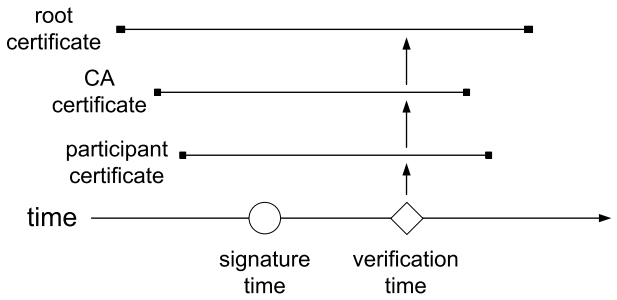
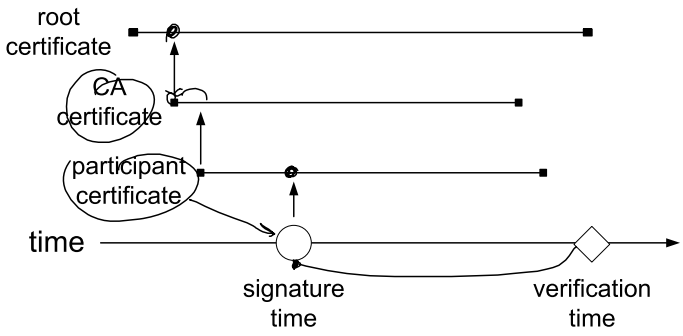
Validity Models

