An Introduction to ASPA

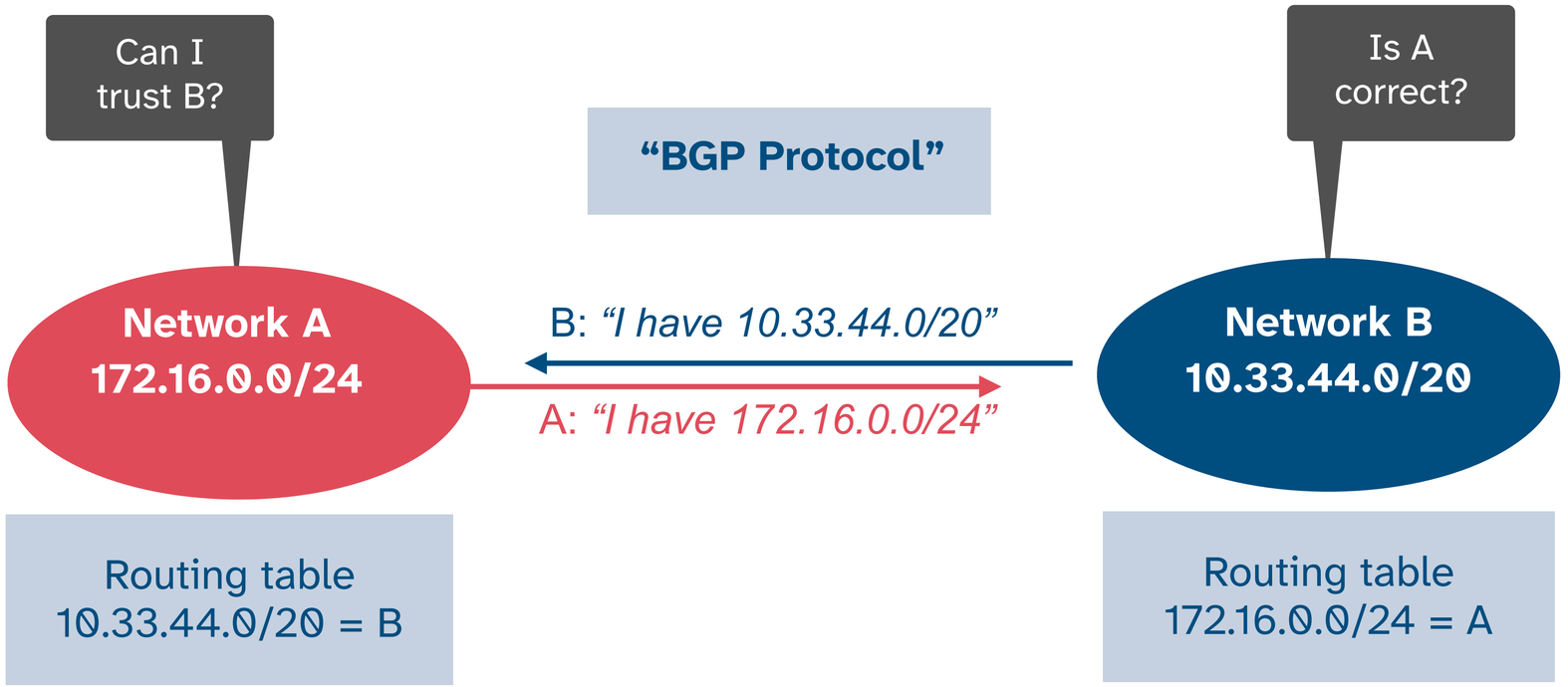
Validating AS-Paths with the help of RPKI

