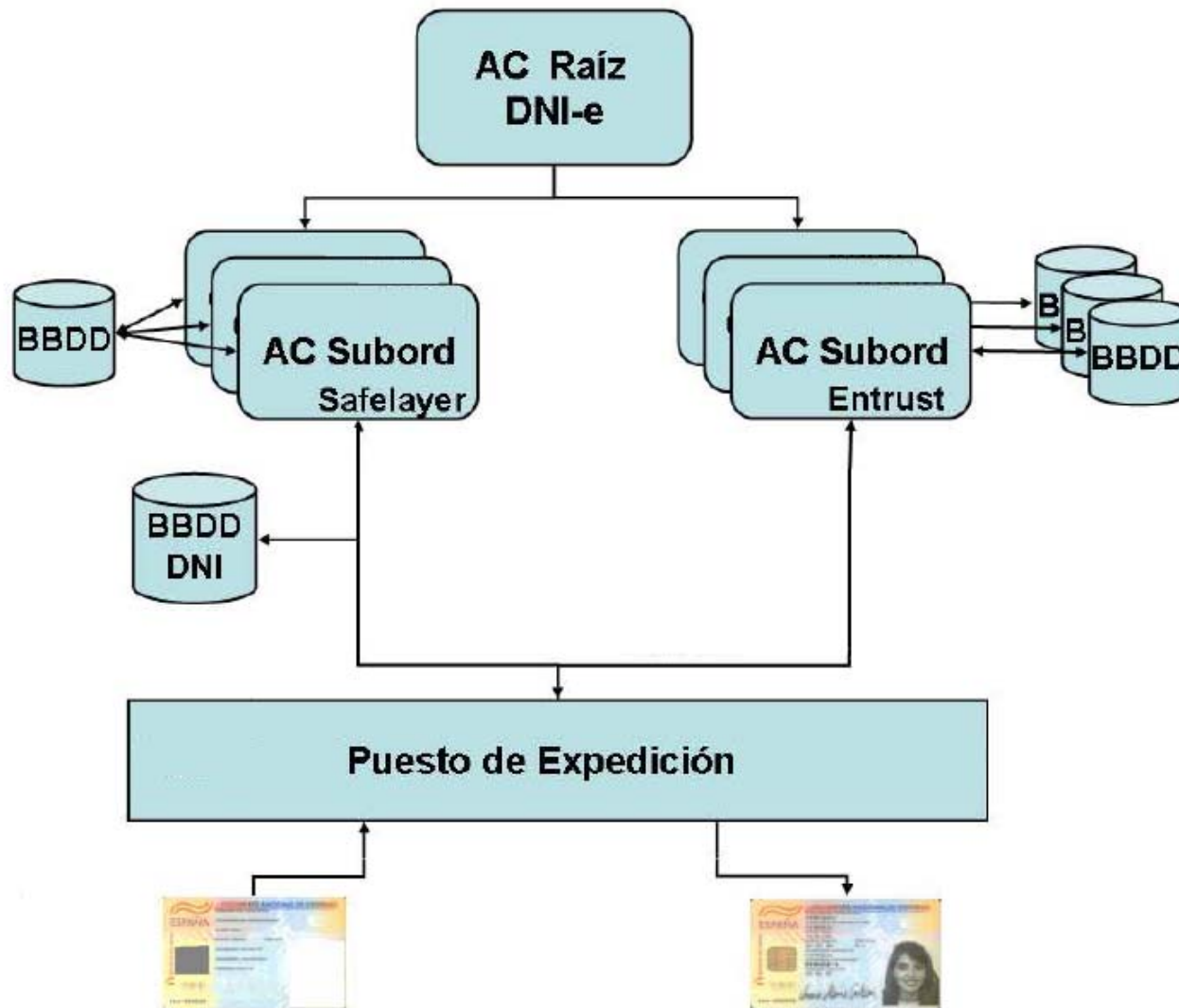


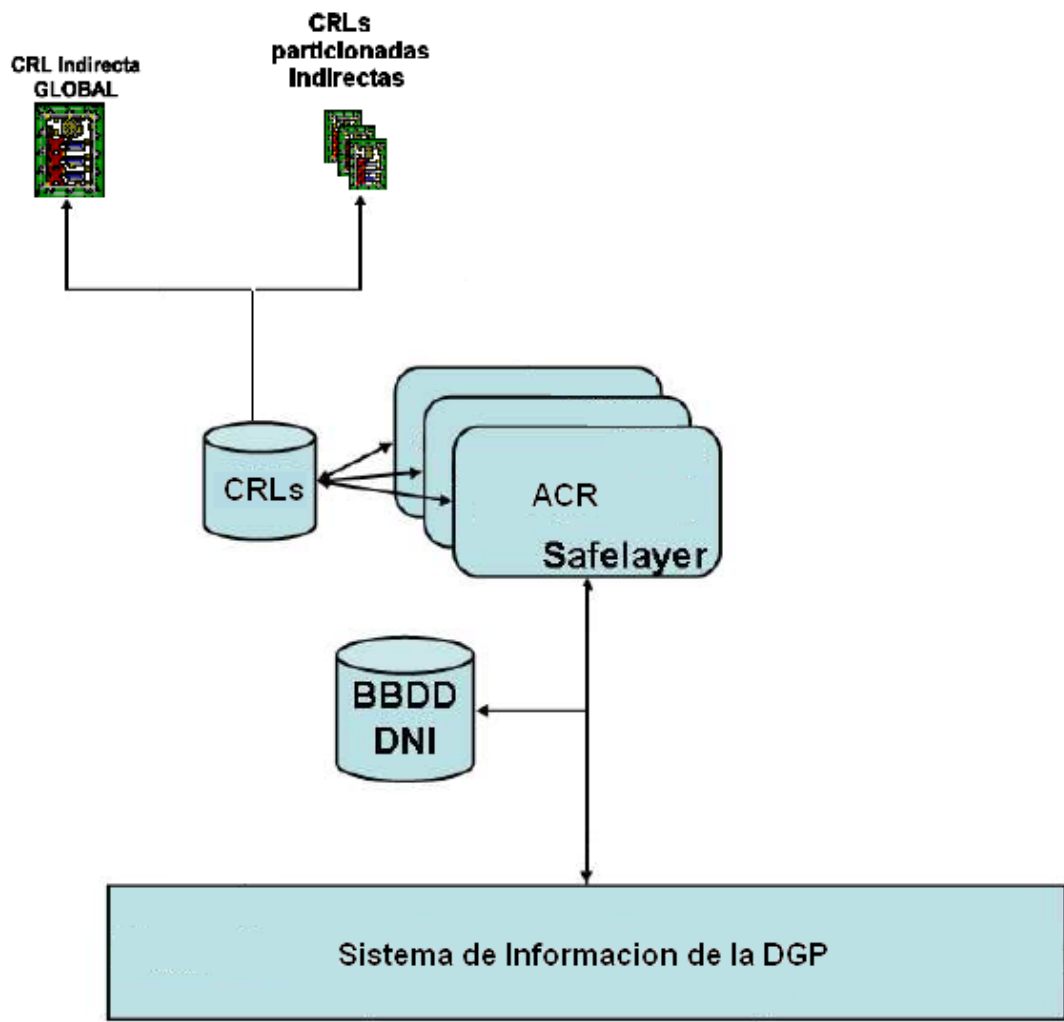
Jornada de presentación del



Aspectos técnicos del proyecto

Madrid, 23 de febrero de 2006





Algoritmia y Claves.

•Raíz: 30 Años.

- Certificado Autofirmado con SHA1 y SHA256.
- Claves RSA 4096.
- Key Usage: Firma de certificados, Firma CRL sin conexión, Firma CRL

•Subordinadas: 15 Años

- Certificados firmados con SHA1 y SHA256.
- Claves RSA 2048
- Key Usage: Firma de certificados, Firma CRL sin conexión, Firma CRL

•Ciudadano: 30 Meses.