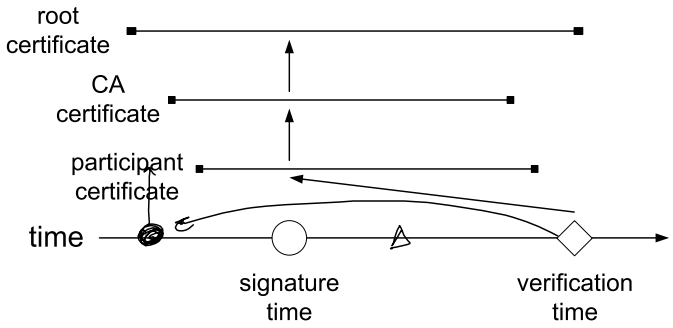
Shell model

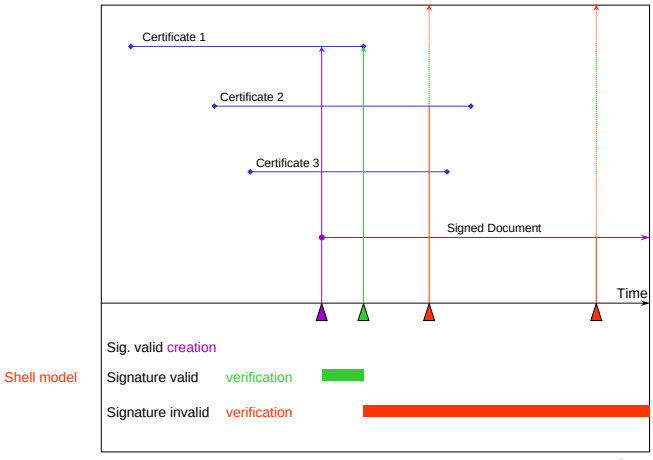


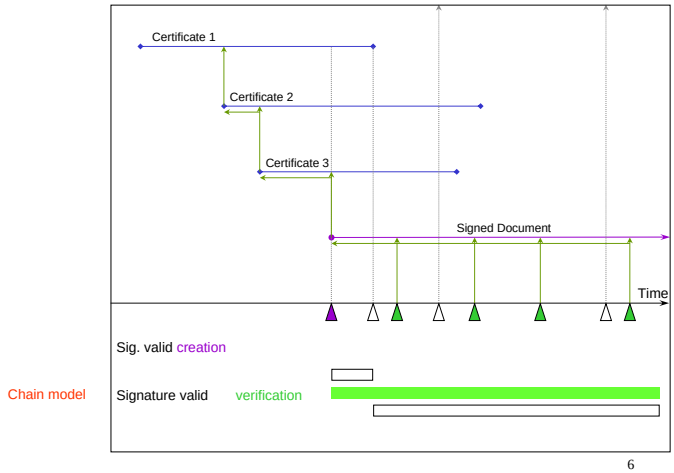
Chain model

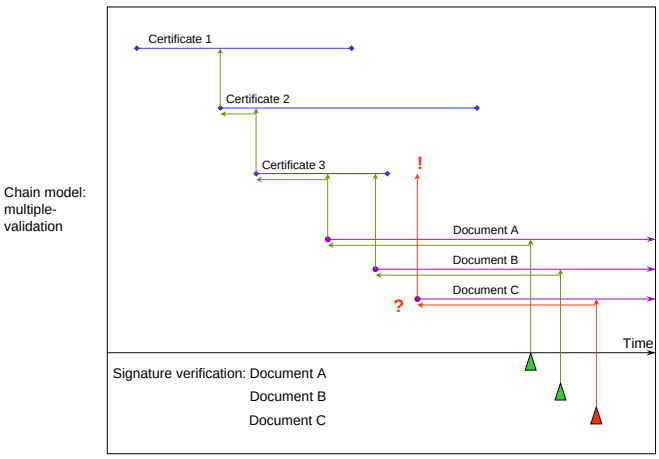


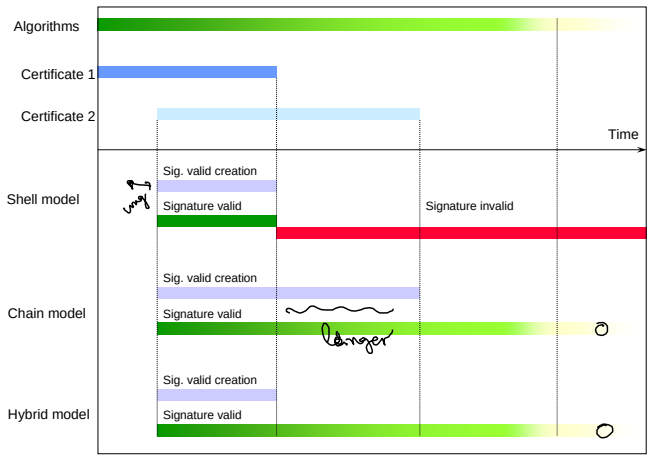
Modified or hybrid model

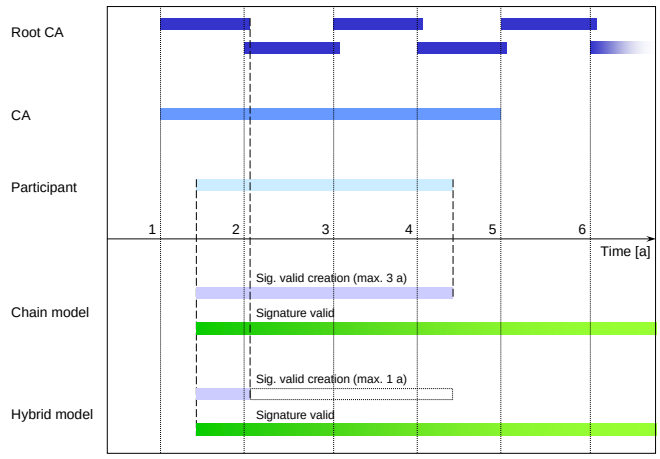












Certification Path Validation…

Path validation

Path Validation

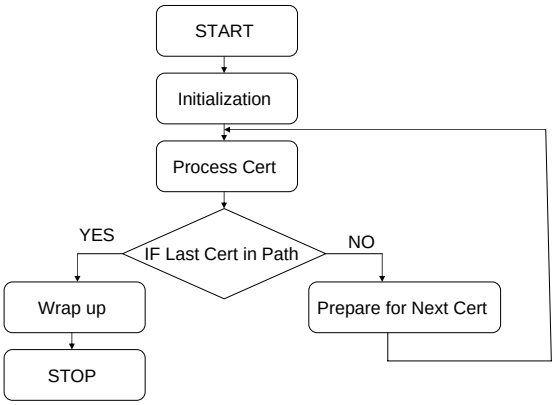
Verify the binding between a subject distinguished name (SDN) or subject alternative name (SAN) and a subject public key.

