CRL Processing Rules

Santosh Chokhani

March 17 2005

Orion
Security Solutions

Orion
SECURITY SOLUTIONS

Briefing Contents

- Historical Timeline
- Issues and Resolution
- Summary of Recommended Editorial Changes to RFC 3280 and RFC 2560, and X.509
- Path Matching Algorithm
- Backup Slides

Orion
Security Solutions

Historical Timeline

- DoD PKI motivates development of CRL Processing Rules (1997-98)
- Rules submitted to X.509 Editor (1998-99)
- X.509 accepted Input as Normative Annex (1999)
- RFC 3280 uses the Annex to define CRL Processing Rules (??) (2002)
- Issue of some CA products not asserting IDP for partial CRL comes to light (2002)
- Three discussion threads on PKIX on the issue of similarity of certificate “Certification Path” and CRL “Certification Path” (2002-04)

Orion
Security Solutions

Issues and Resolution

- What identifies a CA: name only or name + key?
- What does absence of IDP mean?
- How to ensure a CRL is from a CRL Issuer as intended by the certificate issuing CA?
- Should circularity be permitted during revocation status checking?

Orion Security Solutions

What identifies A CA

- **Issue**
  - For certificates and CRL processing logic, is a CA defined by name only or by name and a signing private key/signature verification public key
- **Resolution**
  - A CA is identified by name alone
- **Basis**
  - Numerous places in X.509 and RFC 3280
  - Section 7 of X.509
- **Recommendation**
  - Add a statement to RFC 3280 that a CA is identified by name

What Does Absence of IDP in a CRL Mean

- **Issue**
  - What does absence of IDP in a CRL mean for the scope of that CRL
- **Resolution**
  - Absence of DP in IDP means that the CRL is complete for the scope implied by the presence or absence of other fields in the IDP for the CRL Issuer
  - Corollary: Absence of IDP in a CRL means that CRL is complete for all certificates issued by the CA
- **Basis**
  - IDP extension description in RFC 3280
  - IDP extension description in X.509
  - CRL processing rules in RFC 3280
  - CRL processing rules in X.509 (Annex B)
- **Recommendations**
  - No change

Orion
Security Solutions

How to Ensure CRL is from the Correct CRL Issuer

- **Issue**
  - How to ensure a CRL is from a CRL Issuer as intended by the certificate issuing CA
- **Resolution**
  - If the CRL and certificate to validate are signed by the same key and the Issuer name in certificate = Issuer Name in CRL, done
  - Else use the algorithm defined next
- **Basis**
  - Need to ensure that the CRL obtained was issued by a CRL Issuer that the certificate issuer intended
  - Need to account for multiple CAs with the same name
- **Recommendations**
  - Add the text to 3280
  - Text already recommended for X.509

Path Matching Algorithm: Motivation

- There can be more than one CA with the same name
- If the certificate and CRL are signed using different keys, how do you know if these are two different CAs or the same CA is using different key
  - Different keys can be used due to having different certificate and CRL signing keys or due to CA re-key
- Starting with a TA, the relying party can match the CA names in the certificate and CRL certification paths
  - Assumes that a CA will not certify two distinct CAs with the same name

Path Matching Algorithm: Assumption

- For indirect CRL, we have some choices to define the algorithm
  - State that specification does not address it
  - Make one of the following trust assumptions
  - Assume that Indirect CRL Issuer is issued a certificate by the certificate issuer
  - Assume that the indirect CRL issuer is one of the ancestors
  - Assume that the indirect CRL issuer is issued a certificate by one of the ancestors (selected – appears to be most flexible)
  - Assume that the indirect CRL issuer is one of the ancestors or issued a certificate by the trust anchor ((selected – appears to be most flexible)

Path Matching Algorithm: Initialization One

- Develop certificate certification path
- Develop a list of (certpath-subject$_0$) (certpath-issuer$_1$, certpath-subject$_1$) (certpath-issuer$_2$, certpath-subject $_2$) etc., where certpath-subject$_0$ is the trust anchor DN and item (certpath-issuer$_i$, certpath-subject$_i$) is the issuer and subject DNs from the ith certificate
- Delete all entries i, where certpath-issuer$_i$ = certpath-subject$_i$
  - Get rid of self-issued certificates
- Renumber the entries to 1 through N$_{cert}$

