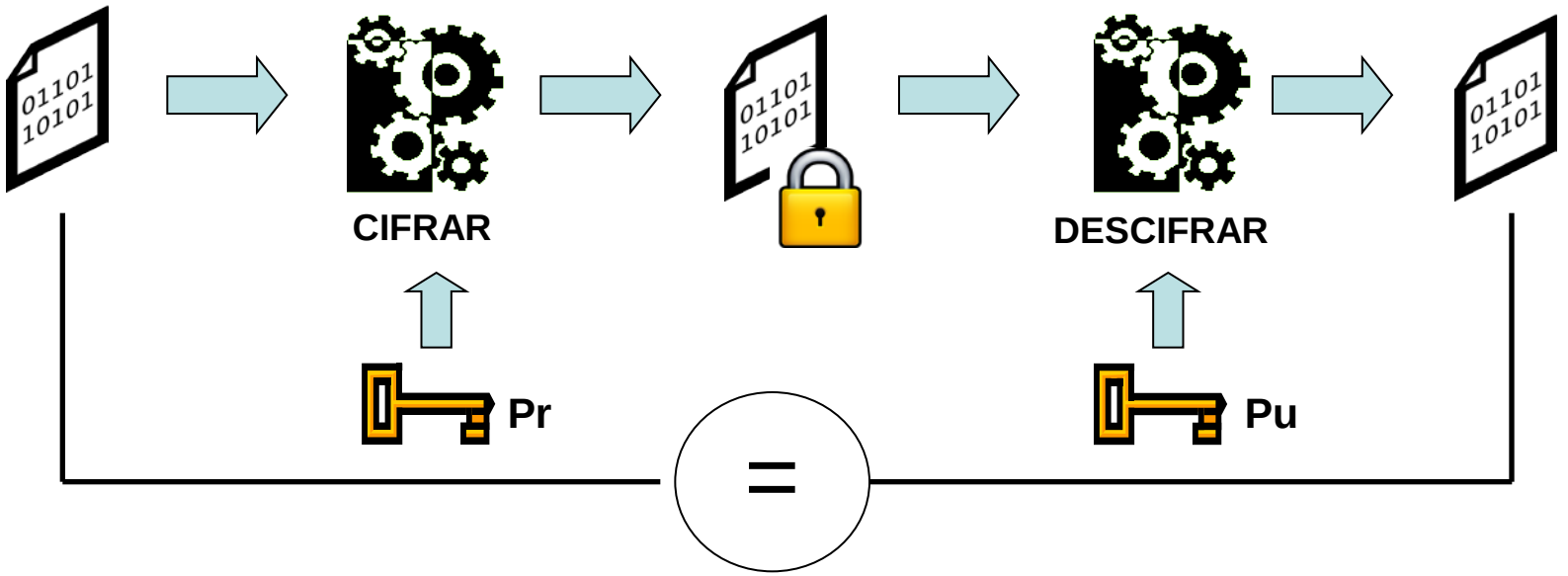
- Firma electrónica que cumple los siguientes requisitos:
  - Requerir información de exclusivo conocimiento del firmante, permitiendo su identificación unívoca.
  - Ser creada por medios que el firmante pueda mantener bajo su exclusivo control;
  - Ser susceptible de verificación por terceros;
  - Estar vinculada a un documento electrónico de tal modo que cualquier alteración subsiguiente en el mismo sea detectable;
  - Haber sido creada utilizando un dispositivo de creación de firma técnicamente seguro y confiable y estar basada en un certificado reconocido válido al momento de la firma.

- ¿Cómo se logra la firma electrónica avanzada?

Tilsor



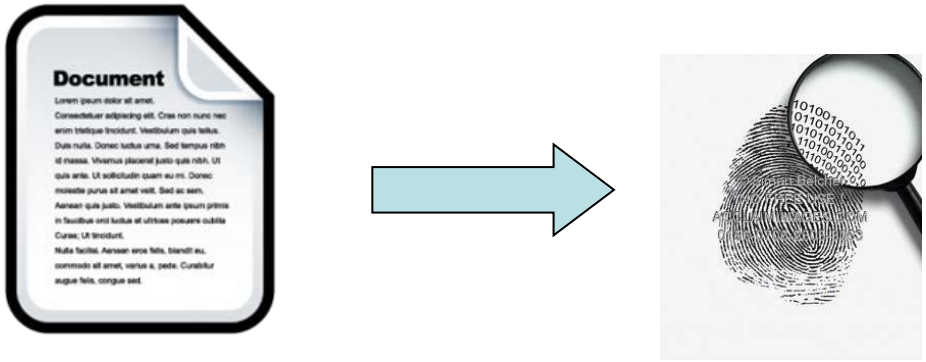
Tilsor



- Sin conocer la clave, no se ha descubierto otro proceso más sencillo que enumerar los resultados uno por uno.

