La Identidad digital como factor habilitador de e-government .

Agosto 7, 2015

SAFRAN
Morpho

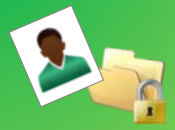
LA GESTION DE IDENTIDAD

1 ENROLAMIENTO

2 VERIFICACIÓN

RECHAZAR

AUTORIZAR



3 BD POBLACIÓN

6 USO DEL DOCUMENTO (e-trust)

5 ENTREGA DEL DOCUMENTO

4 PERSONALIZ. DEL DOCUMENTO

SAFRAN Morpho

BUENAS PRACTICAS DE IMPLEMENTACIÓN DE UN SISTEMA DE GESTION DE IDENTIDAD NACIONAL

ENROLAMIENTO

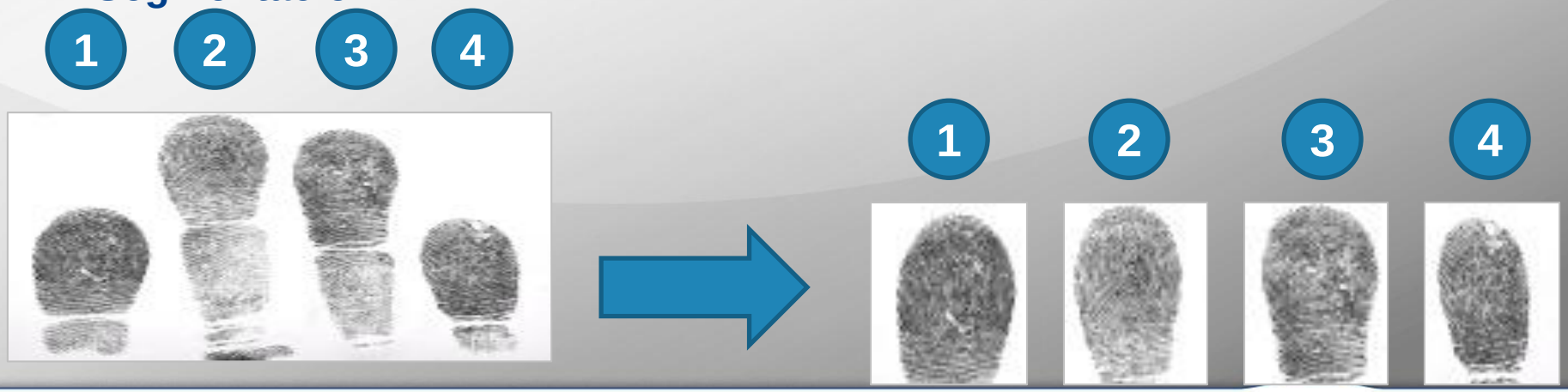
- Menores de 18 años usando algoritmo Juvenil , 18+ usando el algoritmo estándar
- Gestión de la captura y cotejo de Retrato siguiendo normas ICAO (posición cabeza, buena iluminación, fondo de un color, etc)
- Capacitar a los funcionarios en la correcta captura de biométricos para asegurar la calidad.
- toma de huellas rodadas 4-4-2,
- Integración con sistema de registro civil (coherencia con datos anteriores tales como Reg civil, T.I, etc)
- Formato de imagen de las huellas en WSQ
- Formato de la minucia de la huella en ISO,

SAFRAN Morpho

BUENAS PRACTICAS DE IMPLEMENTACIÓN DE UN SISTEMA DE GESTION DE IDENTIDAD NACIONAL

MOTOR BIOMETRICO

- Multi-biometría Fingerprint, Face, Iris y hacer busquedas en paralelo.
- La precisión biometrica debe ser un requisito indispensable (FAR, FRR).
- Gestión de multiresgistro para una misma persona.
- Algoritmos basados 100% en software
- No se usa HW propietario
- Implementación independiente de los equipos utilizados
- Integración sencilla con otros sistema: concepción basada en tecnología estándar como JMS/XML y servicios web.
- **Segmentación:**

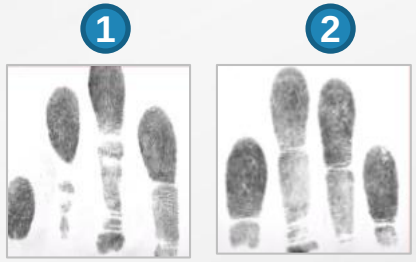


SAFRAN Morpho

BUENAS PRACTICAS DE IMPLEMENTACIÓN DE UN SISTEMA DE GESTION DE IDENTIDAD NACIONAL

MOTOR BIOMETRICO

- Corrección automática de errores.



