Certificado Digital

AC MRE

Autoridade Certificadora do Ministério das Relações Exteriores

Passaporte 10 anos

Data: 09/2015

Líder em soluções de TI para governo

O SERPRO atua no atendimento ao Ministério das Relações Exteriores e da Polícia Federal no projeto de emissão Passaporte Brasileiro desde 2005.

Neste ano foi iniciando o desenvolvimento dos sistemas

SINPA (Sistema de Passaporte da PF).
Sistema de emissão de passaporte pela Polícia Federal.

SCEDV (Sistema de Controle de emissão de documentos de viagens).
Sistema de emissão de passaporte nas representações do Brasil no exterior

O sistema SINPA entrou em produção em 2006.

O SERPRO iniciou a implantação do sistema SCEDV em 2008 e finalizou a implantação em 2010, este sistema foi implantado em 195 postos consulares no mundo.

Passaportes eletrônicos (2010).

- Assinados com certificados ICP-Brasil.
- Certificados do tipo A1.
- Certificados não conforme ao Padrão ICAO.
- Passaporte com validade de no máximo 5 anos.

Certificado Digital – ACMRE

ICP Brasil

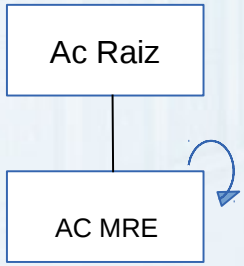
ICAO Public Key Directory (PKD)

ICAO PKD

SERPRO

RESOLUÇÃO Nº 101, DE 09 DE OUTUBRO DE 2013

Art. 1º Autorizar, excepcional e exclusivamente, a autoridade certificadora responsável pela emissão dos certificados digitais ICP-BRASIL que assinam digitalmente os documentos de viagem dos brasileiros a gerar os certificados auto-assinados, correspondentes ao CSCA (Country Signing Certificate Authority), e suas respectivas LCRs, utilizando os mesmos pares de chaves atrelados aos certificados das cadeias ICP-BRASIL, de modo a atender aos requisitos mínimos da ICAO, no que tange à inscrição do Brasil no Diretório de Chaves Públicas(PKD) dessa mesma entidade.



§1° A autoridade certificadora referida no caput deverá emitir certificados digitais ICP-BRASIL, correspondentes ao Document Signer da ICAO, com o único propósito de assinar digitalmente os documentos de viagem eletrônicos brasileiros, impedida a mesma de emitir certificados para outros fins.

PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL (DOC ICP01.01)

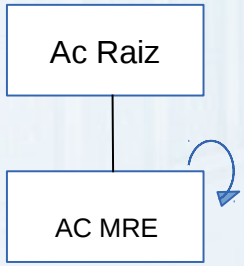
Geração de Chaves Assimétricas de AC	
Normativo ICP-Brasil	DOC-ICP-01 - item 6.1.1.3 DOC-ICP-04 - item 6.1.1.3 DOC-ICP-01 - item 6.1.5 DOC-ICP-05 - item 6.1.5
Algoritmo	RSA ou ECC-Brainpool (conforme RFC 5639)
Tamanho de chave	RSA 2048, RSA 4096, brainpoolP512r1

Nota (1): A função *hash* SHA-1 e os algoritmos criptográficos RSA 1024 bits para certificados de usuário final e RSA 2048 bits para certificados de AC NÃO DEVEM mais ser utilizados, a partir de 2012, nas emissões de certificados digitais, inclusive em suas requisições, conforme anexo II da Resolução n° 68. Suas previsões encontram-se nos normativos da ICP-Brasil somente para preservar a compatibilidade com os certificados emitidos até o final de 2011.

Geração de Chaves Assimétricas de Usuário Final	
Normativo ICP-Brasil	DOC-ICP-04 - item 6.1.5.2
Algoritmo	RSA ou ECC-Brainpool (conforme RFC 5639)
Tamanho de chave A1, A2, A3, S1, S2, S3, T3	RSA 1024, RSA 2048, brainpoolP256r1
Tamanho da chave A4, S4, T4	RSA 2048, RSA 4096, brainpoolP512r1

RESOLUÇÃO Nº 101, DE 09 DE OUTUBRO DE 2013

Art. 1º Autorizar, excepcional e exclusivamente, a autoridade certificadora responsável pela emissão dos certificados digitais ICP-BRASIL que assinam digitalmente os documentos de viagem dos brasileiros a gerar os certificados auto-assinados, correspondentes ao CSCA (Country Signing Certificate Authority), e suas respectivas LCRs, utilizando os mesmos pares de chaves atrelados aos certificados das cadeias ICP-BRASIL, de modo a atender aos requisitos mínimos da ICAO, no que tange à inscrição do Brasil no Diretório de Chaves Públicas(PKD) dessa mesma entidade.