Path Matching Algorithm: Initialization Two

- Develop CRL certification path
- Develop a list of ($CRLpath\text{-}subject_0$) ($CRLpath\text{-}issuer_1$, $CRLpath\text{-}subject_1$) ($CRLpath\text{-}issuer_2$, $CRLpath\text{-}subject_2$) etc., where $CRLpath\text{-}subject_0$ is the trust anchor DN and item ($CRLpath\text{-}issuer_i$, $CRLpath\text{-}subject_i$) is the issuer and subject DNs from the i^{th} certificate
- Delete all entries i, where $CRLpath\text{-}issuer_i = CRLpath\text{-}subject_i$
  - Get rid of self-issued certificates
- Renumber the entries to 1 through N_{CRL}

Path Matching Algorithm: Initialization Three

- If certpath-issuer$_{Ncert}$ = CRLpath-subject$_{NCRL}$ verify that $N_{cert} = N_{CRL} + 1$
  - For direct CRL, the CRL certification path is one less than certificate certification path
- If certpath-issuer$_{Ncert}$ ≠ CRLpath-subject$_{NCRL}$, set $N_{CRL} = N_{CRL} - 1$
  - For indirect CRL, the CRL issuer may or may not be in the certificate certification path
  - Verify that $N_{CRL} < N_{cert}$
- $N_{cert} = N_{cert} - 1$
  - Ignore the end entity certificate for the match
- Set j = 1
  - Set iteration count
- Set N = Min (N_{CRl}, N_{cert})
  - Set number of DNs to match

Orion Security Solutions

Path Matching Algorithm: Path Names Matching Logic

- Verify certpath-subject$_0$ = CRLpath-subject$_0$
  - Match the trust anchor DNs
- Do while j ≤ N
  - Verify certpath-issuer$_j$ = CRLpath-issuer$_j$
  - Verify certpath-subject$_j$ = CRLpath-subject$_j$
- Enddo

Orion Security Solutions

Path Matching Algorithm: CRL Issuer Name Matching Logic

- Verify that the Subject DN in the last certificate in the CRL certification path = Issuer Name in the CRL
- Apply RFC 3280 Section 6.3 logic
- You still need to apply all certification path validation rules to the CRL certification path

Orion
SECURITY SOLUTIONS

Benefits

- **Mitigates Threats:**
  - **Microsoft → Orion CA → Chokhani (#10 compromised)**
  - **VeriSign → Orion CA (not the same) → CRL (does not have number 10**
  - **Room for mischief or honest error**
- **Efficiency in path development for CRL**

Orion Security Solutions

Path Matching Algorithm: Epilogue

- One way to achieve some of the requirements is to use the requirement to guide the certification path building for CRL
- This obviates the need for extra logic and makes the CRL certification path development efficient
- Algorithm presented can be optimized for computational complexity and code foot print
  - Some checks are redundant
  - They are listed here to provide a modular and easy to understand algorithm

Orion Security Solutions

IETF PKIX November Meeting

- 3280 Editors Response: Common TA solves 80% of problem
- Problems with Editors' View
  - Hopefully TA does not mean the same key, but simply the same DN (TA could also re-key)
  - 3280 and X.509 are trust model neutral; they do not even recommend using name constraints
  - Reticence of 3280 authors unclear given that the logic presented can ensure security and help with performance by finding the CRL path extremely efficiently

Other CRL Processing Related Points

- Keep in mind, you always have the CRL before you build the path to it
- You can build the CRL “certification path” using issuer, subject pairs from the certificate “certification path”
  - Can be used to build the path in either direction (TA to CRL Issuer or CRL Issuer to TA)
- You can use AKID in the CRL to select the CRL Issuer certificate