How *Path Construction* is performed is outside the scope of the algorithm

Steps

1. Initialization
   Performed exactly once
2. Basic Certificate Processing
   Once for each certificate
3. Preparation for the next certificate
   Once for each certificate (except the last one)
4. Wrap-up
   Performed exactly once

Certificate Path Processing Flowchart



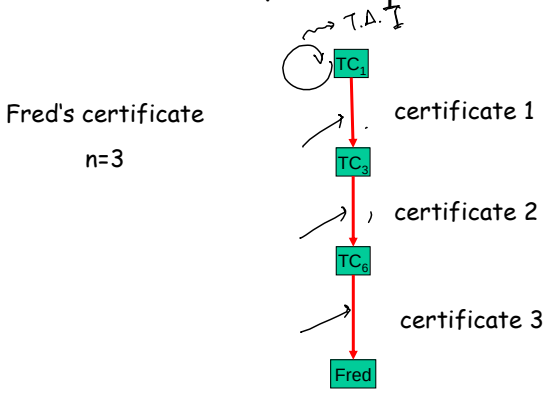
Input variables

1. a prospective certification path of length n.
2. the current date/time
3. user-initial-policy-set
4. trust anchor information
   a. the trusted issuer name
   b. the trusted public key algorithm
   c. the trusted public key
   d. optionally, the trusted public key parameters associated with the public key.
5. initial-policy-mapping-inhibit
6. initial-explicit-policy
7. initial-any-policy-inhibit

Inputs

1. prospective certification path of length n

Certification path



Inputs

2. current date/time

   This is the time in which the path validation runs.

Inputs

3. user-initial-policy-set

   A set of certificate policy identifiers naming the policies that are acceptable to the certificate user. The user-initial-policy-set contains the special value any-policy if the user is not concerned about certificate policy.

Example: { 1.2.3.4, 9.8.7.6}
or more "readable" {gold, silver}

Inputs

4. trust anchor information

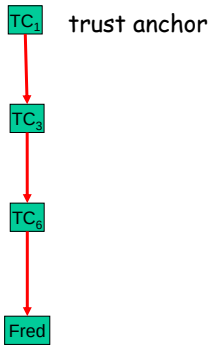
Trust anchor information

(1) the trusted issuer name

(2) the trusted public key algorithm,

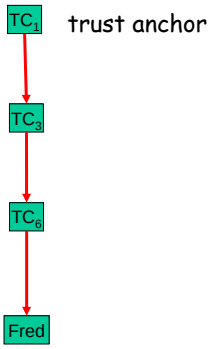
(3) the trusted public key, and

(4) optionally, the trusted public key parameters associated with the public key.



Trust anchor information

The trust anchor information may be provided to the path processing procedure in the form of a self-signed certificate. The trusted anchor information is trusted because it was delivered to the path processing procedure by some trustworthy out-of-band procedure.



Inputs

5. initial-policy-mapping-inhibit

Indicates if policy mapping is allowed in the certification path.

Either true or false.

↓
p.m. nicht erlaubt!

Policy Mappings extension

Only for CA certificates. !

Lists one or more pairs of OIDs; each pair includes an issuerDomainPolicy and a subjectDomainPolicy. The pairing indicates the issuing CA considers its issuerDomainPolicy equivalent to the subject CA's subjectDomainPolicy.

PolicyMappings ::= SEQUENCE SIZE (1..MAX) OF SEQUENCE {
issuerDomainPolicy CertPolicyId,
subjectDomainPolicy CertPolicyId }

