International Civil Aviation Organization

Sixth Symposium and Exhibition
on ICAO MRTDs, Biometrics
and Security Standards

ICAO Headquarters, Montréal, Canada
1 - 4 November 2010

The role of PKD in ensuring compliance to Doc 9303

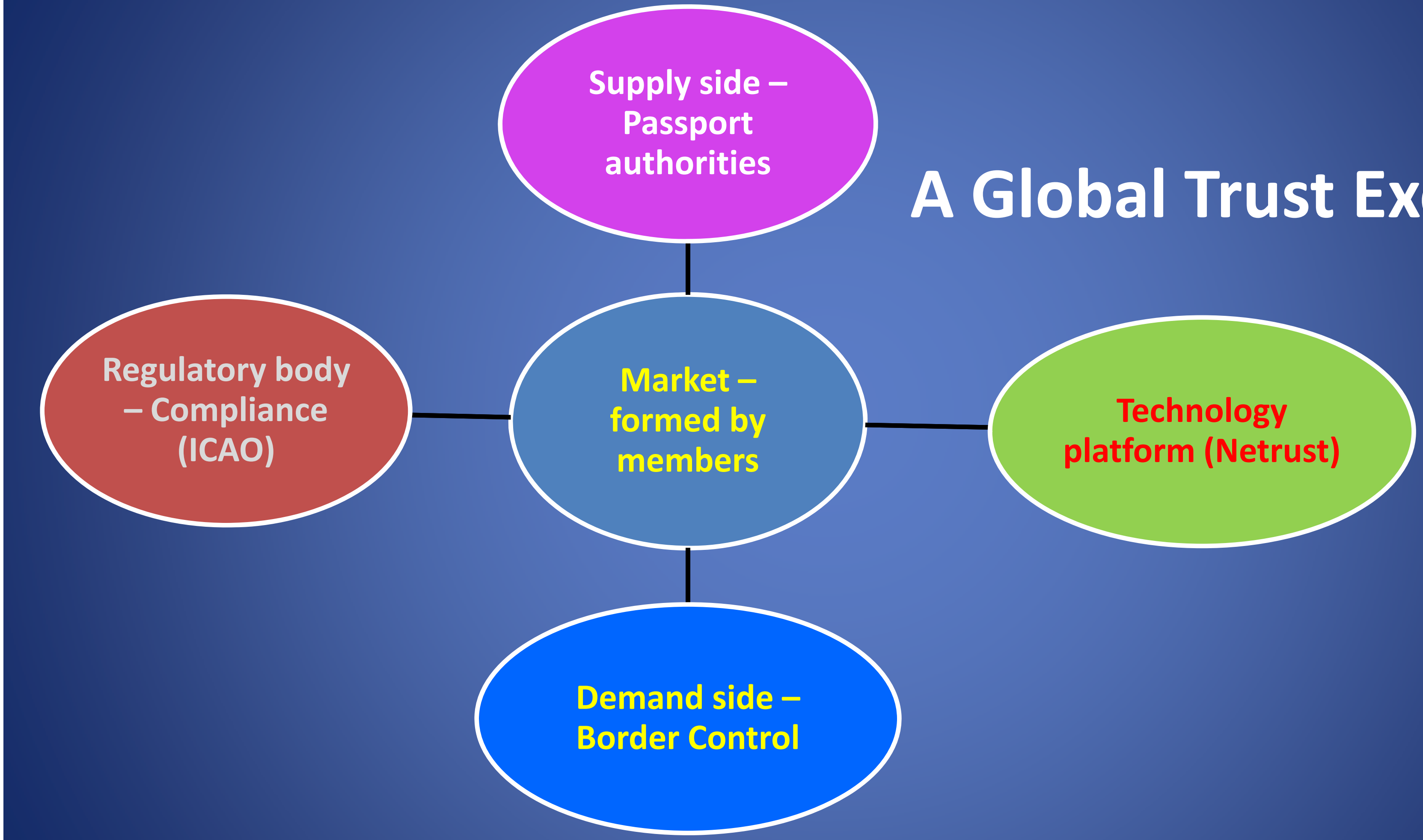
R Rajeshkumar

Dy. CEO

Netrust Pte Ltd

PKD Concept

A Global Trust Exchange



Supply side – Passport authorities

Regulatory body – Compliance (ICAO)

Market – formed by members

Technology platform (Netrust)

Demand side – Border Control

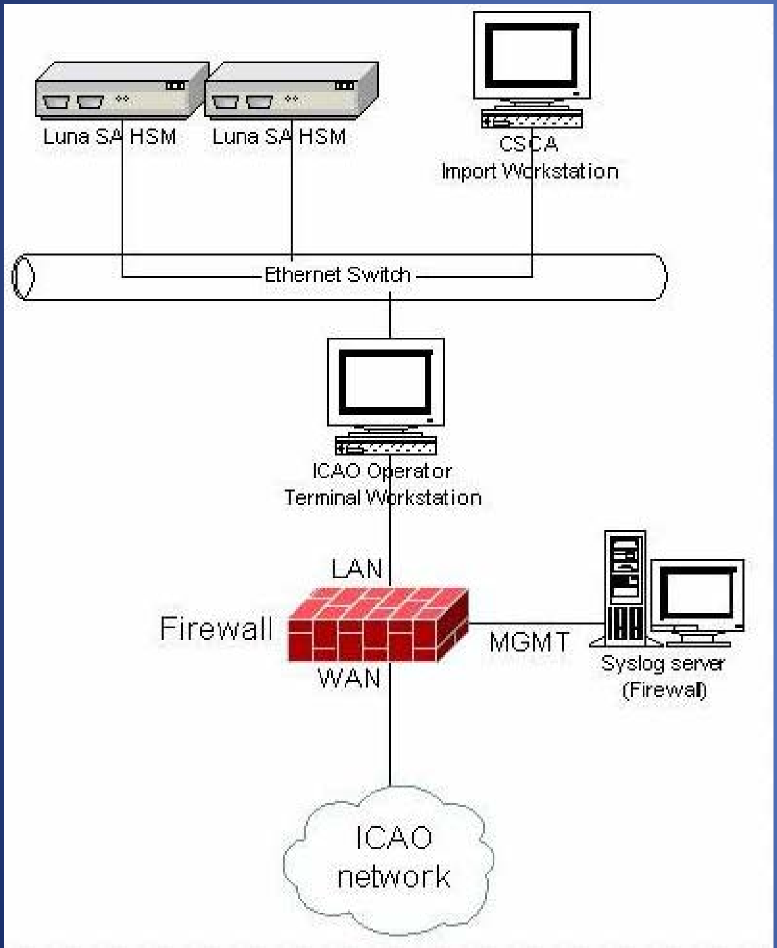
Current Services of the PKD

- Document Signers and CRLs of Participants
- CSCA Registry – Yellow Pages for the Passport Issuance Agency of the Participant
- CSCA Master List – List of CSCAs used by Participants
- Compliance website to check DSC/CRL/ML against Doc 9303