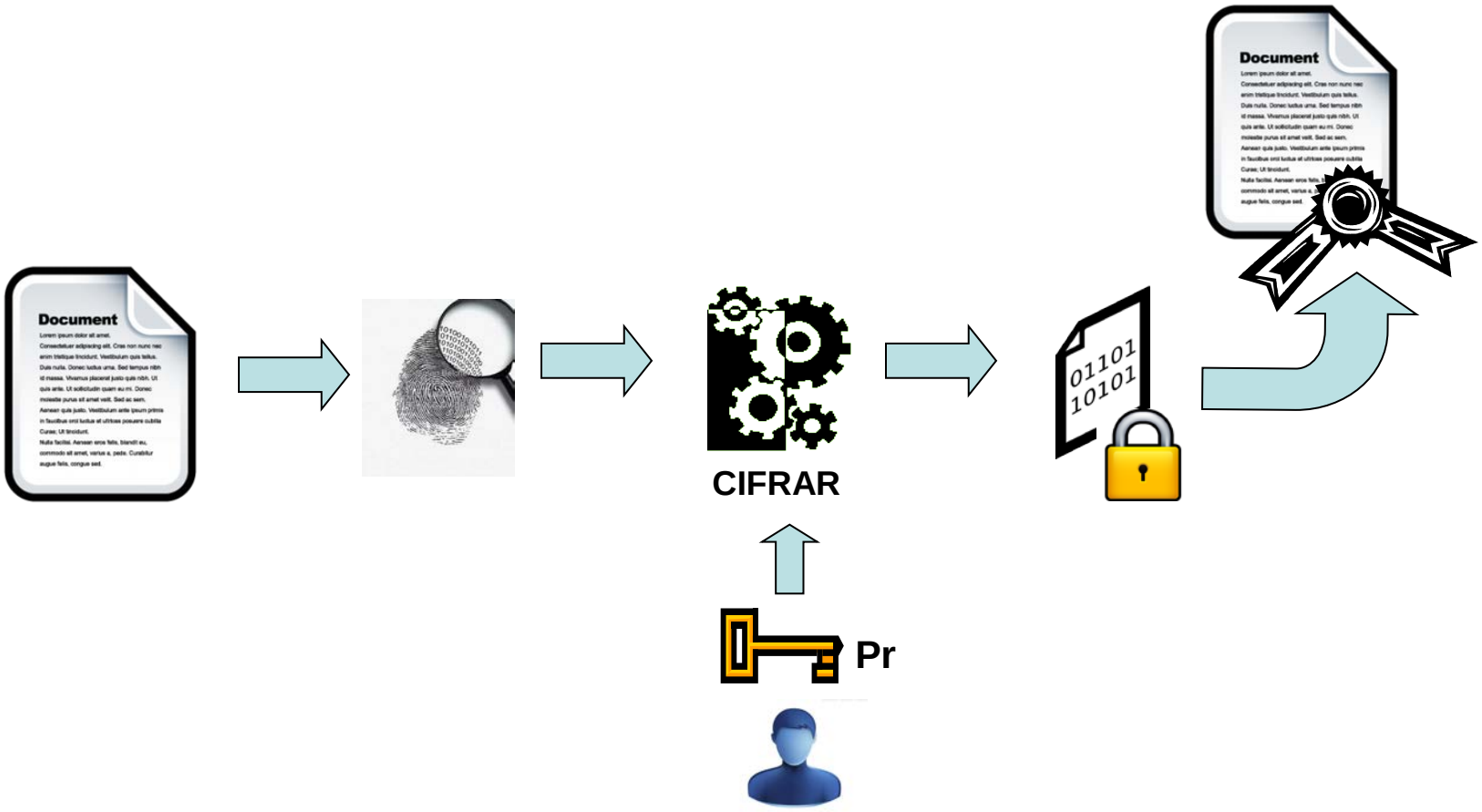
- La probabilidad de que otra clave produzca el mismo resultado es cero.