Massimiliano Stucchi

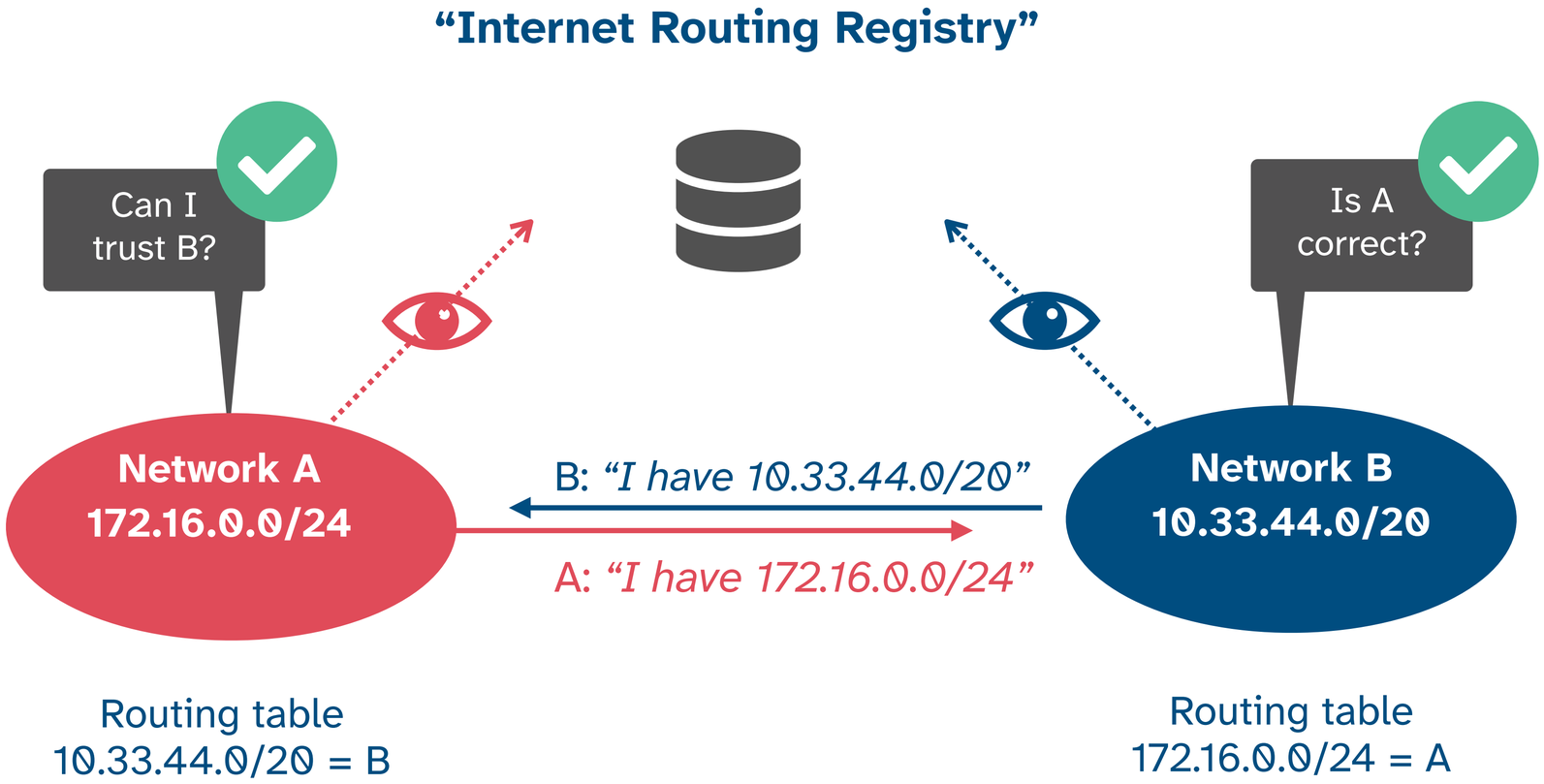
RPKI

Section 1

Routing on the Internet



How can you have secure routing?



Problem Statement

- Some IRR data cannot be fully trusted
  - Accuracy
  - Incomplete data
  - Lack of maintenance
- Third party databases are widely used
  - No verification of who holds IPs/ASNs

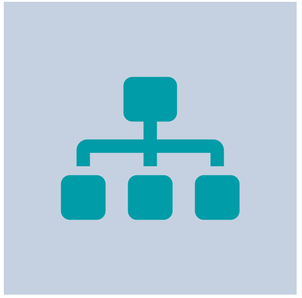
A Short History

- Operated since 2008 by all RIRs
  - Community-driven standardisation (IETF)

- Adds crypto-security to IP addresses and ASNs
  - Provides data you can trust

Resource Public Key Infrastructure

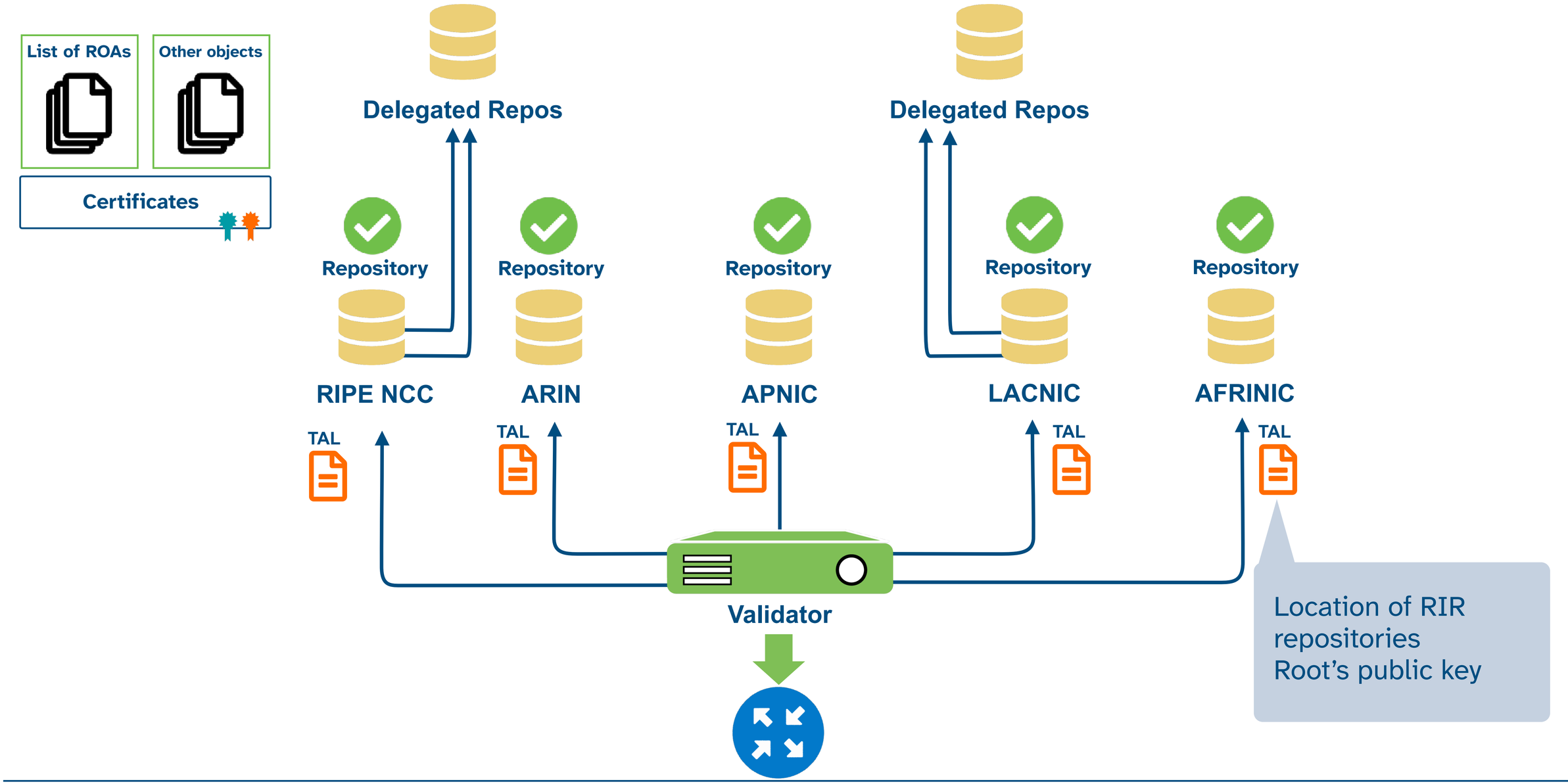
Ties IP addresses and ASNs to public keys