1.2.3.4 → 9.8.7.6
gold → blue

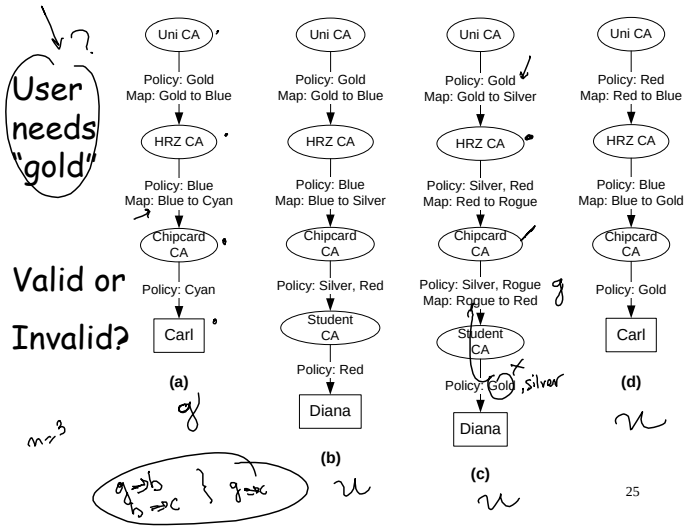
Policy Constraints extension

The policy constraints extension can be used in certificates issued to CAs. The policy constraints extension constrains path validation in two ways:

- It can be used to prohibit policy mapping (the number of certificates that may appear in a path before policy mapping is no longer permitted)
- or require an explicit policy (the number of certificates that may appear in a path before an explicit policy is required)

PolicyConstraints ::= SEQUENCE {
- requireExplicitPolicy [0] SkipCerts OPTIONAL,
  inhibitPolicyMapping [1] SkipCerts OPTIONAL }

SkipCerts ::= INTEGER (0..MAX)



Inputs

6. initial-explicit-policy

Indicates if the path must be valid for at least one of the certificate policies in the user- initial-policy-set.

Either true or false.

Inputs

7. initial-any-policy-inhibit

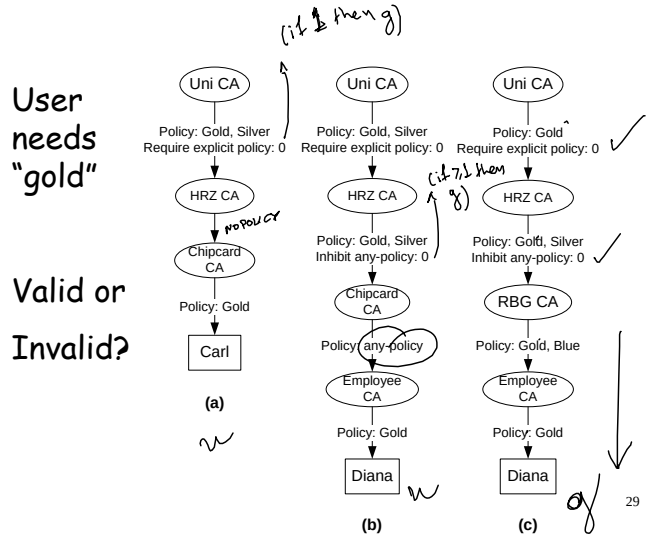
Indicates whether the anyPolicy OID should be processed if it is included in a certificate.

Either true or false.

Inhibit Any-Policy extension

The inhibit any-policy extension can be used in certificates issued to CAs. The inhibit any-policy indicates that the special anyPolicy OID, with the value { 2 5 29 32 0 }, is not considered an explicit match for other certificate policies. The value indicates the number of additional certificates that may appear in the path before anyPolicy is no longer permitted. For example, a value of one indicates that anyPolicy may be processed in certificates issued by the subject of this certificate, but not in additional certificates in the path. This extension MUST be critical.

InhibitAnyPolicy ::= SkipCerts
SkipCerts ::= INTEGER (0..MAX)



Initialisation

Eleven (11) variables are set:

1. valid_policy_tree
2. permitted_subtrees
3. excluded_subtrees
4. explicit_policy
5. inhibit_any-policy
6. policy_mapping
7. working_public_key_algorithm
8. working_public_key
9. working_public_key_parameters
10. working_issuer_name
11. max_path_length

Name Constraints extension

Must be used only in CA certificates

Indicates a name space within which all subject names in subsequent certificates in a certification path MUST be located.