Tilsor

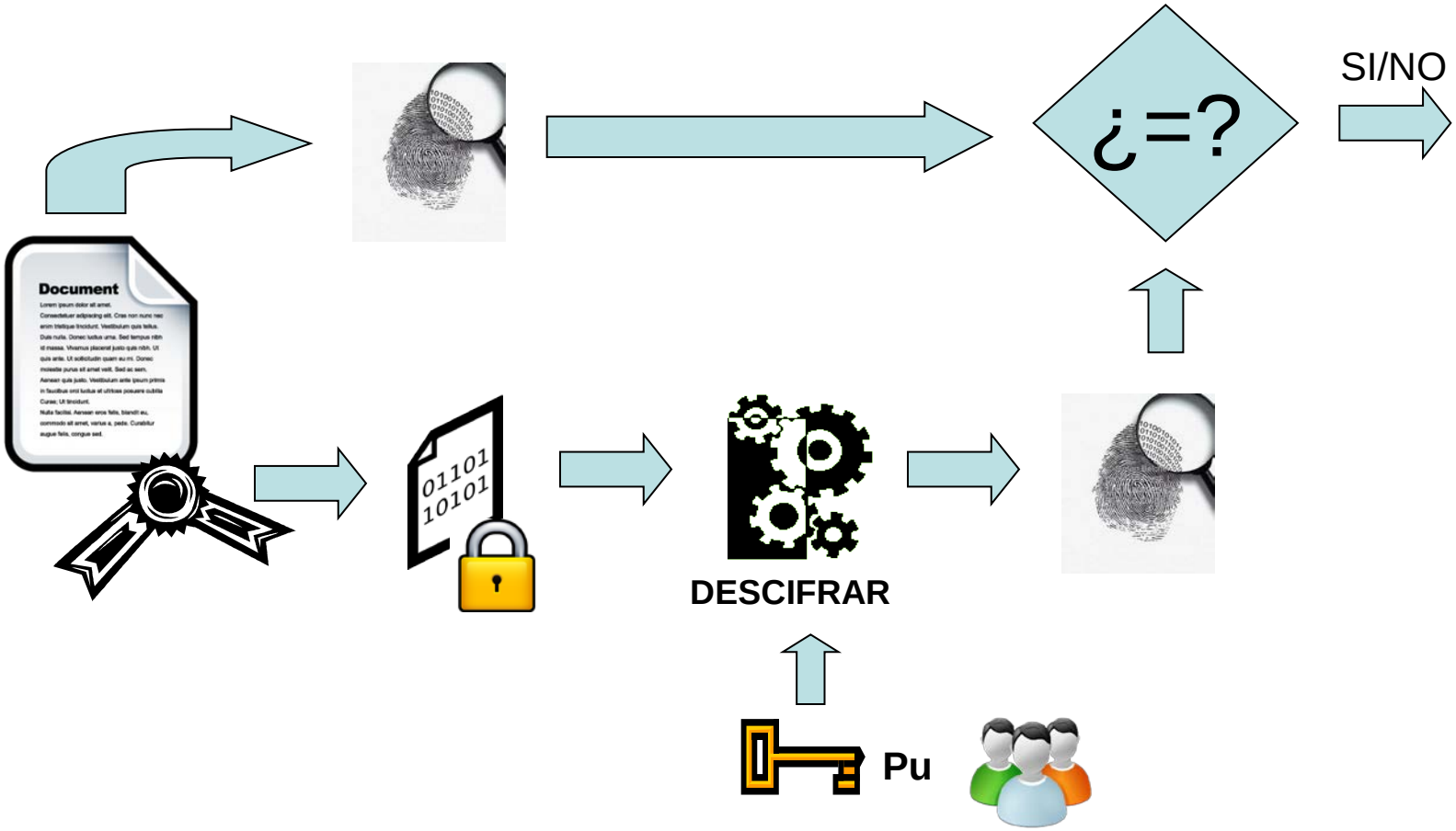


- Sensiblemente más pequeña que el documento.
- Huellas diferentes implican documentos diferentes.
- Es complejo invertir la función o encontrar un documento diferente que tenga la misma huella.

