BGPSEC Quick Tutorial

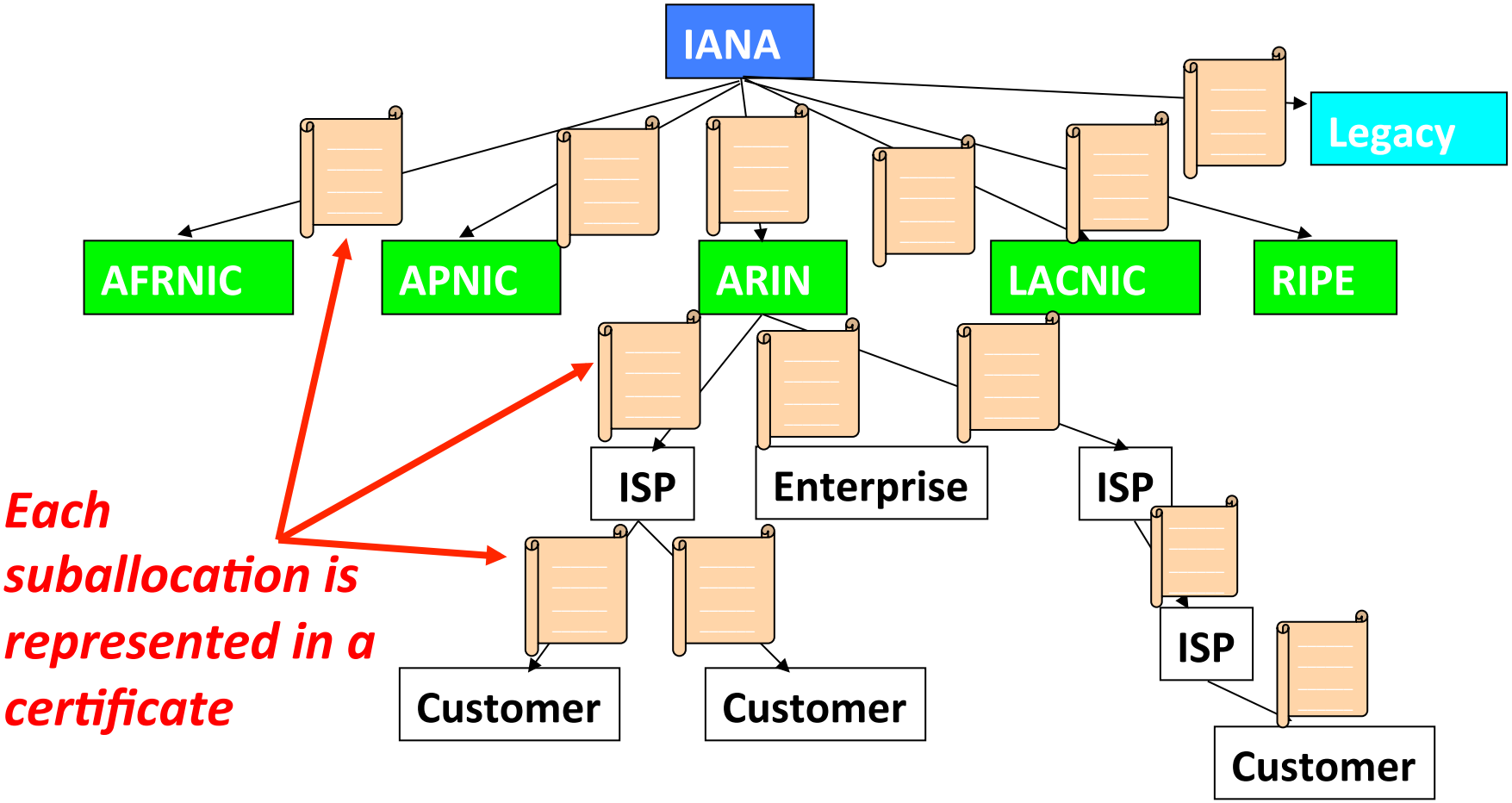
Sandra Murphy sandy@tislabs.com

Chris Morrow morrowc@ops-netman.net

Why BGPSEC, isn't RPKI enough?