Orion Security Solutions

Alternative Extension to CRL Path Matching Algorithm: Motivation

- In lieu of path matching algorithm presented, one can determine if the CRL is from the same CA as the certificate issuer, if
  - CRL contains keys or hash of keys used by the CA to sign certificates; and
  - Certificate in question is signed using one of the keys or key hashes asserted (enumerated) in the CRL by the CA claiming to be certificate signing keys
  - Enhance cryptographic binding between the CRL signing key and certificate signing key

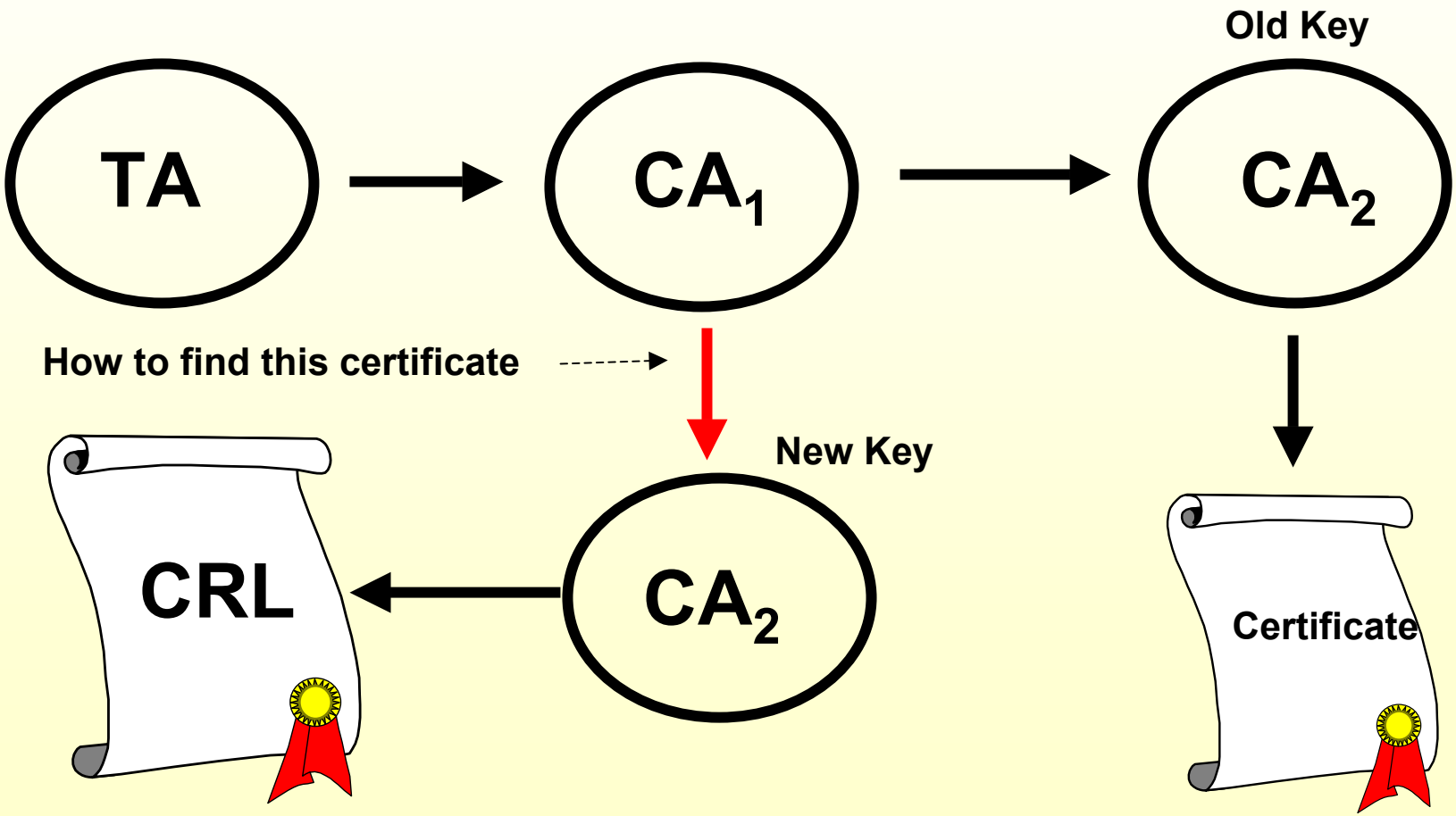
Orion Security Solutions

Alternative Extension to CRL Path Matching Algorithm