Corregir los errores de mano invertida.

Corregir los errores de secuencia

SAFRAN Morpho

BUENAS PRACTICAS DE IMPLEMENTACIÓN DE UN SISTEMA DE GESTION DE IDENTIDAD NACIONAL

MOTOR BIOMETRICO

- El algoritmo de cotejo debe haber ocupado al menos una de las primeras 5 mejores posiciones en precisión biométrica de las Siguientes evaluaciones NIST :
  - 2013 : IREX IV .
  - 2012: FPVTE.
  - 2011: IREX III.
  - 2010: Multiple Biometrics Evaluation (MBE2010) .
  - 2005: Ongoing Minutiae Interoperability Exchange Test (OMINEX)
  - 2006: Iris Challenge.
  - 2013: NIST Proprietary Fingerprint Template (PFT) Evaluation.
  - 2008: MINEX II
- Escalabilidad del sistema y actividades de mantenimiento del sistema deben poder ejecutarse “en caliente”

.

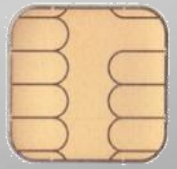
DOCUMENTOS SEGUROS:

En el aspecto Físico

- Información personal: Foto y textos.
- Características de seguridad

En el aspecto digital

- Información personal
- Seguridad: Bóveda digital
- Certificación Common Criteria garantiza niveles de seguridad.
- Criptografía para protección de datos:
  - Symetric: AES, 3DES.
  - Asymetric: Se requiere una llave para encrip/desencip RSA, elliptic curve)



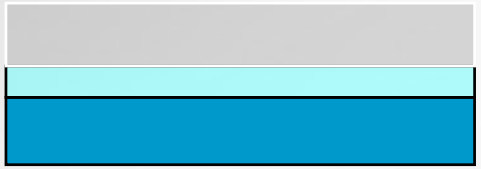
SAFRAN Morpho

DOCUMENTOS NO HOMOGÉNEOS (LAMINADOS)