Tilsor



Tilsor



Tilsor

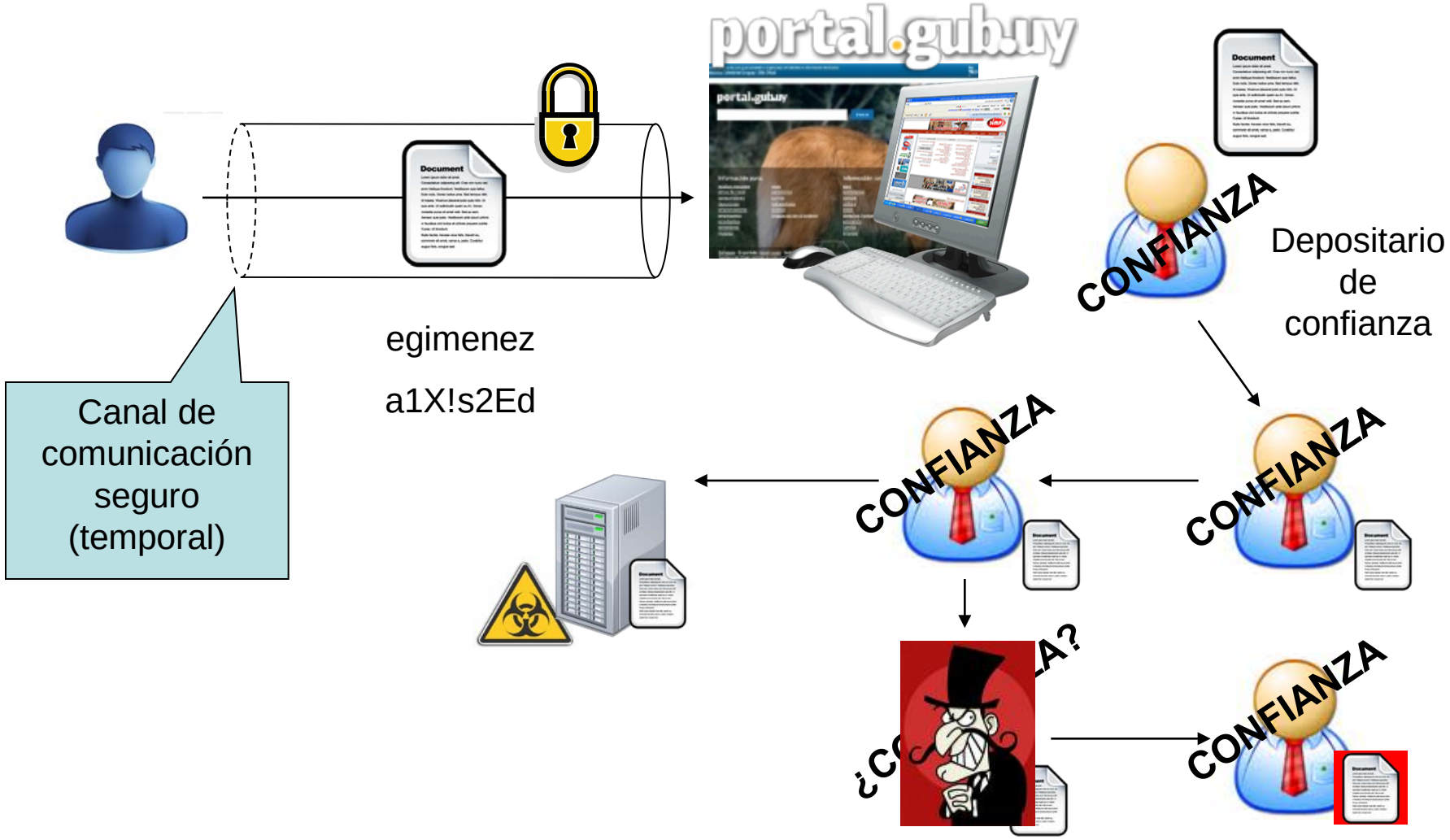
- Autenticidad:
  - El firmante puede ser reconocido inequívocamente.

- Integridad:
  - Cualquier cambio en el documento hace que la huella (y por tanto la firma) sea inválida.

