ATHENE
Nationales Forschungszentrum
für angewandte Cybersicherheit

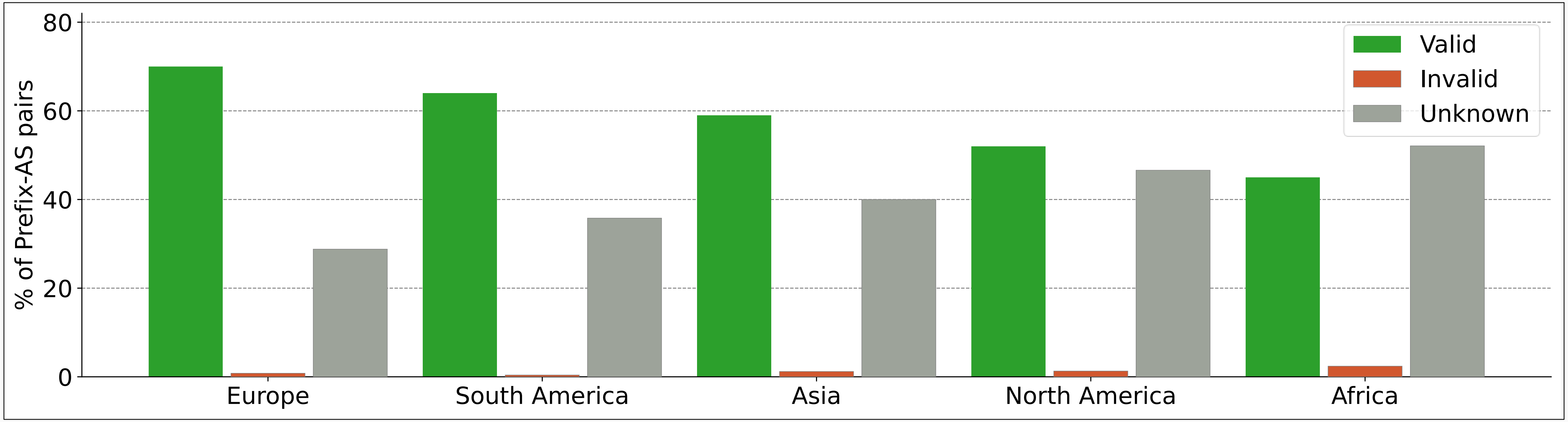
Pruning the Tree:

Rethinking **RPKI** Architecture from the Ground Up

Haya Schulmann and Niklas Vogel

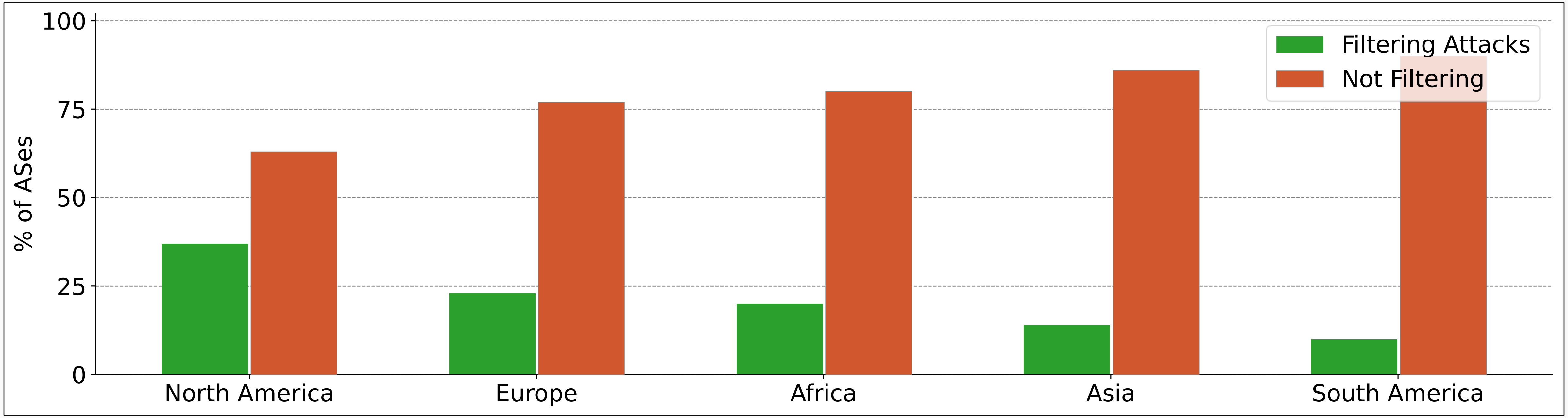
German National Research Center for Applied Cybersecurity ATHENE
Goethe-University Frankfurt