- A CRL entry extension could be defined that contains the hash of the certificate issuer subjectPublicKeyInfo
- A CRL extension could be defined containing SEQUENCE of hashes of the certificate issuer subjectPublicKeyInfo
  - SET may be better from the point of view of matching efficiency
- If the Issuer certificate signing key hash matches any of these values, the CRL is from the same CA as the certificate
- Useful for OCSP Responders
- IDP still defines the scope
- The assumption that a CA will not be an indirect CRL Issuer for another CA with the same name is reasonable
- Still need to discover CRL path

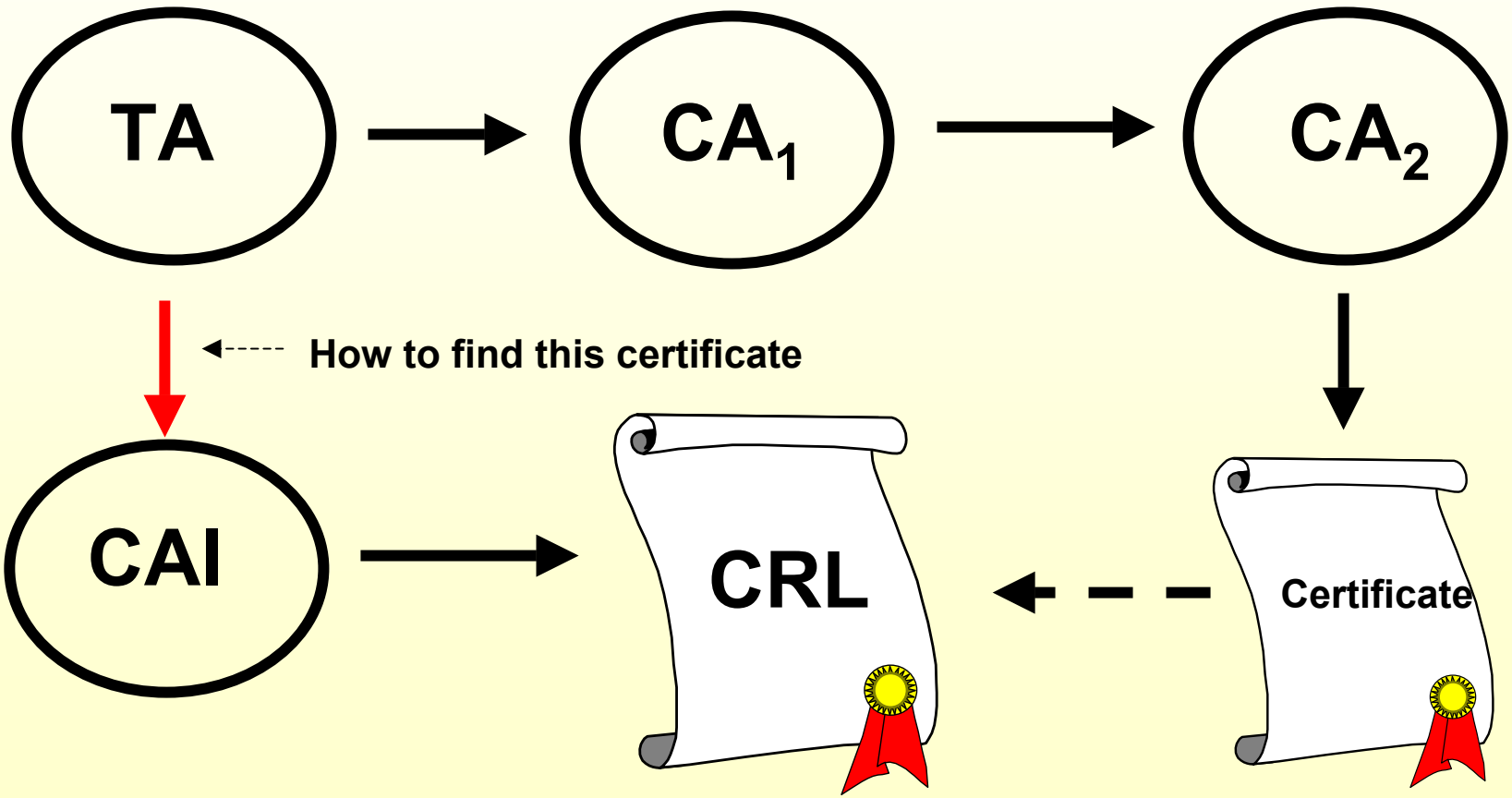
Problem of Locating CRL Signer Certificate: Direct CRL Example