§1° A autoridade certificadora referida no caput deverá emitir certificados digitais ICP-BRASIL, correspondentes ao Document Signer da ICAO, com o único propósito de assinar digitalmente os documentos de viagem eletrônicos brasileiros, impedida a mesma de emitir certificados para outros fins.

REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL - DOC-ICP-04 - versão 5.3

6.3.2.3. A Tabela 6, a seguir, define os períodos máximos de validade admitidos para cada tipo de certificado previsto pela ICP-Brasil:

Tabela 6 – Períodos de Validade dos Certificados

Tipo de Certificado	*Período Máximo de Validade do Certificado (em anos)*
A1 e S1	1
A2 e S2	2
A3, S3, T3	5
A4, S4, T4	11 (para cadeias hierárquicas completas em Curvas Elípticas)
	6 (para as demais hierarquias)

ITI

- Alteração do sistema Ywapa para assinar certificados com algoritmos ECC-Braimpool.
- Regulamentação e Criação da AC-RAIZ v4.

SERPRO

- Desenvolvimento da aplicação para atender aos requisitos do PKD-ICAO.
- Auditoria Operacional do ITI.
- Testes com ICP-Brasil e o PKD-ICAO
- Credenciamento da ACMRE.
- Criação da ACMRE

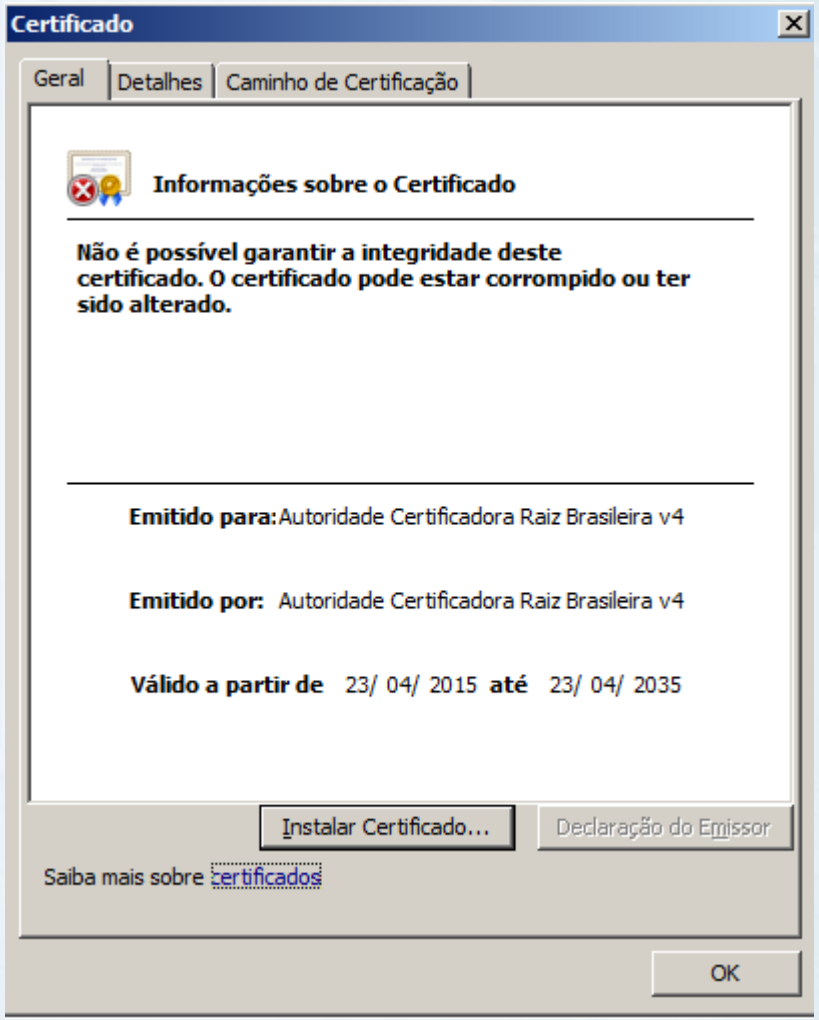
Certificado Digital – ACMRE

INTERNATIONAL CIVIL AVIATION ORGANIZATION

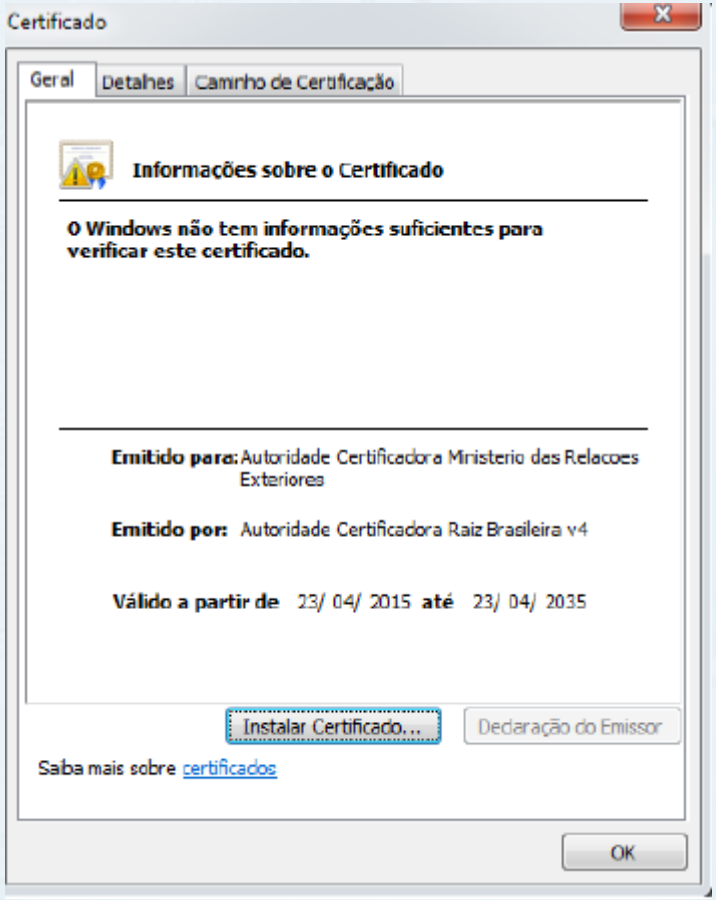
A United Nations Specialized Agency

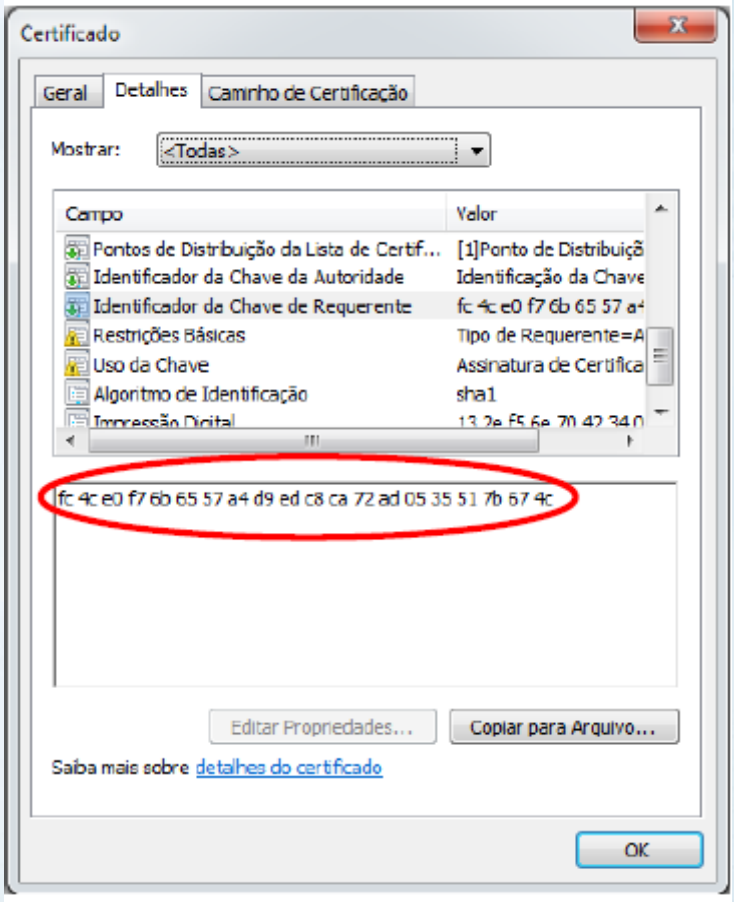
PKD Participant Number	State	Joining Date
1	Australia (PKD Board Member)	19.03.2007
2	New Zealand (PKD Board Member)	19.03.2007
3	Singapore (PKD Board Member)	19.03.2007
4	United Kingdom (PKD Board Member)	19.03.2007
5	Japan (PKD Board Member)	19.03.2007
6	Canada (PKD Board Member)	19.03.2007
7	United States of America (PKD Board Member)	02.11.2007
8	Germany	01.11.2007
9	Republic of Korea	28.03.2008
10	France	19.06.2008
11	People's Republic of China (PKD Board Member)	26.11.2008
12	Republic of Kazakhstan	19.12.2008
13	India	12.02.2009
14	Nigeria (PKD Board Member)	13.04.2009
