ICAO SECURITY & FACILITATION

Spanish National PKD

Esther Fernández Crespo

Spanish National Police

Location/date

Spanish National PKD

Goals:

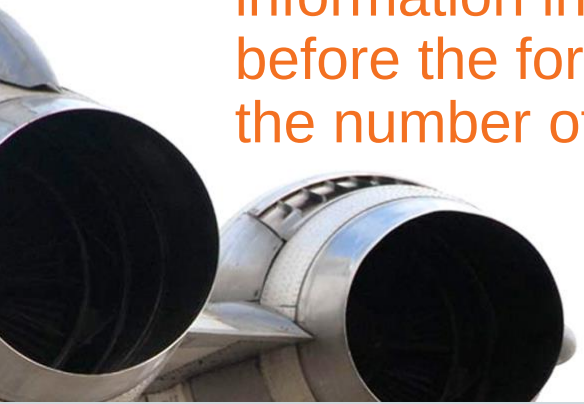
1. Show the new version of the Spanish NPKD
2. Adaptation to the new international regulations
3. New features for the improvement of the management of cryptographic material.

Spanish National PKD

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



Spanish National PKD

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.

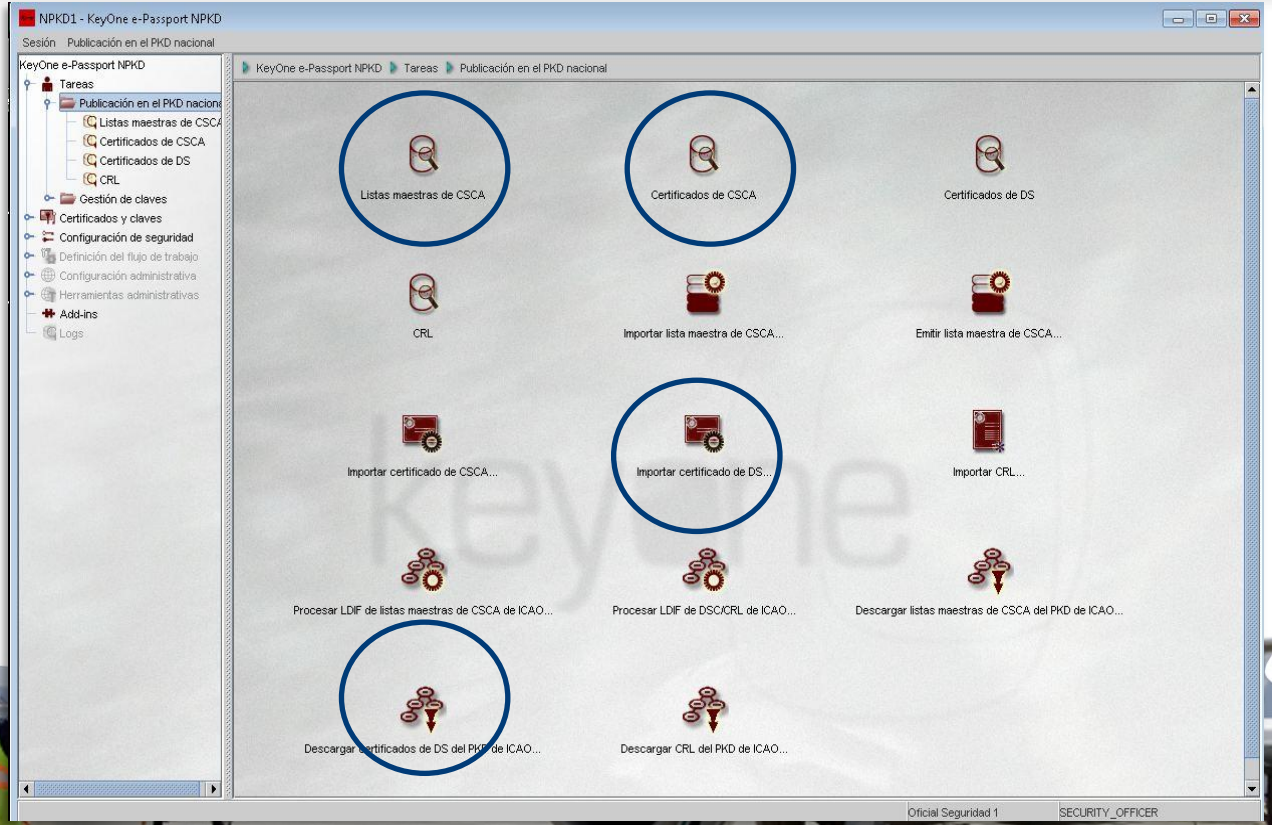
3. Issuing of the Master Lists

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

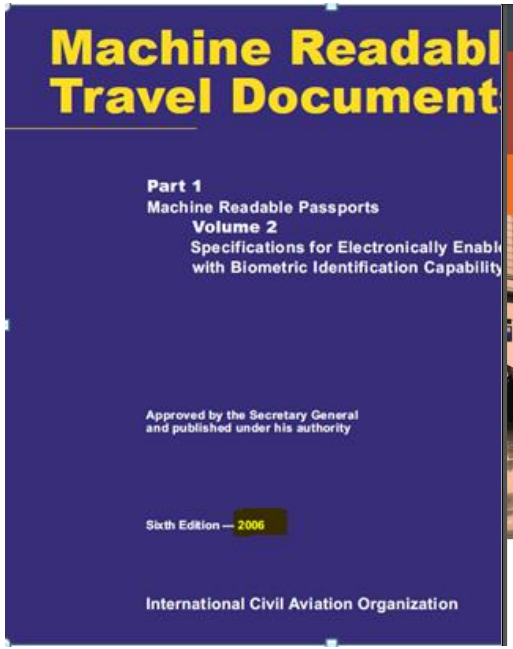
4. Data approval

- 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.

