IMPLEMENTING THE ePASSPORT IN SPAIN: LESSONS LEARNT

Carlos Gómez
R&D Project engineer
FNMT-RCM
Spain

Lección aprendida No. 1

- Comience por asegurar la seguridad y la credibilidad de los documentos de origen
- Defina un pasaporte electrónico de acuerdo con la normativa OACI
- Establezca un sistema de emisión robusto y seguro
- Establezca una PKI de emisión
- Distribuya sus claves. Suscribase al PKD
- Establezca un programa de control de fronteras electrónicas

Índice

Documentos de origen

- **Registro Civil**
  - Origen eclesiástico (bautismos, matrimonios y defunciones) a partir del Concilio de Trento (1545-1563)
  - Creación a partir de la ley de Registro Civil de 1870
  - Dependiente del Ministerio de Justicia
  - Caracter público y gratuito

Documentos de origen

- **Registro Civil (servicios)**
  - Inscripción
    - Nacimiento, filiación
    - Nombre, apellidos y cambios sobre los mismos
    - Declaraciones de ausencia o fallecimiento
    - Nacionalidad y vecindad
    - Patria potestad, tutela
    - Matrimonio
    - Defunción
  - Certificación
    - Certificación literal de nacimiento para la obtención del DNI

Documentos de origen

- **DNI – Documento Nacional de Identidad**
  - Emitido a partir de la información del registro civil
  - Regulado y obligatorio por ley a partir de 1944
  - Comienzo de su expedición a partir de 1951
  - Introducción del DNI electrónico en febrero de 2006

1937

1951

1996

2006

Lección aprendida No. 2

- Para la emisión de pasaporte electrónico:

Establezca un sistema de emisión de pasaportes electrónicos basado en unos documentos de origen seguros, emitidos por organismos de confianza

Definición del PLM

- **Características físicas - construcción**

Formato

Definición del PLM

- **Características físicas - construcción**

Dimensiones

Definición del PLM

- **Características físicas - construcción**

Página de datos

Lección aprendida No. 3

Documento 9303 de ICAO/OACI sobre pasaportes de lectura mecánica

Definición del PLM

- **Medidas de seguridad**

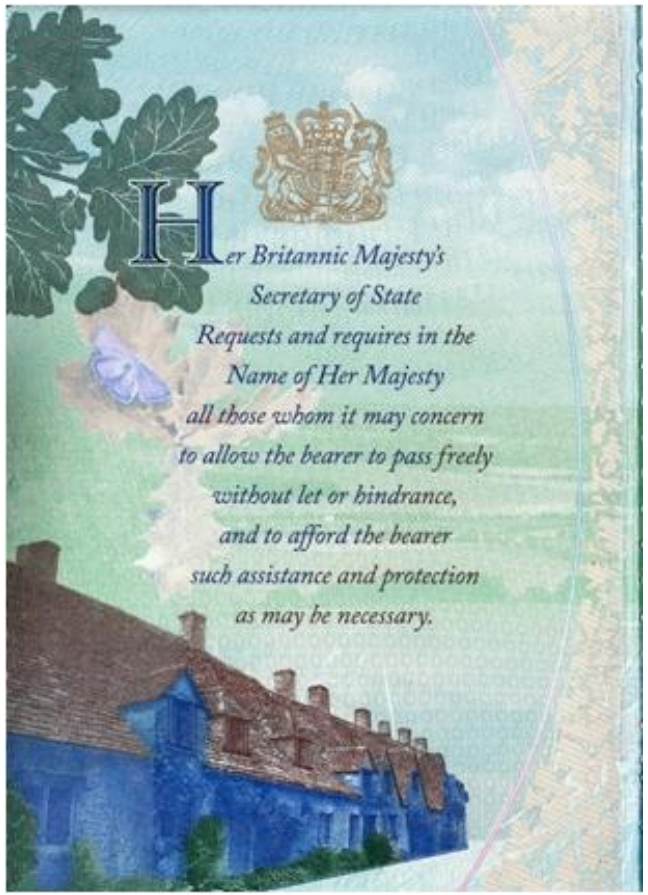
Cubierta

Definición del PLM

- **Medidas de seguridad**

Guardas:

Impresión
calcográfica
en dos colores



Definición del PLM

- **Medidas de seguridad**

Guardas:

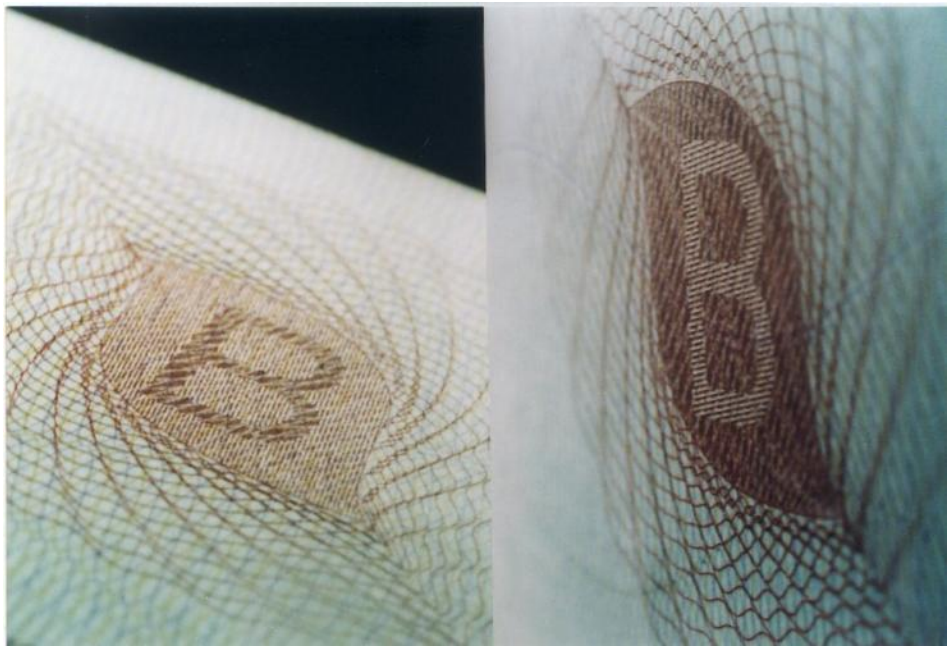
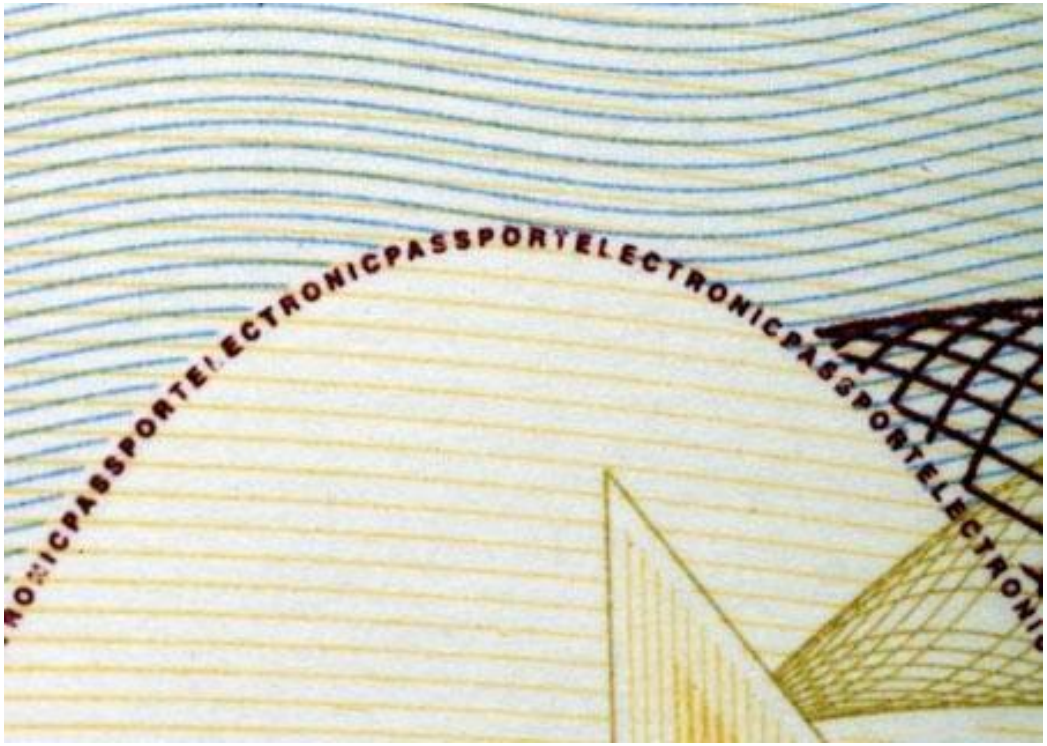


Imagen latente

Definición del PLM

- **Medidas de seguridad**

Guardas:



Microtextos

Definición del PLM

- **Medidas de seguridad**

Guardas:

Tintas ópticamente variables

Definición del PLM

- **Medidas de seguridad**

Papel:

Marca de agua multitonal

Definición del PLM

- **Medidas de seguridad**

Papel:

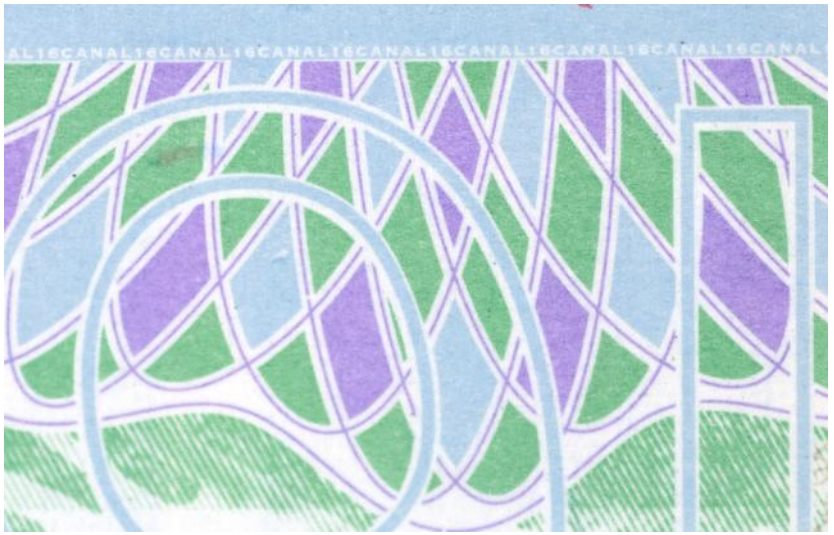
Fibrillas
invisibles

Definición del PLM

- **Medidas de seguridad**

Páginas interiores:

Guilloches en varios colores



Definición del PLM

- **Medidas de seguridad**

  Páginas interiores:

Impresión offset de seguridad

Definición del PLM

- **Medidas de seguridad**

Páginas interiores:

Tramas especiales de seguridad

Definición del PLM

- **Medidas de seguridad**

  Páginas interiores:

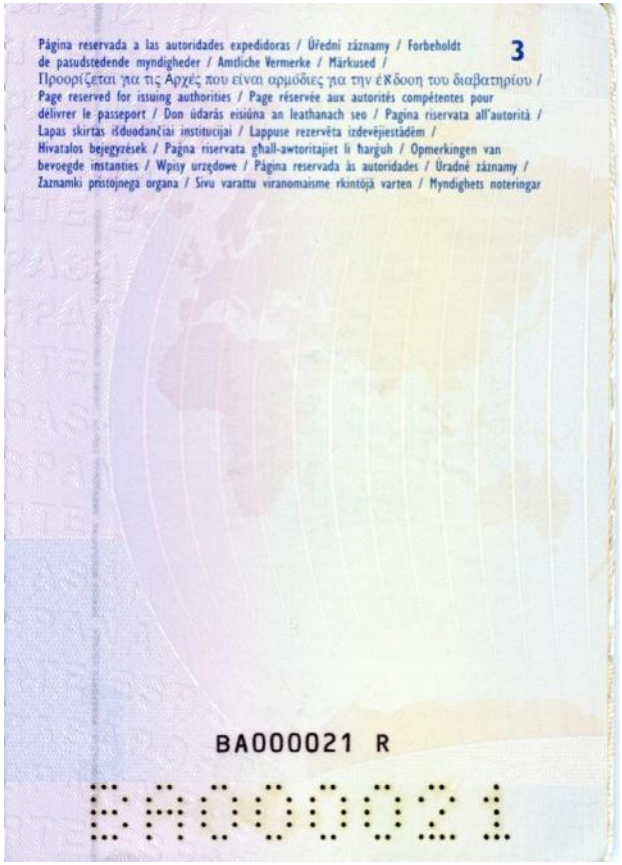
Tintas
invisibles

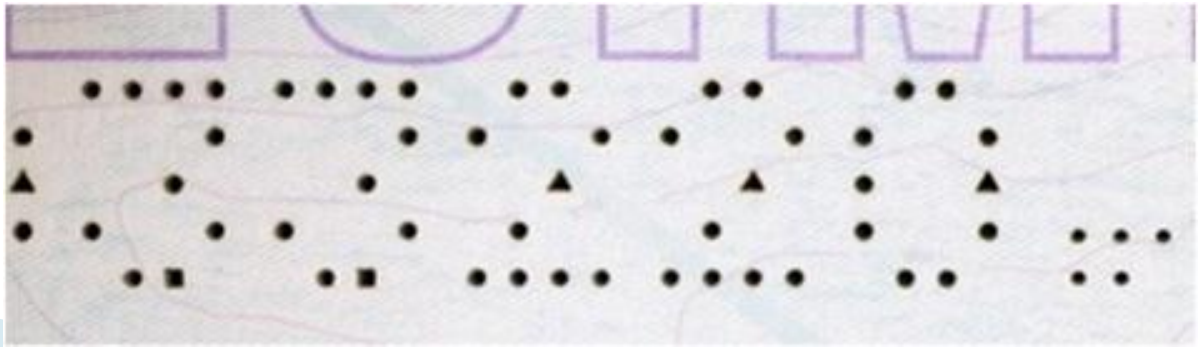
Definición del PLM

- **Medidas de seguridad**

  Páginas interiores:

Numeración por perforado láser



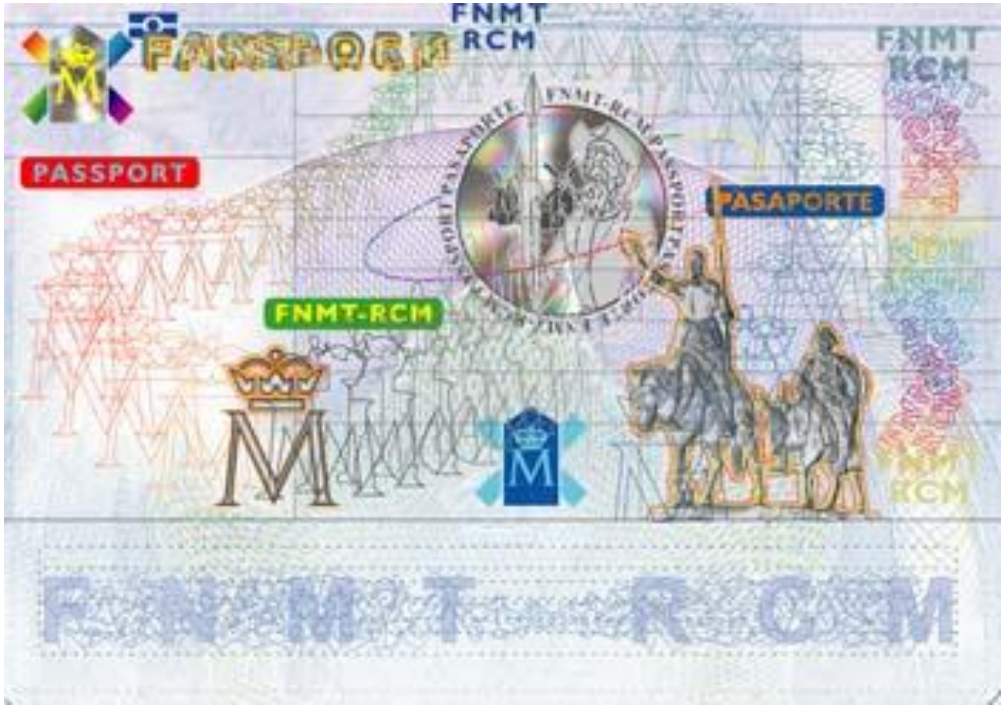


Definición del PLM

- **Medidas de seguridad**

Página de datos:

Lámina holográfica



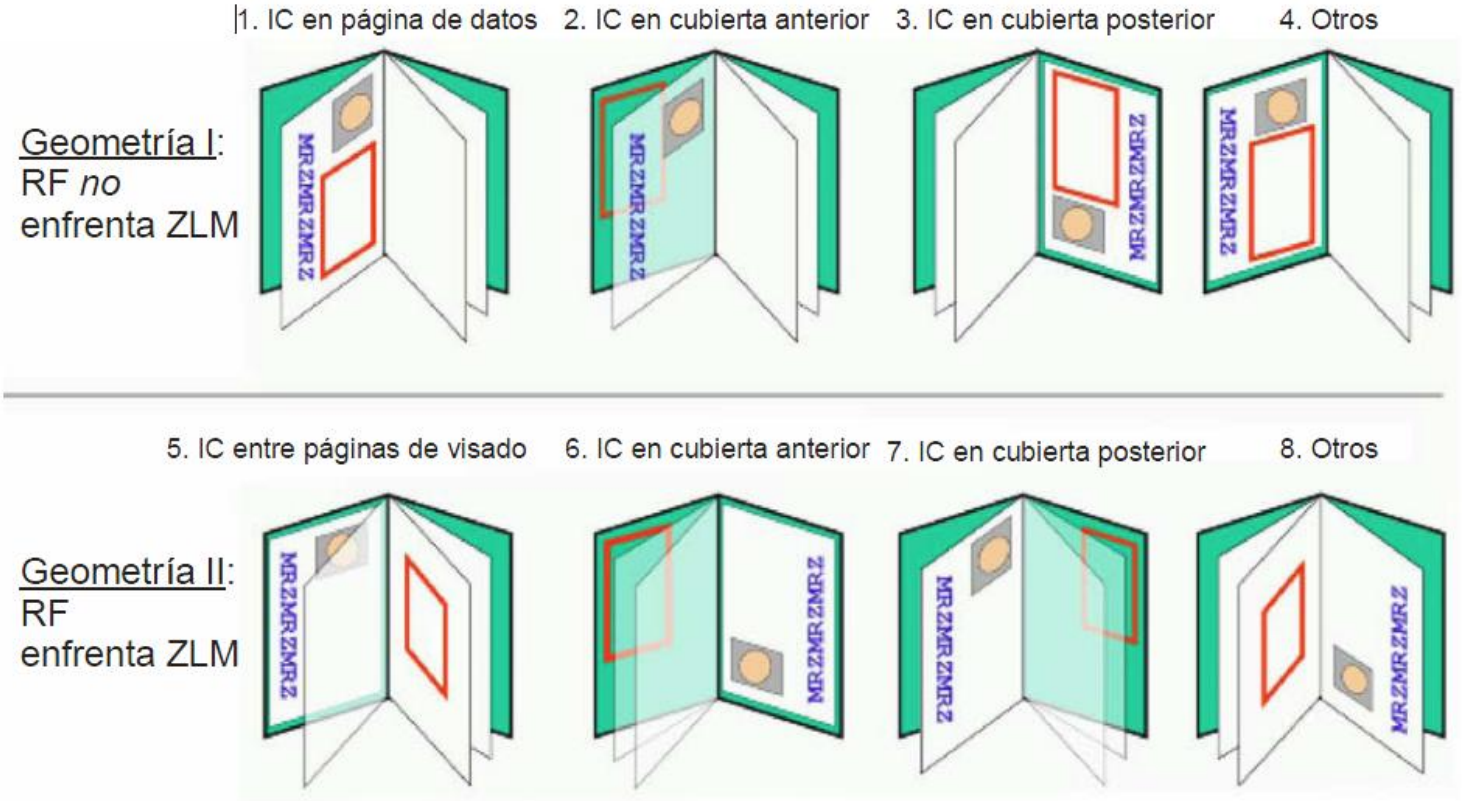
Lección aprendida No. 4

- **Seleccione las medidas de seguridad del pasaporte de acuerdo con las recomendaciones del Doc 9303 de la OACI**
- **Utilice tecnología probada y en uso en otros documentos similares**
- **Evite el uso de tecnología propietaria en manos de un único suministrador**
- **Busque doble fuente de suministradores**
- **Realice pruebas de laboratorio antes de aprobar cualquier material o característica de seguridad**

Definición del PLM

- Chip – antena

Opciones de integración



Definición del PLM

- Chip – antena

Página de datos en papel o en policarbonato

Definición del PLM

- Chip – antena

Página de datos en policarbonato

✓ Deslaminación imposible	✗ Página de datos y chip en un mismo elemento
✓ La laminación protege la impresión y la personalización	✗ Debilidad ante sustitución de página de datos
✓ Personalización de datos en capas internas	✗ Impresión de fondos diferente al papel
✓ Hologramas integrados en capas internas	✗ Fotografía en blanco y negro
✓ Alta durabilidad	✗ Sistemas de personalización muy caros
✓ Datos personalizados en relieve	✗ Integración de medidas de seguridad en sustrato
✓ Resistencia al agua	✗ Necesidad de medidas adicionales de seguridad
	✗ Página de datos reescribible
	✗ Ataques por adhesión de láminas
	✗ Microfisuras