15	Switzerland (Chair of PKD Board)	10.07.2009
16	Ukraine	30.10.2009
17	Latvia	28.06.2010
18	The Czech Republic	30.06.2010
19	Macao, China	28.09.2010
20	United Arab Emirates (PKD Board Member)	25.10.2010
21	Hong Kong, China	26.10.2010
22	Slovak Republic	23.11.2010
23	The Netherlands (PKD Board Member)	08.12.2010
24	Kingdom of Morocco	29.12.2010
25	Austria	31.12.2010
26	Hungary	15.02.2011
27	Norway	20.06.2011
28	Bulgaria	12.10.2011
29	Luxembourg	30.11.2011
30	Sweden (PKD Board Member)	01.12.2011
31	United Nations	14.06.2012
32	Spain	10.07.2012
33	Russian Federation	31.08.2012
34	Malaysia (PKD Board Member)	09.11.2012
35	Argentina	13.12.2012
36	Thailand	05.03.2013
37	Ireland	08.03.2013
38	Republic of Moldova	11.06.2013
39	Belgium	31.10.2013
40	Brazil (PKD Board Member)	03.01.2014
41	Qatar	10.03.2014
42	Seychelles	14.03.2014
43	Uzbekistan	19.03.2014
44	Philippines	21.03.2014
45	Iran (Islamic Republic of)	18.05.2014
46	Colombia	19.05.2015