Apply to SubjectDN and SubjectAlternativeName

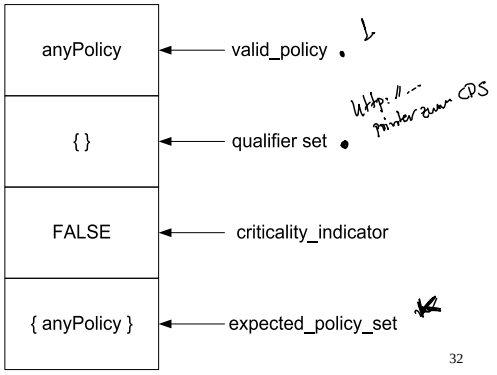
MUST be critical

```
NameConstraints ::= SEQUENCE {
      permittedSubtrees [0] GeneralSubtrees OPTIONAL,
      excludedSubtrees [1] GeneralSubtrees OPTIONAL }
GeneralSubtrees ::= SEQUENCE SIZE (1..MAX) OF GeneralSubtree
GeneralSubtree ::= SEQUENCE {
      base GeneralName,
      minimum [0] BaseDistance DEFAULT 0,
      maximum [1] BaseDistance OPTIONAL }
BaseDistance ::= INTEGER (0..MAX)
```

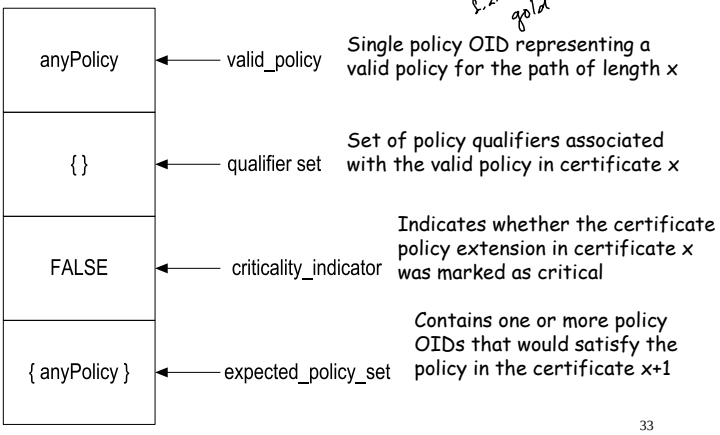

valid_policy_tree

a tree of certificate policies

initial state:



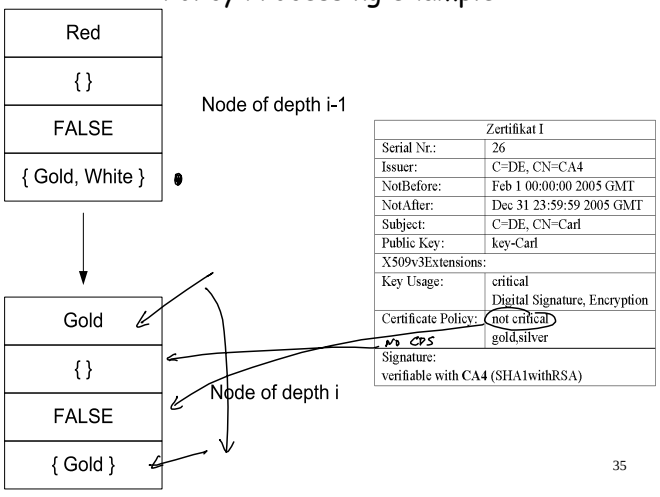
valid_policy_tree



Basic Certificate Processing

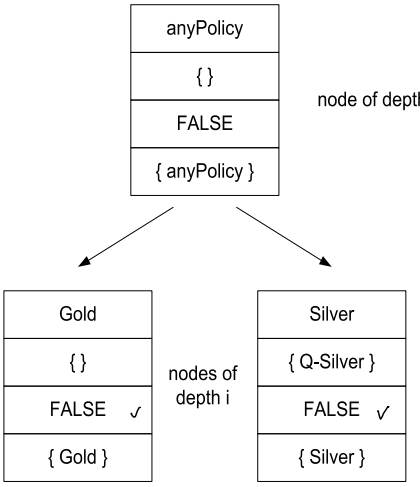
1. Basic verification
   a) Certificate was signed with the algorithm, public key, parameters?
   b) Certificate is valid in time?
   c) Not revoked or on hold?
   d) Issuer Name =? working_issuer_name
2. SDN and SAN belongs to permitted_subtrees?
3. SDN and SAN does not belong to excluded_subtrees
4. Policy Processing
5. If policies not present, then set valid_policy_tree to NULL
6. Verify explicit_policy or valid_policy_tree