Definición del PLM

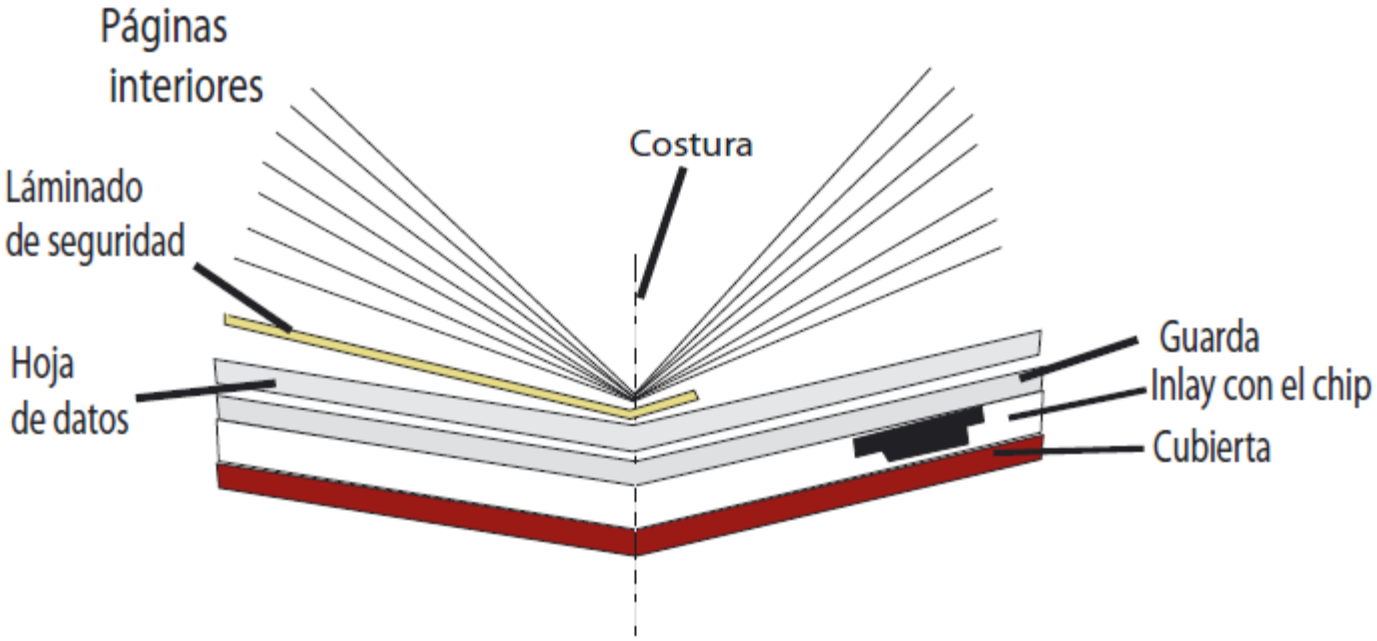
- Chip – antena

Página de datos en papel

✓ Página de datos y chip en distinta ubicación	✗ Necesidad de protección de la página de datos
✓ Mayor dificultad de sustitución	✗ Láminas de seguridad caras
✓ Impresión de fondos sobre papel	✗ Necesidad de garantizar el pegado del inlay
✓ Fotografía en color	✗ Cubiertas más rígidas y aislantes
✓ Sistema inkjet, penetra en el papel	
✓ Bajo coste	
✓ Integración de medidas en el sustrato	
✓ Posibilidad de personalizar con tintas UV	

Definición del PLM

- Chip – antena



Integración del chip en la cubierta

Lección aprendida No. 5

- **Realice pruebas de laboratorio y de producción para averiguar la ubicación idónea del chip y la antena**
- **Haga un estudio para ver si el uso de páginas de datos de policarbonato o de papel son adecuadas a su proyecto**
- **Utilice tecnología probada y en uso en otros documentos similares**
- **Busque doble fuente de suministradores de chips – inlays - eCovers**

Definición del PLM

- Sistema operativo – Estructura lógica de datos
  - **Características del Sistema Operativo:**
    - Sistemas operativos nativos vs Java Card
    - Carácterísticas mínimas:
      - Debe soportar autenticación pasiva y BAC
      - Debe funcionar sobre al menos dos plataformas
      - Debe soportar la estructura lógica de datos (LDS)
      - Soporte para funciones de Secure Messaging.
      - Posibilidad de personalizar por canal cifrado a elección
      - Certificación CC EAL 4+
      - **Control absoluto de ciclos de vida**

