



| ICAO

SECURITY & FACILITATION



Spanish National PKD

Esther Fernández Crespo

Spanish National Police



Location/date



Goals:

1. Show the new version of the Spanish NPKD
2. Adaptation to the new international regulations
3. New features for the improvement of the management of cryptographic material.

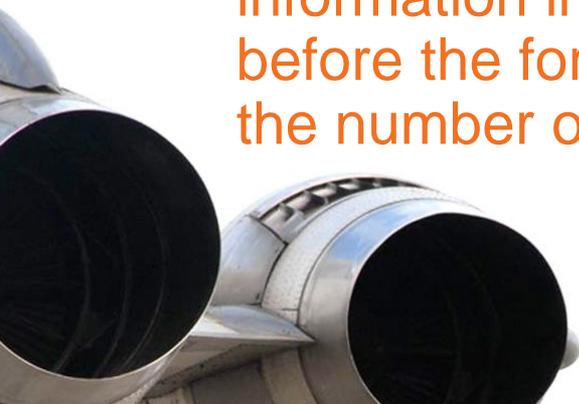




It allows:

1. That the Inspection Systems verify easily and reliably the authenticity of the passports.
2. The simple management of information included in the PKD before the foreseeable increase in the number of:

- a. Countries from which MRTDs will be verified
- b. Passengers crossing the borders
- c. The number and variety of inspection systems





1. Communications with ICAO PKD

- Upload of the national Master lists, DS certificates and CRLs.
- Download of the foreign Master lists, DS certificates and CRLs

2. Send to the Inspection Systems the information to validate eMRTDs

- Certificates of the Document Signer.
- Certificates of the CSCAs .
- CRLs issued by the CSCAs.
- Web services available to request this data.
- Automatic publication inside of a National PKD LDAP.

3. Issuing of the Master Lists

- Containing the national CSCA certificates and the chosen trusted foreign CSCA certificates.

4. Data approval

- Manual approval of the countries to be trusted (CSCA certificates).
- Automatic approval of the foreign CSCA certificates using CSCA link certificates.
- Automatic approval of DS certificates and CRLs issued by trusted CSCAs.





ICAO

SECURITY & FACILITATION

Spanish National PKD



NPKD1 - KeyOne e-Passport NPKD

Sesión: Publicación en el PKD nacional

KeyOne e-Passport NPKD

- Tareas
 - Publicación en el PKD nacional
 - Listas maestras de CSCA
 - Certificados de CSCA
 - Certificados de DS
 - CRL
 - Gestión de claves
 - Certificados y claves
 - Configuración de seguridad
 - Definición del flujo de trabajo
 - Configuración administrativa
 - Herramientas administrativas
 - Add-ins
 - Logs

KeyOne e-Passport NPKD > Tareas > Publicación en el PKD nacional

KeyOne e-Passport NPKD

- Listas maestras de CSCA
- Certificados de CSCA
- Certificados de DS
- CRL
- Importar lista maestra de CSCA...
- Emitir lista maestra de CSCA...
- Importar certificado de CSCA...
- Importar certificado de DS...
- Importar CRL...
- Procesar LDIF de listas maestras de CSCA de ICAO...
- Procesar LDIF de DSC/CRL de ICAO...
- Descargar listas maestras de CSCA del PKD de ICAO...
- Descargar certificados de DS del PKD de ICAO...
- Descargar CRL del PKD de ICAO...