PKD Architecture

- Two locations – connected through redundant MPLS connection – Synchronised in real time
- 4 directories each location + 2 backup directories
- Upload is the only directory that can be accessed by the internet. Copy of data from Upload to Staging directory handled by software
- All other directory access requires VPN
- Download accessible through LDAP proxy servers only

PKD Architecture



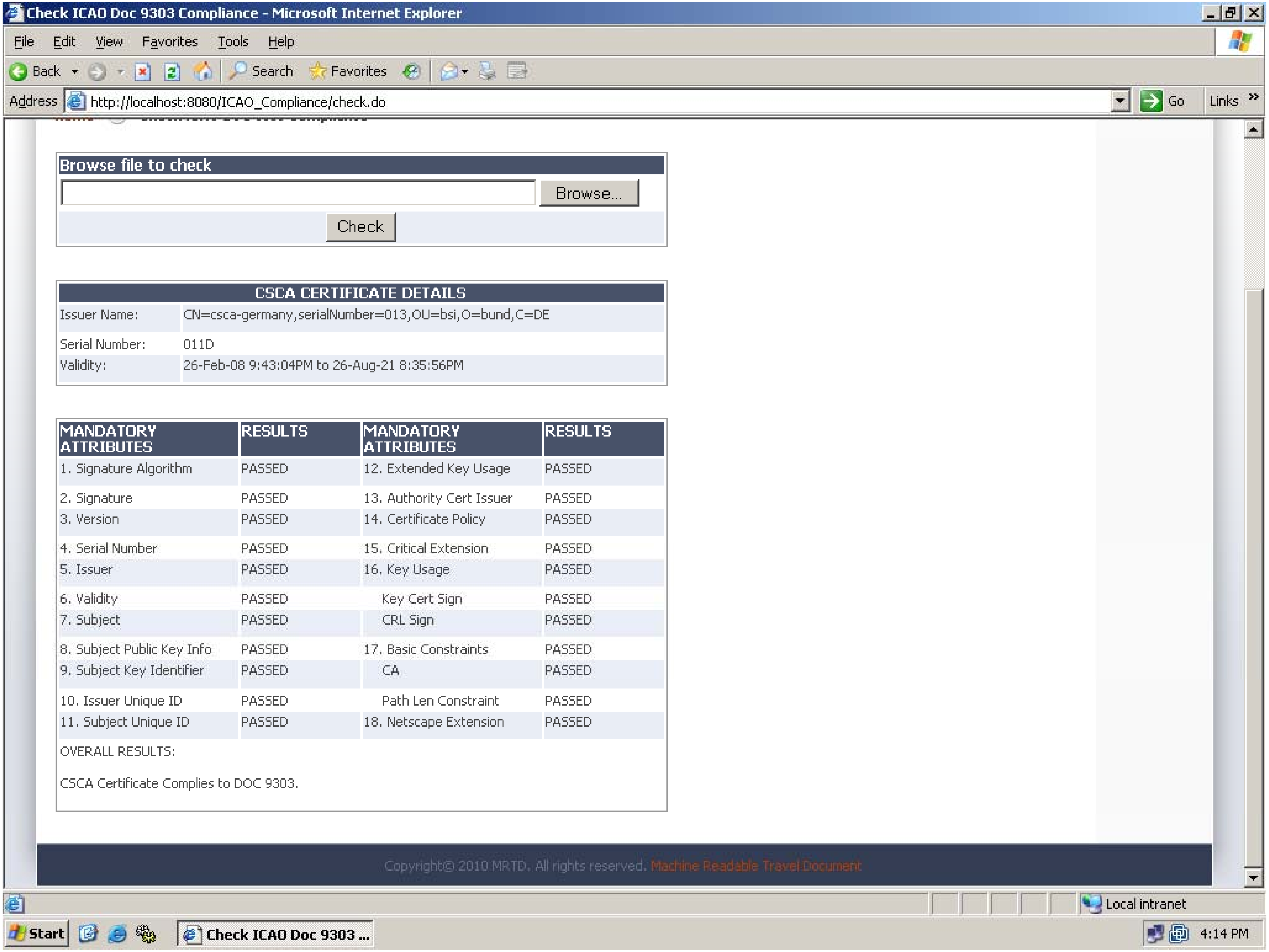
- Montreal Operations office
- Can only connect to Netrust datacenter through VPN
- CSCAs of Participants are maintained in HSM

PKD-Compliance Testing

- PKI TR is more restrictive than RFC 3280.
- An agreed set of checks are imposed on the uploaded CSCA/DSC/CRL.
- Any entry that fails verification is rejected.
- Any deviations that are accepted have to be discussed in PKD Board and approved by ICAO

E-Passport Trust Model

- Country Signing Certificate Authority (CSCA) is root of trust
- Document Signing Certificates (DSC) are issued with specific intent and authorization to sign Passport Data
- Link Certificates are used to exchange subsequent CSCAs among countries
- Link Certificates are not part of verification chain of DSC


Check ICAO Doc 9303 Compliance - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://localhost:8080/ICAO_Compliance/check.do
Go Links
Browse...
Check
Local intranet
Start
Check ICAO Doc 9303 ...
4:14 PM