Definición del PLM

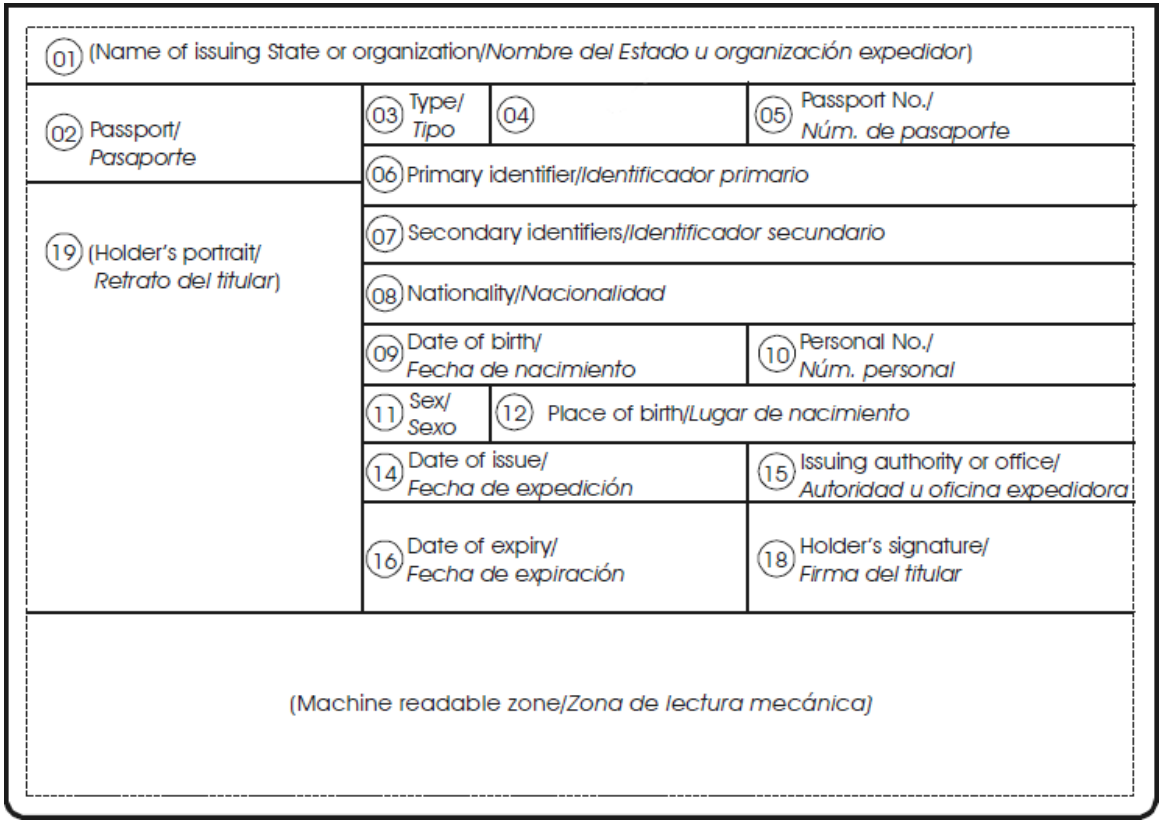
- Sistema operativo – Estructura lógica de datos
  - **Características del Sistema Operativo:**
    - Sistemas operativos nativos vs Java Card
    - Carácterísticas mínimas:
      - Debe soportar autenticación pasiva y BAC
      - Debe funcionar sobre al menos dos plataformas
      - Debe soportar la estructura lógica de datos (LDS)
      - Soporte para funciones de Secure Messaging.
      - Posibilidad de personalizar por canal cifrado a elección
      - Certificación CC EAL 4+
      - **Control absoluto de ciclos de vida**

Lección aprendida No. 6

- **Utilice tecnología probada y en uso en otros documentos similares**
- **Busque un sistema operativo funcional sobre al menos dos plataformas**
- **Realice pruebas de laboratorio (eléctricas y funcionales) del conjunto chip + antena + sistema operativo antes de aprobar el producto**
- **Exija la certificación de seguridad de los productos**
- **Controle el ciclo de vida del S.O.**

Definición del PLM

- Personalización de la hoja de datos



Esquema de datos OACI

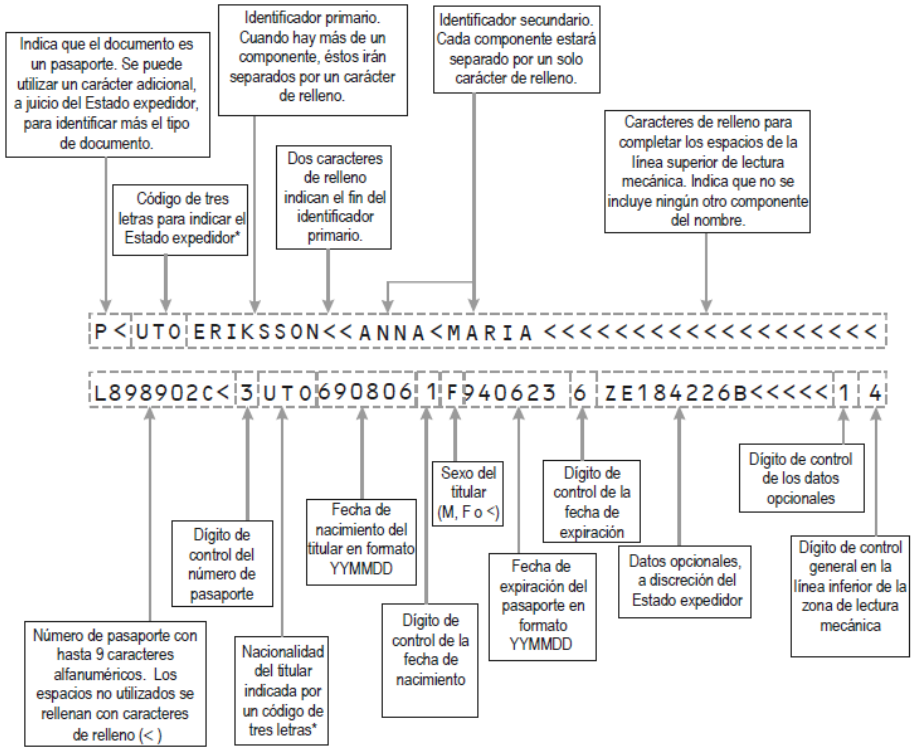
Definición del PLM

- Personalización de la hoja de datos

Esquema de datos simple

Definición del PLM

- Personalización de la hoja de datos

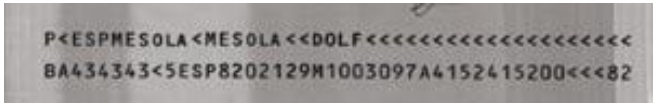


Zona de lectura mecánica

Definición del PLM

Interoperabilidad

Definición del PLM



Lección aprendida No. 7

- **Utilice el esquema de personalización de datos definido por la OACI**
- **Mantenga el diseño de la página de datos lo más simple posible**
- **Utilice la página contigua a la página de datos para los datos opcionales**
- **Asegure la correcta codificación de líneas de lectura mecánica y de los contenidos del chip**
- **Verifique la interoperabilidad de su pasaporte**