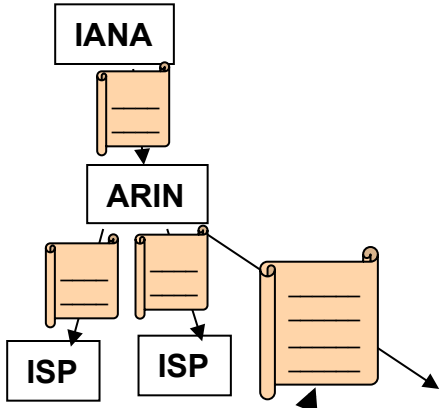
- RPKI is the set of data which provides certification of resource allocation
- Right now, RPKI can be used to protect origin validation
- BGPSEC is about protecting path validation

RPKI – Resource Certificates



Resource **certificate, not identity certificate**

Certs & Route Origin Authorization



Sign a Route Origin Authorization (ROA) for your address space. Your certificate validates the signature

Enterprise

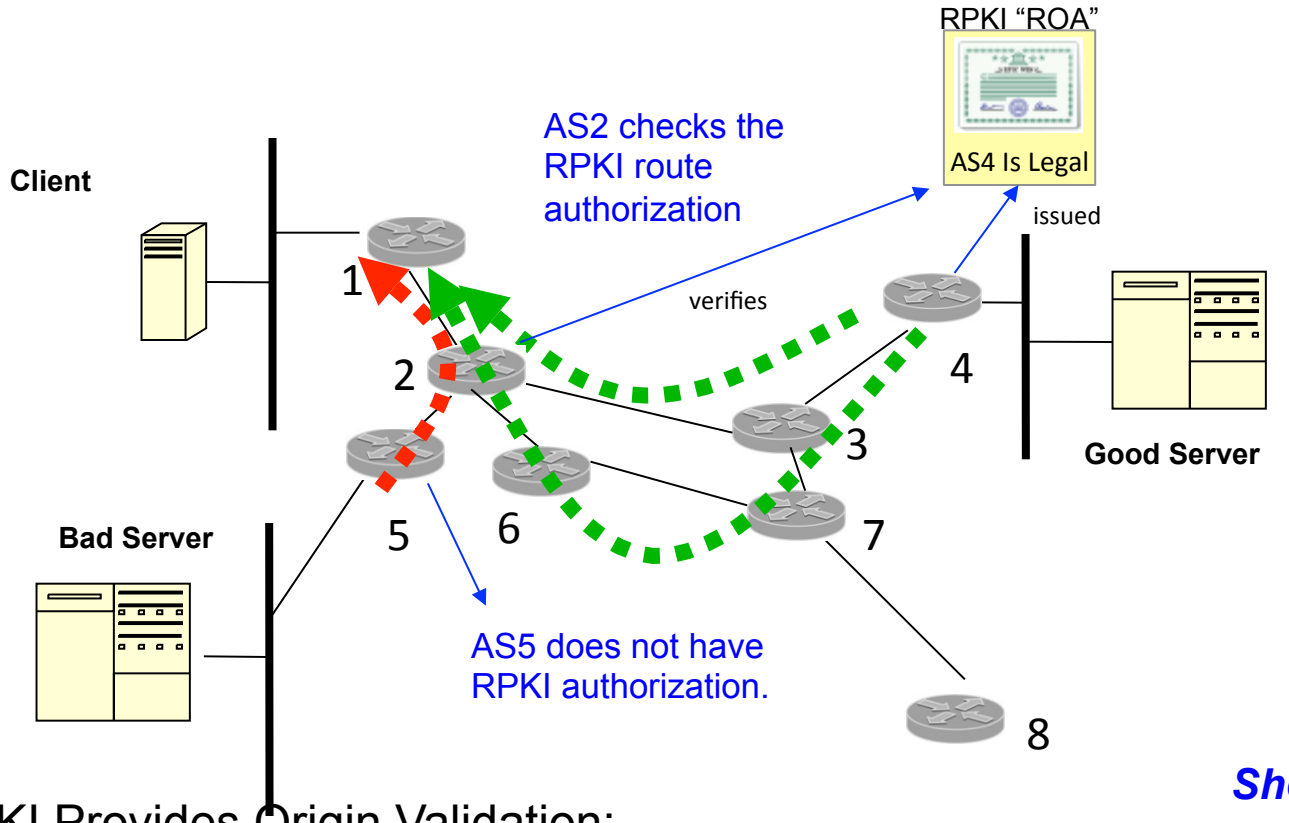
Certificate lists the addresses you hold and who gave them to you