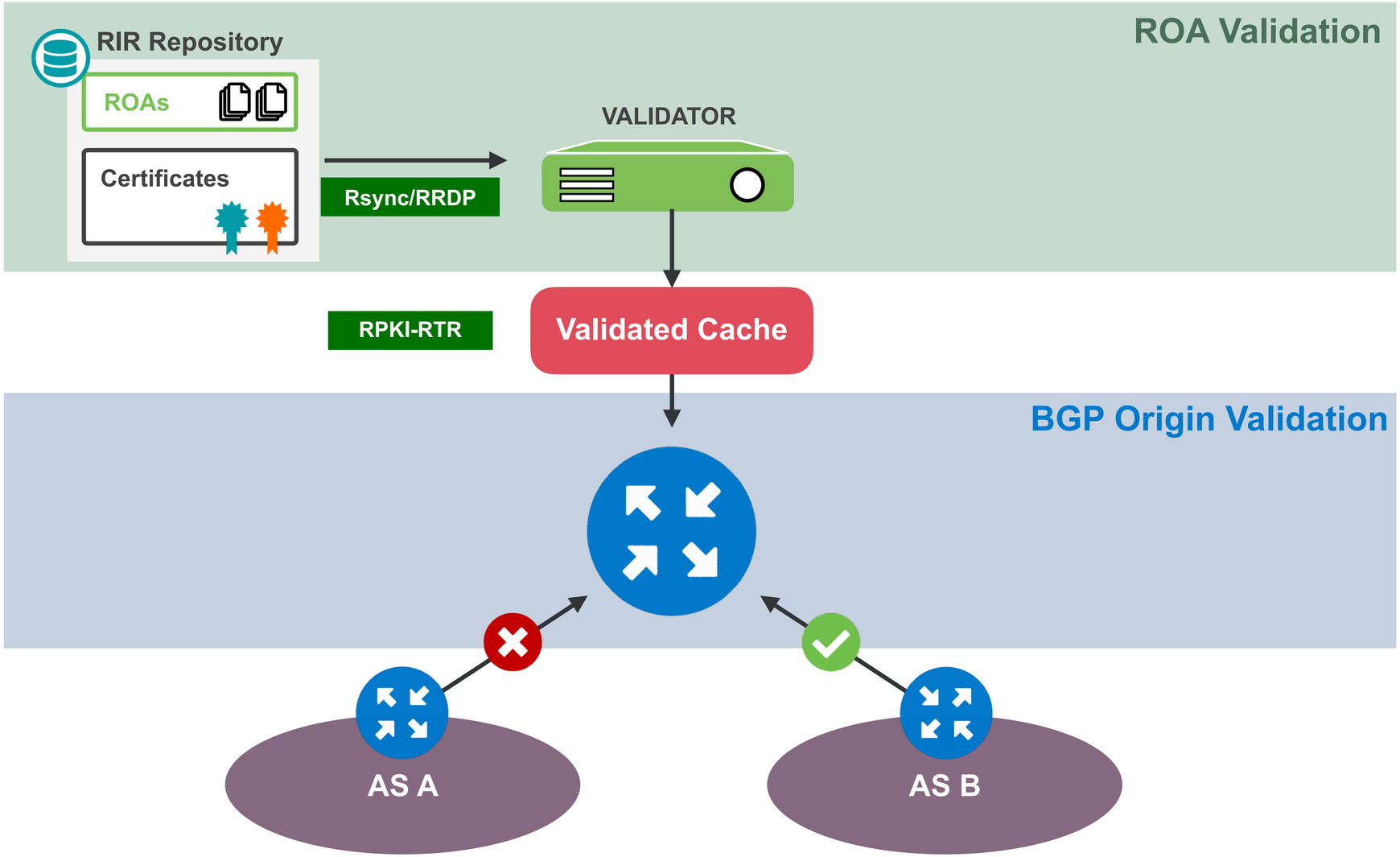
Follows the hierarchy of the registries

Statement from resource holders:
“ASNx is authorized to announce prefix Y”
Signed: Holder of prefix Y