Assumption: Relying party can not access a directory/repository



Problem of Locating CRL Signer Certificate: Indirect CRL Example

Assumption: Relying party can not access a directory/repository

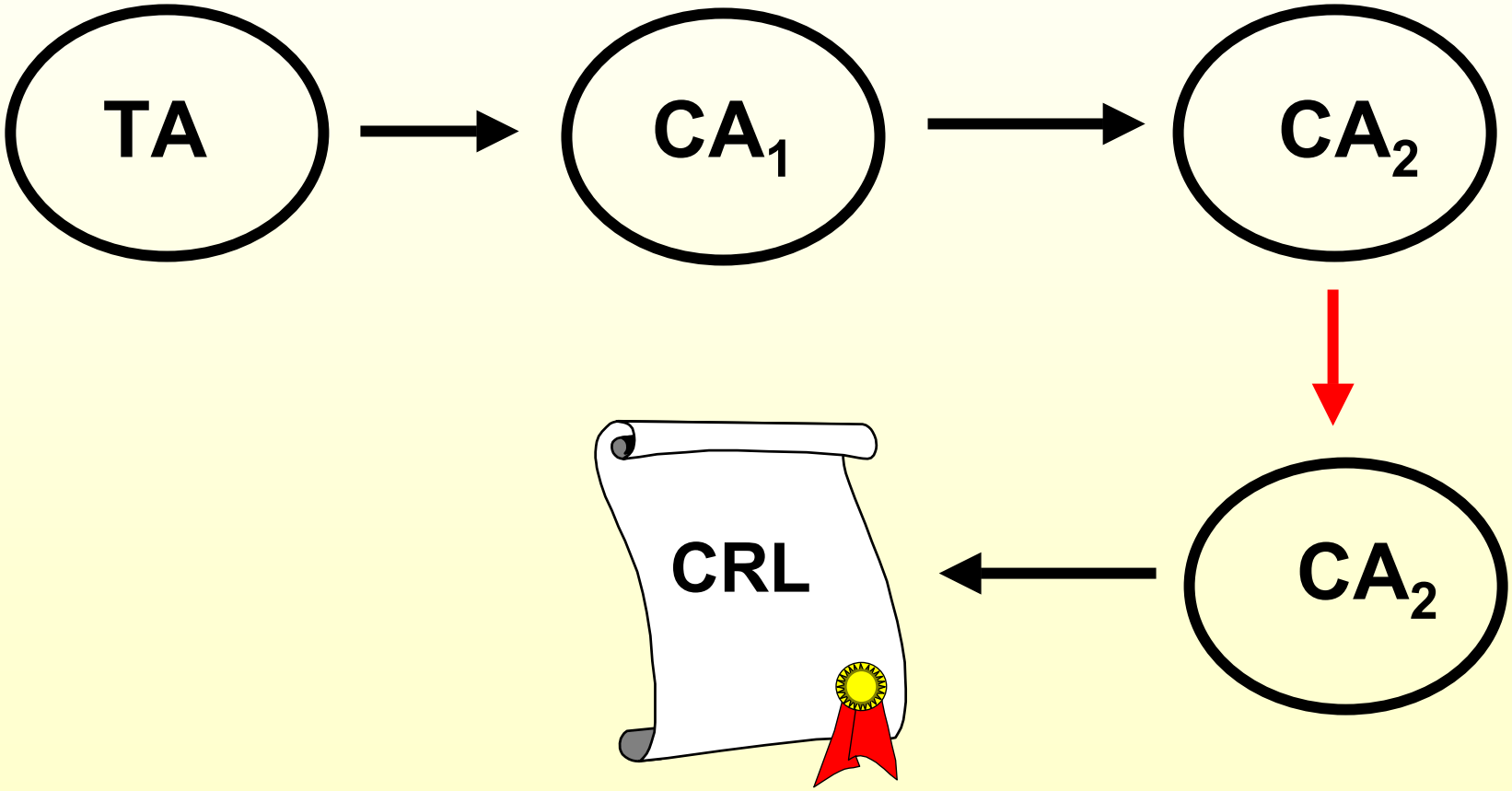


Orion Security Solutions

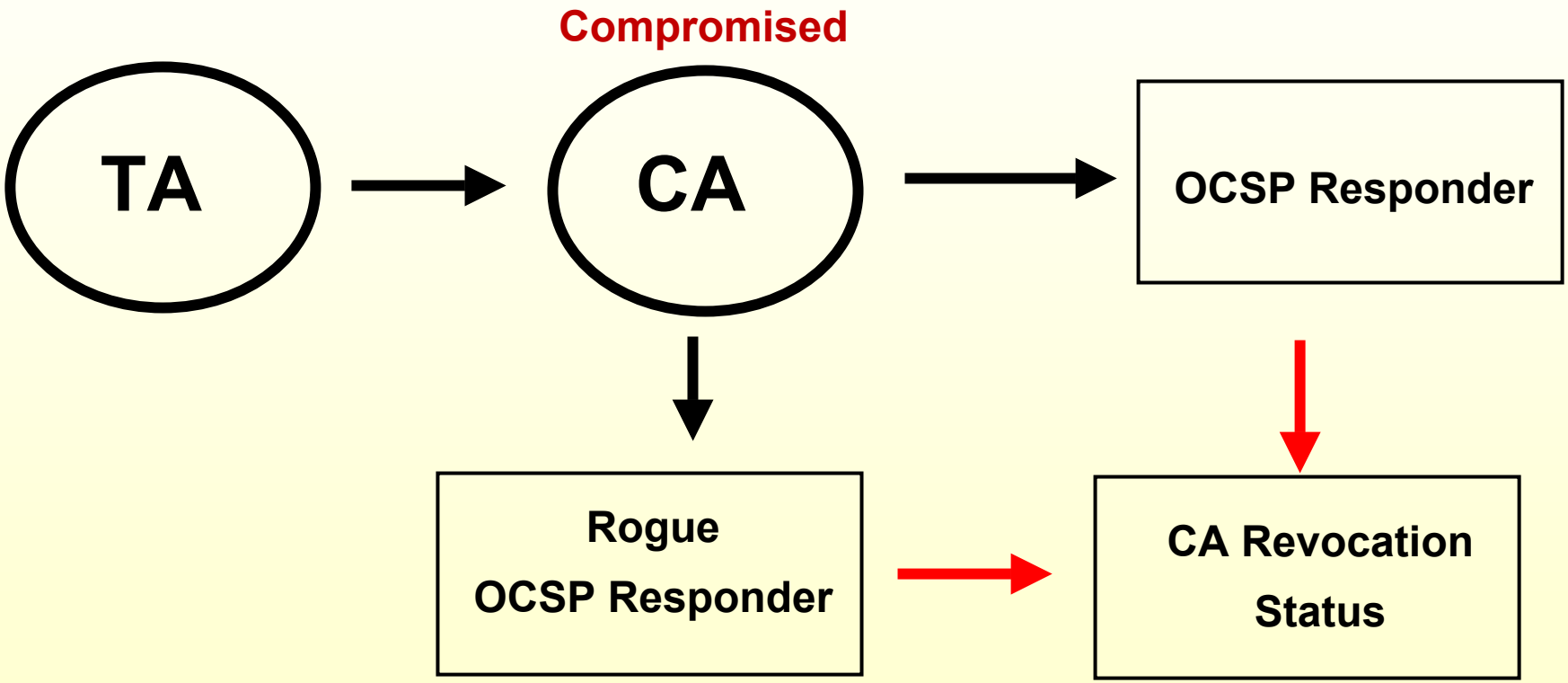
Solution: AIA Extension in CRL

- Solution originator: Stefan
- Put a non-critical AIA extension in the CRL
- CRL can be used to locate the CRL signer certificate
- Requires minor revision to RFC 3280 description of AIA
  - Replace CA with authority
  - Make appropriate changes to attribute type for DAP access
  - Opportunity to clarify the format of AIA target (certificate or p7 file)

Circularity in Revocation Checking: CRL



Circularity in Revocation Checking: OCSP



Issue for Local Policy

Product Behavior

Circularity in Revocation Checking

- Issue
  - What if a certificate whose revocation status is being checked is in the path to verify the signature on the CRL or OCSP response for that same certificate