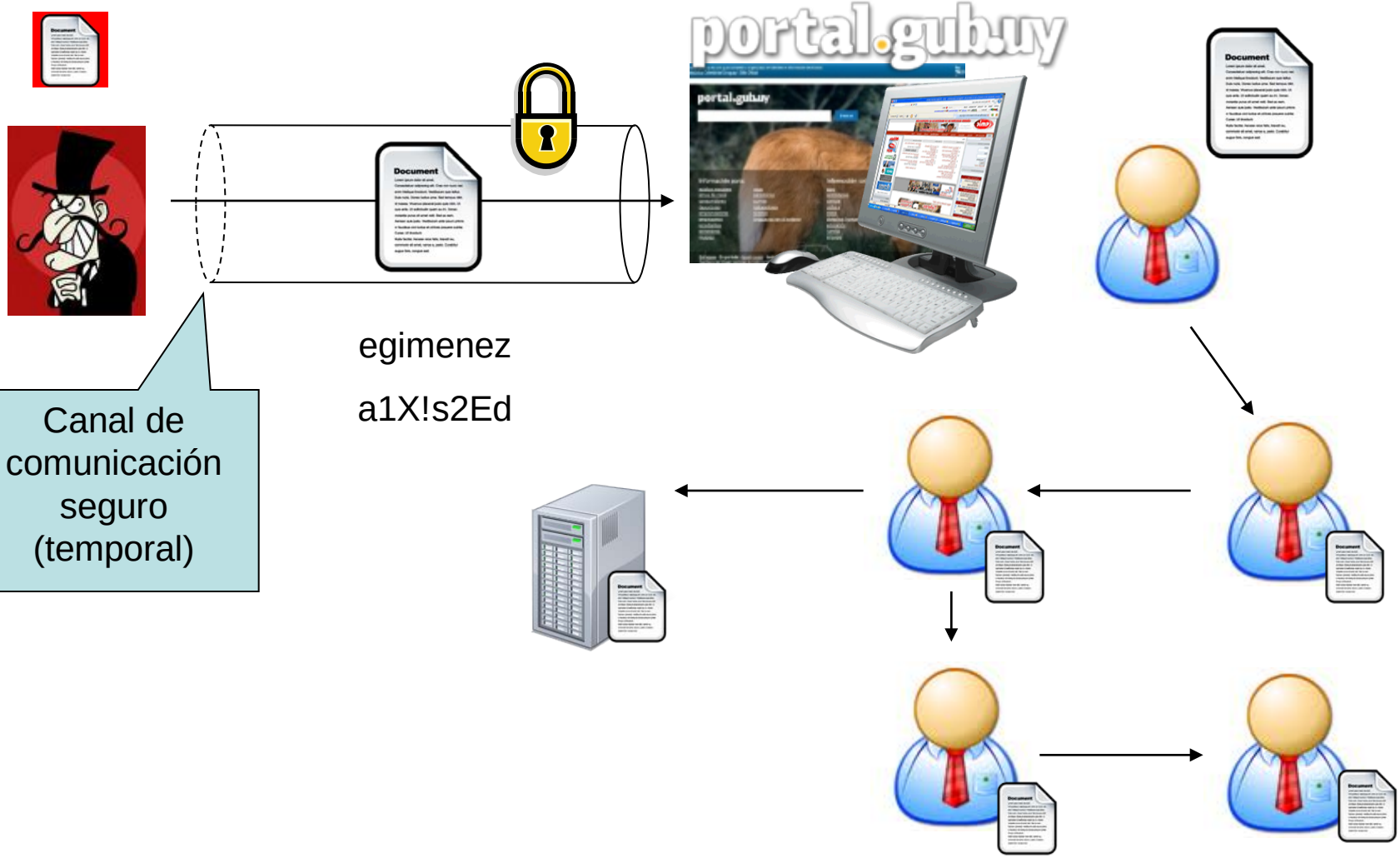
Tilsor

- No repudio:
  - El firmante no puede negar haber firmado el documento.
  - Evidencia que se puede almacenar y que viaja con el documento.
  - Reducción del número de “terceros de confianza” necesarios al proceso.
  - Mayores garantías para los ciudadanos.