Policy Processing example



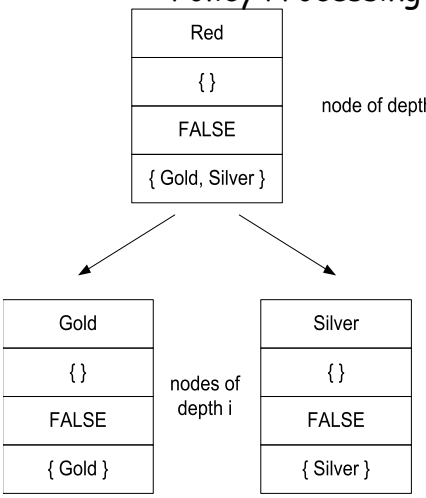
Zertifikat I	
Serial Nr.:	26
Issuer:	C=DE, CN=CA4
NotBefore:	Feb 1 00:00:00 2005 GMT
NotAfter:	Dec 31 23:59:59 2005 GMT
Subject:	C=DE, CN=Carl
Public Key:	key-Carl
X509v3Extensions:	
Key Usage:	critical Digital Signature, Encryption
Certificate Policy:	not critical gold,silver
Signature: verifiable with CA4 (SHA1withRSA)	

Policy Processing example



Zertifikat I	
Serial Nr.:	26
Issuer:	C=DE, CN=CA4
NotBefore:	Feb 1 00:00:00 2005 GMT
NotAfter:	Dec 31 23:59:59 2005 GMT
Subject:	C=DE, CN=Carl
Public Key:	key-Carl
X509v3Extensions:	
Key Usage:	critical Digital Signature, Encryption
Certificate Policy:	not critical gold,silver(Q-silver)
Signature: verifiable with CA4 (SHA1withRSA)	

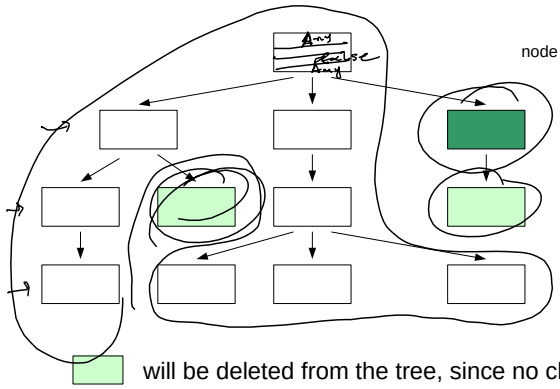
Policy Processing example



node of depth i-1

Zertifikat I	
Serial Nr.:	26
Issuer:	C=DE, CN=CA4
NotBefore:	Feb 1 00:00:00 2005 GMT
NotAfter:	Dec 31 23:59:59 2005 GMT
Subject:	C=DE, CN=Carl
Public Key:	key-Carl
X509v3Extensions:	
Key Usage:	critical Digital Signature, Encryption
Certificate Policy:	not critical any-Policy
Signature: verifiable with **CA4** (SHA1withRSA)	

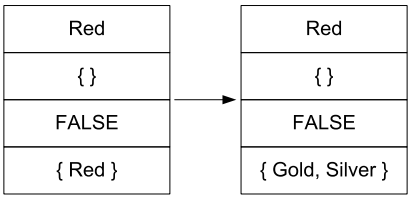
Policy Processing example



will be deleted from the tree, since no children

will be deleted from the tree, too

"Prepare for" example



node of depth i

Zertifikat I	
Serial Nr.:	26
Issuer:	C=DE, CN=CA3
NotBefore:	Feb 1 00:00:00 2005 GMT
NotAfter:	Dec 31 23:59:59 2005 GMT
Subject:	C=DE, CN=CA4
Public Key:	key-Carl
X509v3Extensions:	
Key Usage:	critical Certificate Sign, CRL Sign
Certificate Policy:	not critical red
Policy Mappings:	not critical red ⟶ gold red ⟶ silver
Signature: verifiable with **CA3** (SHA1withRSA)	

"Prepare for" example

This is not allowed!