RPKI Model


List of ROAs
Other objects
Certificates
Delegated Repos
Delegated Repos
Repository
Repository
Repository
Repository
Repository
RIPE NCC
ARIN
APNIC
LACNIC
AFRINIC
TAL
TAL
TAL
TAL
TAL
Validator
Location of RIR repositories
Root's public key

Origin Validation

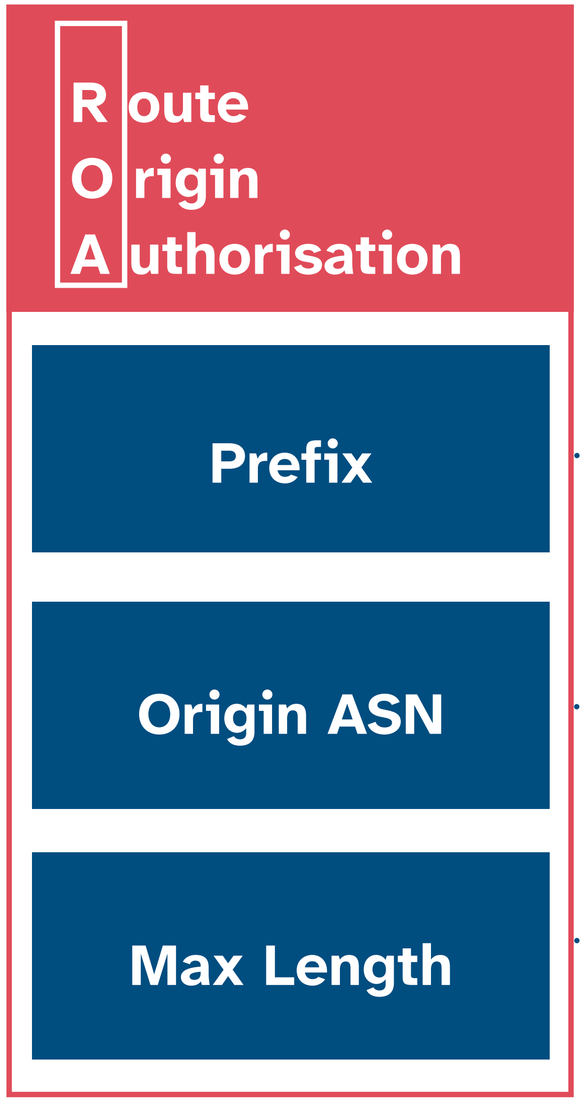


What is a ROA ?

An Authorised Statement from a resource holder

AS Number
is authorised to announce
Prefix

What is in a ROA ?



The network for which you are creating the ROA

The ASN supposed to originate the BGP Announcement

The maximum prefix length that ROA is authorised to advertise

Where do we go from here ?

- ROAs are only one of the steps towards full BGP Validation
  - Paths are not validated

- We need more building blocks

RPKI Objects

ROAs	BGPSec
Validate Origin	Validate path by signing

BGPSec

- RPKI does not protect against path redirection attacks

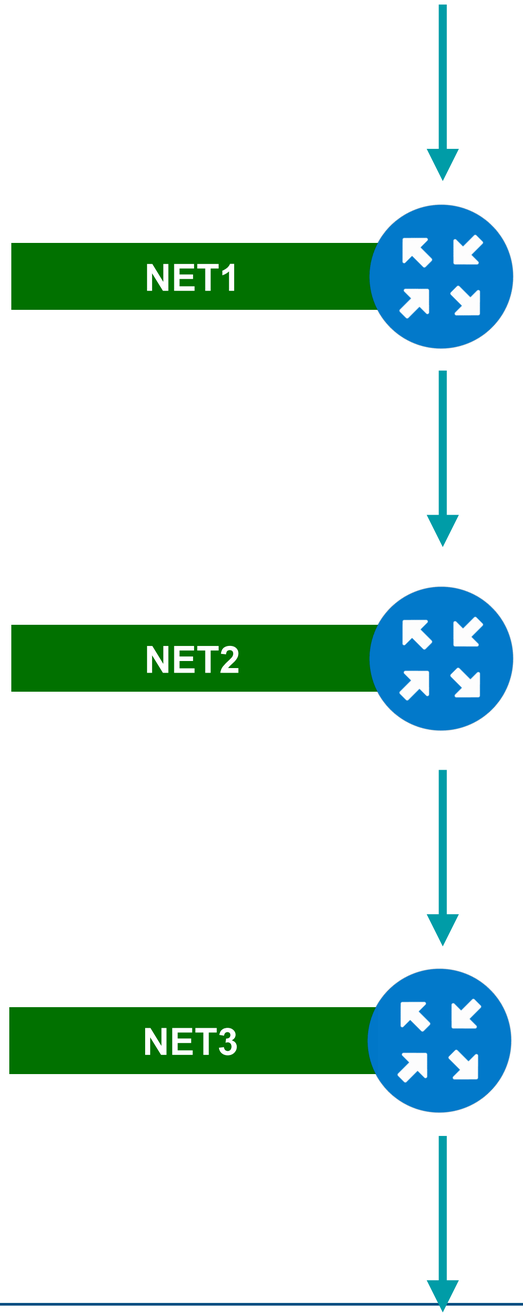
- We need a way to verify the AS-Path of a given BGP Announcement
  - And understand if anyone tampered with the data on the way to our routers