- Certificados firmados con SHA1.
- Claves RSA 2048.
- Utiliza para firmar SHA1.
- Key Usage: Autenticación y Firma o Sin Repudio

Campos del Certificado del Ciudadano

CAMPO	CONTENIDO	CRÍTICA
Campos de X509v1		
1. Versión	V3	
2. Serial Number	No secuencial	
3. Signature Algorithm	sha256withRsaEncryption[1]	
4. Issuer Distinguished Name	CN=AC DNIE XXX [OU=PRUEBAS OU=PREPRODUCCION] OU=DNIE O=DIRECCION GENERAL DE LA POLICIA C=ES	
5. Validez	30 meses	
6. Subject	CN=APELLIDO1 APELLIDO2, NOMBRE (AUTENTICACIÓN) GN=NOMBRE SN=APELLIDO1 NÚMERO DE SERIE=DNI (con letra) C=ES	
7. Subject Public Key Info	Algoritmo: RSA Encryption Longitud: 2048 bits	

Campos del Certificado del Ciudadano

Campos de X509v2		
1. issuerUniqueId	No se utilizará	
2. subjectUniqueId	No se utilizará	
Extensiones de X509v3		
1. Subject Key Identifier	Función hash SHA-1 sobre la clave pública del sujeto.	NO (RFC 3280)
2. Authority Key Identifier	Función de hash SHA-1 sobre la clave pública de la AC emisora (AC subordinada). NO SE incluye la identificación del certificado de la AC emisora (en este caso, DN de la AC Raíz, número de serie de la AC Subordinada).	NO (RFC 3280)
3. KeyUsage		SI (RFCs 3280 y 3739)
Digital Signature	0	
Non Repudiation	1	
Key Encipherment	0	
Data Encipherment	0	
Key Agreement	0	
Key Certificate Signature	0	
CRL Signature	0	
4.extKeyUsage	No se utilizará	
5. privateKeyUsagePeriod	No se utilizará	

Campos del Certificado del Ciudadano

6. Certificate Policies		
Policy Identifier	OID asociado a la DPC o PC de certificado de firma de ciudadano. A determinar, perteneciente a la estructura de OIDs de ISO/ITU-T España (2.16.724.1.2.2.2.3)	NO
URL CPS	http://www.dnie.es/dpc [http://www.pruebas.dnie.es/dpc] [http://www.prepro.dnie.es/dpc]	
Notice Reference	No se utilizará	
7. Policy Mappings		
qcStatements	id-etsi-qcs-QcCompliance id-etsi-qcs-QcSSCD	NO
8. Subject Alternate Names	No se utilizará	
9. Issuer Alternate Names	No se utilizará	
10. Subject Directory Attributes	dateOfBirth	NO (RFC 3280)

Campos del Certificado del Ciudadano

11. Basic Constraints		SI
Subject Type	Entidad Final	
Path Length Constraint	No utilizado	
12. Policy Constraints	No utilizado	
13. CRLDistributionPoints	No utilizado	
14. Auth. Information Access	OCSP: http://ocsp.[pruebas].dnie.es:puerto CA: http://www.[pruebas].dnie.es/certs/ACRai z.crt	NO (RFC 3280)
15. netscapeCertType	No se utilizará	
16. netscapeRevocationURL	No procede	
17. netscapeCAPolicyURL	No procede	
18. netscapeComment	No procede	
19. BiometricInfo	Hash SHA256 de los datos biométricos: •firma manuscrita (PNG) •foto (JPEG) •huella posada de dos dedos (JPEG)	NO (RFC 3739)
20. personalDataInfo (2.16.724.1.2.2.4.1)	Hash SHA256 de los datos biográficos (datos impresos en el DNI-e).	NO