Motivation: Deployment RPKI Coverage



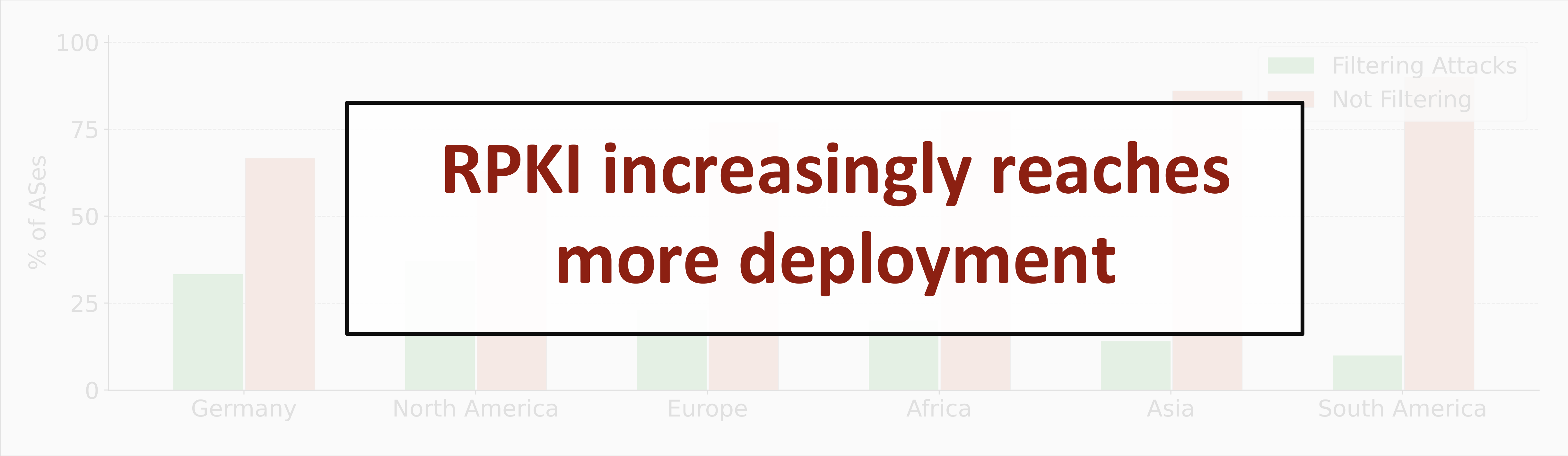
Data Source: Own Measurement

Motivation: Deployment RPKI Filtering



Data Source: APNIC ROV Map

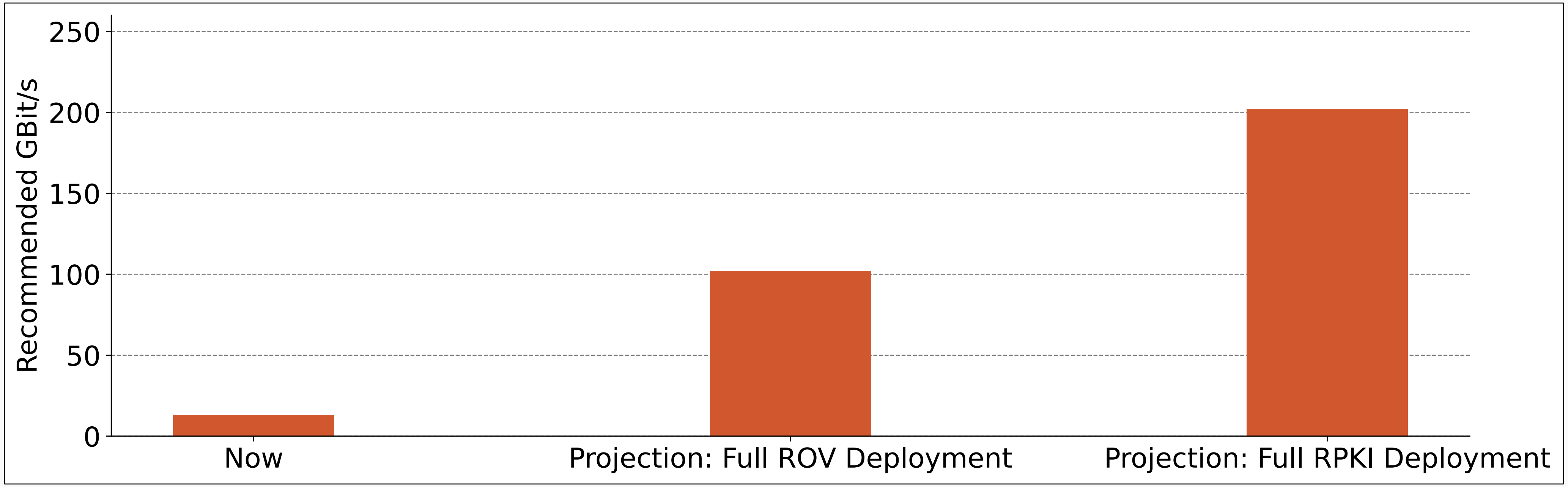
Motivation: Deployment RPKI Filtering



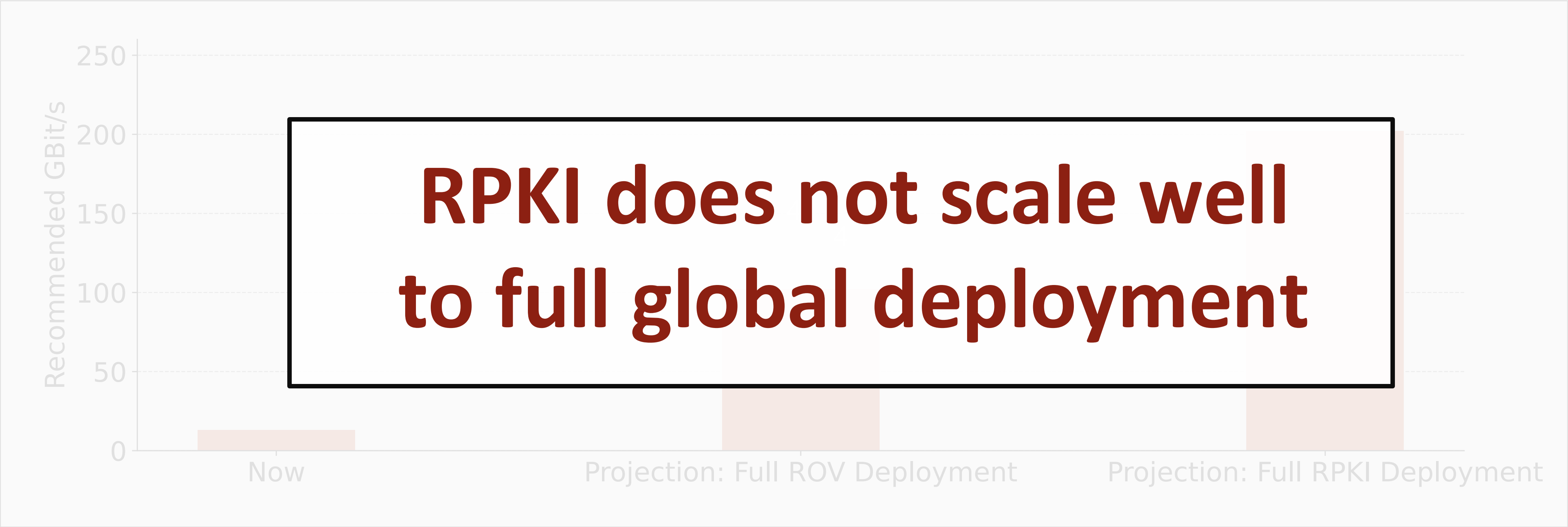
RPKI increasingly reaches more deployment

Data Source: APNIC ROV Map

Motivation: Projecting RPKI to full Deployment

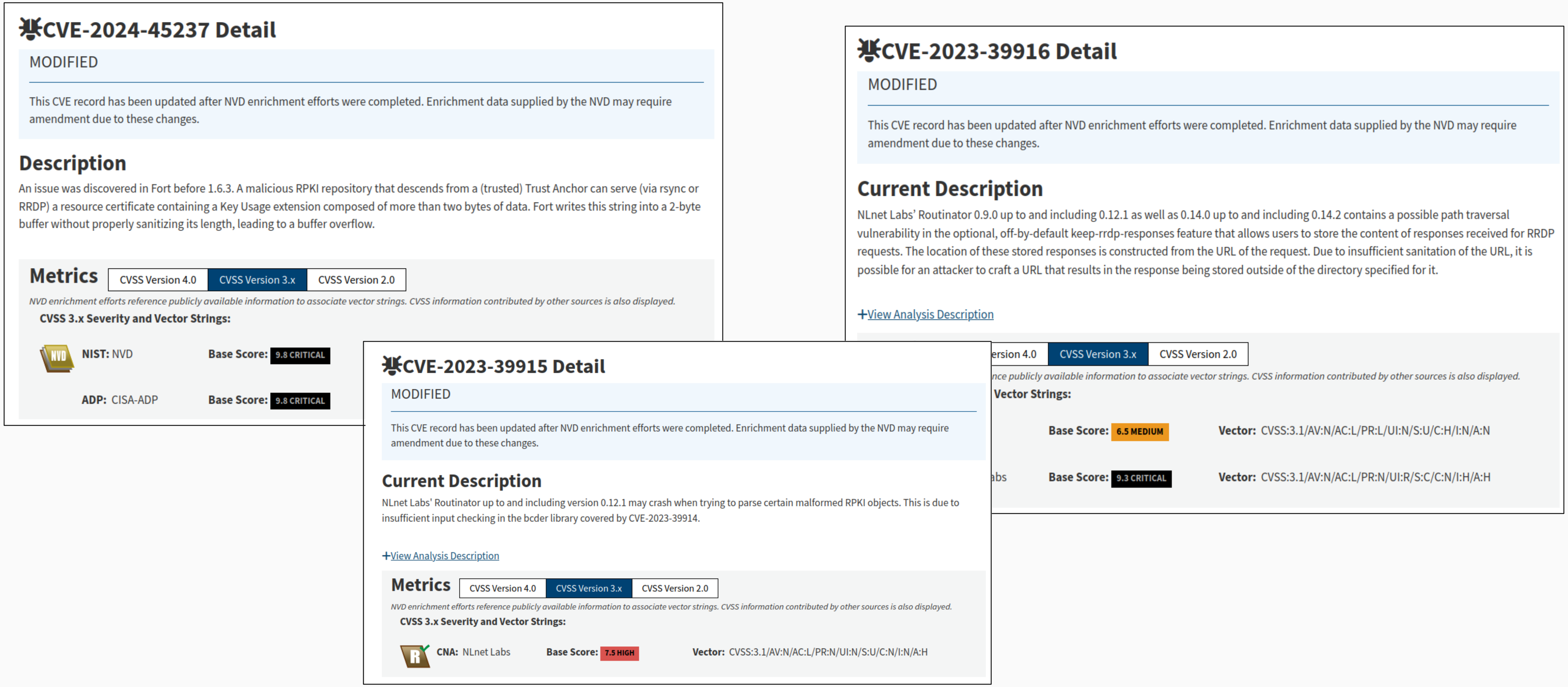


Motivation: Projecting RPKI to full Deployment



RPKI does not scale well to full global deployment

Motivation: RPKI is prone to Implementation Errors



CVE-2024-45237 Detail

MODIFIED

This CVE record has been updated after NVD enrichment efforts were completed. Enrichment data supplied by the NVD may require amendment due to these changes.

Description

An issue was discovered in Fort before 1.6.3. A malicious RPKI repository that descends from a (trusted) Trust Anchor can serve (via rsync or RRDP) a resource certificate containing a Key Usage extension composed of more than two bytes of data. Fort writes this string into a 2-byte buffer without properly sanitizing its length, leading to a buffer overflow.

Metrics

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 3.x Severity and Vector Strings:

NIST: NVD **Base Score:** 9.8 CRITICAL

ADP: CISA-ADP **Base Score:** 9.8 CRITICAL

CVE-2023-39916 Detail

MODIFIED

This CVE record has been updated after NVD enrichment efforts were completed. Enrichment data supplied by the NVD may require amendment due to these changes.