BGPSec Path Validation

- With BGPSec, the AS-Path attribute is cryptographically signed
  - Using the operator's certificate from RPKI

- In order to validate an AS-Path, routers verify the chain of trust of all the signatures of the AS-Path

BGPSec



Network: 192.168.0.0/16
AS Path: NET1, …
BGPSEC: (key1, signature1)

Network: 192.168.0.0/16
AS Path: NET2, NET1, …
BGPSEC: (key1, signature1)
(key2, signature2)

Network: 192.168.0.0/16
AS Path: NET3, NET2, NET1, …
BGPSEC: (key1, signature1)
(key2, signature2)
(key3, signature3)

BGPSec is not here

- BGPSec is standardized, but unfortunately no full implementation exists right now
- It requires too many resources for the moment
- So, for now, we can call it “the future”

RPKI Objects

ROAs	BGPSec	ASPA
Validate Origin	Validate path by signing	Validate paths by declaring upstreams

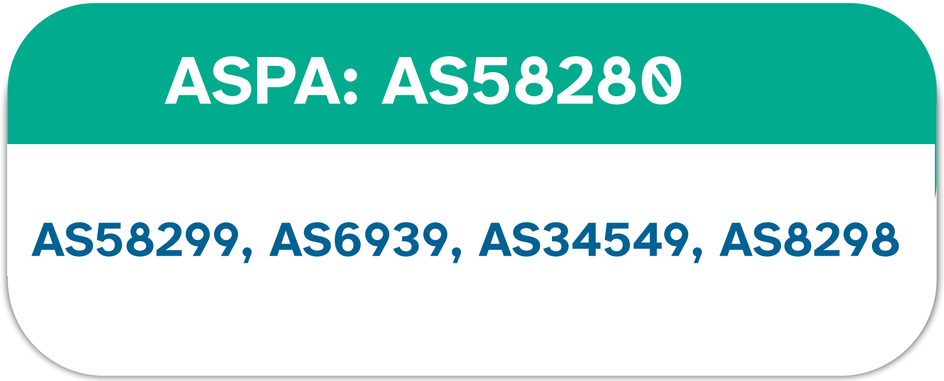
The Present of RPKI path validation

Section 2

ASPA

- Autonomous System Provider Authorisation
- New objects in RPKI that list the upstreams of an ASN
- IETF work is still in draft, but expected to become RFCs soon