    - Can occur with self-issued certificates
    - Can occur when an OCSP Responder covers all certificates in a PKI Domain
- Resolution
  - Provide some guidance in the Security Consideration section of RFC 3280 and RFC 2560
- Basis
  - Checking the revocation status of a certificate via a revocation information whose signature is verified using a certification path involving the very same certificate causes chicken and egg problem
    - Validating path requires certificate status
    - Obtaining certificate status requires validated path
- Recommendations
  - Add text from slide 22 to Security Considerations Section in RFC 3280
  - Add text from slide 23 to Security Considerations Section in RFC 2560

Orion
Security Solutions

Alternatives for CRL

1. Say nothing
2. Clarify that a CA is supposed to request revocation of all certificates issued to it when a key associated with self-issued certificate requires revocation
3. Use no-check extension in self-issued certificates
4. Transition from 2 to 3
5. Say something in Security Considerations (selected in order to make no changes to the standard)

Orion
Security Solutions

Alternatives for OCSP

- Say something in security consideration section
- Revise 2560 for client processing rules to detect circularity

Orion
Security Solutions

Text for RFC 3280 Security Consideration Section

- Revocation status of a certificate must not be checked using a CRL whose signature validation requires that same certificate in the certification path. For example, this may occur in self-issued certificates for key roll over or when a CA issues itself a certificate for CRL signing. A simple way to avoid this for key roll over certificates is to sign two CRLs (one using the old key and another using the new key). A simple way to avoid this for CRL signing key is to have the parent CA issue two certificates or if the CA is a trust anchor, promulgate two trust anchors.