Current Description

NLnet Labs' Routinator 0.9.0 up to and including 0.12.1 as well as 0.14.0 up to and including 0.14.2 contains a possible path traversal vulnerability in the optional, off-by-default keep-rrdp-responses feature that allows users to store the content of responses received for RRDP requests. The location of these stored responses is constructed from the URL of the request. Due to insufficient sanitation of the URL, it is possible for an attacker to craft a URL that results in the response being stored outside of the directory specified for it.

+View Analysis Description

nce publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

Vector Strings:

Base Score: 6.5 MEDIUM **Vector:** CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N

abs **Base Score:** 9.3 CRITICAL **Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:H/A:H

CVE-2023-39915 Detail

MODIFIED

This CVE record has been updated after NVD enrichment efforts were completed. Enrichment data supplied by the NVD may require amendment due to these changes.

Current Description

NLnet Labs' Routinator up to and including version 0.12.1 may crash when trying to parse certain malformed RPKI objects. This is due to insufficient input checking in the bcder library covered by CVE-2023-39914.

+View Analysis Description

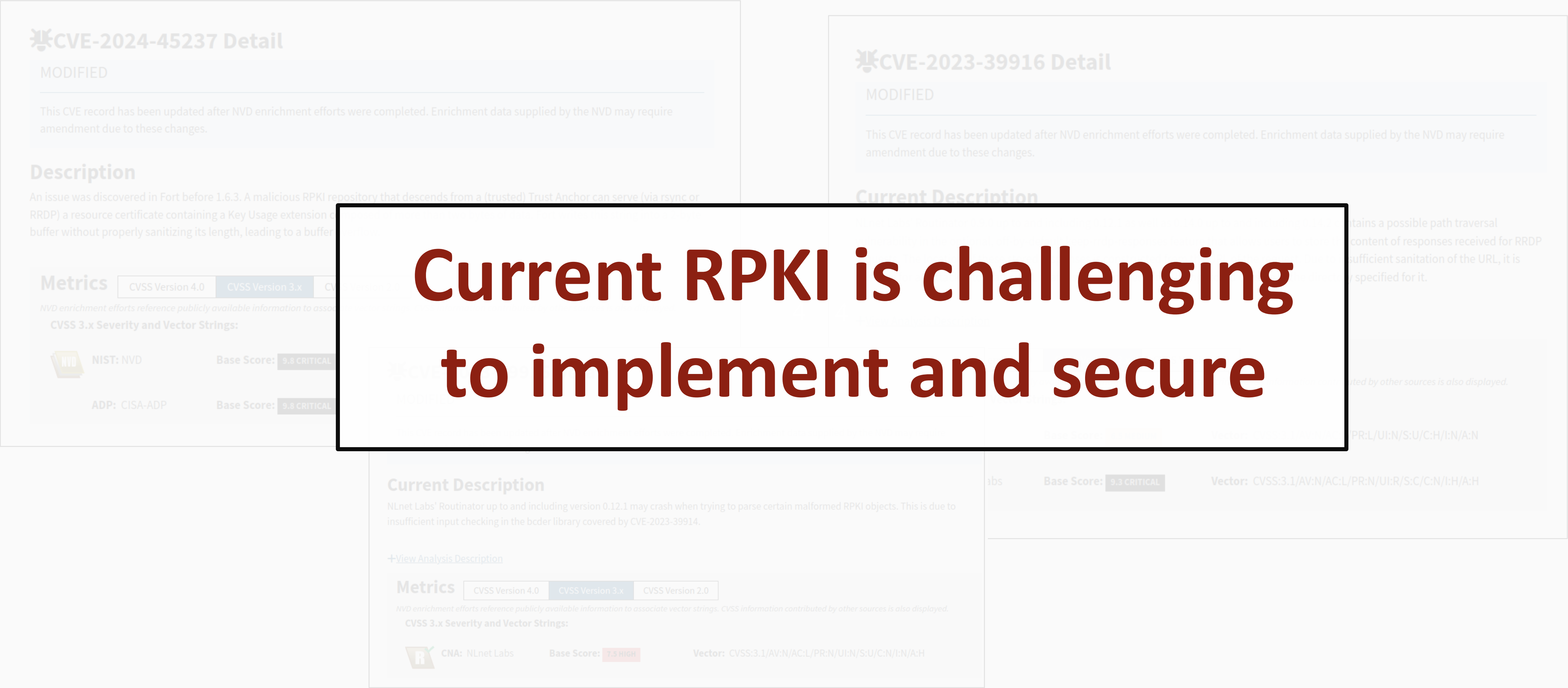
Metrics

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 3.x Severity and Vector Strings:

CNA: NLnet Labs **Base Score:** 7.5 HIGH **Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Motivation: RPKI is prone to Implementation Errors



CVE-2024-45237 Detail

MODIFIED

This CVE record has been updated after NVD enrichment efforts were completed. Enrichment data supplied by the NVD may require amendment due to these changes.

Description

An issue was discovered in Fort before 1.6.3. A malicious RPKI repository that descends from a (trusted) Trust Anchor can serve (via rsync or RRDP) a resource certificate containing a Key Usage extension c
buffer without properly sanitizing its length, leading to a buffer

Metrics CVSS Version 4.0 | CVSS Version 3.x | CV

NVD enrichment efforts reference publicly available information to asso

CVSS 3.x Severity and Vector Strings:

NIST: NVD Base Score: 9.8 CRITICAL

ADP: CISA-ADP Base Score: 9.8 CRITICAL

CVE-2023-39916 Detail

MODIFIED

This CVE record has been updated after NVD enrichment efforts were completed. Enrichment data supplied by the NVD may require amendment due to these changes.

Current Description

tains a possible path traversal
content of responses received for RRDP
sufficient sanitation of the URL, it is
specified for it.

ted by other sources is also displayed.

PR:L/UI:N/S:U/C:H/I:N/A:N

abs Base Score: 9.3 CRITICAL Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:H/A:H

Current Description

NLnet Labs' Routinator up to and including version 0.12.1 may crash when trying to parse certain malformed RPKI objects. This is due to insufficient input checking in the bcder library covered by CVE-2023-39914.

+View Analysis Description

Metrics CVSS Version 4.0 | CVSS Version 3.x | CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

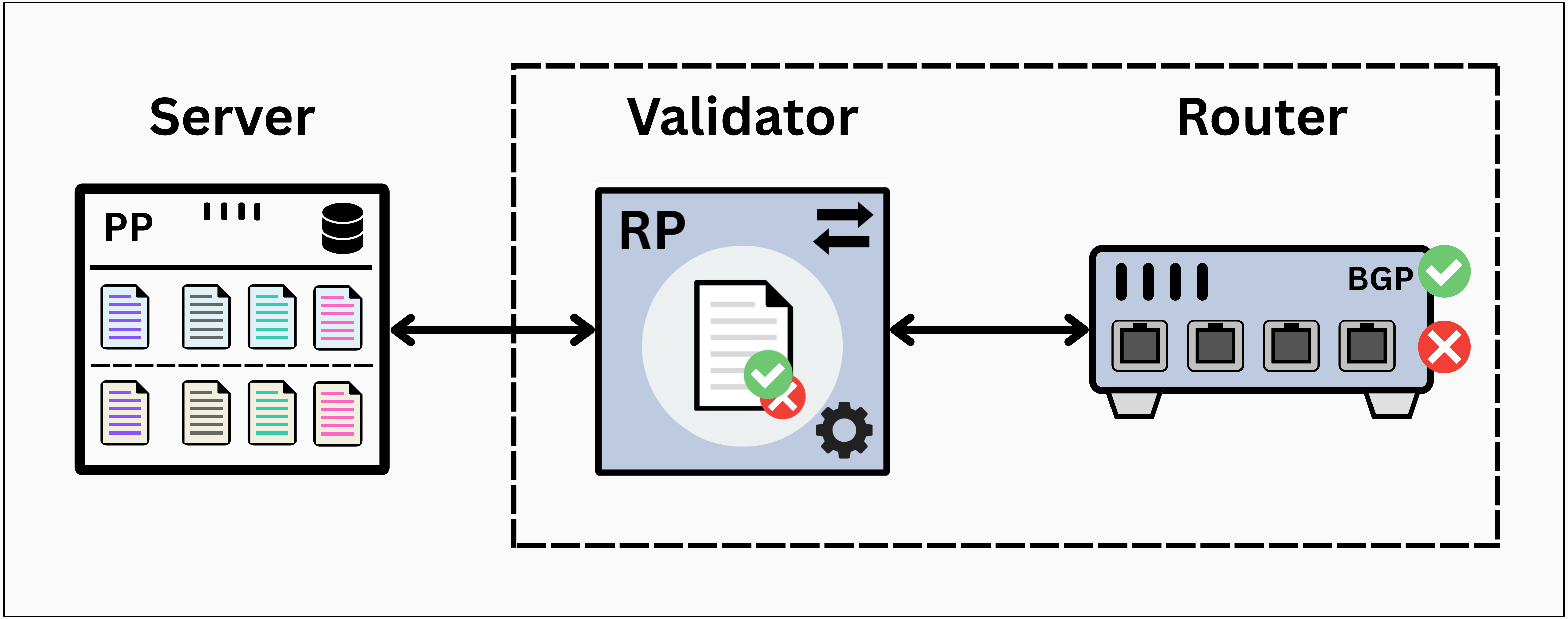
CVSS 3.x Severity and Vector Strings:

CNA: NLnet Labs Base Score: 7.5 HIGH Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

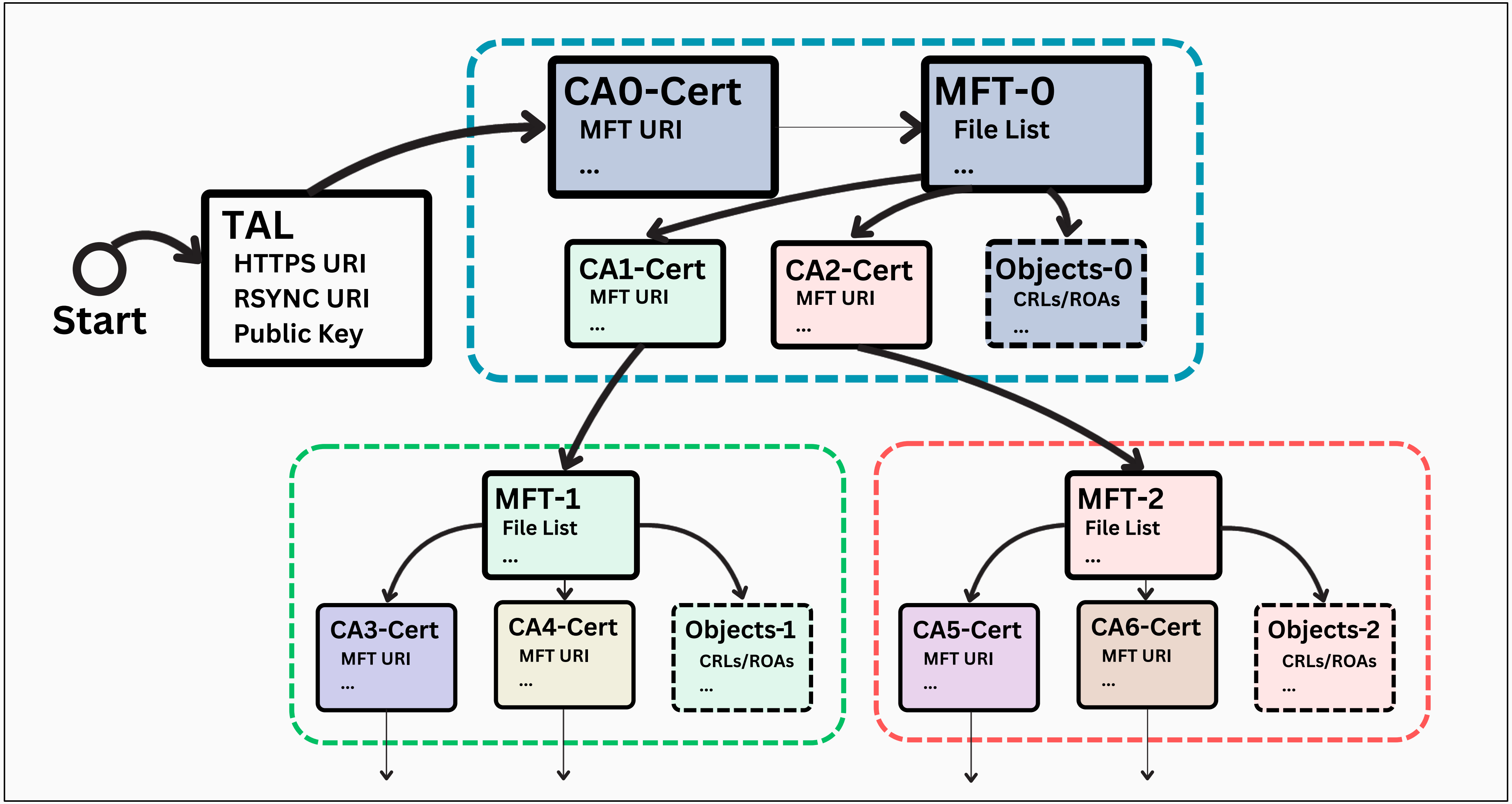
Current RPKI is challenging to implement and secure

RPKI is (very) complex...