ICP-Brasil v4

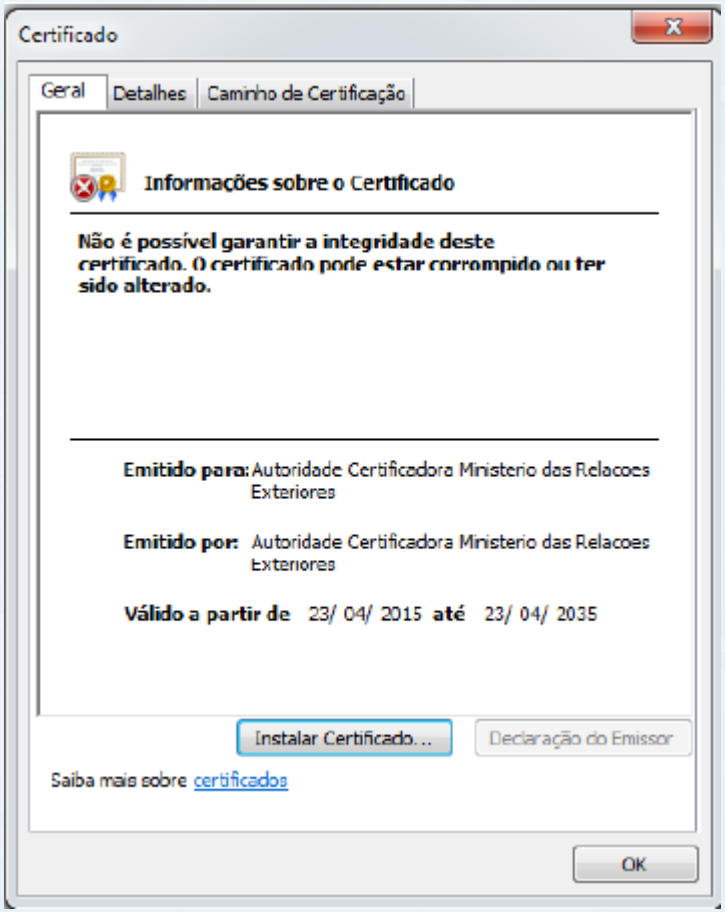


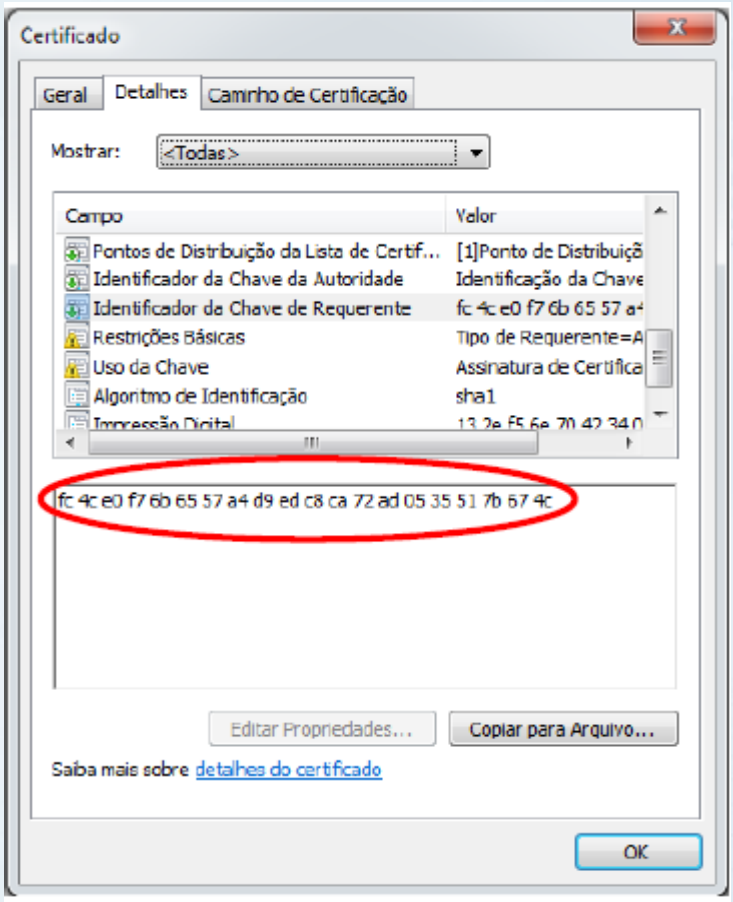
Certificado ACMRE – ASSINADO PELA ICP-BRASIL



