



**Lösungsvorschlag zur  
9. Übung zur Vorlesung  
Public-Key-Infrastrukturen  
SS 2006**

**Aufgabe 1: Prüfung von Zertifikatsketten nach RFC3280**

Der RFC3280 Prüfalgorithmus ist hier zu finden:

<http://www.cdc.informatik.tu-darmstadt.de/lehre/SS06/vorlesung/PKI/misc/AlgorithmusFlussdiagramm.pdf>

In dieser Darstellung des Algorithmus sind einige unbedeutende Schritte weggelassen. Gehen Sie bei diesen Schritten davon aus, dass etwaige Prüfungen erfolgreich sind (z.B.: Die Prüfung der name constraints ist immer erfolgreich). Bitte beachten Sie auch, dass Policy Qualifier nicht verwendet werden. Entsprechend ist auch kein Feld in den Knoten des valid\_policy\_trees vorgesehen. Der Algorithmus ist in mehrere Teile zerlegt. Das erste Diagramm zeigt das Layout des gesamten Algorithmus. Der Prozeßschritt **STOP** signalisiert, dass die Ausführung des Algorithmus mit einem Fehler beendet wird. Gelangt die Ausführung zu **OUTPUT**, signalisiert dies eine erfolgreiche Prüfung.

Der Übersichtlichkeit halber sind die Zertifikate in tabellarischer Form angegeben.

Verwenden Sie folgende Initialisierung für den Algorithmus:

a)	certification path	Pfad gemäß Aufgabenstellung
b)	current date/time	Jun 22 2005 GMT
c)	user-initial-policy-set	{ANY}
d)	trust anchor information	entsprechende Angaben zu Zertifikat A
e)	initial-policy-mapping-inhibit	false
f)	initial-explicit-policy	true
g)	initial-any-policy-inhibit	false

Gehen Sie bei der Bearbeitung dieser drei Aufgaben wie folgt vor:

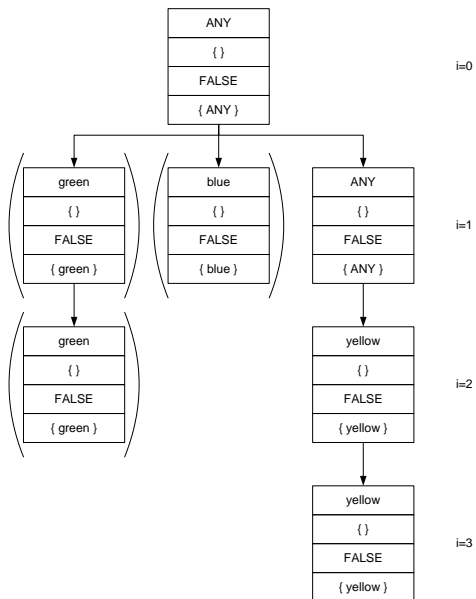
- Geben Sie die Länge der Zertifikatskette  $n$  an.
- Stellen Sie den Zustand des Algorithmus während der Prüfung tabellarisch dar: Tragen Sie senkrecht die Zustandsvariablen und waagrecht die Zählvariable  $i$  (Iterationen des Algorithmus) ein. Der Startzustand nach der Initialisierung ist  $i = 1$ .
- Zeichnen Sie den `valid_policy_tree` (die entsprechende Variable muss natürlich nicht in der Tabelle sein). Es reicht ein Baum pro Aufgabe. Notieren Sie dazu zu jeder Ebene im Baum das passende  $i$ . Falls Sie im Baum Knoten löschen müssen, klammern Sie diese ein und ergänzen die aktuelle Belegung von  $i$ , damit klar ist, wann der Knoten gelöscht wurde.
- Gehen sie davon aus, dass keines der angegebenen Zertifikate gesperrt ist.
- Falls die Prüfung erfolgreich ist, geben Sie das Ergebnis an.
- Falls die Prüfung nicht erfolgreich ist, geben Sie die Stelle an, an der die Prüfung gescheitert ist.