Spanish National PKD



Doc 9303: ICAO Regulations on certificate profiles



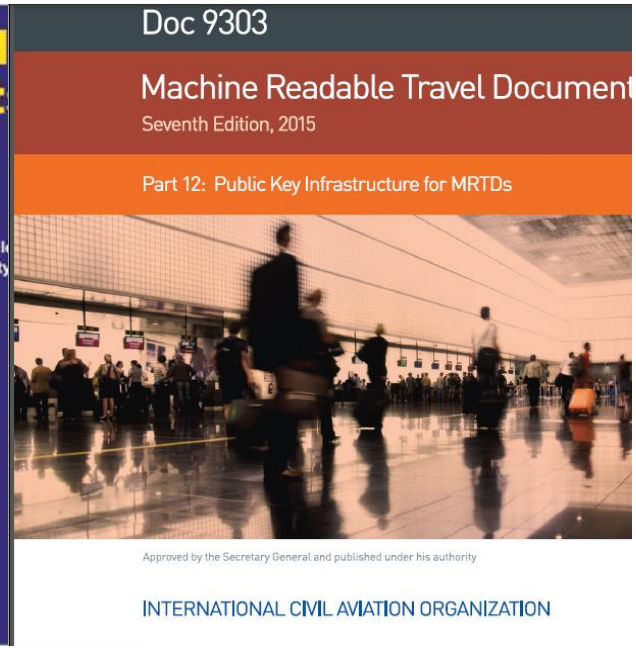


Table 4. Certificate Extensions Profile

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		

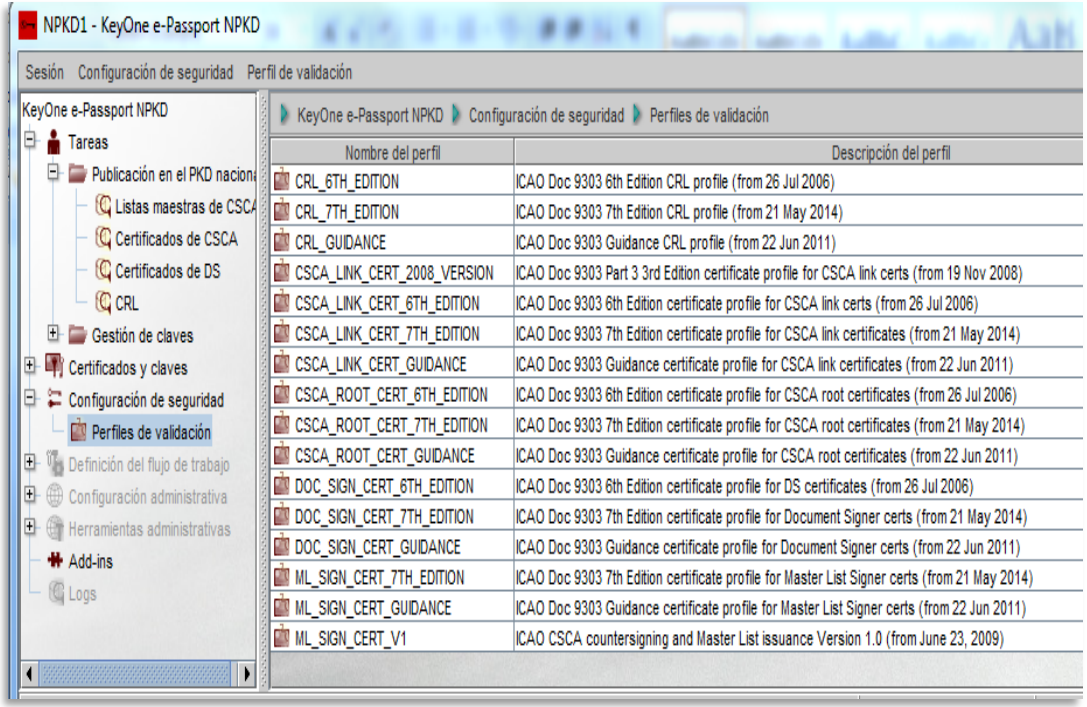
Spanish National PKD

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.



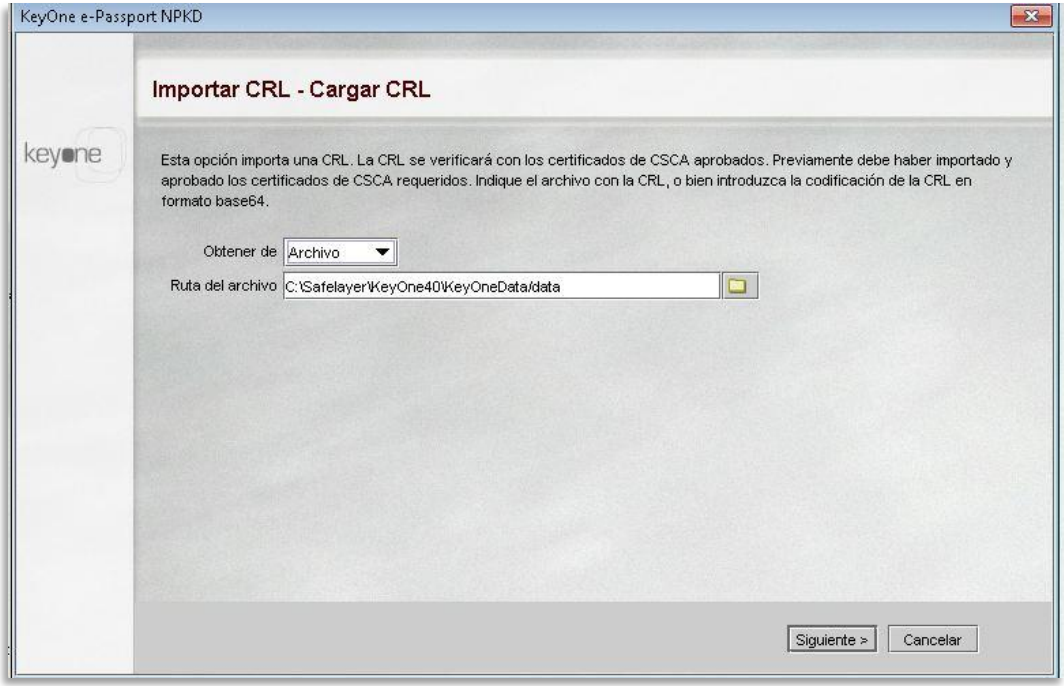
Nombre del perfil	Descripción del perfil
CRL_6TH_EDITION	ICAO Doc 9303 6th Edition CRL profile (from 26 Jul 2006)
CRL_7TH_EDITION	ICAO Doc 9303 7th Edition CRL profile (from 21 May 2014)
CRL_GUIDANCE	ICAO Doc 9303 Guidance CRL profile (from 22 Jun 2011)
CSCA_LINK_CERT_2008_VERSION	ICAO Doc 9303 Part 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)