Capa transparente

Adhesivo

Sustrato de Papel



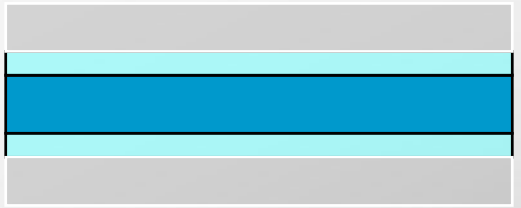
Capa transparente

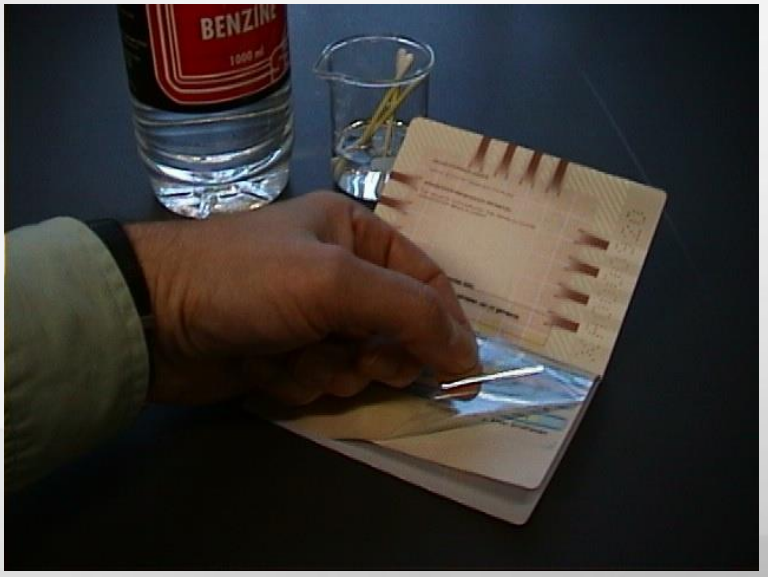
Adhesivo

Sustrato

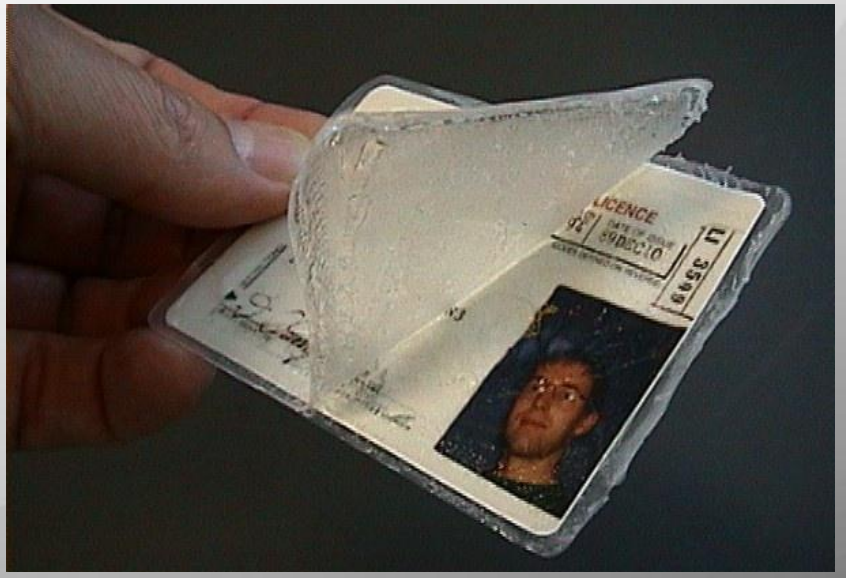
Adhesivo

Capa transparente





Deslaminado con ayuda de un alcohol de limpieza



Separación con ayuda de temperatura

SAFRAN Morpho

POLICARBONATO

Antes

Después

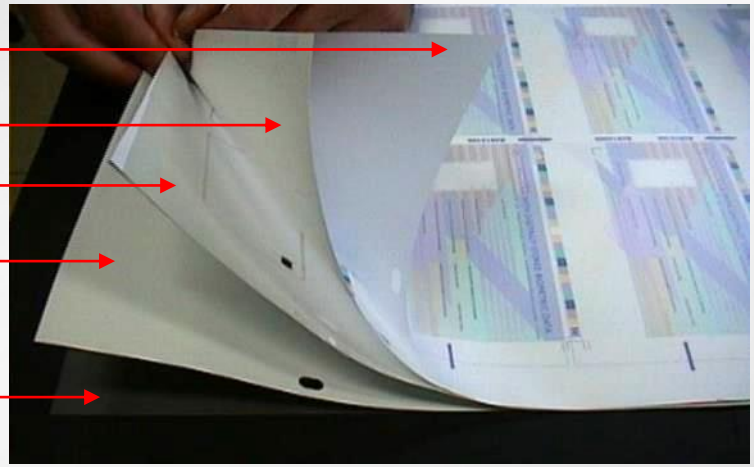
Capa transparente

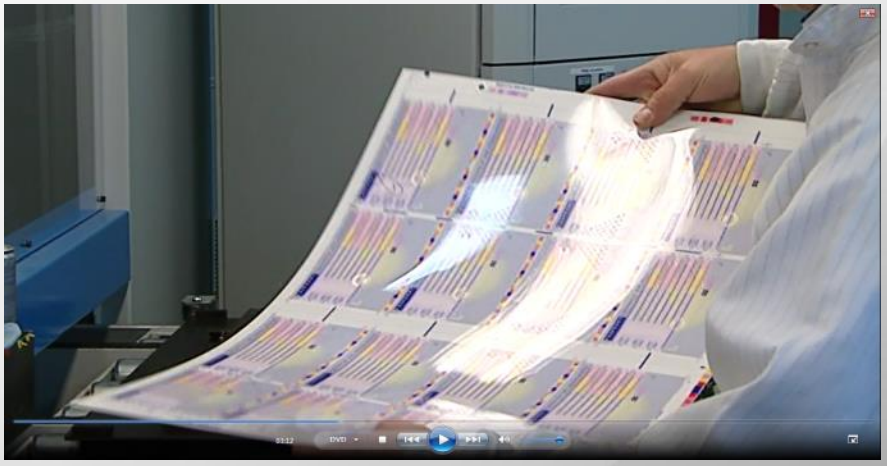
Capa impresa

Núcleo (Chip)