Entorno de Uso



Usabilidad – Cadena de Confianza

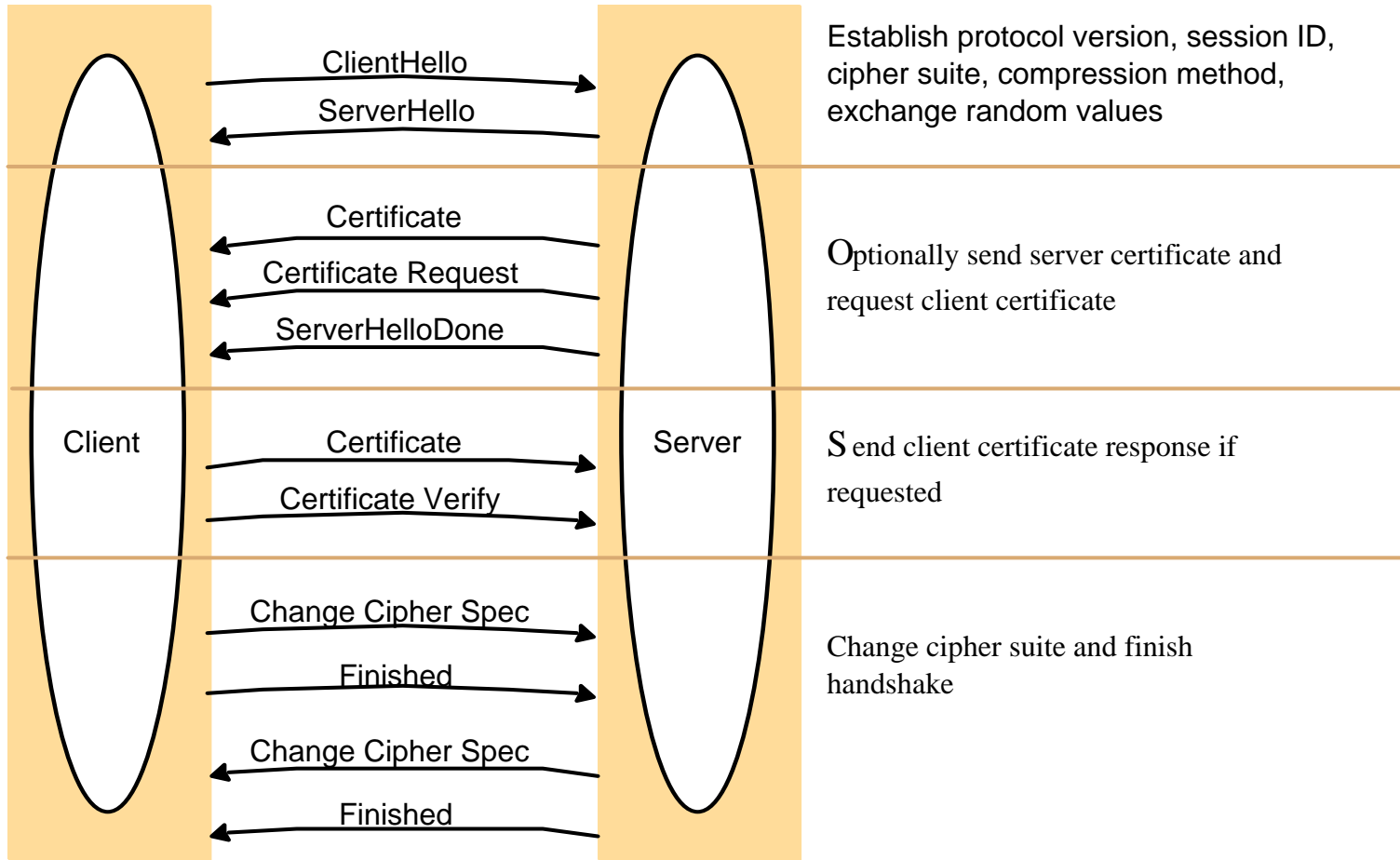
La Cadena de confianza del DNI electrónico se conforma con los certificados del Ciudadano y el Certificado de la Autoridad de Certificación emisora que se encuentran incluidos en el DNle. Esta cadena se completa con el Certificado de la Autoridad de Certificación Raíz cuya ubicación se encuentra especificada en una extensión de los certificados del Ciudadano, en concreto <http://www.dnie.es/certs/ACRaiz.crt>



Usabilidad – Autenticación

De los Certificados contenidos en el DNI, el de Identidad (Key Usage = Firma Digital) es el que utilizaremos para el establecimiento del Canal Seguro con autenticación de Cliente y Servidor. Para ello los prestadores de Servicio deberán tener instalados en sus Servidores los Certificados de las Autoridades de Certificación del DNI (Raíz y Emisoras), firmados con la Algoritmia correspondiente a los Servidores que utilicen.

Además el prestador de Servicio podrá, si le interesa, verificar el estado del Certificado comprobando en la extensión Valido-Hasta si ha caducado y su posible revocación mediante la consulta a la Autoridad de Validación.