Oficial Seguridad 1 SECURITY_OFFICER



Doc 9303: ICAO Regulations on certificate profiles

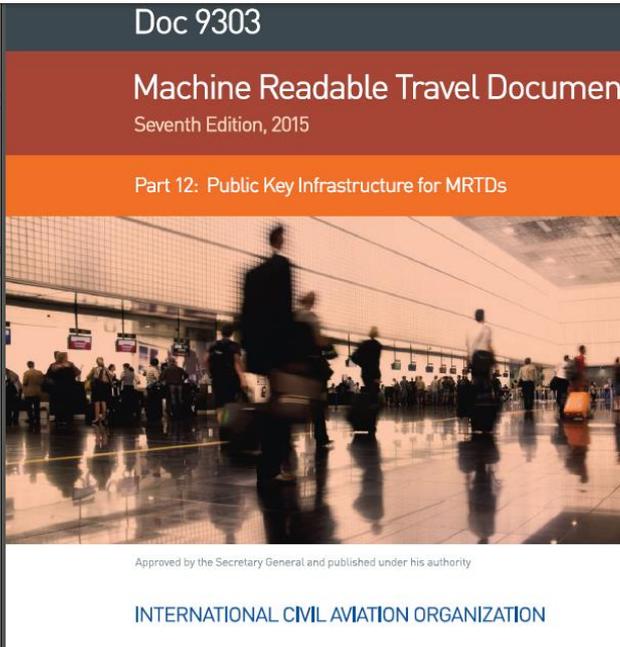
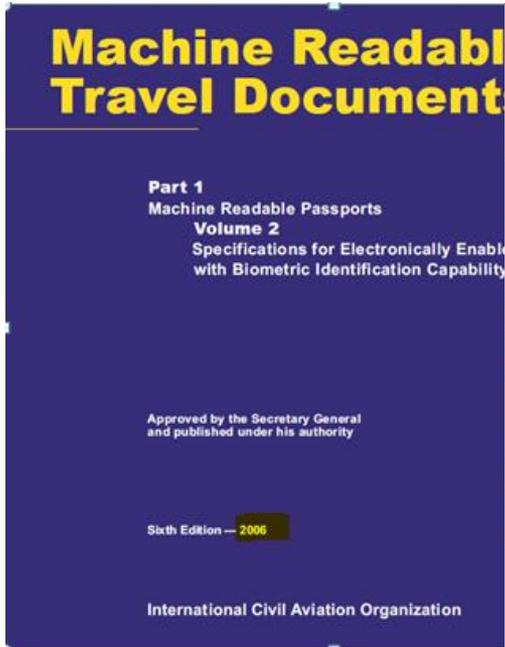


Table 4. Certificate Extensions Profile

Extension name	CSCA Self-Signed Root		CSCA Link		Document Signer		Master List Signer and Deviation List Signer		Communication		Comments
	Presence	Criticality	Presence	Criticality	Presence	Criticality	Presence	Criticality	Presence	Criticality	
AuthorityKeyIdentifier	o	nc	m	nc	m	nc	m	nc	m	nc	
keyIdentifier	m		m		m		m		m		
authorityCertIssuer	o		o		o		o		o		
authorityCertSerialNumber	o		o		o		o		o		
SubjectKeyIdentifier	m	nc	m	nc	o	nc	o	nc	o	nc	
subjectKeyIdentifier	m		m		m		m		m		
KeyUsage	m	c	m	c	m	c	m	c	m	c	
digitalSignature	x		x		m		m		o		Some communication certificates (e.g. TLS certificates) require that the keyUsage bits be set in accordance with the particular cipher suite used. Some cipher suites do, and some do not require the digitalSignature bit to be set.
nonRepudiation	x		x		x		x		x		



New features:

Compliance check of the ICAO Doc 9303 profiles

The possible results are:

- The certificate complies with the profile of doc 9303.
- The certificate does not comply with the profile of doc 9303; in this case it shows information about the extensions that do not conform to the regulations.

The screenshot shows the 'NPKD1 - KeyOne e-Passport NPKD' application window. The interface includes a navigation tree on the left and a main table of validation profiles on the right.

Navigation Tree:

- Tareas
 - Publicación en el PKD nacional
 - Listas maestras de CSCA
 - Certificados de CSCA
 - Certificados de DS
 - CRL
 - Gestión de claves
 - Certificados y claves
 - Configuración de seguridad
 - Perfiles de validación
 - Definición del flujo de trabajo
 - Configuración administrativa
 - Herramientas administrativas
 - Add-ins
 - Logs

Table of Validation Profiles:

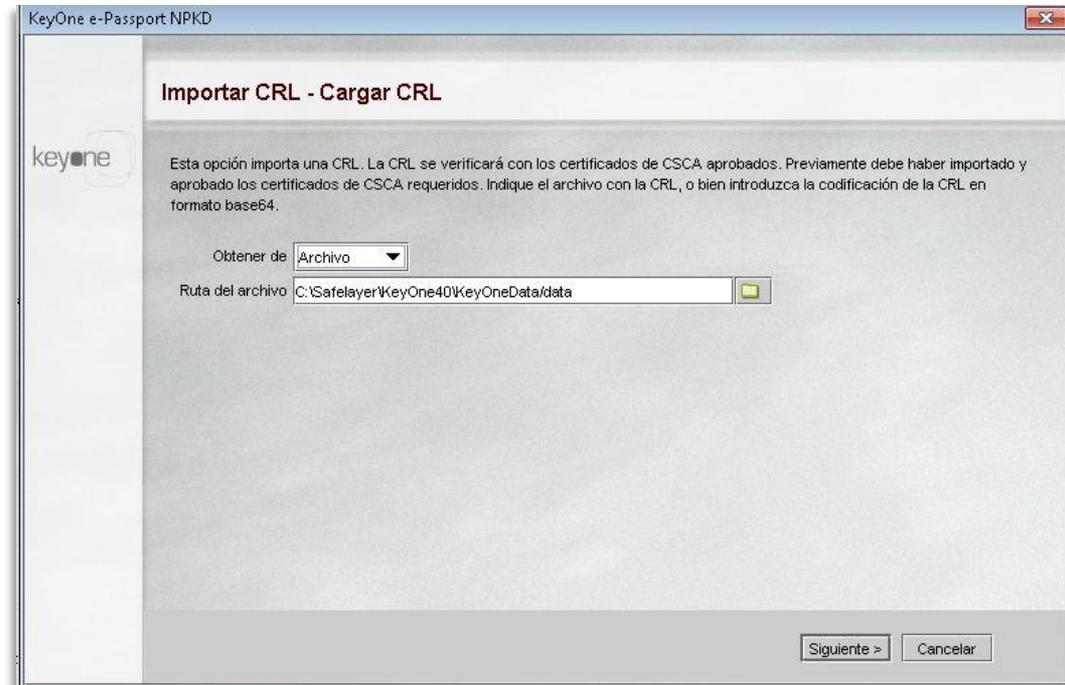
Nombre del perfil	Descripción del perfil
CRL_6TH_EDITION	ICAO Doc 9303 6th Edition CRL profile (from 26 Jul 2006)
CRL_7TH_EDITION	ICAO Doc 9303 7th Edition CRL profile (from 21 May 2014)
CRL_GUIDANCE	ICAO Doc 9303 Guidance CRL profile (from 22 Jun 2011)
CSCA_LINK_CERT_2008_VERSION	ICAO Doc 9303 Part 3 3rd Edition certificate profile for CSCA link certs (from 19 Nov 2008)
CSCA_LINK_CERT_6TH_EDITION	ICAO Doc 9303 6th Edition certificate profile for CSCA link certs (from 26 Jul 2006)
CSCA_LINK_CERT_7TH_EDITION	ICAO Doc 9303 7th Edition certificate profile for CSCA link certificates (from 21 May 2014)
CSCA_LINK_CERT_GUIDANCE	ICAO Doc 9303 Guidance certificate profile for CSCA link certificates (from 22 Jun 2011)
CSCA_ROOT_CERT_6TH_EDITION	ICAO Doc 9303 6th Edition certificate profile for CSCA root certificates (from 26 Jul 2006)
CSCA_ROOT_CERT_7TH_EDITION	ICAO Doc 9303 7th Edition certificate profile for CSCA root certificates (from 21 May 2014)
CSCA_ROOT_CERT_GUIDANCE	ICAO Doc 9303 Guidance certificate profile for CSCA root certificates (from 22 Jun 2011)
DOC_SIGN_CERT_6TH_EDITION	ICAO Doc 9303 6th Edition certificate profile for DS certificates (from 26 Jul 2006)
DOC_SIGN_CERT_7TH_EDITION	ICAO Doc 9303 7th Edition certificate profile for Document Signer certs (from 21 May 2014)
DOC_SIGN_CERT_GUIDANCE	ICAO Doc 9303 Guidance certificate profile for Document Signer certs (from 22 Jun 2011)
ML_SIGN_CERT_7TH_EDITION	ICAO Doc 9303 7th Edition certificate profile for Master List Signer certs (from 21 May 2014)
ML_SIGN_CERT_GUIDANCE	ICAO Doc 9303 Guidance certificate profile for Master List Signer certs (from 22 Jun 2011)
ML_SIGN_CERT_V1	ICAO CSCA countersigning and Master List issuance Version 1.0 (from June 23, 2009)