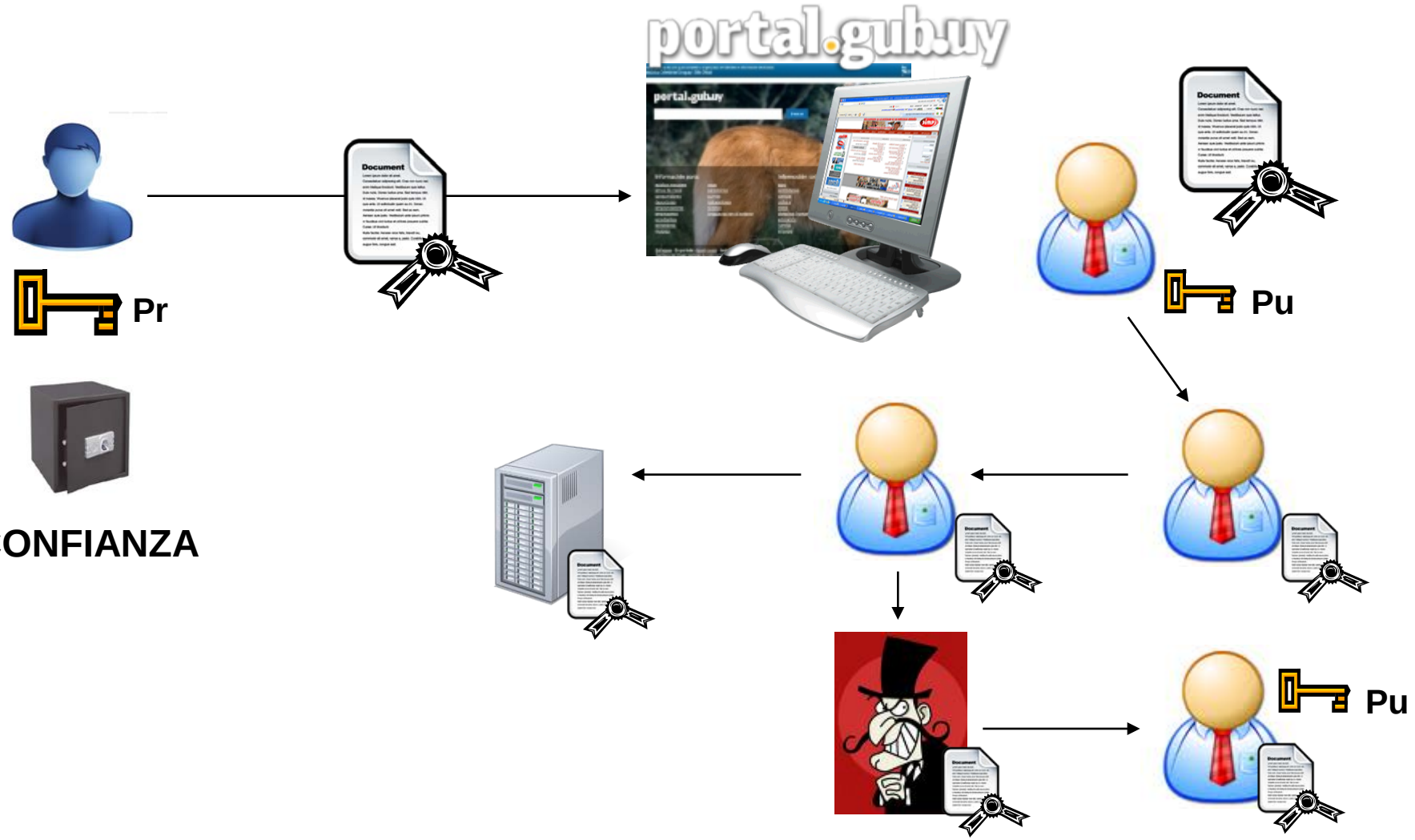
Tilsor


portal.gub.uy
Document
CONFIANZA
Depositario de confianza
egimenez
a1X!s2Ed
Canal de comunicación seguro (temporal)
CONFIANZA
CONFIANZA
CONFIANZA

Tilsor


portal.gub.uy
Document
egimenez
a1X!s2Ed
Canal de comunicación seguro (temporal)

Tilsor

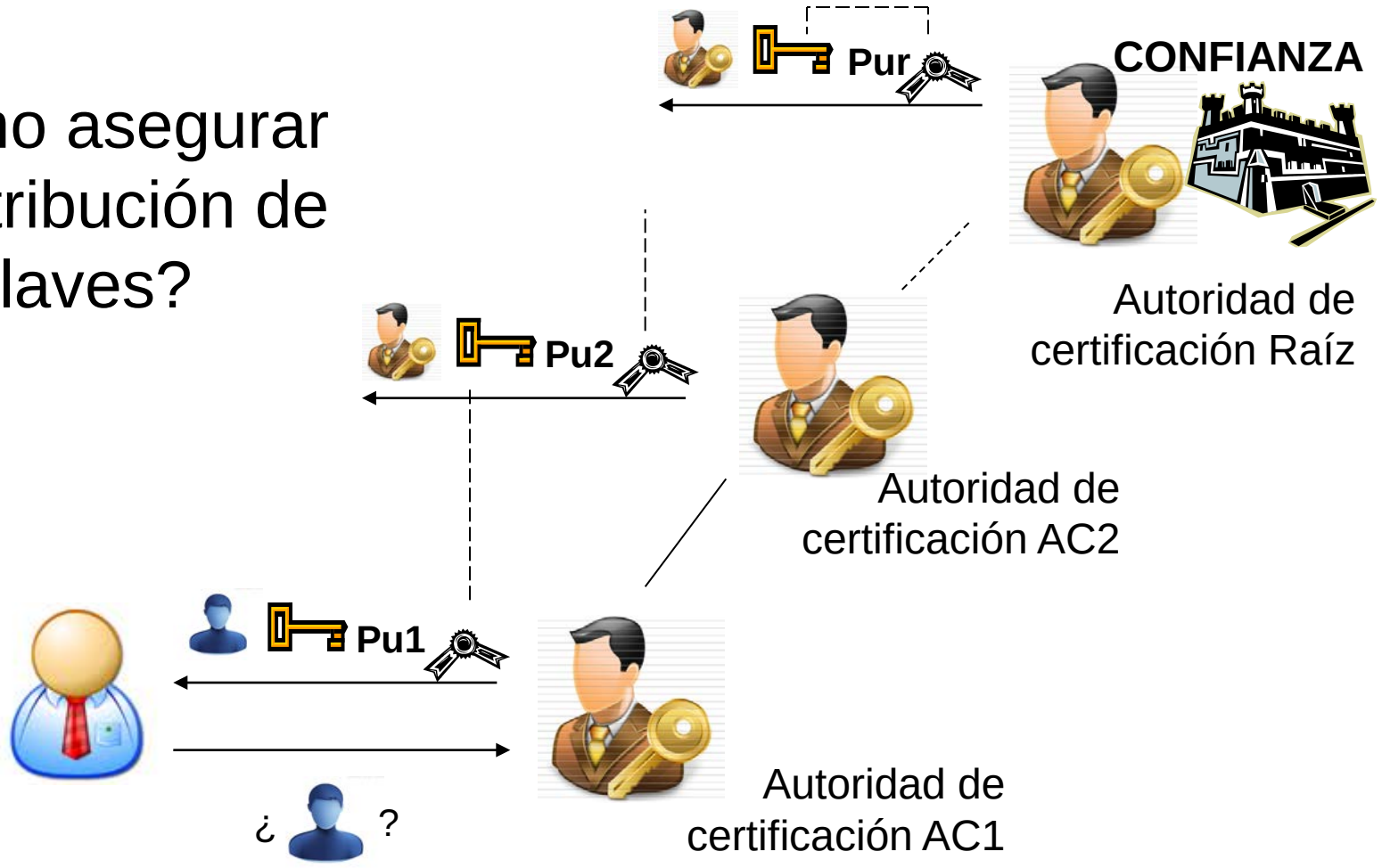


Tilsor

1. Tenemos la calve pública correcta
2. Siempre vamos a poder verificar la firma
3. Solo el firmante posee la clave privada

Tilsor

¿Cómo asegurar la distribución de claves?