SSL: Confidencialidad e Integridad

• Cifrado simétrico

- Flujo
 - RC4 con claves de 40 bits
 - RC4 con claves de 128 bits
- Bloque
 - RC2 con claves de 40 bits
 - DES con claves de 40 bits
 - DES con claves de 56 bits
 - 3DES-EDE con claves de 168 bits
 - IDEA con claves de 128 bits
 - Fortezza con claves de 96 bits

• Cifrado asimétrico

- Diffie-Hellman
- RSA 512 bits
- RSA 1024 bits
- RSA 2048 bits.

• Firma digital

- Hash
 - MD5 de 128 bits
 - SHA de 160 bits
 - SHA 256 bits.

Usabilidad – Firma

De los Certificados contenidos en el DNI, el de Firma (Key Usage = No Repudio) es el que utilizaremos para la Firma de Documentos. Permitiendo garantizar la Integridad del Documento firmado y el No Repudio de Origen.

La firma de Documentos se realiza mediante la aplicación de un Algoritmo de Hash o resumen, que permite reducir un fichero, sin tener en cuenta su tamaño, a un número determinado de bits, en este caso a 160 bits.

Una vez realizada esta función se cifra su resultado con la clave privada del certificado de No Repudio.

Usabilidad – Firma

El receptor para verificar la firma, deberá:

- Ejecutar la función hash o resumen del documento.
- Descifrar con la Clave Pública del Certificado de No Repudio del Ciudadano el hash del documento recibido.
- Comparar ambos resúmenes.

Seguidamente debería Verificar la fecha de caducidad del Certificado y el estado de Revocación del mismo consultado a la Autoridad de Validación, para comprobar la validez del Certificado usado en la firma del documento

Seguridad Jurídica

•Firma Electrónica:

- Directiva 1999/93/CE.
- Ley 59/2003.

•Protección de Datos Personales y su procesamiento:

- Directivas 1995/46/CE, 97/66/EC, 2002/58/CE.
- Reglamento (EC) 45/2001.
- L.O.P.D. 15/1999 y Real Decreto 994/1999. Ley 32/2003 y 34/2002

•Específica del D.N.I.:

- L.O. 1/1992, de Protección de la Seguridad Ciudadana.
- R.D. 1553/2005. Expedición del DNI y sus Certificados electrónicos

Contenido del chip

Toda la información está firmada por la Arquitectura de certificación del DNI para garantizar su Integridad y su Autenticidad.

Contenido:

- Certificado de autenticación y Claves asociadas
- Certificado de firma y Claves asociadas.
- Certificado de la autoridad de certificación emisora.
- Datos de filiación del ciudadano.
- Imagen de la fotografía.
- Imagen de la firma manuscrita.
- Plantilla de la impresión dactilar.
- Aplicación de Match On Card.



Nivel de Seguridad del CHIP

CC EAL 5+. El componente ha sido Certificado por el esquema francés de evaluación y certificación de las T.I.

CC EAL 4+ SOFT HIGH. – La mascara se esta Certificando Common Criteria según el Perfil de Protección europeo para tarjetas inteligentes. Por el esquema de Certificación Nacional.

CWA 14169 –3. SSCD. Dispositivo Seguro de Creación de Firma.

CWA 14.890. - Autenticación Mutua de Dispositivo.

Sistema de Expedición. Acreditación por el Organismo Nacional de Certificación.

Estándares Aplicables

- **ETSI TS 102 042.** Policy requirements for certification authorities issuing public key certificates. En lo relativo a las prácticas de certificación.
- **ETSI TS 101 456.** Policy requirements for certification authorities issuing qualified certificates. En lo relativo a las prácticas de certificación.
- **ETSI TS 101 862.** Para la definición del Perfil como certificado Reconocido (Qualified Certificate profile).
- **CWA 14167-1.** En lo relativo a la seguridad del sistema de certificación.
- **CWA 14172-1-2-3.** EESSI Conformity Assessment Guidance. Para la verificación del cumplimiento de los requisitos de emisión de los certificado.

Fin de la Presentación
Muchas Gracias