New features:

Obtaining of CSCAs, DSs y CRLs list

- CSCAs certificates approved and valid (no expired)
- Imported and valid DS certificates (no expired)
- Valid CRLs imported into the system (no expired)

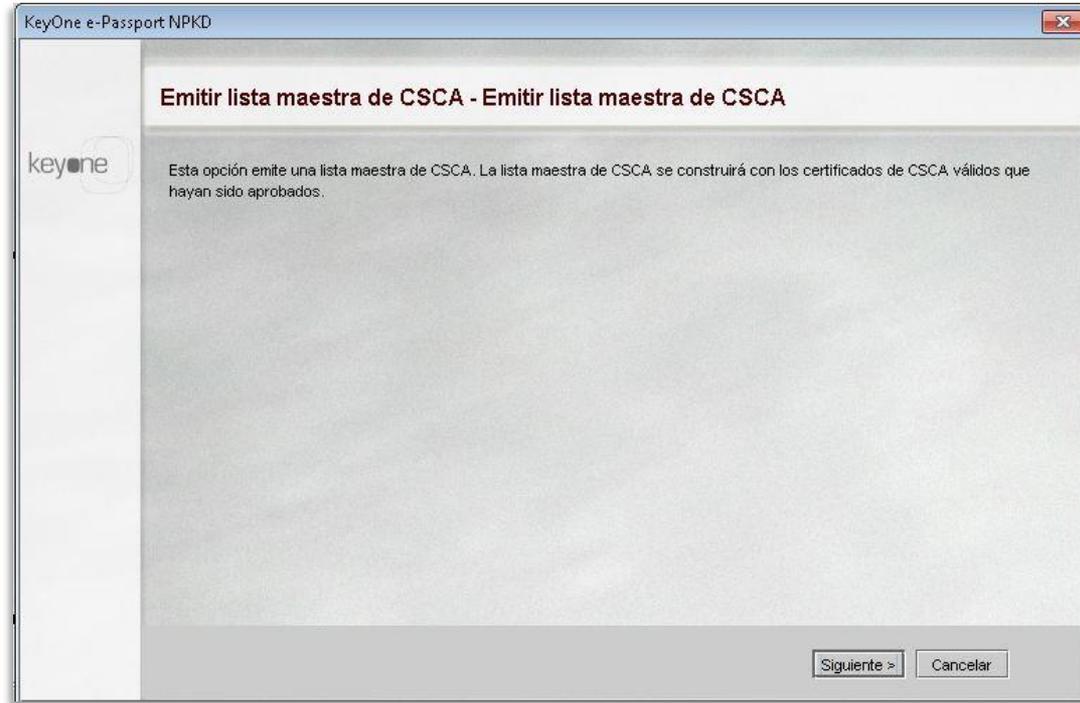




New features:

Inclusion of CSCA certificates in the Master Lists based on validations performed by Inspection Systems

- It allows the necessary validation threshold so that a CSCA certificate is included in the Master List.
- Inclusion of CSCA certificate in the Master List if the certificate is approved and in addition the validation threshold is exceeded.





NPKD1 - KeyOne e-Passport NPKD

Sesión Publicación en el PKD nacional

KeyOne e-Passport NPKD

- Tareas
 - Publicación en el PKD nacional
 - Listas maestras de CSCA
 - Certificados de CSCA
 - Certificados de DS
 - CRL
 - LDIF de ICAO
 - Gestión de claves
 - Certificados y claves
 - Configuración de seguridad
 - Definición del flujo de trabajo
 - Configuración administrativa
 - Herramientas administrativas
 - Add-ins
 - Logs