ASPA Objects



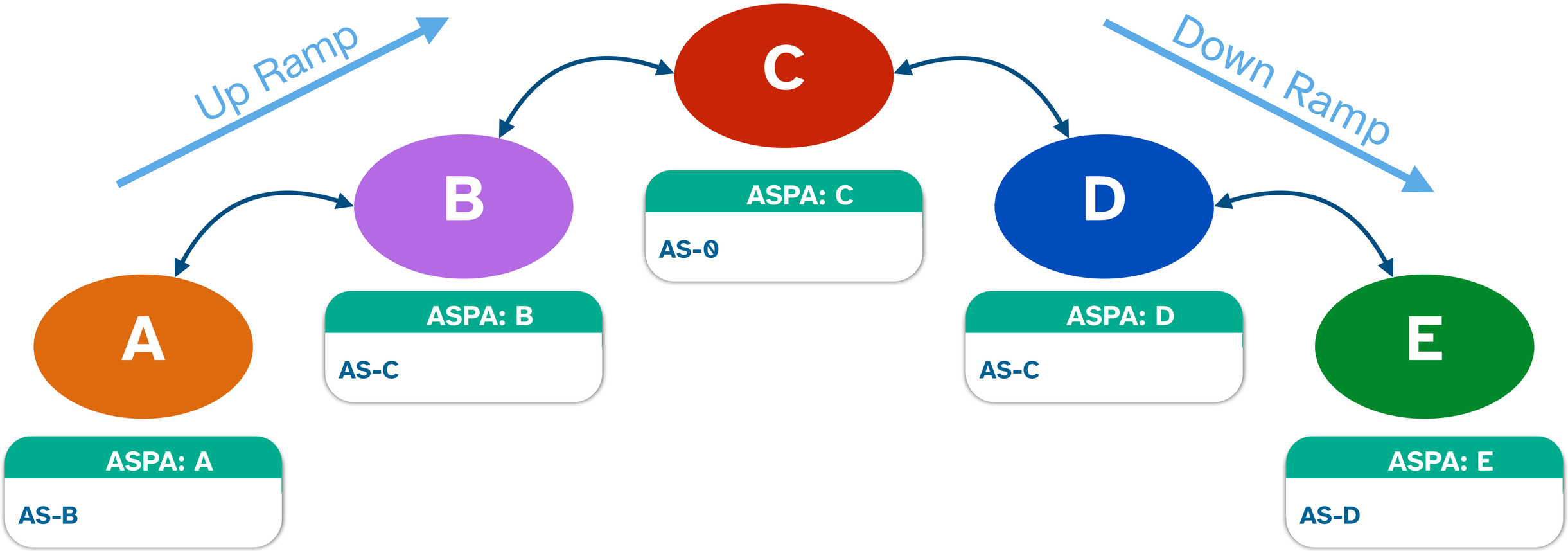
Content: A list of Authorized upstreams

ASPA Objects

- Distributed as part of the RPKI data set
  - Signed
  - Supported in RPKI-RTR version 2, draft (RFC8210-bis)
- Available on (as of April 2026)
  - **RIPE NCC** hosted RPKI, **ARIN** hosted RPKI, **APNIC** hosted RPKI end of Q2/2026
  - Krill as delegated RPKI
- Every ASN should have one

ASPA Relationships

- With ASPA we can build a graph of relationships



ASPA States

Provider

ASPA exists,
and defines this ASN
as an upstream

Not Provider

ASPA exists,
but does not define
this ASN as an
upstream

Something is wrong

No Attestation

There is no ASPA, so
no relationship can
be verified

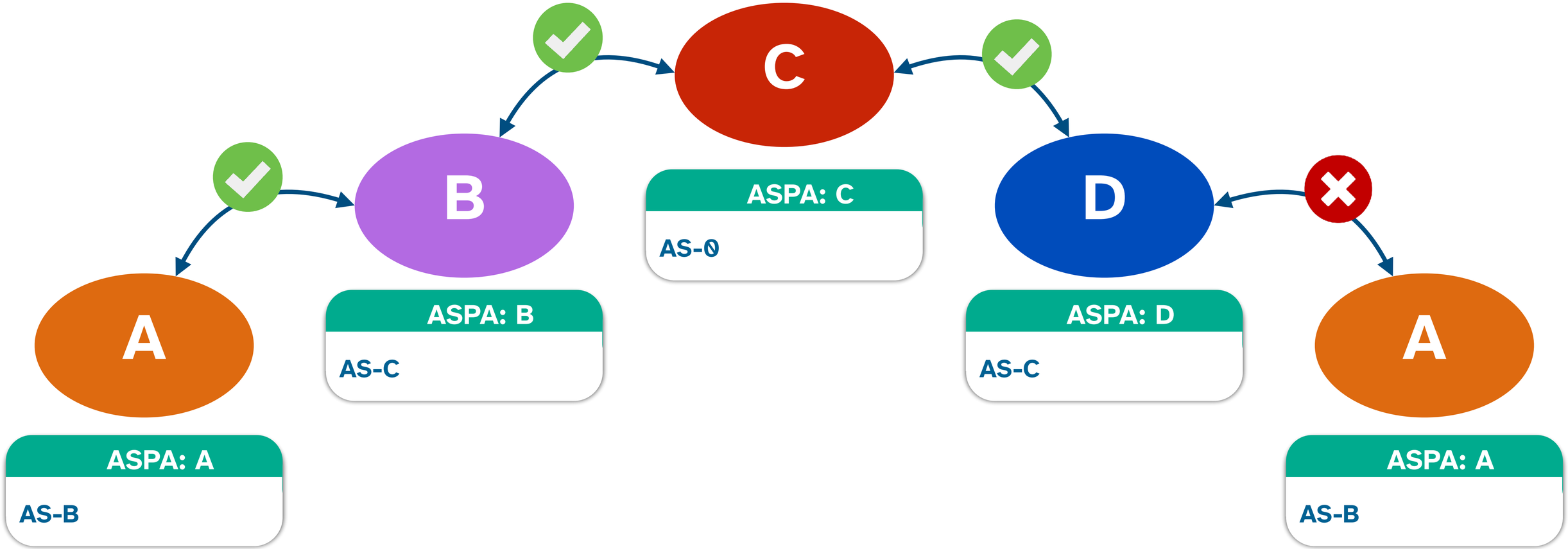
ASPA Verification

- As long as you don’t find any “Not Provider” relationship, everything is okay
- This helps in “failing open” and also in situations with No Attestation
- Verification available in Bird, OpenBGPd
  - Cisco IOS-XR still in testing
  - Arista should be ready at the end of June
- Routinator and rpki-client include support for ASPA objects