Capa impresa

Capa transparente





Ventajas

- ✓ **Seguridad**
- ✓ **Durabilidad**
- ✓ **La mayoria de seguridades nivel 1 se soportan en material policarbonato.**
- ✓ **Posibilidad de usar lentes en la superficie del documento**
- ✓ **No requiere insumos durante la producción.**

RECOMENDACIONES DE LA ICAO

Security of MRP production and issuance facilities

4. The State issuing the MRP shall ensure that the premises in which the MRP is printed, bound, personalized and issued are appropriately secure and that staff employed therein have an appropriate security clearance. Appropriate security shall also be provided for MRPs in transit between facilities and from the facility to the MRP's holder. Appendix 3 to this Section provides recommendations as to how these requirements can be met.

5. Control of issuing facilities

5.1 A State should consider issuing all passports from one or, at most, two centres. This reduces the number of places where blank documents and other secure components are stored. The control of such a central facility can be much tighter than is possible at each of many issuing centres. If central issuance is adopted, the provision of centres where applicants can attend interviews is required.

Uno o máximo dos centros de personalización debidamente protegidos por país.

SAFRAN Morpho

BENEFICIOS DE UN E-ID

Beneficios para el gobierno.

Reducción de fraude y robo de identidad

Firma digital

Desarrollo de eServices

Reduce carga administrativa

eTravel

Beneficios para Ciudadanos / Clientes.

Confianza en una identidad primaria

Conveniencia

criptografia

BIOMETRICS

SAFRAN Morpho

IDENTIDAD DIGITAL Y CONFIANZA ELECTRÓNICA (E-TRUST)

E-Trust

E TRUST

El mundo de hoy se caracteriza por:

- Un crecimiento exponencial de proveeedores de servcios digitales.
  (inmenso y diversificado)
- Incremento del “mobility” de las personas.
  (reduciendo distancias).
- Cultura de globalización
  (menos barreras y más rapido).

En el cual , los individuos (ciudadanos) tienen una posición relevante.

(ejerciendo sus derechos & cumpliendo sus obligaciones)

SAFRAN Morpho

E TRUST

Misión:

- **Establecer un circulo de confianza entre el ciudadano y los proveedores de servicio en el mundo digital basado en la cedula electrónica de identidad..**

Cómo:

- **Simplificando el uso de la tecnología**
- **Sin intervenir el negocio de los proveedores.**
- **Facil acceso a la platafoma.**
- **Respetando la privacidad del ciudadano.**
- **Compartiendo la plataforma para el sector publico y privado.**
- **…**

E TRUST – ARQUITECTURA ALTO NIVEL

A) SMART ID CARDS

- ID application
- Firma dogital (PKI)
- Match on Card

B) REPOSITORIO DE IDENTIDAD

- Atributos
- Biometricos
- Validación de derechos

Solution de Identificación

SAFRAN Aleat

Plataforma de servicios de ident.

eTRUST

servicios Identidad

Servicios Transaccionales

Sector Publico "eGovernment"

Private Sector "eServices" (Bancos, Salud, Telco …)

SAFRAN Morpho

E TRUST

Identidad & Servicios Transaccionales

STRONG AUTHENTICATION
(Verificar la identidad del ciudadano cuando accesa un servicio)

Firma Digital
(Crear un firma electrónica sujeta a una prueba legal universal)

E-Trust

Elegibilidad (Eid Data)
(Crear un firma electrónica sujeta a una prueba legal universal)

Derivación
(A otros contenedores)

Auditoría
(Trazabilidad segura)

Ejemplo de casos de uso

- LOGIN A BANCOS
- PAGO SEGURO
- APERTURA DE CUENTAS

- TRANZAR ACCIONES
- COMPRAR PRODUCTOS
- PRESTAMOS

- SALUD
- E- INVOICING

SAFRAN Morpho

E TRUST – CASOS DE USO

SECTOR PUBLICO		SECTOR PRIVADO
• Tax Declaration • Health Data • ID Check • Birth Certificate • Lost or Stolen EID • Voting	     	• Online Banking Login • Secure Payment • Account Opening • Buying Financial Product • Loan Subsription • eSafe • Paperless Invoices

STRONG AUTHENTICATION

Autenticación es un medio para verificar la identiad del ciudadano a recursos , servicios y operaciones sensibles.

Factores de autenticación tradicionales.

Login/password, OTP, OTP-SMS, EMV CAP/DPA, or by certificate.