Sistema de emisión

- Sistema de emisión del pasaporte electrónico español
  - Responsabilidad del Cuerpo Nacional de Policía
  - Banco central de datos y base de datos de antecendentes centralizados
  - Expedición descentralizada en 256 oficinas distribuidas en 52 provincias
  - El único documento de origen válido para la obtención del ePasaporte es el DNI español
  - Emisión del documento inmediata: el ciudadano obtiene su DNIe o ePasaporte en un único acto y en 20 minutos

Sistema de emisión

- Problemas encontrados durante el desarrollo del sistema de emisión del ePasaporte
  - Distribución de libretas en blanco
  - Captura de biométricos
  - Equipos de personalización de pasaportes
  - Personalización de chips
  - Seguridad del proceso de emisión
  - Personal
  - Coste elevado

Sistema de emisión

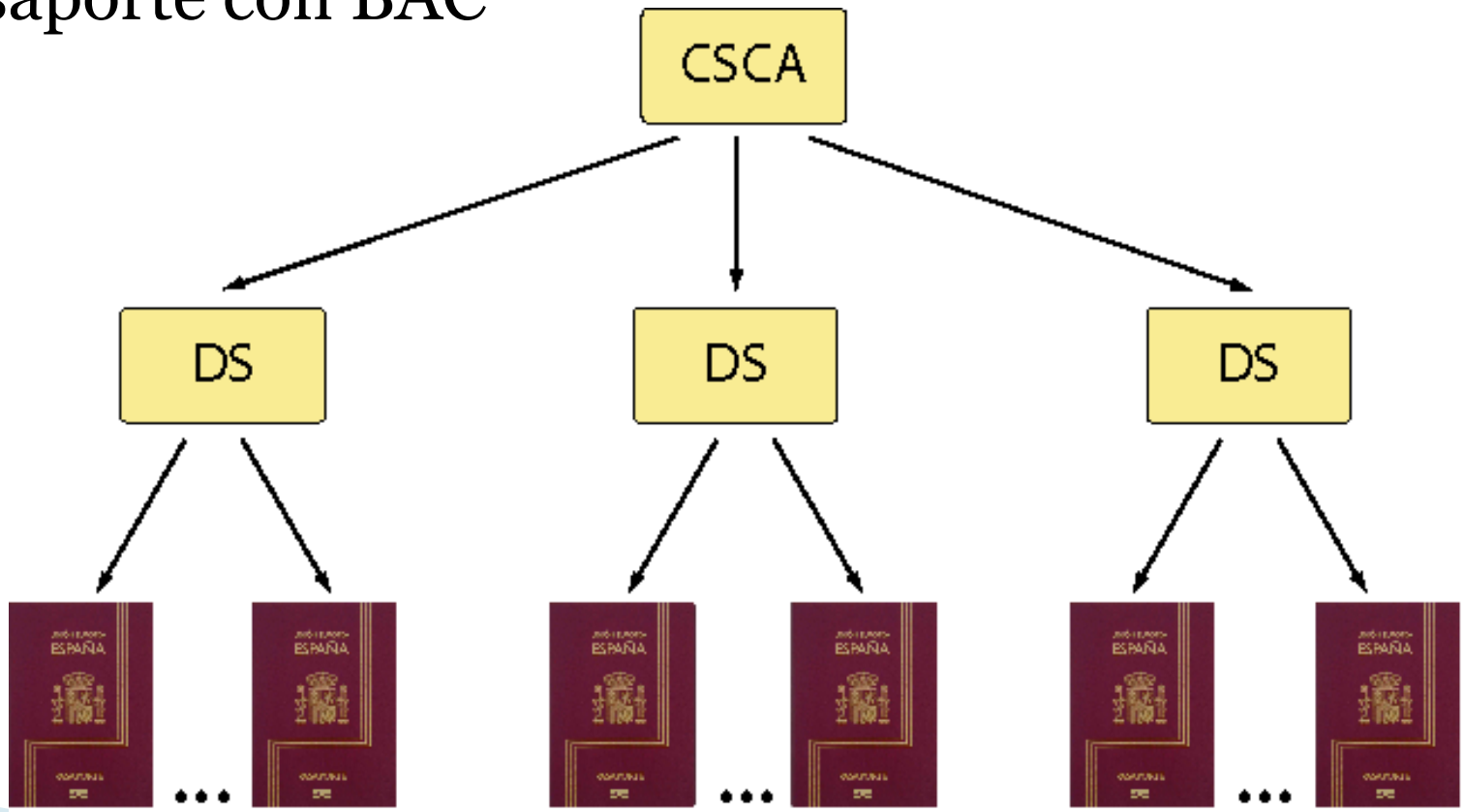
- Procesos de emisión, y seguridad
  - El ciudadano solicita cita previa por teléfono o internet
  - El ciudadano se persona en una oficina de expedición de la Policía Nacional con su DNI
  - El oficial de Policía se autentica antes el sistema y realiza la captura de datos biográficos y biométricos
  - Se realizan las comprobaciones contra las bases de datos de DNI, antecendentes policiales, personas con prohibición de entrada, pasaportes falsos o duplicados, Europol, Interpol
  - Se imprime la página de datos y se personalizan los contenidos del chip
  - El ciudadano obtiene su ePasaporte en 15 minutos