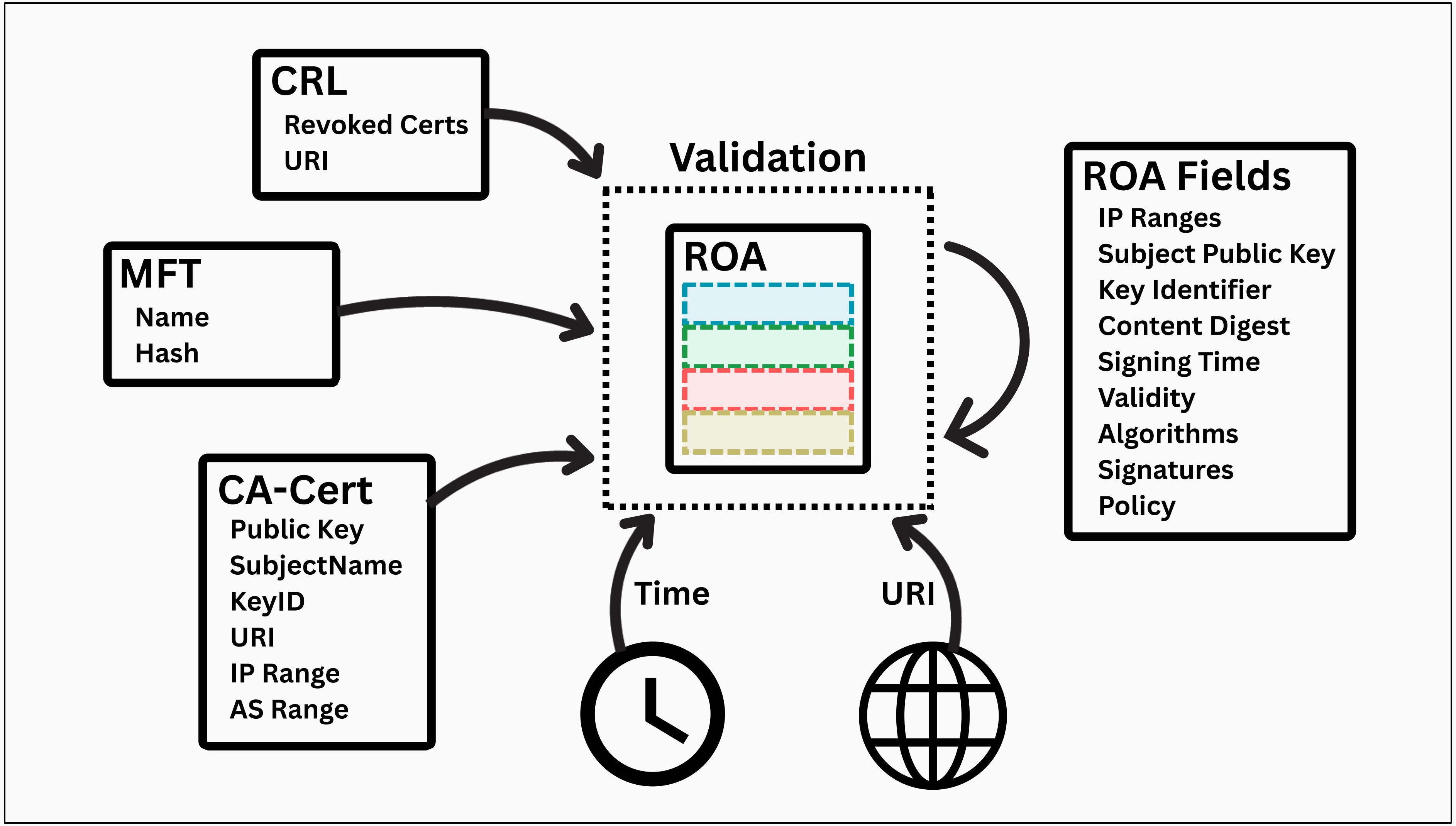
Fundamentals of RPKI



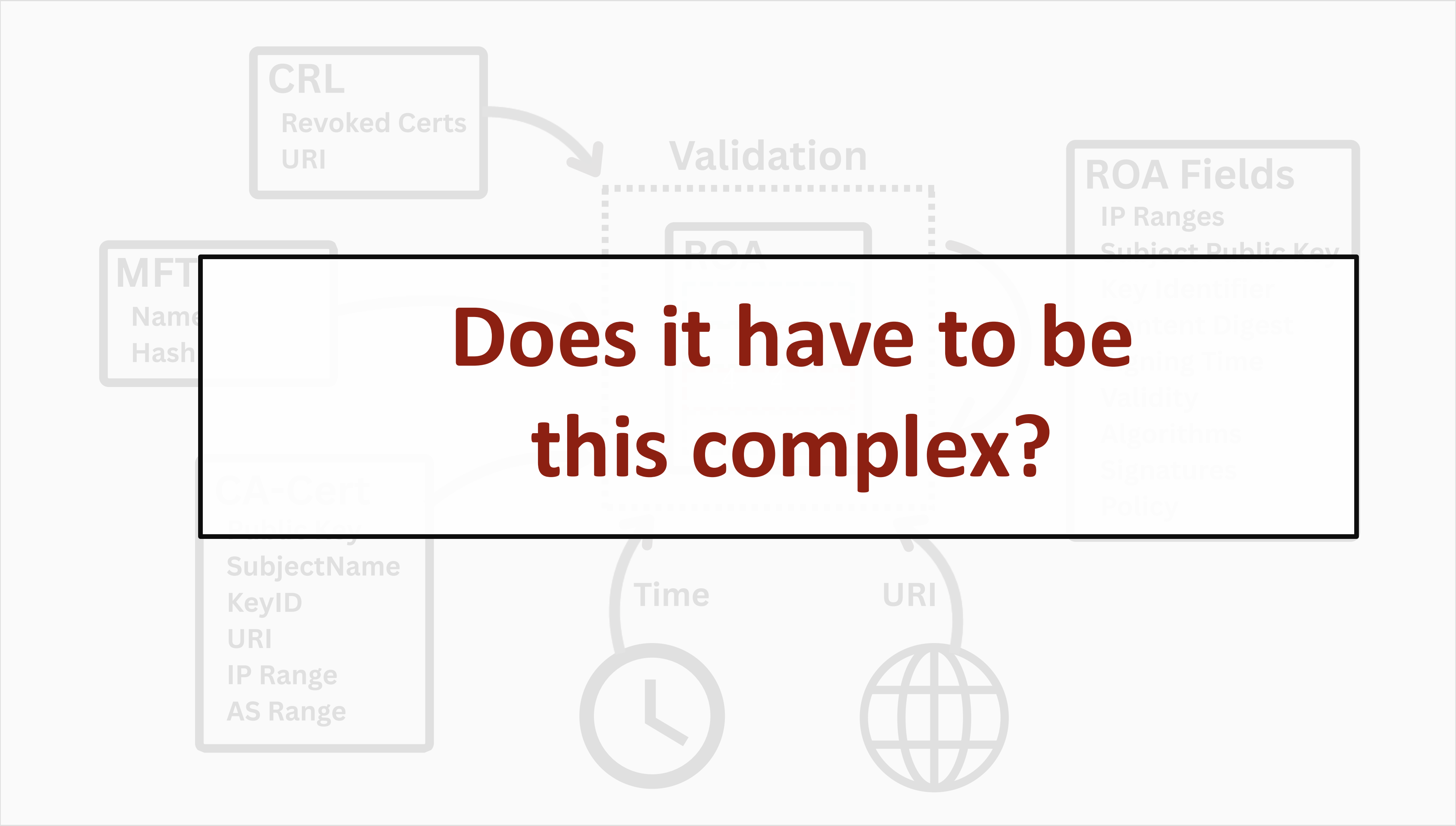
Fundamentals of RPKI



Fundamentals of RPKI



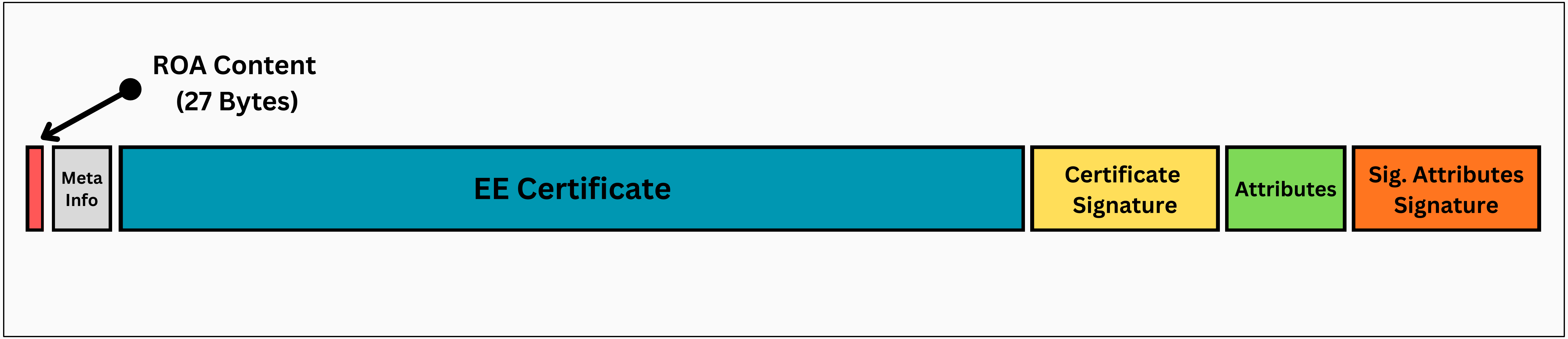
Fundamentals of RPKI



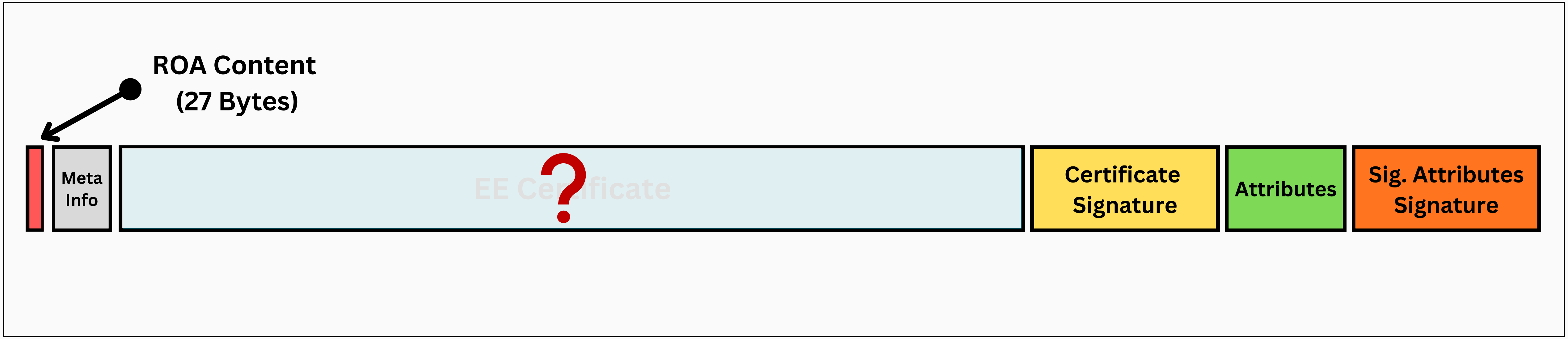
Does it have to be this complex?

Questioning fundamental Design Choices of RPKI

Analyzing RPKI Overhead – ROA Object



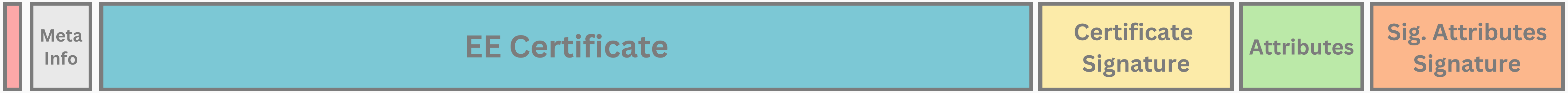
Analyzing RPKI Overhead – Do we need the EE-Cert?