Factores de autenticación innovadores

Biometric (Fingerprint, voice, facial, iris recognition) and mobile and cloud solution.

SAFRAN Morpho

MULTIPLES FACTORES DE AUTENTICACIÓN

Elemento seguro en hardware

Puede ser protegido por:

- Smart card
- UICC
- eSE
- Token
- Mobile Connect

Mobile Connect

Elemento seguro en Software

Es protegido con una combinación smartphone / cloud /HSM system

smartPhone

Cloudcard

Factor de activación

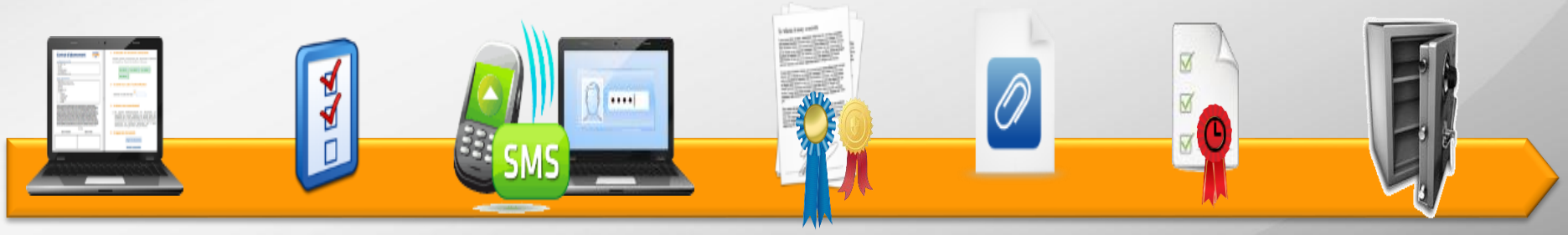
El usuario tiene el control del elemento seguro con un PIN (password) y/o una autenticación biometrica

SAFRAN Morpho

FIRMA DIGITAL & GESTIÓN DE PRUEBA

➔ Solución e-contracting

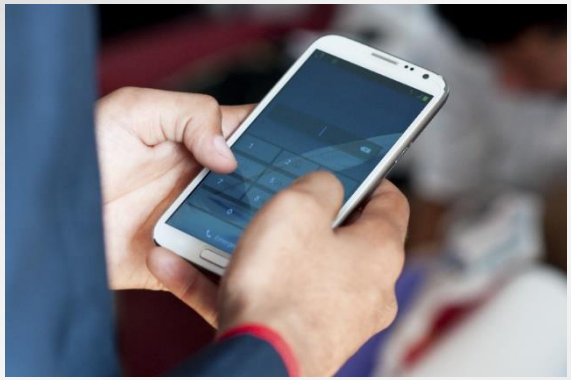
- Administración y trazabilidad de la transacción
- Autenticación, sello y firma personal
- Una prueba legal de la transacción



SAFRAN Morpho

CLOUD CARD

Morpho Cloudcard



Morpho Cloudcard es una identidad electronica (e-ID) basado en un sistema distribuido entre el propietario del dispositivo (smartphone) y un sistema en la nube (Cloud).

CloudCard

Multi uso

- STONG AUTHENTICATION
- TRANSACTION AUTHORIZATION
- DIGITAL SIGNATURE

Multi factor

- RECO FACIAL
- HUELLA
- PIN CODE

SAFRAN Morpho

CLOUD CARD

Cloudcard hace un balance perfecto entre Seguridad, Mobilidad y TCO

CLOUDCARD SYSTEM

SECURITY

Contra ataques del mercado actual y futuro

MOBILITY

Solucion compatible con todos los tipos de dispositivos(TABLETS, SMARTPHONES)

TCO

Implementacion no requiere HW adcional (SMARTCARDS, TOKENS)