Zertifikat I	
Serial Nr.:	26
Issuer:	C=DE, CN=CA3
NotBefore:	Feb 1 00:00:00 2005 GMT
NotAfter:	Dec 31 23:59:59 2005 GMT
Subject:	C=DE, CN=CA4
Public Key:	key-Carl
X509v3Extensions:	
Key Usage:	critical Certificate Sign, CRL Sign
Certificate Policy:	not critical red
Policy Mappings:	not critical red ⟶ ANY
Signature: verifiable with **CA3** (SHA1withRSA)	

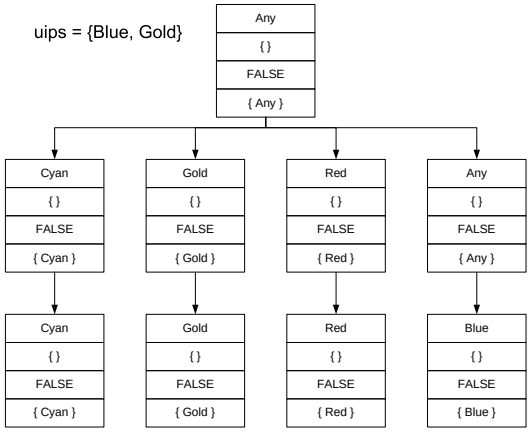
"Prepare for" example

This is not allowed, too!

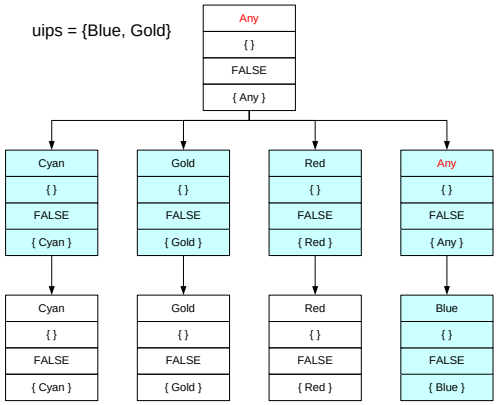
Zertifikat I	
Serial Nr.:	26
Issuer:	C=DE, CN=CA3
NotBefore:	Feb 1 00:00:00 2005 GMT
NotAfter:	Dec 31 23:59:59 2005 GMT
Subject:	C=DE, CN=CA4
Public Key:	key-Carl
X509v3Extensions:	
Key Usage:	critical Certificate Sign, CRL Sign
Certificate Policy:	not critical ANY
Policy Mappings:	not critical ANY ⟶ red
Signature: verifiable with **CA3** (SHA1withRSA)	

Wrap Up – g)

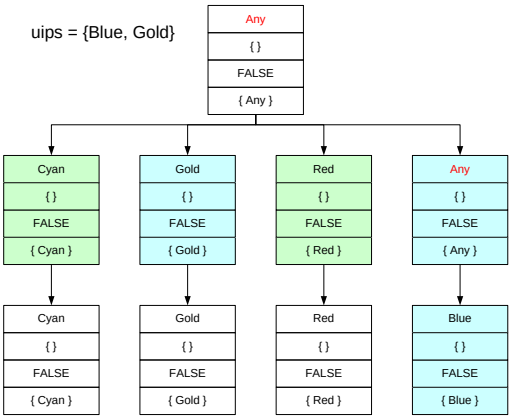
uips = {Blue, Gold}



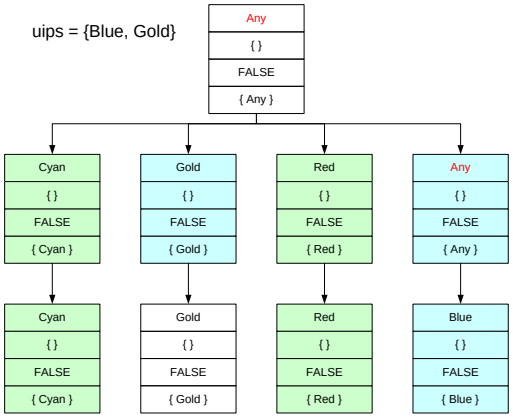
Wrap Up - g), (iii), 1)