Spanish National PKD

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)

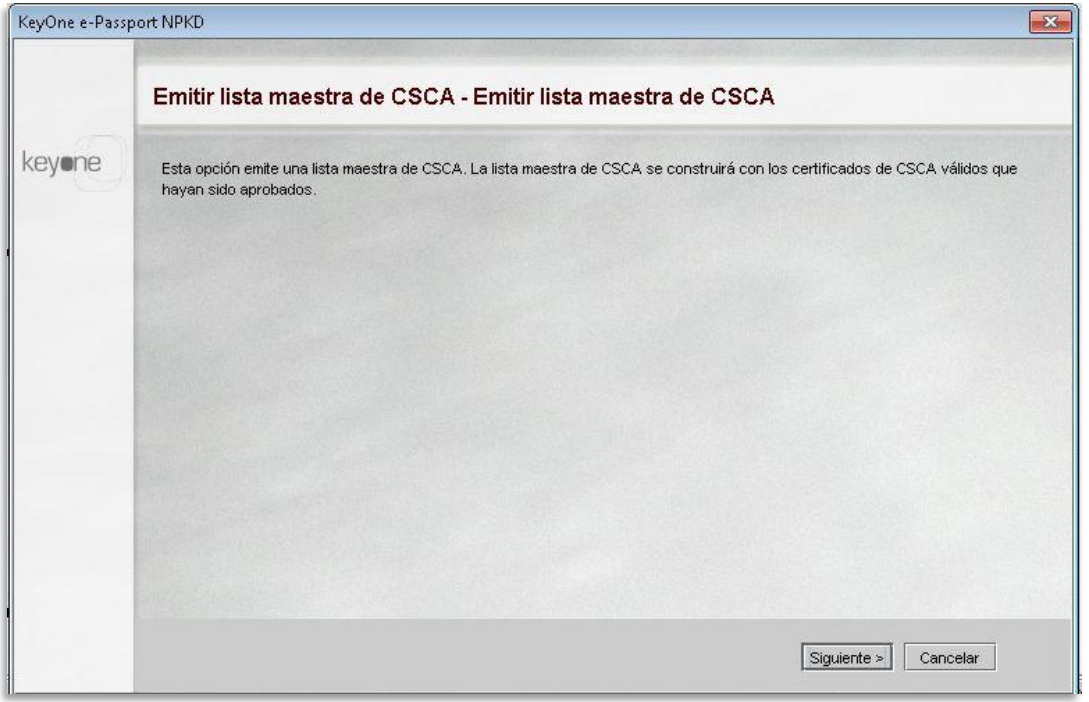


Spanish National PKD