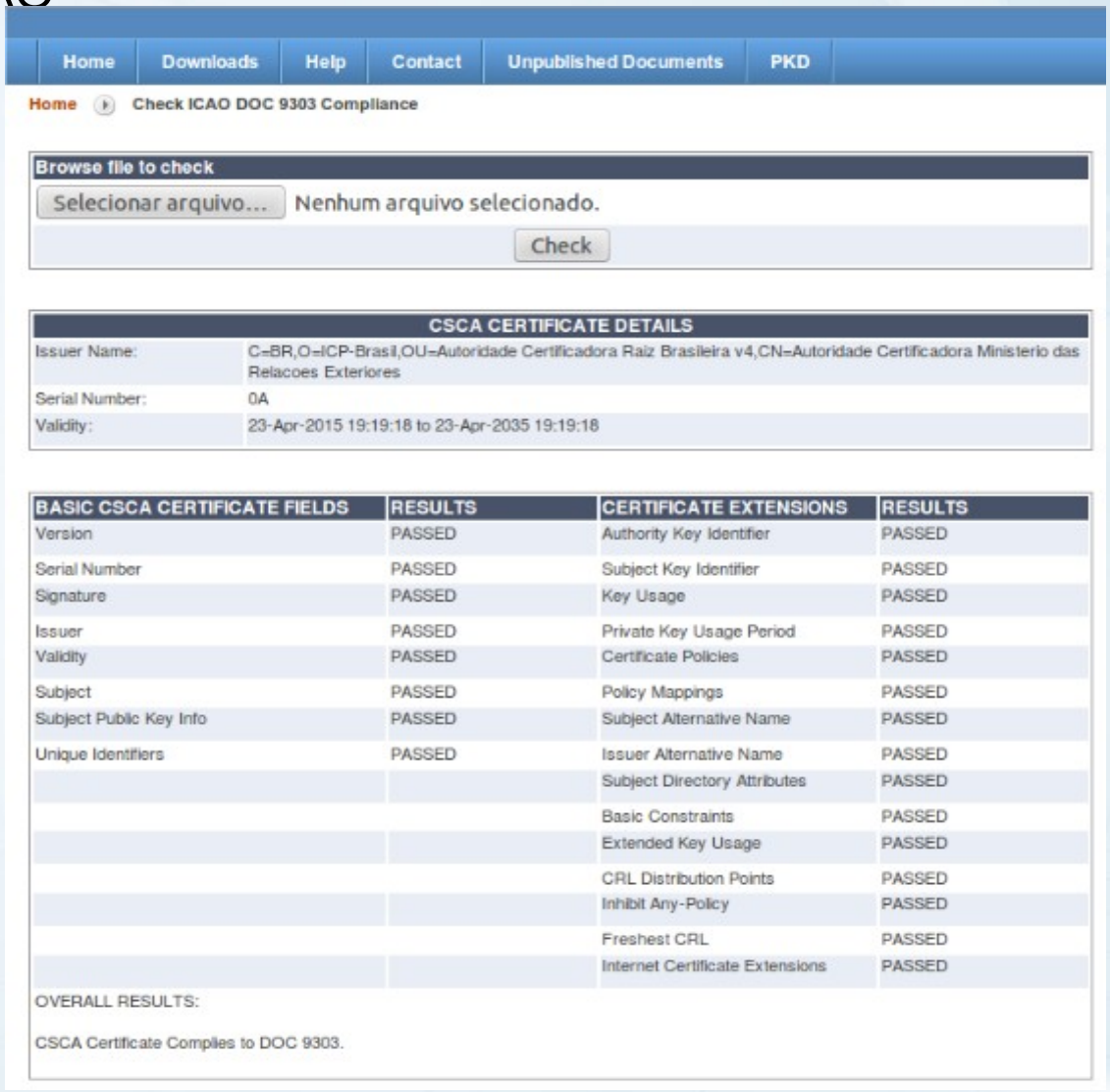


Certificado ACMRE – AUTO-ASSINADO





PKD-ICAO



Home | Downloads | Help | Contact | Unpublished Documents | PKD

Home ▸ Check ICAO DOC 9303 Compliance

Browse file to check

Selecionar arquivo... Nenhum arquivo selecionado.

Check

CSCA CERTIFICATE DETAILS

Issuer Name:	C=BR,O=ICP-Brasil,OU=Autoridade Certificadora Raiz Brasileira v4,CN=Autoridade Certificadora Ministerio das Relacoes Exteriores
Serial Number:	0A
Validity:	23-Apr-2015 19:19:18 to 23-Apr-2035 19:19:18

BASIC CSCA CERTIFICATE FIELDS	RESULTS	CERTIFICATE EXTENSIONS	RESULTS
Version	PASSED	Authority Key Identifier	PASSED
Serial Number	PASSED	Subject Key Identifier	PASSED
Signature	PASSED	Key Usage	PASSED
Issuer	PASSED	Private Key Usage Period	PASSED
Validity	PASSED	Certificate Policies	PASSED
Subject	PASSED	Policy Mappings	PASSED
Subject Public Key Info	PASSED	Subject Alternative Name	PASSED
Unique Identifiers	PASSED	Issuer Alternative Name	PASSED
		Subject Directory Attributes	PASSED
		Basic Constraints	PASSED
		Extended Key Usage	PASSED
		CRL Distribution Points	PASSED
		Inhibit Any-Policy	PASSED
		Freshest CRL	PASSED
		Internet Certificate Extensions	PASSED

OVERALL RESULTS:

CSCA Certificate Complies to DOC 9303.

PKD-ICAO

- Os certificados emitidos para as instituições que emitem passaportes são postados no diretório da ICAO para distribuição aos países membros.
- A cada dois meses é postada a LCR (Lista de Certificados Revogados) da ACMRE diretório da ICAO para distribuição aos países membros.