Tilsor

- Ciertos documentos deben ser conservados legalmente por decenas de años.
  - Ejemplos: facturas, títulos de propiedad, etc.

- Almacenar solo la firma no es suficiente:
  - Las claves pueden perderse o ser robadas.
  - Las AC pueden cesar su actividad.
  - Los algoritmos de criptografía pueden volverse obsoletos, ser quebrados, o depender de muchos parámetros implícitos.

Tilsor

- Solución: volver la firma digital autocontenida.

- Se adjunta al documento información sobre:
  - Algoritmo utilizado para genera la firma
  - Parámetros del algoritmo
  - Cadena de certificados de los que la firma depende
  - Estado de cada certificado utilizado (válido, revocado, etc)
  - Sellos de tiempo de cada elemento utilizado
  - Sellos de tiempo regulares que atesten reverificación.

- Crucial: utilizar estándares para estructurar y almacenar esta información (Ejemplo: XAdes).

Tilsor

Listas de revocación de claves (CRL/OSCP).

Autoridad de certificación

Pu ×
Pu ×
Pu ×
Pu ×

Dispositivos de almacenamiento portátiles de alta seguridad.

Chip

Pr

Tilsor

- Firma electrónica que cumple los siguientes requisitos:

√ Requerir información de exclusivo conocimiento del firmante, permitiendo su identificación unívoca.

√ Ser creada por medios que el firmante pueda mantener bajo su exclusivo control;

√ Ser susceptible de verificación por terceros;

√ Estar vinculada a un documento electrónico de tal modo que cualquier alteración subsiguiente en el mismo sea detectable;

√ Haber sido creada utilizando un dispositivo de creación de firma técnicamente seguro y confiable y estar basada en un certificado reconocido válido al momento de la firma.

Tilsor

- Las organizaciones deberían contar con una plataforma de firma que:
  - encapsule servicios que serán necesarios para muchas aplicaciones de gobierno electrónico,
  - respete estándares internacionales,
  - su implementación asegure las propiedades de seguridad deseadas
  - pueda funcionar como un servicio horizontal no intrusivo por todas las aplicaciones de gobierno electrónico.

Tilsor

tb·solutions

Tilsor

Firma y PKI

Registro Telemático

Notificaciones Electrónicas

Portafirmas

Factura Electrónica

Pasarela de Pagos

Archivo Confidencial

Contratación Electrónica

Tilsor

- Servicios de AC Raíz del Uruguay y de una AC subordinada de primer nivel.
- Servicios de:
  - generación de claves en ambiente de máxima seguridad,
  - creación de Autoridades de Certificación,
  - políticas de seguridad centralizadas,
  - publicación de listas de revocación,
  - validación de certificados,
  - etc.
- Licitación AGESIC 01-2010 ✓
- Ceremonia de claves de la AC Raíz en 2011

Firma y PKI

Tilsor

AGESIC

tb·solutions

Autoridad de certificación Raíz

Tilsor

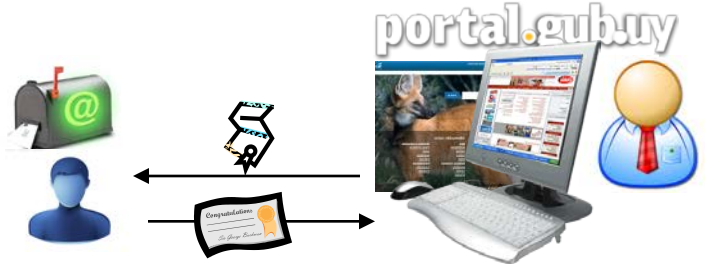
- Solución para integración de procesos de registro de documentos.
- Asientos de entrada y salida, consulta de documentos hacia y desde una organización pública.
- Servicios de:
  - Firmado de formularios,
  - Acuse de recibo de documentos,
  - Sellado de tiempo,
  - Manejo de calendario de días hábiles de la organización.

Registro Telemático

Tilsor

- Solución para procesos de notificaciones fehacientes (telegrama colacionado).
- Dirección única del ciudadano en la cual recibir todas las notificaciones de la administración.
- Servicios para:
  - Manejo de plazos de vencimiento,
  - Constancias de rechazo,
  - Evidencias del momento de emisión y recepción de la notificación, etc.

Notificaciones Electrónicas

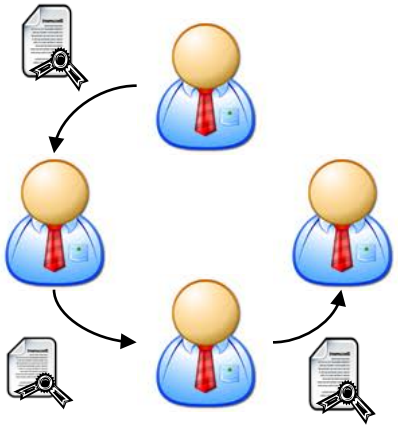


Tilsor

- Punto de gestión único para gestionar todas las firmas de un documento o trámite.