Browse file to check

CSCA CERTIFICATE DETAILS

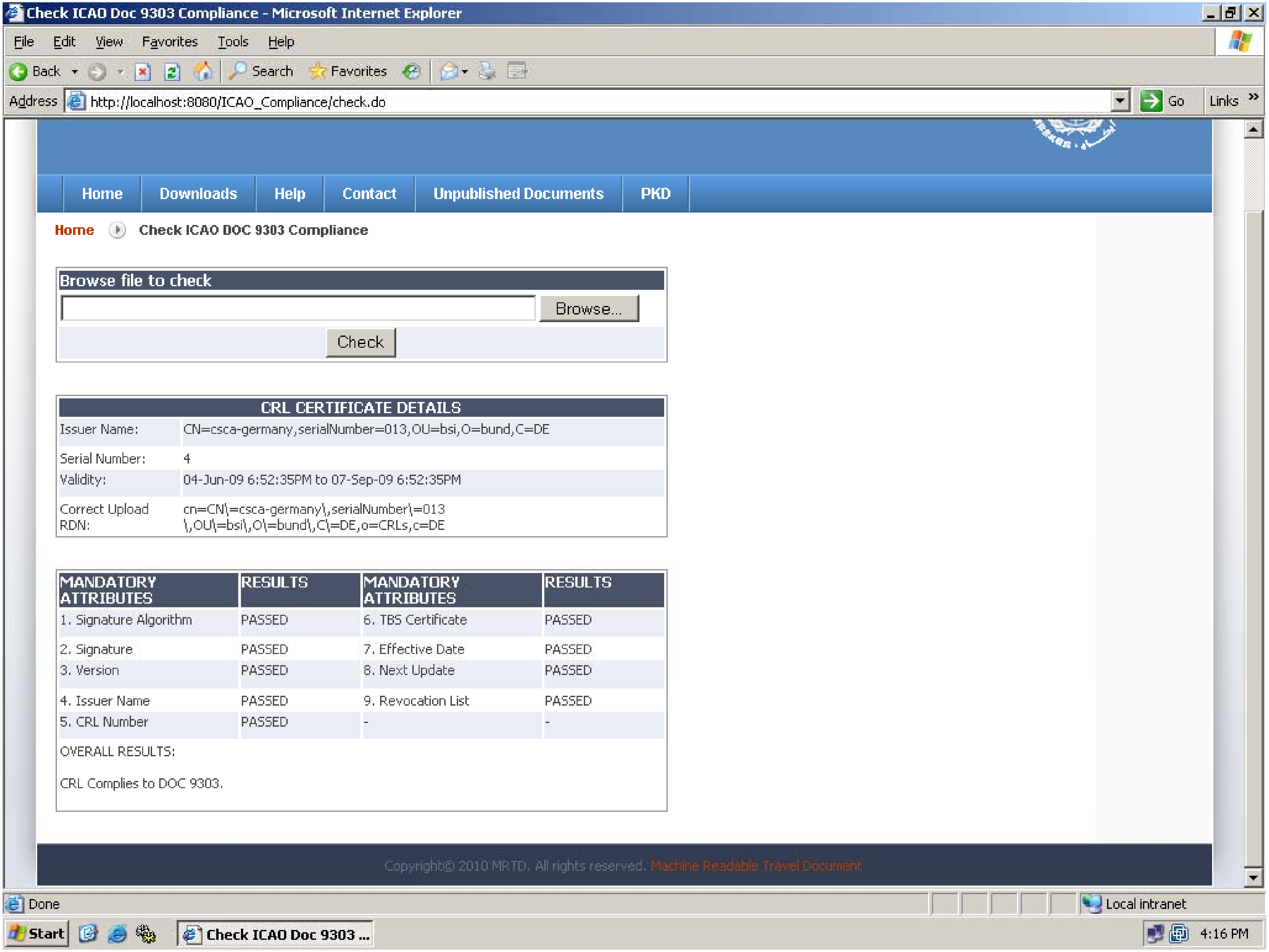
Issuer Name:	CN=csca-germany,serialNumber=013,OU=bsi,O=bund,C=DE
Serial Number:	011D
Validity:	26-Feb-08 9:43:04PM to 26-Aug-21 8:35:56PM

MANDATORY ATTRIBUTES	RESULTS	MANDATORY ATTRIBUTES	RESULTS
1. Signature Algorithm	PASSED	12. Extended Key Usage	PASSED
2. Signature	PASSED	13. Authority Cert Issuer	PASSED
3. Version	PASSED	14. Certificate Policy	PASSED
4. Serial Number	PASSED	15. Critical Extension	PASSED
5. Issuer	PASSED	16. Key Usage	PASSED
6. Validity	PASSED	Key Cert Sign	PASSED
7. Subject	PASSED	CRL Sign	PASSED
8. Subject Public Key Info	PASSED	17. Basic Constraints	PASSED
9. Subject Key Identifier	PASSED	CA	PASSED
10. Issuer Unique ID	PASSED	Path Len Constraint	PASSED
11. Subject Unique ID	PASSED	18. Netscape Extension	PASSED

OVERALL RESULTS:

CSCA Certificate Complies to DOC 9303.

Copyright© 2010 MRTD. All rights reserved. Machine Readable Travel Document


Check ICAO Doc 9303 Compliance - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://localhost:8080/ICAO_Compliance/check.do
Go Links
Home Downloads Help Contact Unpublished Documents PKD
Home Check ICAO DOC 9303 Compliance
Browse...
Check
Done
Local intranet
Start
Check ICAO Doc 9303 ...
4:16 PM