Do we need the EE-Cert?

RFC6480

> »The private key associated with an EE certificate is used to sign **a single RPKI signed object**, i.e., the EE certificate is used to **validate only one object**«



Meta Info

EE Certificate

Certificate Signature

Attributes

Sig. Attributes Signature

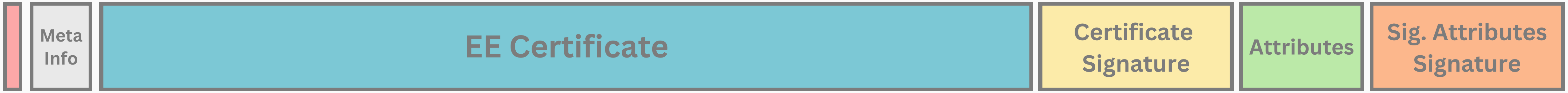
Do we need the EE-Cert?

RFC6480

> »The private key associated with an EE certificate is used to sign a **single RPKI signed object**, i.e., the EE certificate is used to validate **only one object**«

RFC6480

> »Because of the **one-to-one relationship** between EE certificate and signed object, **revocation of** the **certificate** effectively **revokes** the corresponding **signed object**«



Do we need the EE-Cert?

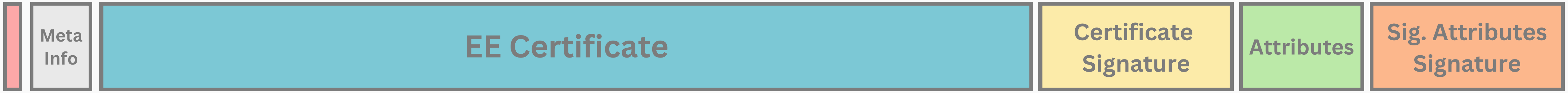
RFC6480

»The private key associated with an EE certificate is used to sign a single RPKI signed object, i.e., the EE certificate is used to validate only one object«

RFC6480

»Because of the **one-to-one** relationship between the EE certificate and the signed object, revocation of the certificate effectively revokes the corresponding signed object«

EE Certificate (mostly) for revocation is exessive



Do we need the EE-Cert?

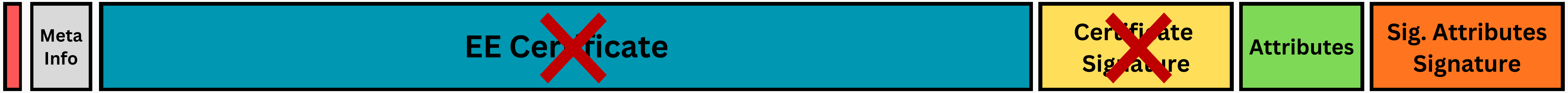
RFC6480

»The private key associated with an EE certificate is used to sign a single RPKI signed object, i.e., the EE certificate is used to validate only one object«

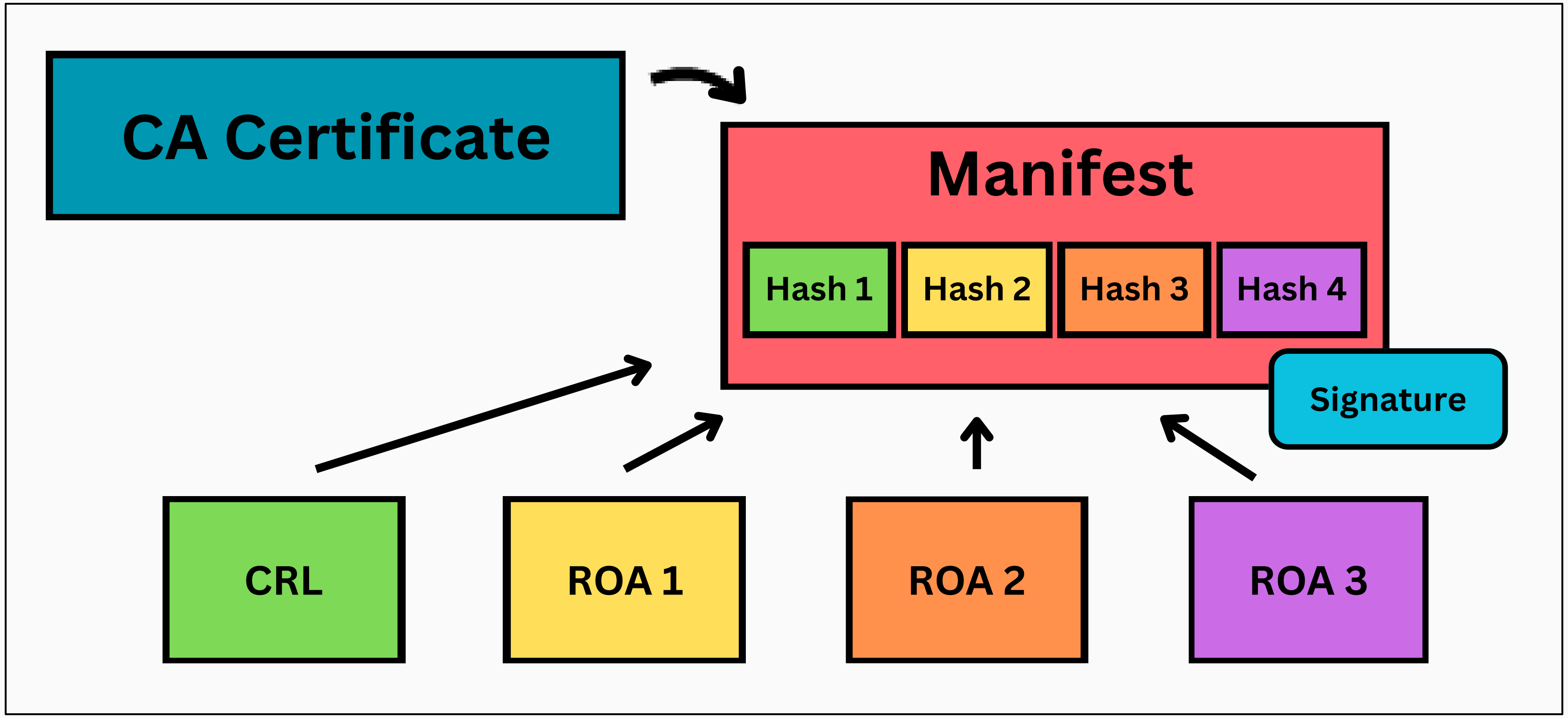
RFC6480

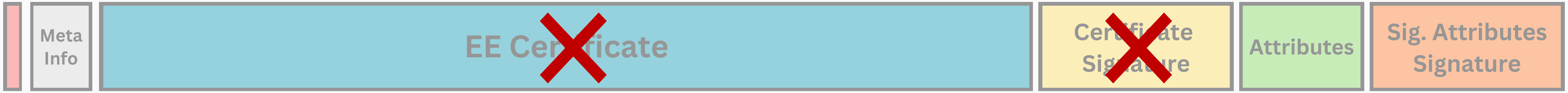
»Because of the **one-to-one** relationship between EE certificate and signed object, revocation of the certificate effectively revokes the corresponding signed object«