Lección aprendida No. 8

- Evalúe la viabilidad de un sistema de emisión centralizado vs descentralizado
- Establezca un esquema de protección de documentos en blanco
- Verifique la seguridad y credibilidad de los documentos de origen en la emisión
- Compruebe la seguridad de todo el proceso de emisión
- Establezca medidas de seguridad para el personal a cargo de la emisión
- Evalúe los costes del proceso

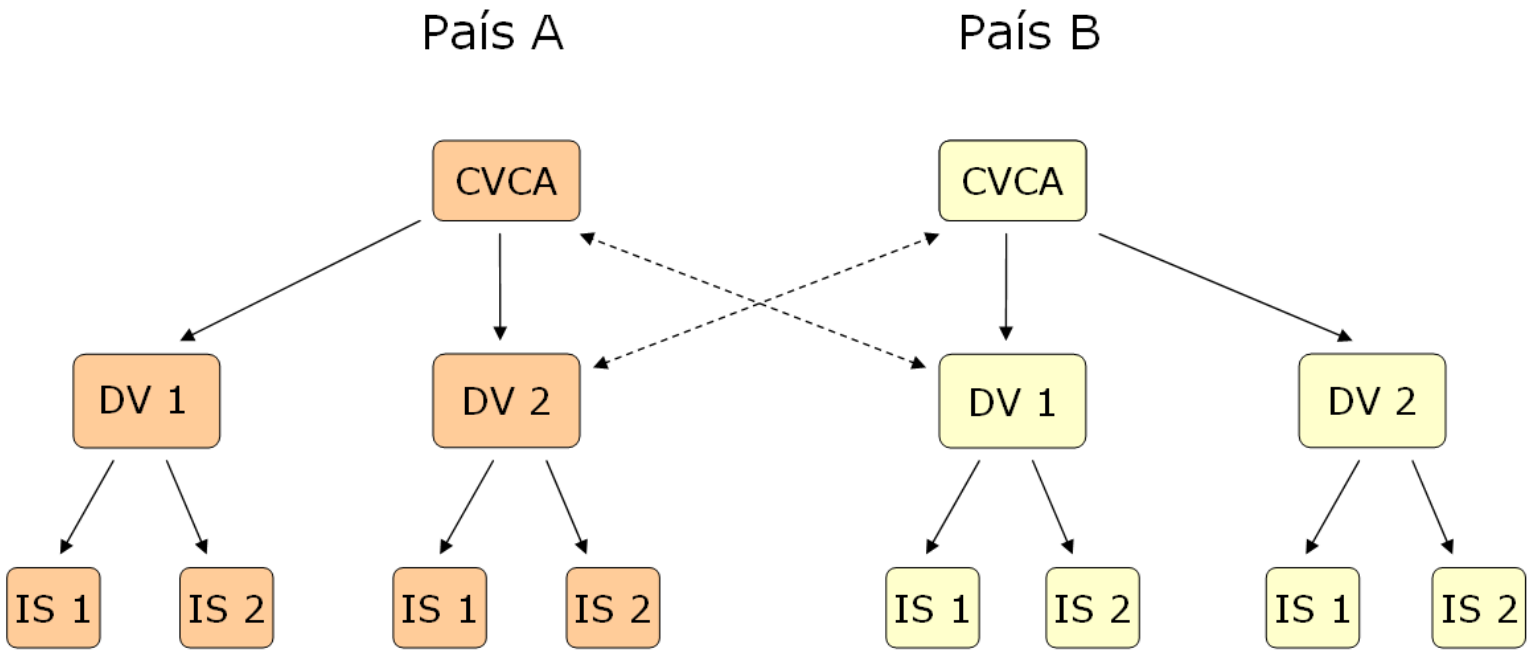
PKI de emisión. PKD

- 2006. Establecimiento de la PKI de emisión del ePasaporte con BAC



PKI de emisión. PKD

- 2009. Establecimiento de la PKI de verificación de documentos para el EAC



PKI de emisión. PKD

- Próximos pasos:
  - Distribución de claves y CRLs – intercambios bilaterales
  - 2012. Integración de España en el PKD de la OACI

  - 2014. Puesta en marcha del protocolo SPOC para el intercambio de certificados de verificación de documentos
  - 2014. Integración del Control de Acceso Suplementario y del protocolo PACE.

Lección aprendida No. 9

- **Establezca una PKI de emisión de pasaportes electrónicos basada en tecnologías probadas y de confianza**
- **Comience por la emisión de pasaportes electrónicos BAC**
- **Evalúe la necesidad de establecer el Control de Acceso Extendido (EAC), y sus costes asociados**
- **Distribuya sus claves. Suscríbase al PKD de la OACI**

Lección aprendida No. 10

- **Haga un estudio previo de la situación actual de emisión de pasaportes en su país y planifique cuidadosamente el proyecto de migración a pasaporte electrónico**
- **Siga las recomendaciones del Doc 9303 de la OACI**
- **Utilice tecnologías probadas y en uso por otros países en documentos similares**
- **Evalúe todos los productos y procesos antes de validarlos**
- **Busque asesoramiento especializado**

MUCHAS GRACIAS

Contact Information:
Carlos Gómez
FNMT-RCM
E-mail: cgomez@fnmt.es
Tel.: +34 915 666 651