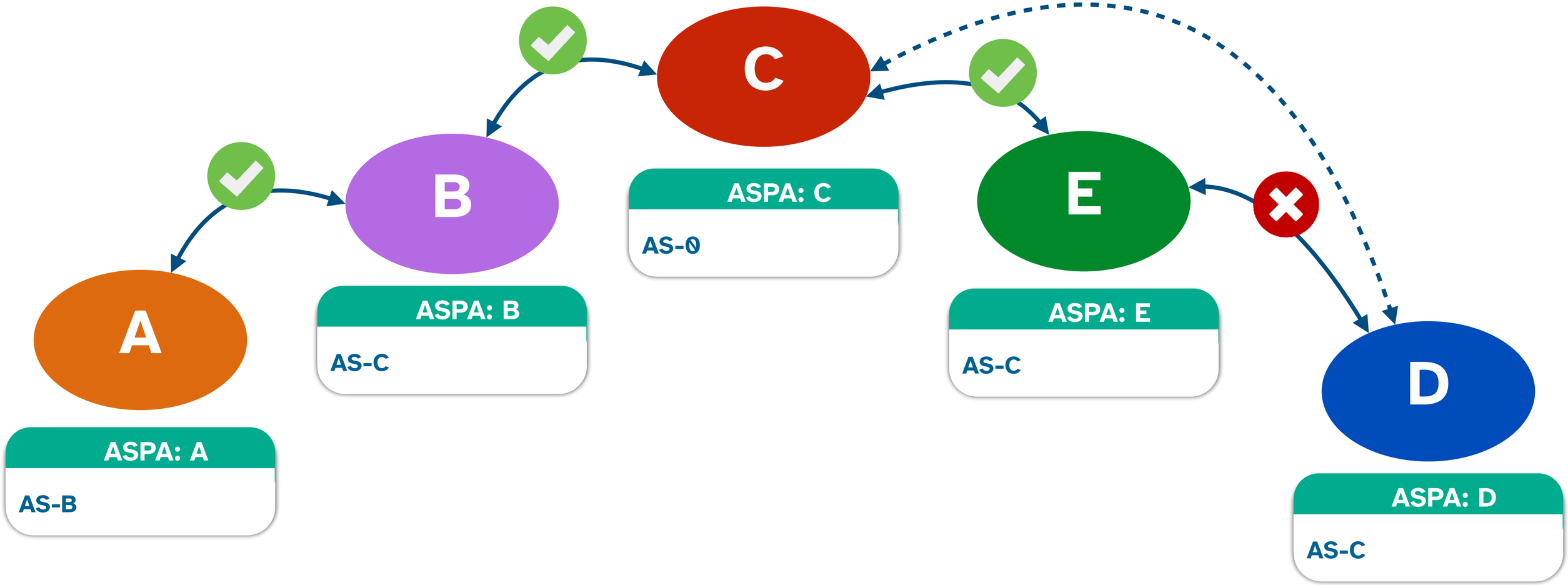
AS0/Bogon ASNs in ASPA

- A common attestation that the ASN has no upstreams
  - If you see it in a path, it’s either at the “Apex” or there is something wrong
- Any other bogon ASN could be used, but AS0 is easily recognizable
- Should be seen used by Tier 1s and IXP Route Servers
  - Also route collectors