**Hinweis:** Im Algorithmus wird das `keyCertSignBit` erwähnt. Das entspricht dem Eintrag `Certificate Sign` in der Extension `X509v3 Key Usage`.

- a) Geben Sie die Zertifikatskette an, die zur Prüfung der öffentlichen Schlüssel von Bob verwendet werden kann!
- b) Prüfen Sie die Zertifikatskette für Bob.

## Lösungsvorschlag

- a) Der Zertifizierungspfad ist `RootCA` → `CA1` → `CA2` → `Bob`, wobei `Root CA` der Vertrauensanker ist.
- b) Das Zertifikat ist gültig. Das Resultat der Prüfung ist die Spalte zu  $i = 3$  zusammen mit dem `Valid Policy Tree`.



Änderung des Zustands während der Algorithmus läuft:

State Variables:		Steps			
		$i = 1$	$i = 2$	$i = 3$	(wrap-up)
a	valid-policy-tree	Siehe Grafik "Valid Policy Tree"			
d	explicit-policy	0	0	0	0
e	inhibit-any-policy	4	3	2	
f	policy-mapping	4	3	2	
h	working-public-key	key-RootCA	key-CA1	key-CA2	key-Bob
j	working-issuer-name	CN=RootCA	CA1	CA2	Bob
k	max-path-length	3	1	0	

Zertifikat A	
Serial Nr.:	1
Issuer:	CN=Root CA
NotBefore:	Jan 1 2002 GMT
NotAfter:	Dec 31 2007 GMT
Subject:	CN=Root CA
Public Key:	key-Root-CA
X509v3Extensions:	
Basic Constraints:	critical CA: TRUE pathlen=2
Key Usage:	critical Certificate Sign
Certificate Policy:	not critical ANY
Signature: verifiable with <b>Root-CA</b> (SHA1withRSA)	

Zertifikat B	
Serial Nr.:	2
Issuer:	CN=Root CA
NotBefore:	Feb 1 2003 GMT
NotAfter:	Dec 31 2005 GMT
Subject:	CN=CA1
Public Key:	key-CA1
X509v3Extensions:	
Basic Constraints:	critical CA: TRUE pathlen=1
Key Usage:	critical Certificate Sign
Certificate Policy:	not critical green, blue, ANY
Signature: verifiable with <b>Root-CA</b> (SHA1withRSA)	

Zertifikat C	
Serial Nr.:	3
Issuer:	CN=CA1
NotBefore:	Jan 2 2002 GMT
NotAfter:	Dec 31 2005 GMT
Subject:	CN=CA2
Public Key:	key-CA2
X509v3Extensions:	
Basic Constraints:	critical CA: TRUE pathlen=0
Key Usage:	critical Certificate Sign
Certificate Policy:	not critical green,yellow
Signature: verifiable with <b>CA1</b> (SHA1withRSA)	

Zertifikat D	
Serial Nr.:	25
Issuer:	CN=CA2
NotBefore:	Feb 1 2005 GMT
NotAfter:	Dec 31 2005 GMT
Subject:	CN=Bob
Public Key:	key-Bob
X509v3Extensions:	
Key Usage:	critical Encryption
Certificate Policy:	not critical yellow
Signature: verifiable with <b>CA2</b> (SHA1withRSA)	

## Aufgabe 2: Online-Registration

Lassen Sie sich registrieren auf einem Online Trust Center.

[http://www.trustcenter.de/produkte/my\\_certificate\\_express.htm](http://www.trustcenter.de/produkte/my_certificate_express.htm)

<http://www.thawte.com/secure-email/personal-email-certificates/index.html#>

- Drucken Sie Ihr Zertifikat mit Hilfe von OpenSSL aus
- Welche Extensions enthält Ihr Zertifikat?
- Wie ist Ihre Subject DN und Issuer DN?
- Wie ist die Seriennummer des Zertifikats?
- Versuchen Sie, die CRL oder einen OCSP Server zu finden, um Ihr Zertifikat zu validieren.

## Lösungsvorschlag

entfällt

*Hinweis* Der Befehl lautet:

```
openssl x509 -inform DER -text -in <certificate Datei>
```