EE Certificate (mostly) for revocation is exessive

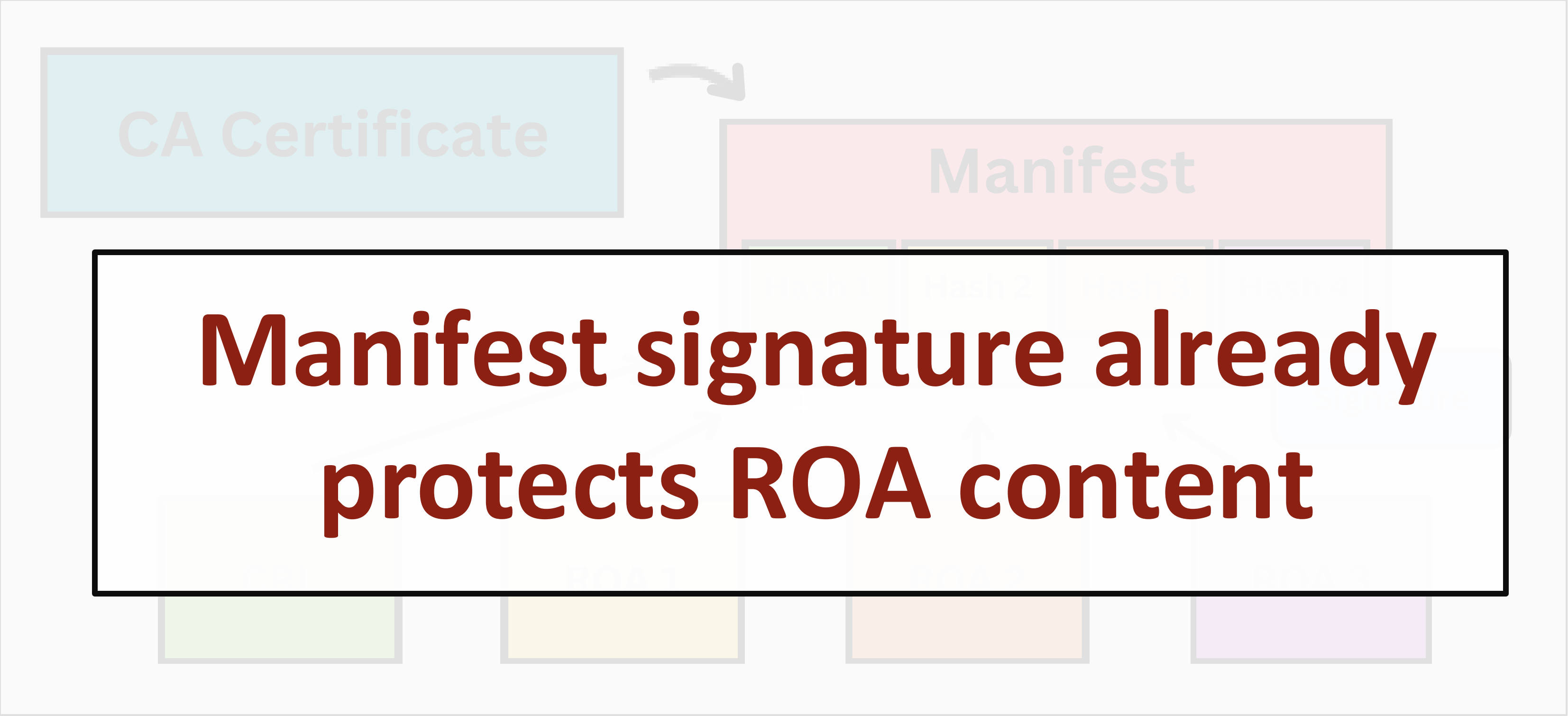


Do we need ROA signatures?

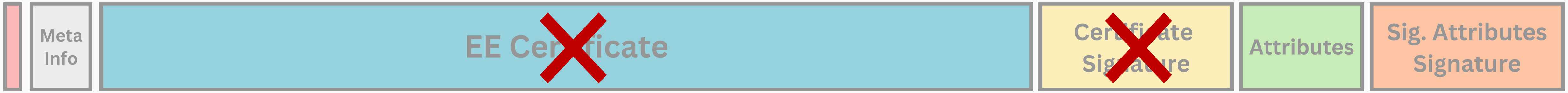




Do we need ROA signatures?



Manifest signature already protects ROA content



Meta Info

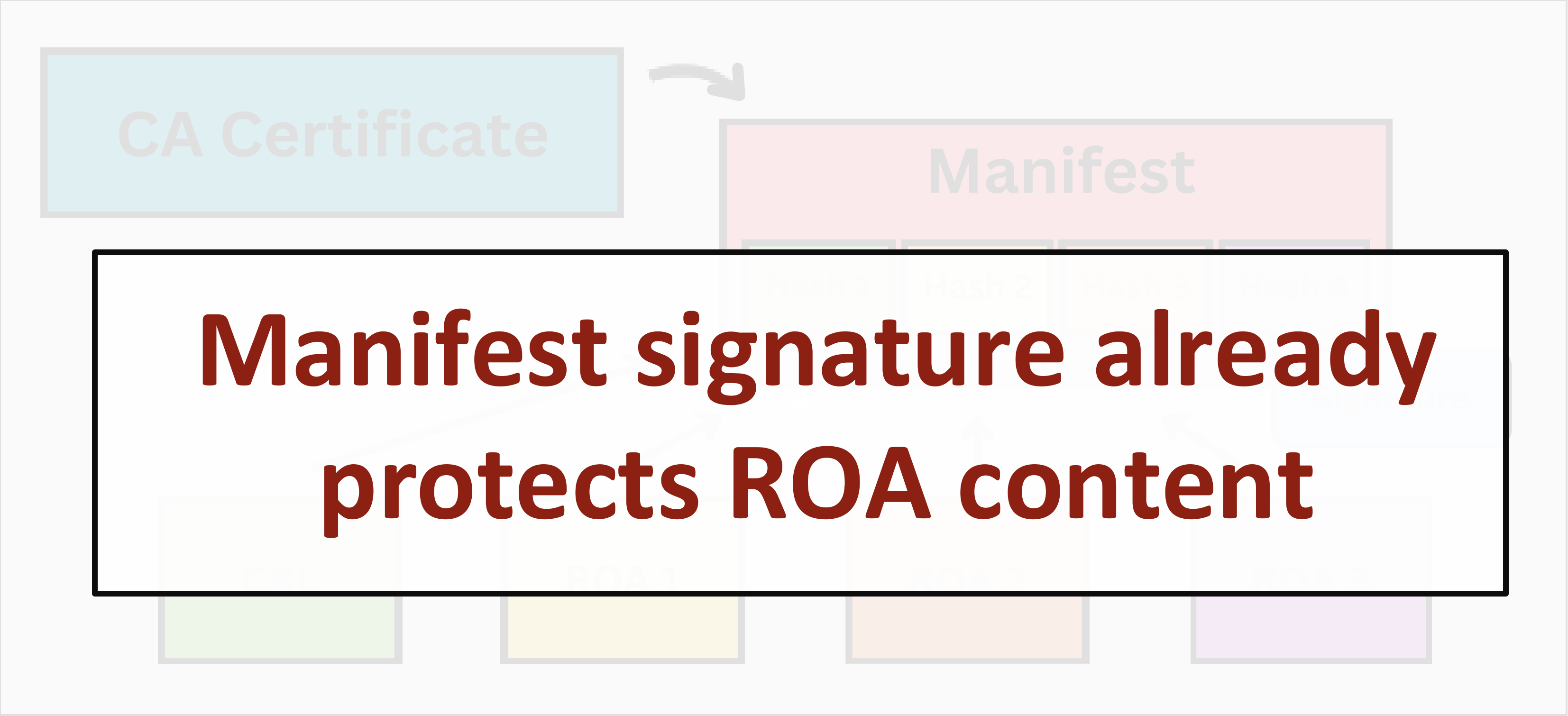
~~EE Certificate~~

~~Certificate Signature~~

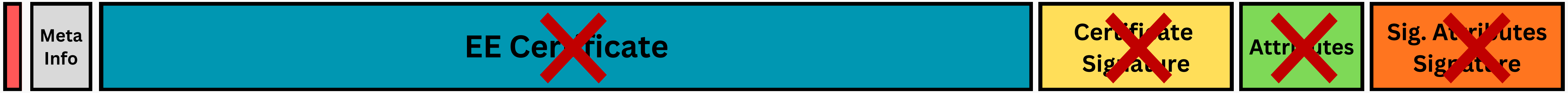
Attributes

Sig. Attributes Signature

Do we need ROA signatures?