Browse file to check

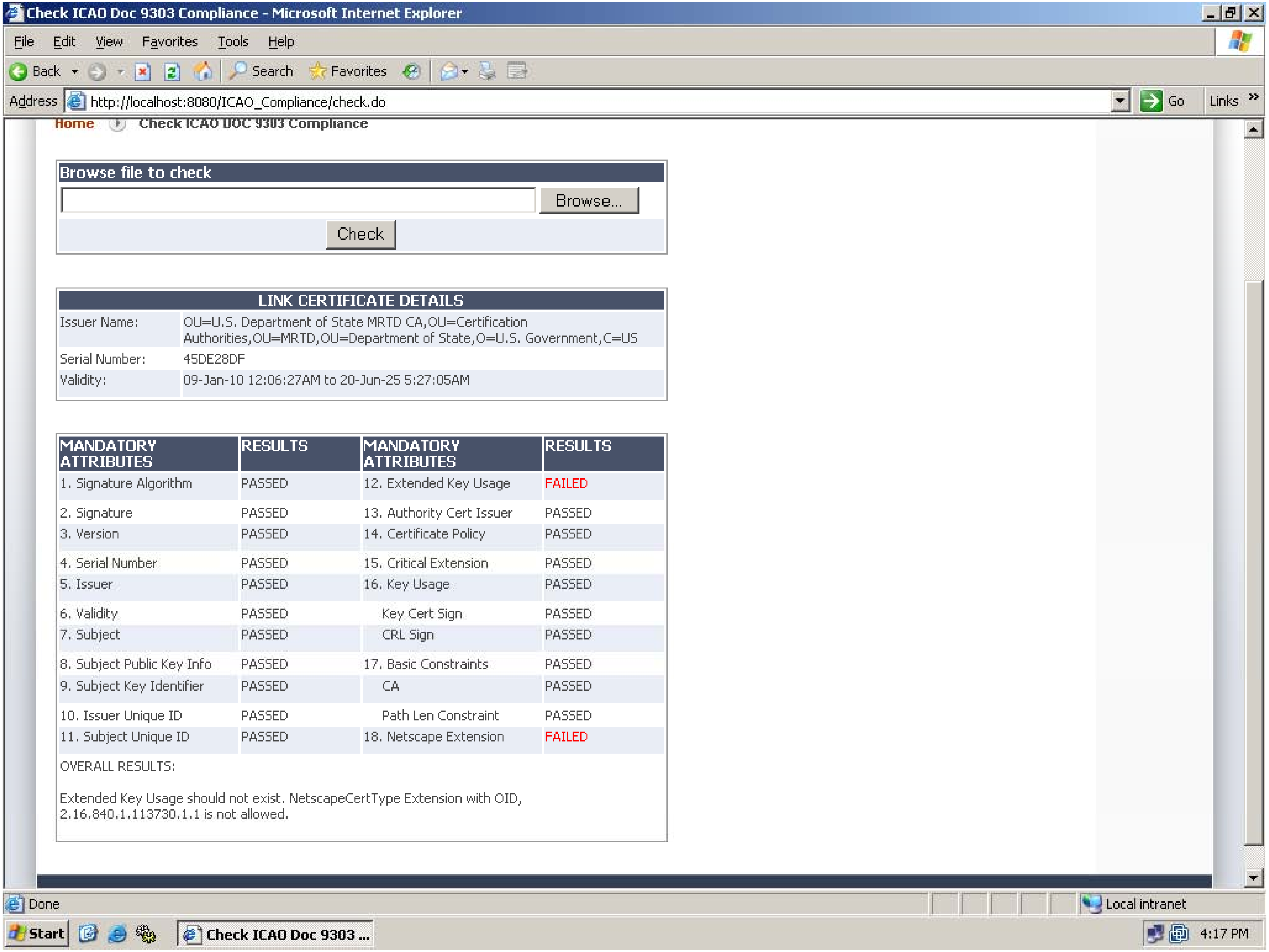
CRL CERTIFICATE DETAILS

Issuer Name:	CN=csca-germany,serialNumber=013,OU=bsi,O=bund,C=DE
Serial Number:	4
Validity:	04-Jun-09 6:52:35PM to 07-Sep-09 6:52:35PM
Correct Upload RDN:	cn=CN\=csca-germany\,serialNumber\=013 \,OU\=bsi\,O\=bund\,C\=DE,o=CRLs,c=DE

MANDATORY ATTRIBUTES	RESULTS	MANDATORY ATTRIBUTES	RESULTS
1. Signature Algorithm	PASSED	6. TBS Certificate	PASSED
2. Signature	PASSED	7. Effective Date	PASSED
3. Version	PASSED	8. Next Update	PASSED
4. Issuer Name	PASSED	9. Revocation List	PASSED
5. CRL Number	PASSED	-	-

OVERALL RESULTS:

CRL Complies to DOC 9303.



LINK CERTIFICATE DETAILS	
Issuer Name:	OU=U.S. Department of State MRTD CA,OU=Certification Authorities,OU=MRTD,OU=Department of State,O=U.S. Government,C=US
Serial Number:	45DE28DF
Validity:	09-Jan-10 12:06:27AM to 20-Jun-25 5:27:05AM

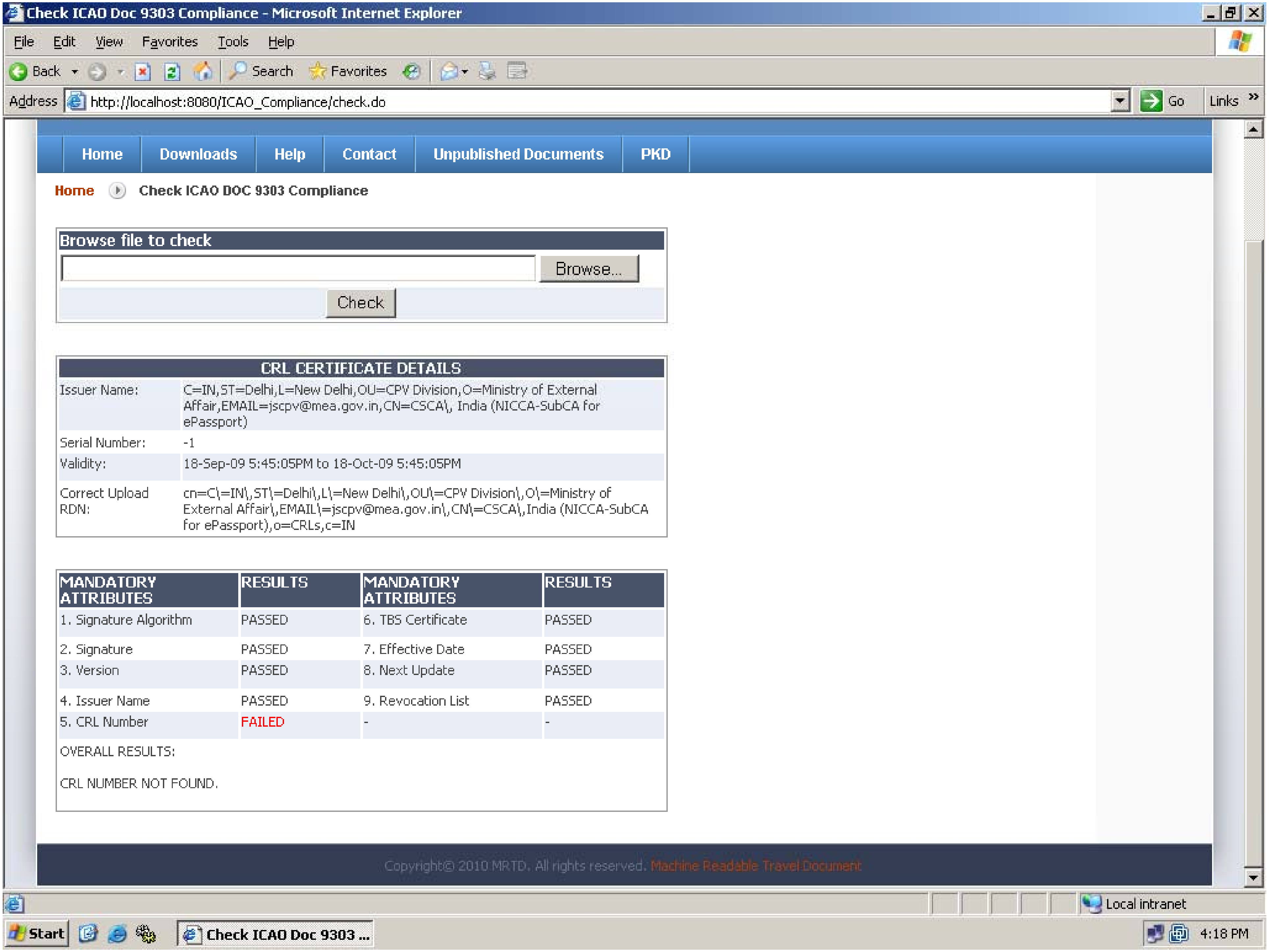
MANDATORY ATTRIBUTES	RESULTS	MANDATORY ATTRIBUTES	RESULTS
1. Signature Algorithm	PASSED	12. Extended Key Usage	FAILED
2. Signature	PASSED	13. Authority Cert Issuer	PASSED
3. Version	PASSED	14. Certificate Policy	PASSED
4. Serial Number	PASSED	15. Critical Extension	PASSED
5. Issuer	PASSED	16. Key Usage	PASSED
6. Validity	PASSED	Key Cert Sign	PASSED
7. Subject	PASSED	CRL Sign	PASSED
8. Subject Public Key Info	PASSED	17. Basic Constraints	PASSED
9. Subject Key Identifier	PASSED	CA	PASSED
10. Issuer Unique ID	PASSED	Path Len Constraint	PASSED
11. Subject Unique ID	PASSED	18. Netscape Extension	FAILED

OVERALL RESULTS:

Extended Key Usage should not exist. NetscapeCertType Extension with OID, 2.16.840.1.113730.1.1 is not allowed.