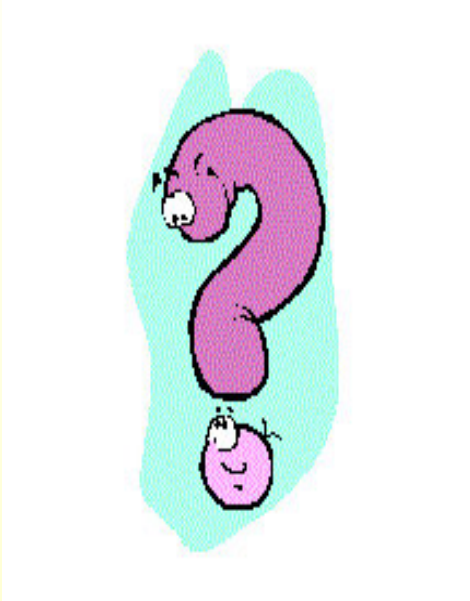
Orion
Security Solutions

Text for RFC 2560 Security Consideration Section

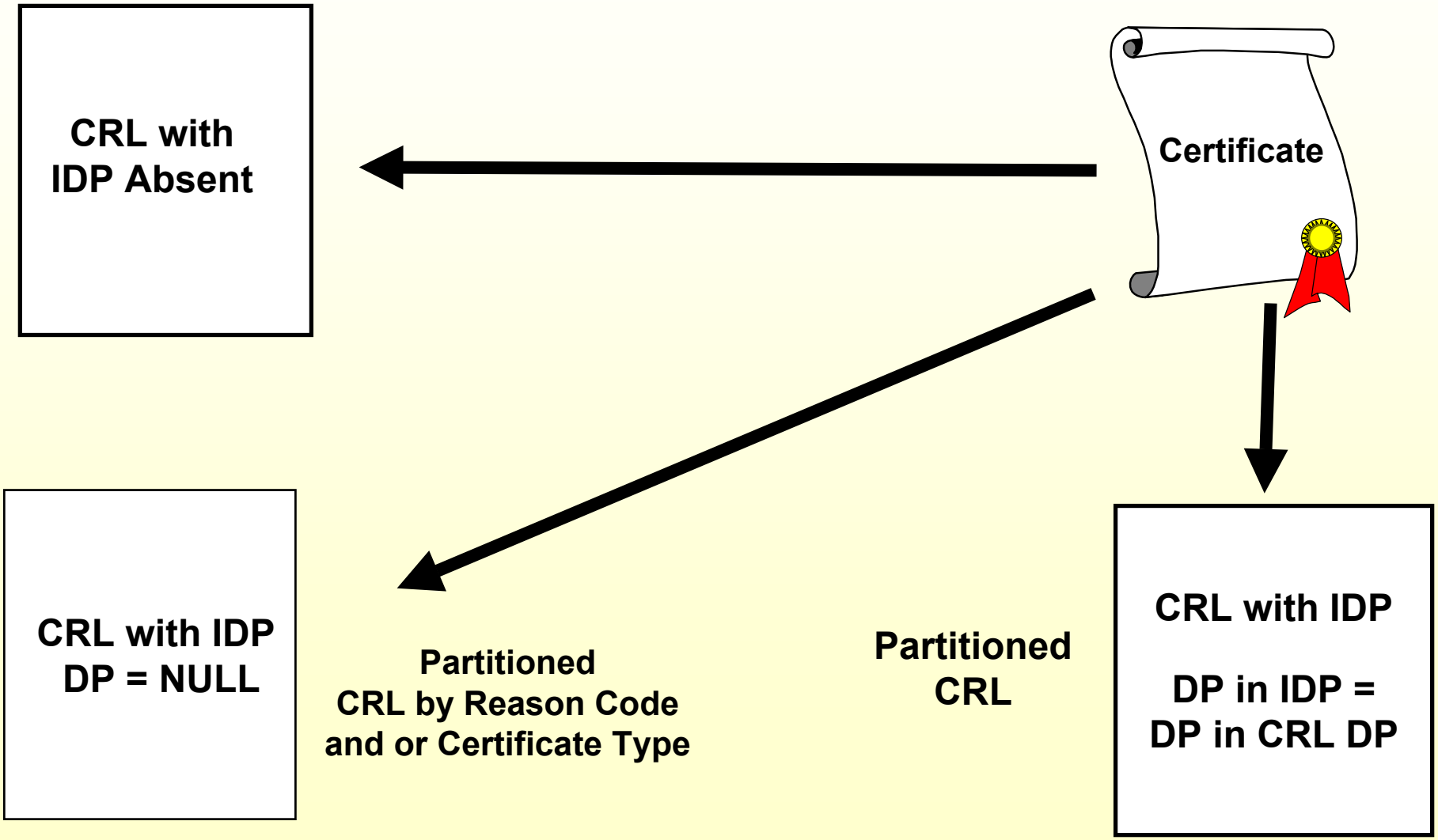
- **Revocation status of a certificate must not be checked using an OCSP Response whose signature validation requires that same certificate in the certification path.**

Orion
Security Solutions

Questions



Matching IDP in CRL and CRL Distribution Point in Certificate



Orion Security Solutions

List of Acronyms and Abbreviations

CA	Certification Authority
CRL	Certificate Revocation List
CRL DP	CRL Distribution Point
DN	Distinguished Name
IDP	Issuing Distribution Point
OCSP	Online Certificate Status Protocol
PKI	Public Key Infrastructure
RFC	Request for Comment
TA	Trust Anchor