Portafirmas

- Servicios para:
  - Entrada de documento a firmar,
  - Firma secuencial,
  - Firma paralela,
  - Rechazo,
  - Delegación,
  - Portal de consulta de documentos a firmar.



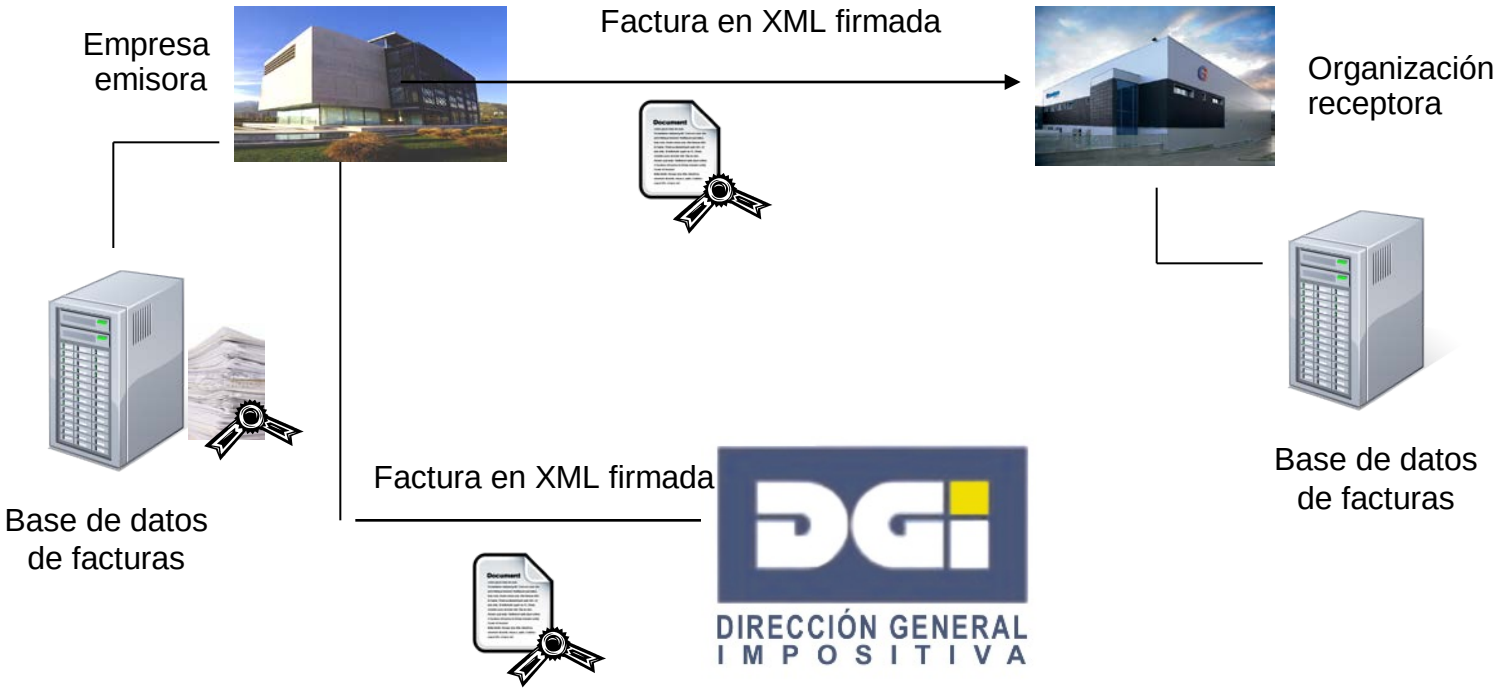
Tilsor

- Solución para procesar las facturas electrónicas de proveedores y clientes de una organización.

- Servicios de:
  - Recepción y verificación de facturas de proveedores,
  - Firma y envío de facturas para clientes y DGI,
  - Almacenamiento de facturas

Factura Electrónica

Tilsor


Empresa emisora
Factura en XML firmada
Organización receptora
Base de datos de facturas
Factura en XML firmada
Base de datos de facturas
DIRECCIÓN GENERAL IMPOSITIVA

Tilsor

- Un gobierno electrónico eficiente y seguro debe reposar sobre garantías sólidas.
- Esas garantías son aportadas por la firma digital avanzada.
- La firma digital debería ser concebida como un servicio horizontal.
- Sobre ese servicio pueden construirse numerosas aplicaciones que disminuirán el papel y permitirán un servicio público más rápido y seguro.

Tilsor

Tilsor

Muchas gracias