Compliance Issue

- Problem
  - Extended Key Usage has been set
  - NetScape Certificate Extensions are present
- Issue
  - If EKU is present, then validation software has to process EKU and accept certificate for purposes that satisfy both basic Key Usage and Extended Key Usage. Will affect validation software
  - NetScape Certificate Extensions are the pre-cursor to EKU



Address: http://localhost:8080/ICAO_Compliance/check.do

Home › Check ICAO DOC 9303 Compliance

Browse file to check

CRL CERTIFICATE DETAILS	
Issuer Name:	C=IN,ST=Delhi,L=New Delhi,OU=CPV Division,O=Ministry of External Affair,EMAIL=jscpv@mea.gov.in,CN=CSCA\, India (NICCA-SubCA for ePassport)
Serial Number:	-1
Validity:	18-Sep-09 5:45:05PM to 18-Oct-09 5:45:05PM
Correct Upload RDN:	cn=C\=IN\,ST\=Delhi\,L\=New Delhi\,OU\=CPV Division\,O\=Ministry of External Affair\,EMAIL\=jscpv@mea.gov.in\,CN\=CSCA\,India (NICCA-SubCA for ePassport),o=CRLs,c=IN

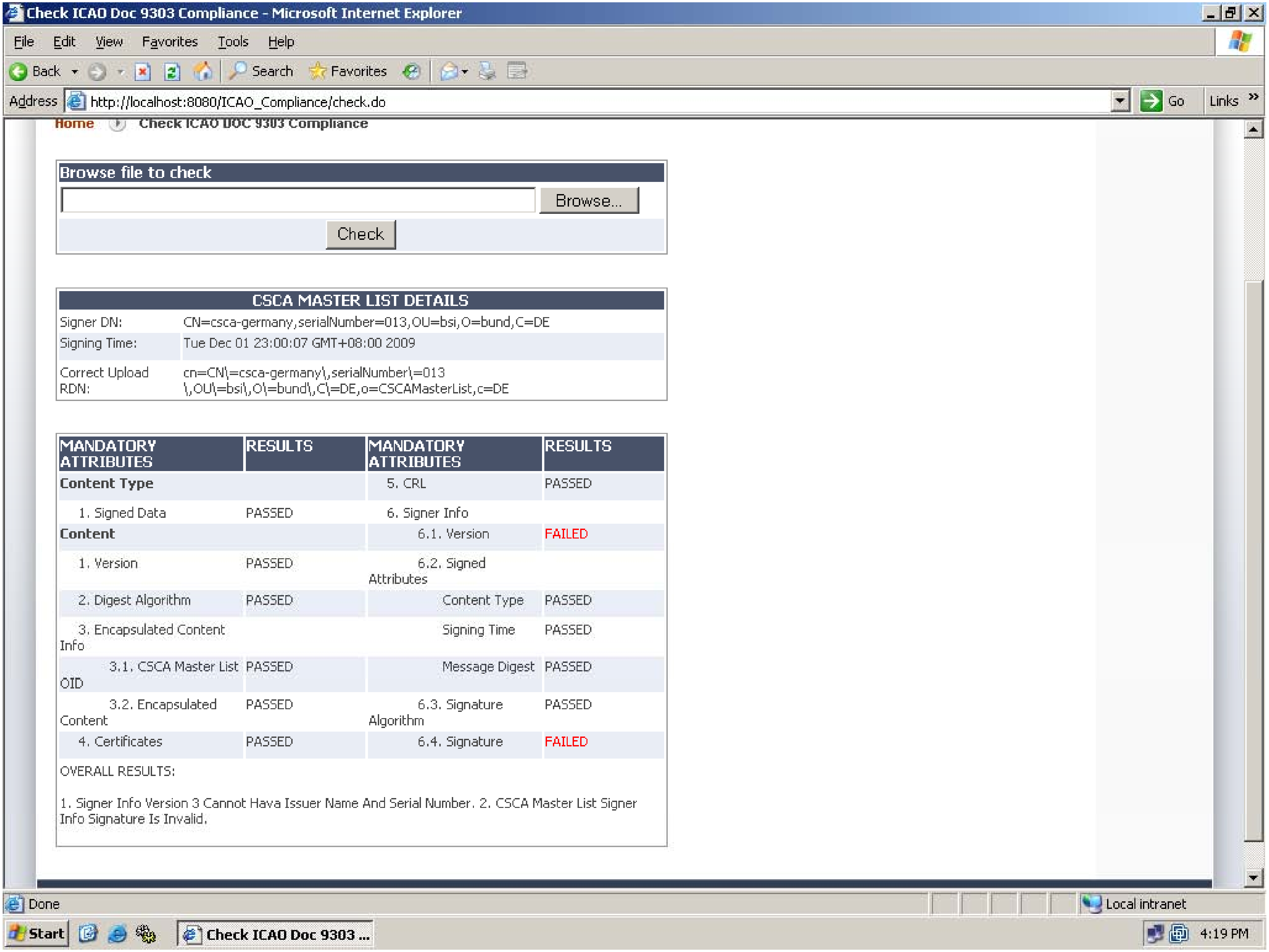
MANDATORY ATTRIBUTES	RESULTS	MANDATORY ATTRIBUTES	RESULTS
1. Signature Algorithm	PASSED	6. TBS Certificate	PASSED
2. Signature	PASSED	7. Effective Date	PASSED
3. Version	PASSED	8. Next Update	PASSED
4. Issuer Name	PASSED	9. Revocation List	PASSED
5. CRL Number	FAILED	-	-

OVERALL RESULTS:

CRL NUMBER NOT FOUND.