CASO DE EXITO: ALBANIA eSERVICES

3.3 M DNI biometricos

95% de la población

- Transparencia
- Anti fraude
- Mejor servicio

TeServices

Proof of Identity

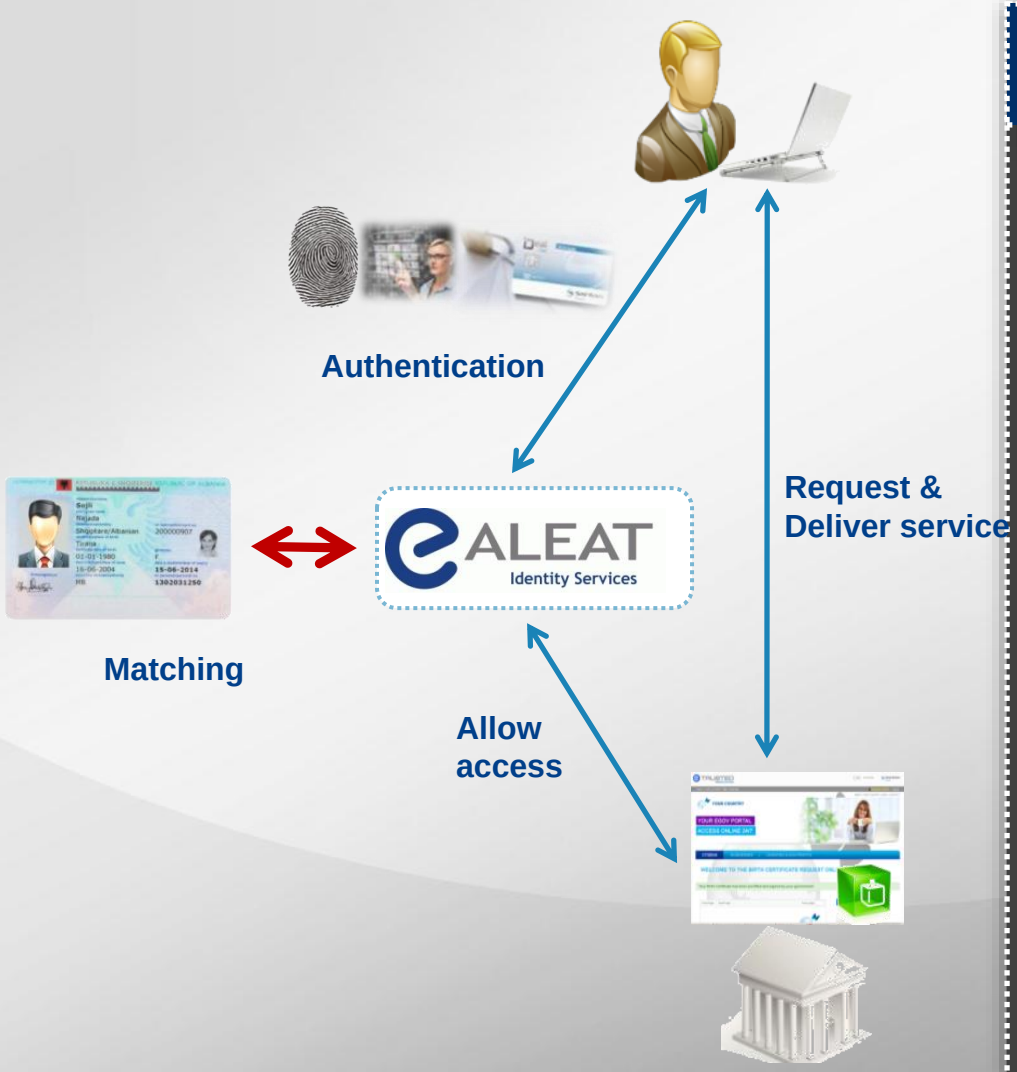
Digital Signature

Proof of Date & Time

= 1 Identidad = 1 DNI

SAFRAN Morpho

AUTENTICACION



Strong Authentication

Prueba de identidad confiable:

Combina card + pin code

OR

Use Biometrics

Fraudes con casi mposibles

→ **Servicios de valor pueden ser ofrecidos online**

SAFRAN Morpho

TRADICIONAL VERSUS E-TRUST

Practica común

Checks the Data against Databases

Service Provider

Personal Data

Code via SMS

Confirms Code

User with Mobile Phone

- Require conexion a la BD paa verificar información !
- No hay prueba de quien está en el telefono !
- Cualquier usuario puede crear una cuenta

eALEAT Identity Services

Service Provider

Authenticated User

Authenticates user

Provides Proven Identity

User with ID Card

Pin or Fingerprint

eALEAT Identity Services

- El DNI garantiza la identidad (User data)
- PIN Code o datos biometricos identifican al usuario
- eAleat provee una prueba de identidad al proveedor

SAFRAN Morpho

DEMO FIRMA ELECTRONICA

PREGUNTAS