Manifest signature already protects ROA content



Introducing Improved RPKI (iRPKI)

Stripping EE Certificate

Unsigned ROAs

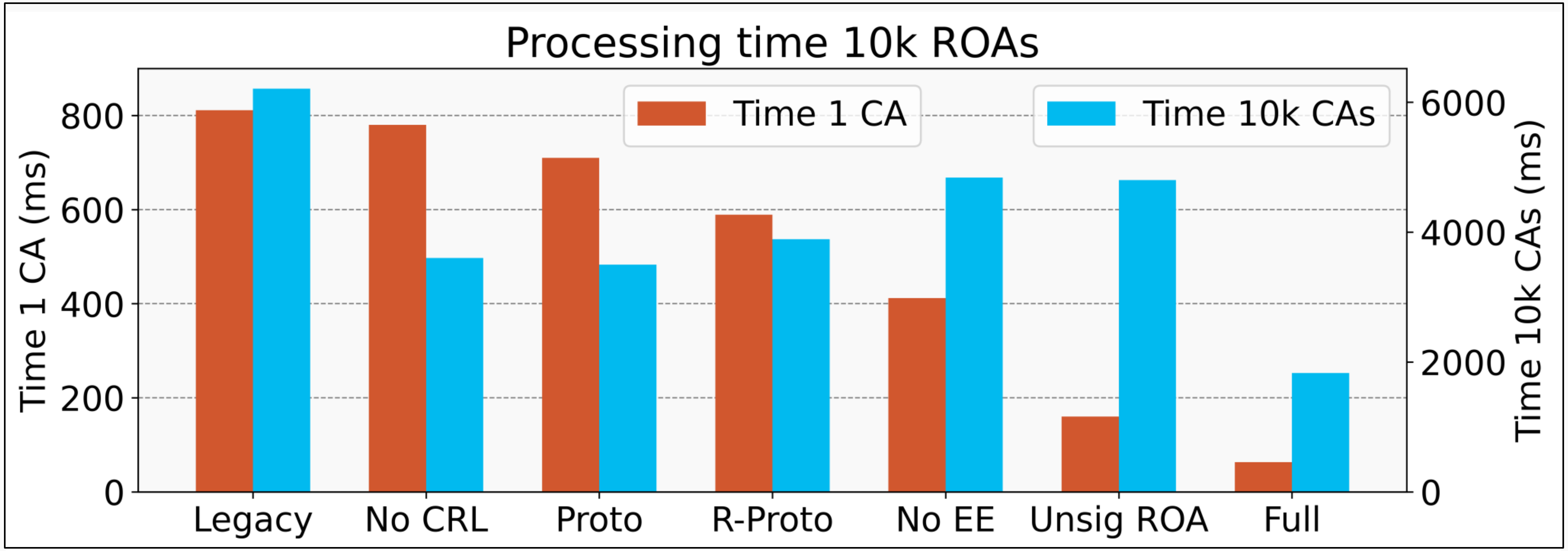
Restructure Objects

Combine MFT and CRL

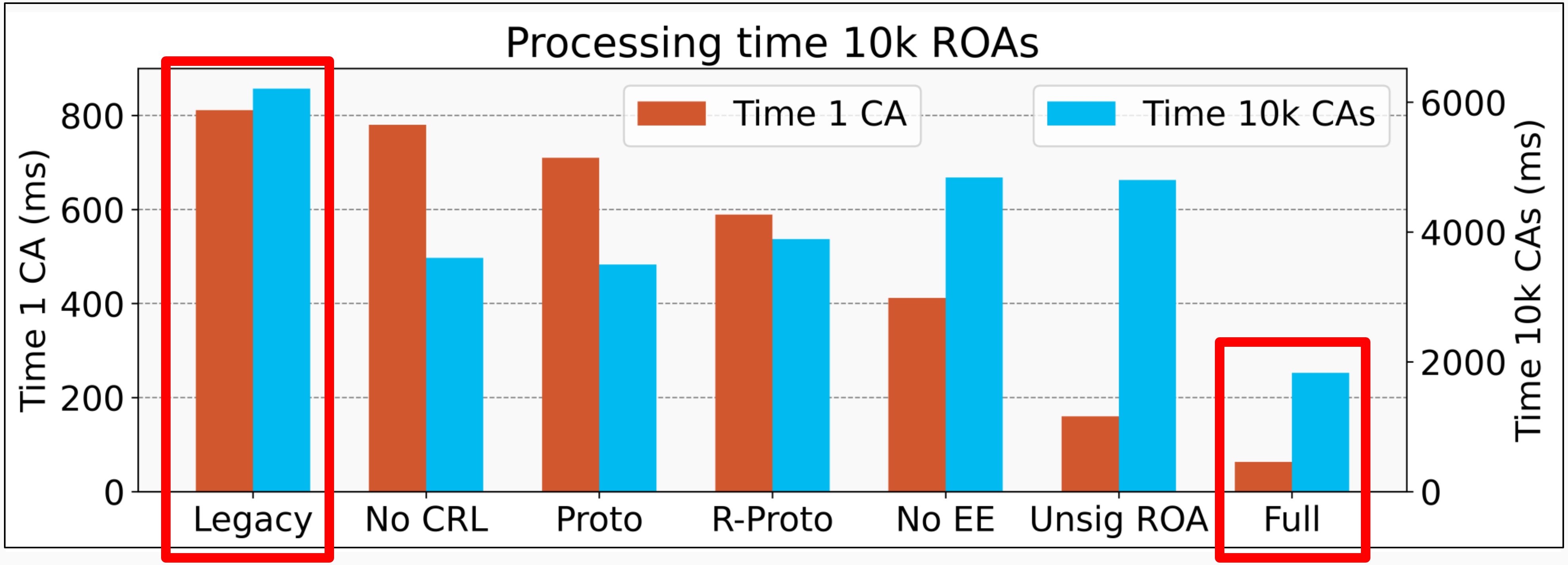
XML -> Protobuf

DER -> Protobuf

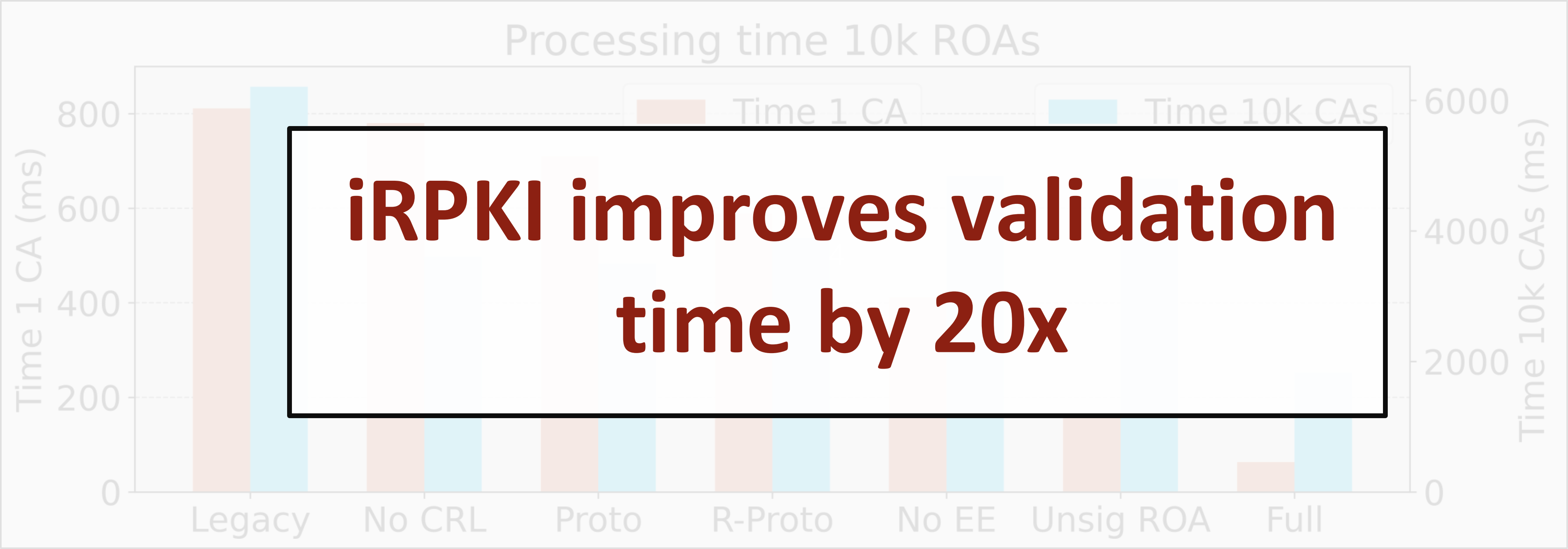
Evaluating iRPKI



Evaluating iRPKI



Evaluating iRPKI



iRPKI improves validation time by 20x

Conclusion

- Current RPKI design is complex and inefficient
- Fundamentally redesigning RPKI yields 20x speed improvements
- iRPKI reduces complexity and improves security

Scan to read the Paper!!

https://arxiv.org/abs/2507.01465

Thank you for your attention!

For more information, please see our Paper https://arxiv.org/abs/2507.01465
For any questions, you can contact me at

n.vogel@em.uni-frankfurt.de

çok
teşekkürler

תודה רבה!

谢谢

Merci
beaucoup!

Thank you
very much!

Dank je
wel!

Vielen
Dank!

Muchas gracias

ありがとうございました

Dziękuję!

zor spas

Grazie mille!

اشكرك