Compliance Issue

- Problem
  - – CRL Number is not present
- Issue
  - – CRLs can be validated based on the parameters “thisUpdate” and “nextUpdate”.
  - – If two valid CRLs are present, CRL number is used to choose the latest CRL



Home › **Check ICAO DOC 9303 Compliance**

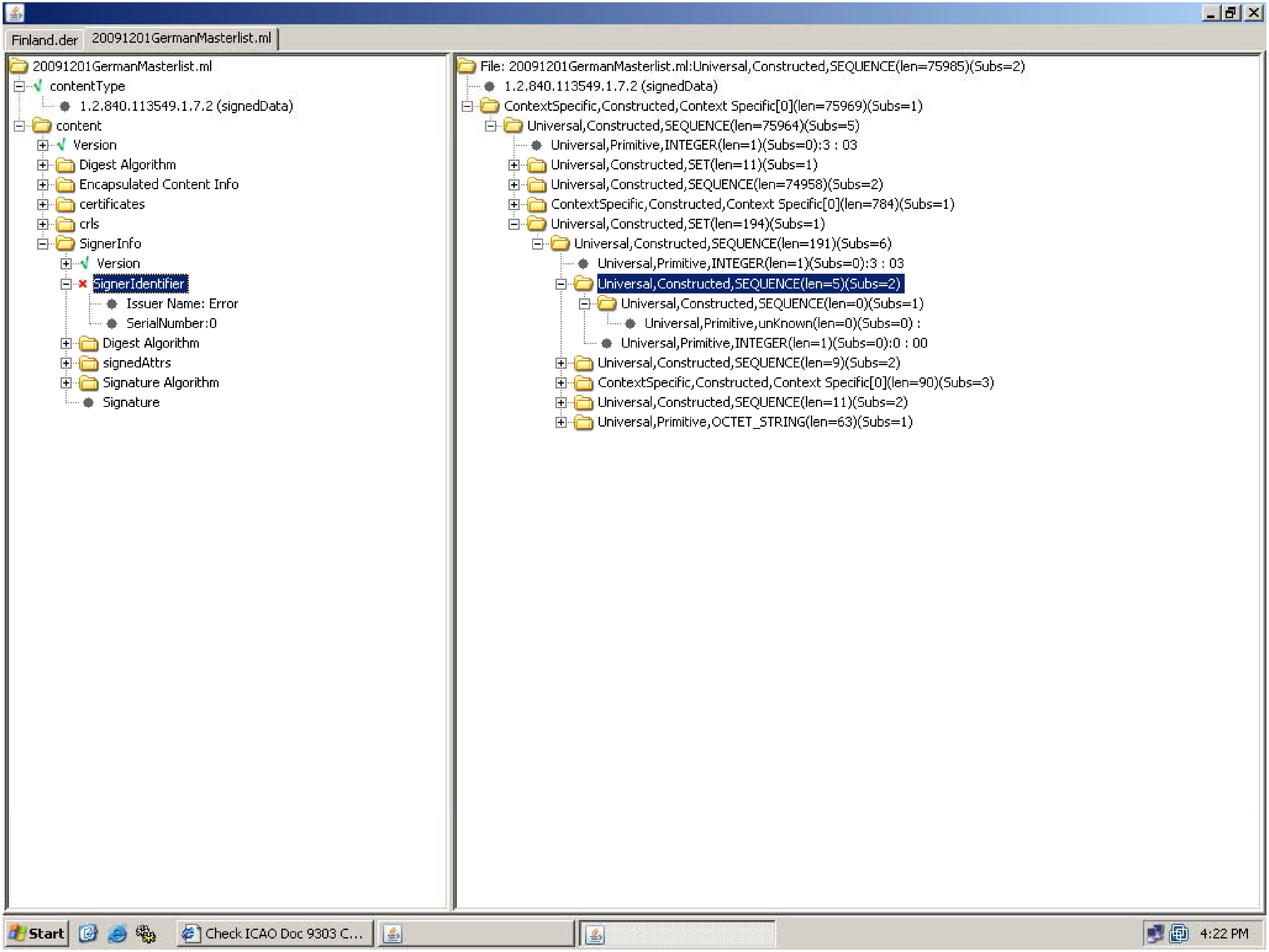
Browse file to check

CSCA MASTER LIST DETAILS	
Signer DN:	CN=csca-germany,serialNumber=013,OU=bsi,O=bund,C=DE
Signing Time:	Tue Dec 01 23:00:07 GMT+08:00 2009
Correct Upload RDN:	cn=CN\=csca-germany\,serialNumber\=013 \,OU\=bsi\,O\=bund\,C\=DE,o=CSCAMasterList,c=DE

MANDATORY ATTRIBUTES	RESULTS	MANDATORY ATTRIBUTES	RESULTS
Content Type		5. CRL	PASSED
1. Signed Data	PASSED	6. Signer Info	
Content		6.1. Version	FAILED
1. Version	PASSED	6.2. Signed Attributes	
2. Digest Algorithm	PASSED	Content Type	PASSED
3. Encapsulated Content Info		Signing Time	PASSED
3.1. CSCA Master List OID	PASSED	Message Digest	PASSED
3.2. Encapsulated Content	PASSED	6.3. Signature Algorithm	PASSED
4. Certificates	PASSED	6.4. Signature	FAILED

OVERALL RESULTS:

1. Signer Info Version 3 Cannot Hava Issuer Name And Serial Number. 2. CSCA Master List Signer Info Signature Is Invalid.