PKD-ICAO

```
dn: o=certificates,c=BR,dc=data,dc=pkddownload
objectClass: top
objectClass: organization
o: certificates

dn: cn=BRA,o=CRLs,c=BR,dc=data,dc=pkddownload
objectClass: top
objectClass: cRLDistributionPoint
certificateRevocationList:: MIIB7TCCAVECAQEwCgYIKoZIzj0EAwQwgZ4xRDBCBgNVBAMMO0
 F1dG9yaWRhZGUgQ2VydGlmaWNhZG9yYSBNaW5pc3RlcmlvIGRhcyBSZWxhY29lcyBFeHRlcmlvcmV
 zMTQwMgYDVQQLDCtBdXRvcmlkYWRlIENlcnRpZmljYWRvcmEgUmFpeiBCcmFzaWxlaXJhIHY0MRMw
 EQYDVQQKDApJQ1AtQnJhc2lsMQswCQYDVQQGEwJCUhcNMTUwNzIwMTMzOTE2WhcNMTUxMDE4MTMzO
 TE2WqCBgDB+MAsGA1UdFAQEAgIIMDBOBggrBgEFBQcBAQRCMEAwPgYIKwYBBQUHMAKGMmh0dHA6Ly
 9yZXBvc2l0b3Jpby5zZXJwcm8uZ292LmJyL2NhZGVpYXMvYWNtcmUucDdiMB8GA1UdIwQYMBaAFPx
 M4PdrZVek2e3IynKtBTVRe2dMMAoGCCqGSM49BAMEA4GJADCBhQJBAJTcmNtokkslZYE8L+pTF66l
 zZzDP9Q2PrbjUtWhmQbpEdIr8/ovEpeVU8Usxmxl6Lq9SfVQZvZTW1QAErfyJvkCQFw3EqiGeC62a
 MSUYLmcnmylI3xARH4enNcE/wVgbllbc9SVtkRyRMQiHkXc+ykhV7hWI1Q4yQT85y2LYh8p53U=
cn: BRA

dn: cn=C\=BR\,O\=ICP-Brasil\,OU\=Autoridade Certificadora Raiz Brasileira v4\,
 CN\=Autoridade Certificadora Ministerio das Relacoes Exteriores+sn=67,o=certi
 ficates,c=BR,dc=data,dc=pkddownload
userCertificate:: MIIGkDCCBfWgAwIBAgIBZzAKBggqhkjOPQQDBDCBnjFEMEIGA1UEAww7QXV0
 b3JpZGFkZSBDZXJ0aWZpY2Fkb3JhIE1pbmlzdGVyaW8gZGFzIFJlbGFjb2VzIEV4dGVyaW9yZXMxN
 DAyBgNVBAsMK0F1dG9yaWRhZGUgQ2VydGlmaWNhZG9yYSBSYWl6IEJyYXNpbGVpcmEgdjQxEzARBg
 NVBAoMCklDUC1CcmFzaWwxCzAJBgNVBAYTAkJSMB4XDTE1MDYxOTE1MDUzN1oXDTI2MDYxNjE1MDU
 zN1owgYMxFjAUBgNVBAMMDWVQYXNzIERTQ0EgdjExRzBFBgNVBAsMPkF1dG9yaWRhZGUgQ2VydGlm
 aWNhZG9yYSBkbyBNaW5pc3RlcmlvIGRhcyBSZWxhY29lcyBFeHRlcmlvcmVzMRMwEQYDVQQKDApJQ
 1AtQnJhc2lsMQswCQYDVQQGEwJCUjCCAjgwggGvBgcqhkjOPQIBMIIBogIBATBMBgcqhkjOPQEBAk
 EAqt2duNvpxIs/1OauM8n8B8swjbOzydIO1mOcynAzCHF9TZsAm8ZoQq7NoSrmo4DmKIH/Ly2CxoU
 oqmBWWDpI8zCBhARAeDCjMYtgO4niMnFFrCNMxZTL3Y09+RYQqDRByuqYY7wt7V1aqCU6oQou8cmL
 msi1fxEXpyvyx7nnwaxNd/yUygRAPfkWEKg0QcrqmGO8Le1dWqglOqEKLvHJi5rItX8RF6cr8se55
 8GsTXf8lMrcCD5nmEBQt1665d0oCb1jgBb3IwSBgQSBruS92C7ZZFohMi6cTGqThe2fcLXZFsG0O2
 Lu9NAJjv87H3ji0NSNUNFoe5O5fV98bVBHQGpeaIs1Igm8ufgifd44XVZjMuzA6r+pz3gi/fIJ9wA
 kpXsaoADFW4gfgRGy3N5JSl9IXlvKS9iKJ2Ou0corL6jwVAZ4zR4POtgIkgJBAKrdnbjb6cSLP9Tm
```

OBRIGADO !!!

pedro.motta@serpro.gov.br