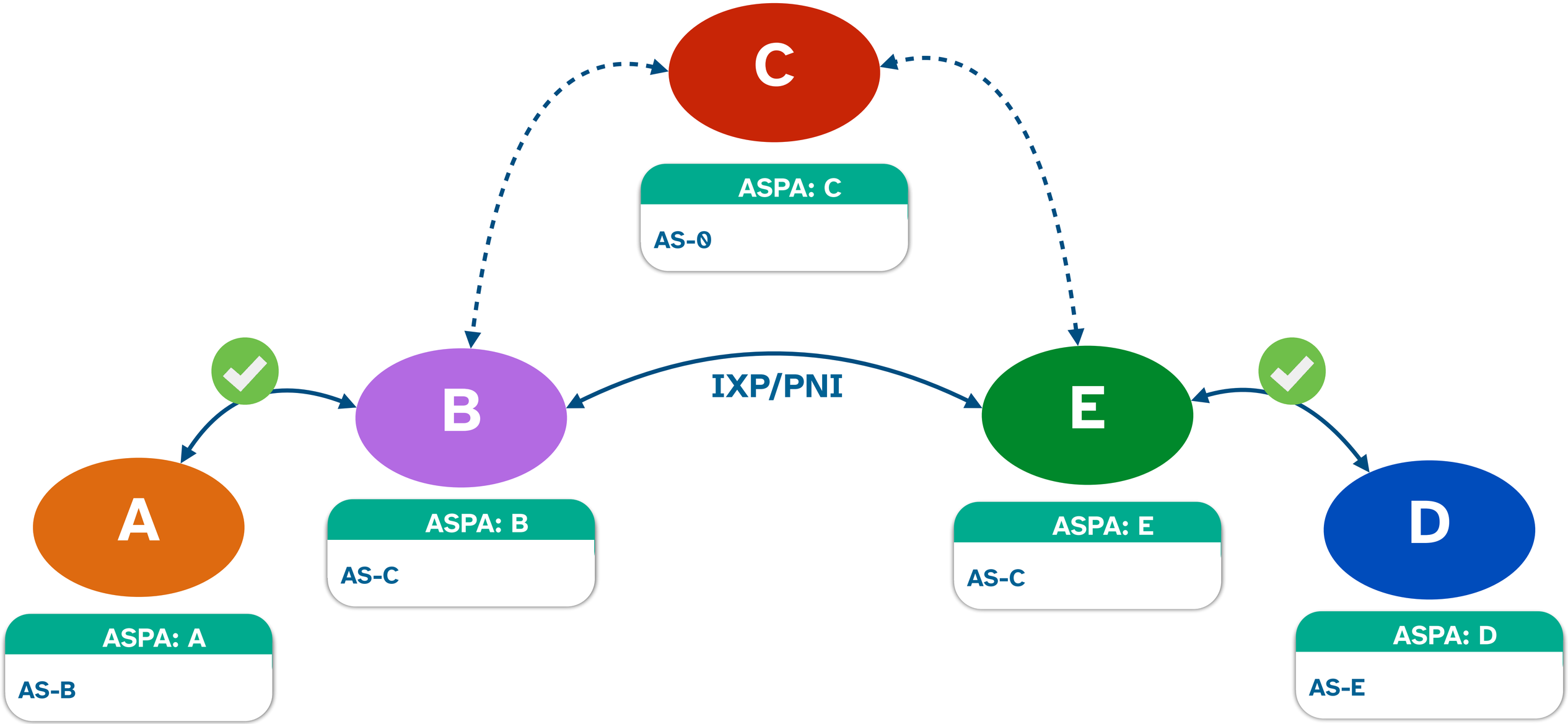
ASPA Verification



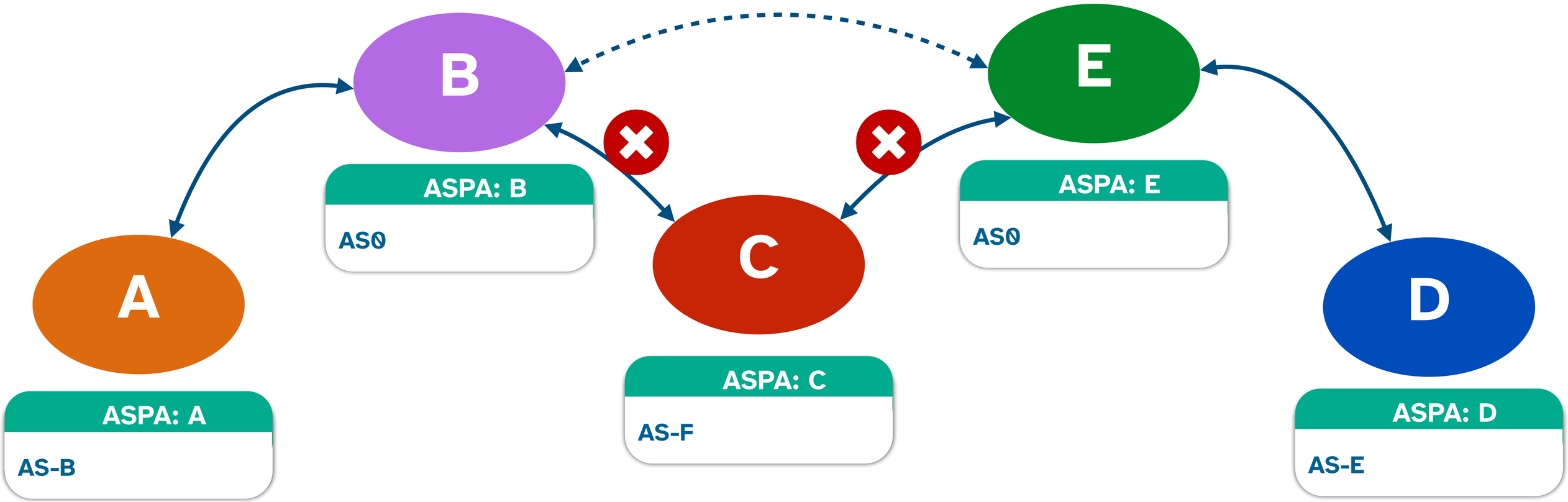
ASPA Verification - Path Hijack



ASPA Verification - IXP/PNI



ASPA Verification - Valleys



Wrap-Up

Section 4

RPKI Objects

ROAs	BGPSec	ASPA	RPKI Signed Checklists
Validate Origin	Validate path by signing	Validate paths by declaring upstreams	Sign data to authenticate it

ASPA

- A new building block to make routing more secure

- Still need to be widely adopted

So, how do I start ?

- Start by creating ROAs and ASPA
- Evaluate Relying Parties
  - You need at least two in your network
- Start by logging, not filtering based on any of the two
  - Check your customers

ASPA Path viewer

- You can visualize ASPA paths using an online tool to simulate validation
  - Also show up-ramp and down-ramp
- Written by Ondřej Caletka
- https://oskar456.github.io/aspa.html

BGPAlerter

- You can use it to monitor your announcements
- https://github.com/nttgin/BGPalerter
- Very quick setup, monitors changes in your announcements based on RIS data
- Also used to provide commercial monitoring service:
  - packetviz.net

Questions ?

max@stucchi.ch

The End!

Fí

Liðugt

Y Diwedd

Край

Соңы

النهاية

Ende

s’Änd

Վերջը

پایان

Finis

Endin

Kraj

Finvezh

Fund

Tmiem

Konec

Кінець

Beigas

Ënn

An Críoch

Lõpp

Endir

Vége

Son

Kpaj

הסוף

「完結」

Fine

Einde

Sfârşit

Fin

Τέλος

Loppu

Slutt

დასასრული

Конец

Slut

Fim

Pabaiga

Koniec

Amaia