Estado	Tipo	Estado del certificado	Válido desde	Válido hasta	Insertado el
Mónaco (MC)	Certificado raíz	Pendiente	2015-06-11 15:33:31	2028-09-08 15:33:31	2016-07-15 12:26:59
Mónaco (MC)	Certificado raíz	Pendiente	2014-11-28 10:17:49	2023-02-28 10:27:49	2016-07-15 12:26:59
Portugal (PT)	Certificado de enlace	Pendiente	2016-03-10 17:34:04	2024-09-04 18:44:04	2016-07-15 12:26:58
Italia (IT)	Certificado raíz	Pendiente	2016-05-18 15:21:59	2031-08-13 15:21:59	2016-07-15 12:26:58
Chipre (CY)	Certificado de enlace	Pendiente	2014-11-06 01:31:21	2029-02-04 13:31:21	2016-07-15 12:26:58
Chipre (CY)	Certificado raíz	Pendiente	2011-08-01 16:16:57	2025-10-31 03:16:57	2016-07-15 12:26:58
Chipre (CY)	Certificado de enlace	Pendiente	2011-08-01 16:18:52	2025-10-31 03:18:52	2016-07-15 12:26:58
Singapur (SG)	Certificado raíz	Aprobado	2016-01-26 08:31:04	2031-01-26 09:01:04	2016-04-20 11:45:52
Singapur (SG)	Certificado de enlace	Aprobado	2016-01-26 11:59:07	2019-01-26 12:29:07	2016-04-20 11:45:30
Portugal (PT)	Certificado raíz	Aprobado	2016-03-22 12:22:55	2024-08-22 13:22:55	2016-04-20 11:44:53
San Cristóbal y Nieves (KN)	Certificado raíz	Pendiente	2010-12-09 15:15:40	2025-12-09 15:45:40	2016-04-20 11:19:07
EU	Certificado raíz	Pendiente	2015-11-04 01:00:00	2027-02-04 01:00:00	2016-04-20 11:19:07
República Checa (CZ)	Certificado raíz	Aprobado	2016-03-24 08:49:10	2031-06-24 09:49:10	2016-04-20 11:19:07
República Checa (CZ)	Certificado de enlace	Aprobado	2016-03-24 08:49:10	2026-06-25 02:00:00	2016-04-20 11:19:07
Irlanda (IE)	Certificado de enlace	Aprobado	2015-12-17 15:41:42	2026-01-06 13:09:31	2016-03-01 15:00:59
Irlanda (IE)	Certificado raíz	Aprobado	2015-12-17 15:41:42	2030-12-17 16:11:42	2016-03-01 15:00:59
Dinamarca (DK)	Certificado raíz	Aprobado	2015-10-28 09:24:23	2031-06-28 10:54:23	2016-03-01 15:00:59
Dinamarca (DK)	Certificado de enlace	Aprobado	2015-10-28 09:24:23	2027-05-05 13:17:22	2016-03-01 15:00:59
Georgia (GE)	Certificado raíz	Pendiente	2011-07-07 16:39:30	2026-10-01 16:39:30	2016-02-23 11:14:47
Finlandia (FI)	Certificado raíz	Aprobado	2016-01-29 09:06:50	2026-04-26 10:06:50	2016-02-23 11:14:47
Albania (AL)	Certificado raíz	Pendiente	2009-01-20 01:00:00	2024-04-22 02:00:00	2016-02-23 11:14:47
Portugal (PT)	Certificado de enlace	Pendiente	2016-01-26 12:04:13	2024-07-22 13:14:13	2016-02-23 11:14:47
Portugal (PT)	Certificado raíz	Pendiente	2016-01-26 11:47:54	2024-07-22 12:57:54	2016-02-23 11:14:47

< Primero < Anterior Siguiente > Último > Nueva consulta... Refrescar

1-30 / 266 Válidos Oficial Seguridad 6 SECURITY_OFFICER



ICAO

SECURITY & FACILITATION



ICAO

North American
Central American
and Caribbean
(NACC) Office
Mexico City

South American
(SAM) Office
Lima

ICAO
Headquarters
Montréal

Western and
Central African
(WACAF) Office
Dakar

European and
North Atlantic
(EUR/NAT) Office
Paris

Middle East
(MID) Office
Cairo

Eastern and
Southern African
(ESAF) Office
Nairobi

Asia and Pacific
(APAC) Sub-office
Beijing

Asia and Pacific
(APAC) Office
Bangkok



THANK YOU