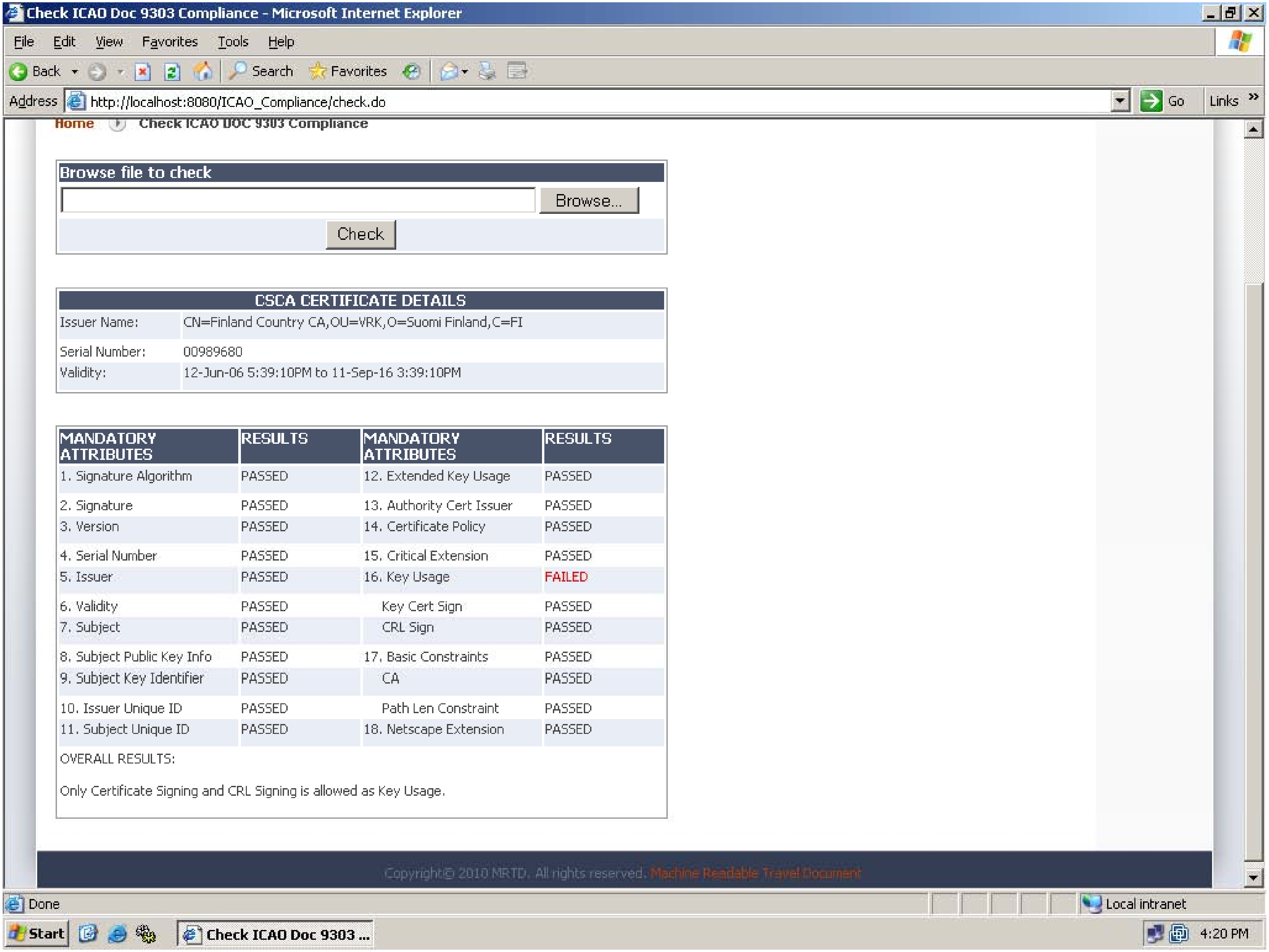


```
20091201GermanMasterlist.ml
  contentType
    1.2.840.113549.1.7.2 (signedData)
  content
    Version
    Digest Algorithm
    Encapsulated Content Info
    certificates
    crls
    SignerInfo
      Version
      SignerIdentifier
        Issuer Name: Error
        SerialNumber:0
      Digest Algorithm
      signedAttrs
      Signature Algorithm
      Signature
```

```
File: 20091201GermanMasterlist.ml:Universal,Constructed,SEQUENCE(len=75985)(Subs=2)
  1.2.840.113549.1.7.2 (signedData)
  ContextSpecific,Constructed,Context Specific[0](len=75969)(Subs=1)
    Universal,Constructed,SEQUENCE(len=75964)(Subs=5)
      Universal,Primitive,INTEGER(len=1)(Subs=0):3 : 03
      Universal,Constructed,SET(len=11)(Subs=1)
      Universal,Constructed,SEQUENCE(len=74958)(Subs=2)
      ContextSpecific,Constructed,Context Specific[0](len=784)(Subs=1)
      Universal,Constructed,SET(len=194)(Subs=1)
        Universal,Constructed,SEQUENCE(len=191)(Subs=6)
          Universal,Primitive,INTEGER(len=1)(Subs=0):3 : 03
          Universal,Constructed,SEQUENCE(len=5)(Subs=2)
            Universal,Constructed,SEQUENCE(len=0)(Subs=1)
              Universal,Primitive,unKnown(len=0)(Subs=0) :
            Universal,Primitive,INTEGER(len=1)(Subs=0):0 : 00
          Universal,Constructed,SEQUENCE(len=9)(Subs=2)
          ContextSpecific,Constructed,Context Specific[0](len=90)(Subs=3)
          Universal,Constructed,SEQUENCE(len=11)(Subs=2)
          Universal,Primitive,OCTET_STRING(len=63)(Subs=1)
```

Compliance Issue

- Problem
  - SignerInfo Version is 3, meaning SKI is used for identifying Master List Signer. Encoding contains “Issuer and Serial Number”.
- Issue
  - The Master List Signer is not properly identified and hence Signature cannot be trusted.


Check ICAO Doc 9303 Compliance - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://localhost:8080/ICAO_Compliance/check.do
Go Links
Home
Check ICAO DOC 9303 Compliance
Browse...
Check
Done
Local intranet
Start
Check ICAO Doc 9303 ...
4:20 PM