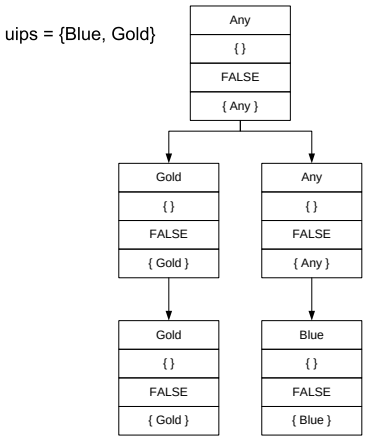
Wrap Up - g), (iii), 2)



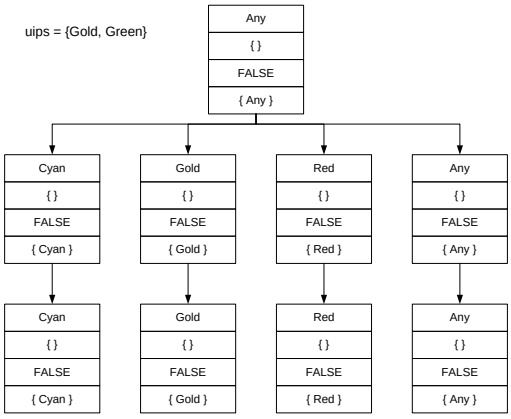
Wrap Up - g), (iii), 2)



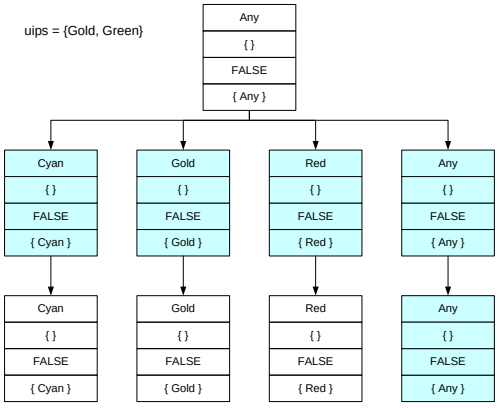
Result



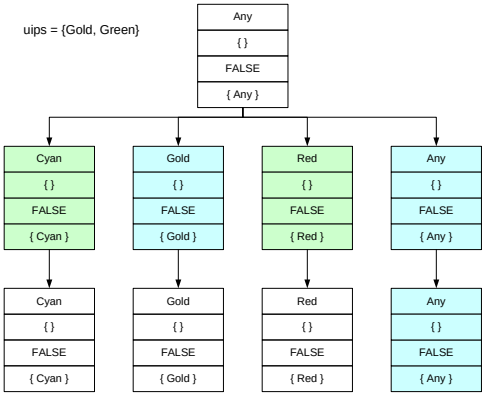
Wrap Up – g)



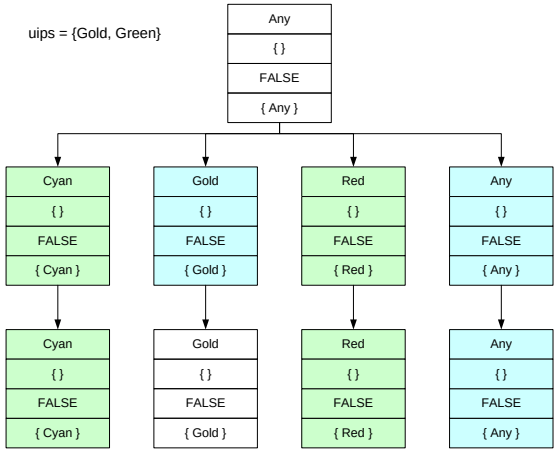
Wrap Up - g), (iii), 1)



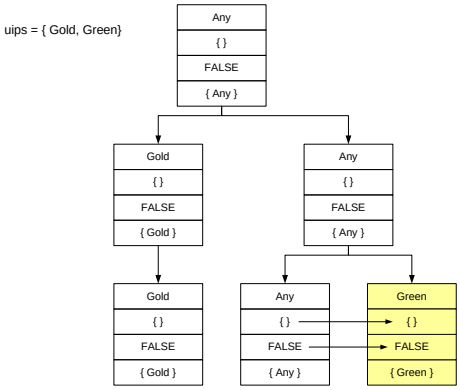
Wrap Up - g), (iii), 2)



Wrap Up - g), (iii), 2)



Wrap Up - g), (iii), 3)



Result