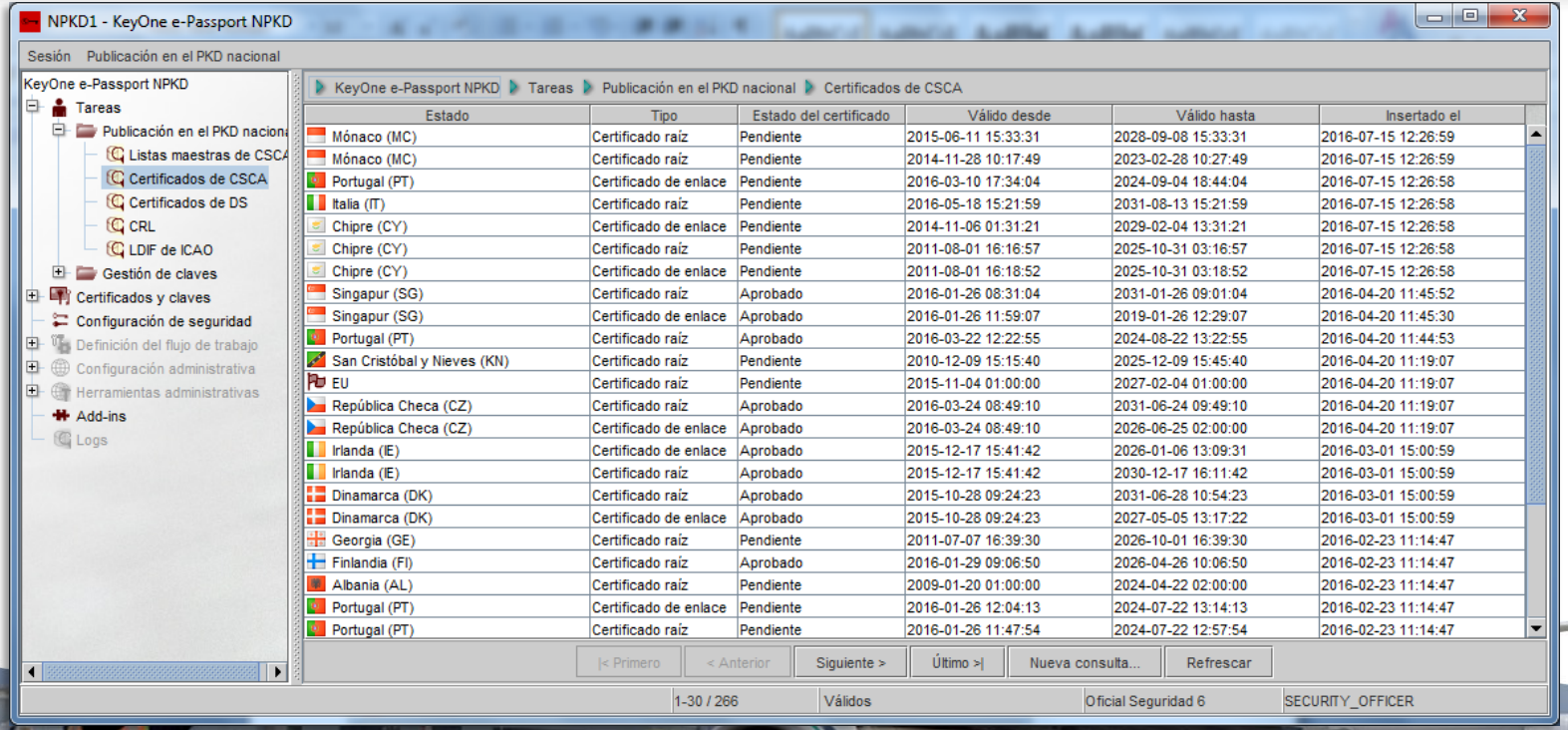
New features:

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.



Spanish National PKD



ICAO

THANK YOU