Browse file to check

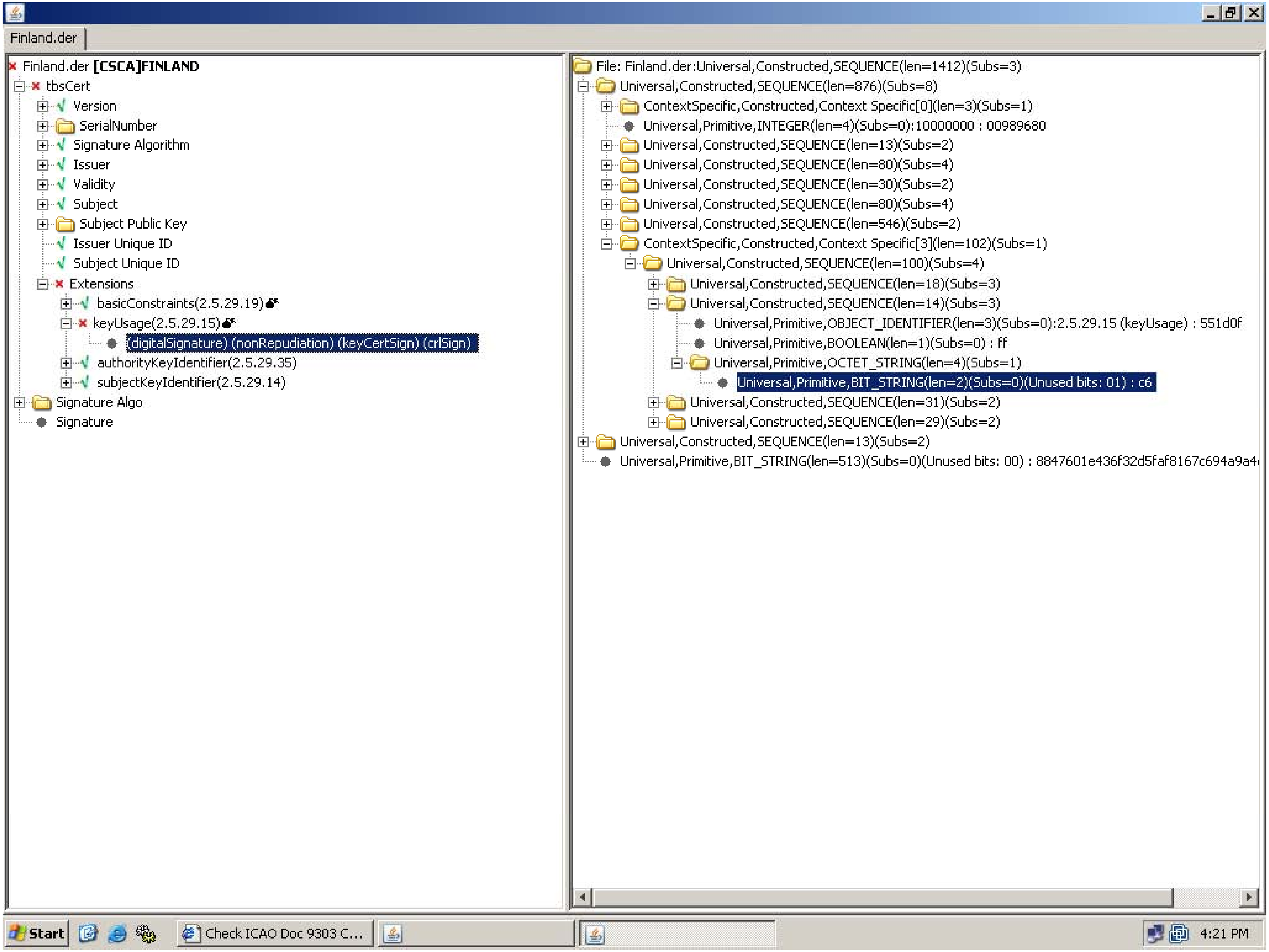
CSCA CERTIFICATE DETAILS

Issuer Name:	CN=Finland Country CA,OU=VRK,O=Suomi Finland,C=FI
Serial Number:	00989680
Validity:	12-Jun-06 5:39:10PM to 11-Sep-16 3:39:10PM

MANDATORY ATTRIBUTES	RESULTS	MANDATORY ATTRIBUTES	RESULTS
1. Signature Algorithm	PASSED	12. Extended Key Usage	PASSED
2. Signature	PASSED	13. Authority Cert Issuer	PASSED
3. Version	PASSED	14. Certificate Policy	PASSED
4. Serial Number	PASSED	15. Critical Extension	PASSED
5. Issuer	PASSED	16. Key Usage	FAILED
6. Validity	PASSED	Key Cert Sign	PASSED
7. Subject	PASSED	CRL Sign	PASSED
8. Subject Public Key Info	PASSED	17. Basic Constraints	PASSED
9. Subject Key Identifier	PASSED	CA	PASSED
10. Issuer Unique ID	PASSED	Path Len Constraint	PASSED
11. Subject Unique ID	PASSED	18. Netscape Extension	PASSED

OVERALL RESULTS:

Only Certificate Signing and CRL Signing is allowed as Key Usage.



Finland.der

```
✗ Finland.der [CSCA]FINLAND
  ⊟ ✗ tbsCert
     ⊞ ✓ Version
     ⊞ SerialNumber
     ⊞ ✓ Signature Algorithm
     ⊞ ✓ Issuer
     ⊞ ✓ Validity
     ⊞ ✓ Subject
     ⊞ Subject Public Key
       ✓ Issuer Unique ID
       ✓ Subject Unique ID
     ⊟ ✗ Extensions
        ⊞ ✓ basicConstraints(2.5.29.19)
        ⊟ ✗ keyUsage(2.5.29.15)
             ● (digitalSignature) (nonRepudiation) (keyCertSign) (crlSign)
        ⊞ ✓ authorityKeyIdentifier(2.5.29.35)
        ⊞ ✓ subjectKeyIdentifier(2.5.29.14)
  ⊞ Signature Algo
    ● Signature
```

```
File: Finland.der:Universal,Constructed,SEQUENCE(len=1412)(Subs=3)
⊟ Universal,Constructed,SEQUENCE(len=876)(Subs=8)
   ⊞ ContextSpecific,Constructed,Context Specific[0](len=3)(Subs=1)
     ● Universal,Primitive,INTEGER(len=4)(Subs=0):10000000 : 00989680
   ⊞ Universal,Constructed,SEQUENCE(len=13)(Subs=2)
   ⊞ Universal,Constructed,SEQUENCE(len=80)(Subs=4)
   ⊞ Universal,Constructed,SEQUENCE(len=30)(Subs=2)
   ⊞ Universal,Constructed,SEQUENCE(len=80)(Subs=4)
   ⊞ Universal,Constructed,SEQUENCE(len=546)(Subs=2)
   ⊟ ContextSpecific,Constructed,Context Specific[3](len=102)(Subs=1)
      ⊟ Universal,Constructed,SEQUENCE(len=100)(Subs=4)
         ⊞ Universal,Constructed,SEQUENCE(len=18)(Subs=3)
         ⊟ Universal,Constructed,SEQUENCE(len=14)(Subs=3)
              ● Universal,Primitive,OBJECT_IDENTIFIER(len=3)(Subs=0):2.5.29.15 (keyUsage) : 551d0f
              ● Universal,Primitive,BOOLEAN(len=1)(Subs=0) : ff
            ⊟ Universal,Primitive,OCTET_STRING(len=4)(Subs=1)
                 ● Universal,Primitive,BIT_STRING(len=2)(Subs=0)(Unused bits: 01) : c6
         ⊞ Universal,Constructed,SEQUENCE(len=31)(Subs=2)
         ⊞ Universal,Constructed,SEQUENCE(len=29)(Subs=2)
⊞ Universal,Constructed,SEQUENCE(len=13)(Subs=2)
  ● Universal,Primitive,BIT_STRING(len=513)(Subs=0)(Unused bits: 00) : 8847601e436f32d5faf8167c694a9a4
```

Compliance Issue

- Problem
  - Key Usage is marked as Digital Signature, Non-Repudiation, keyCertSign and crlSign.
  - Must be keyCertSign and crlSign only.
- Issue
  - A CSCA with Digital Signature capabilites can be used to sign a Passport Directly, without issuing a DSC. The signature will validate as the CSCA is self-signed. Invalidates the two layer model of E-Passport PKI

TF5 Guidance document

- Some deviations may not cause any security breach or Interoperability problems
- TF5 is preparing a guidance paper on deviations that are acceptable and those that are not.
- This is not a license to deviate, but an effort to differentiate between harmless deviations and others.

PKD changes

- Entries that are non-conformant but acceptable, will not be rejected by the PKD
- These entries will be parked in a different location
- For validation, two separate LDIFs will be available
  - Conformant and acceptable
  - Non-Conformant but acceptable
- Entries not conforming to these minimum standards will still be rejected

PKD – other developments

- Currently, only Participants have LDAP access for downloads, which can be automated
- Non-Participants can download from web, which has a script prevention mechanism. These downloads have to be manual.
- In near future, law enforcement agencies of non-Participants will be able to automate download from the web

Summary

- PKD is a Global Trust Exchange
- Compliance to Doc 9303 is necessary for E-Passport Trust
- The PKD ensures that Participants move towards total compliance with Doc 9303

Thank You!

R Rajeshkumar
R.Rajeshkumar@netrust.net
Rajesh@netrust.net
RRaj88@gmail.com
Dy. CEO
Netrust Pte Ltd
http://www.netrust.net