CA certificate
Key: EnterpriseKey
Signed by: ARIN
Addresses: 10.2/16

ROASignedObject
Signed by: EnterpriseKey
Addresses: someofyouraddresses
Valid Origin: some one ASN

The ROA lists the valid origin for those addresses

Example RPKI Origin Validation



Should be rejected

RPKI Provides Origin Validation:

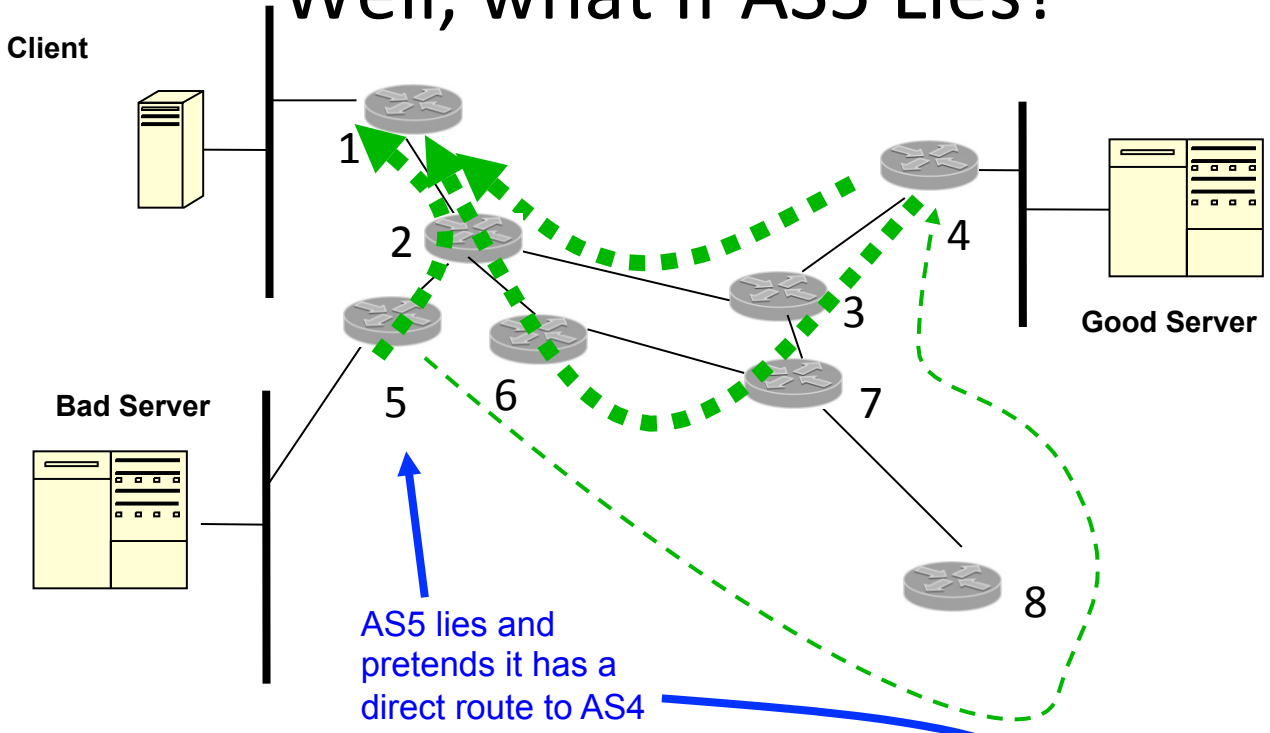
RPKI "ROA": prefix holder authorizes AS4 to advertise routes to Good Server

AS2 checks the validation state of the routes:

- INVALID (Origin is not AS4): AS2 ▶ AS5
- VALID (Origin is AS4): AS2 ▶ AS3 ▶ AS4
- VALID (Origin is AS4): AS2 ▶ AS6 ▶ AS7 ▶ AS3 ▶ AS4

Why isn't origin validation enough?

Well, what If AS5 Lies?



AS5 can still advertise a route to the Good Server with AS4 at the origin:
(even though AS5 isn't connected to AS4)

- VALID (Origin is AS4): AS1 ▶ AS2 ▶ AS5 ▶ AS4
- VALID (Origin is AS4): AS1 ▶ AS2 ▶ AS3 ▶ AS4
- VALID (Origin is AS4): AS1 ▶ AS2 ▶ AS6 ▶ AS7 ▶ AS3 ▶ AS4

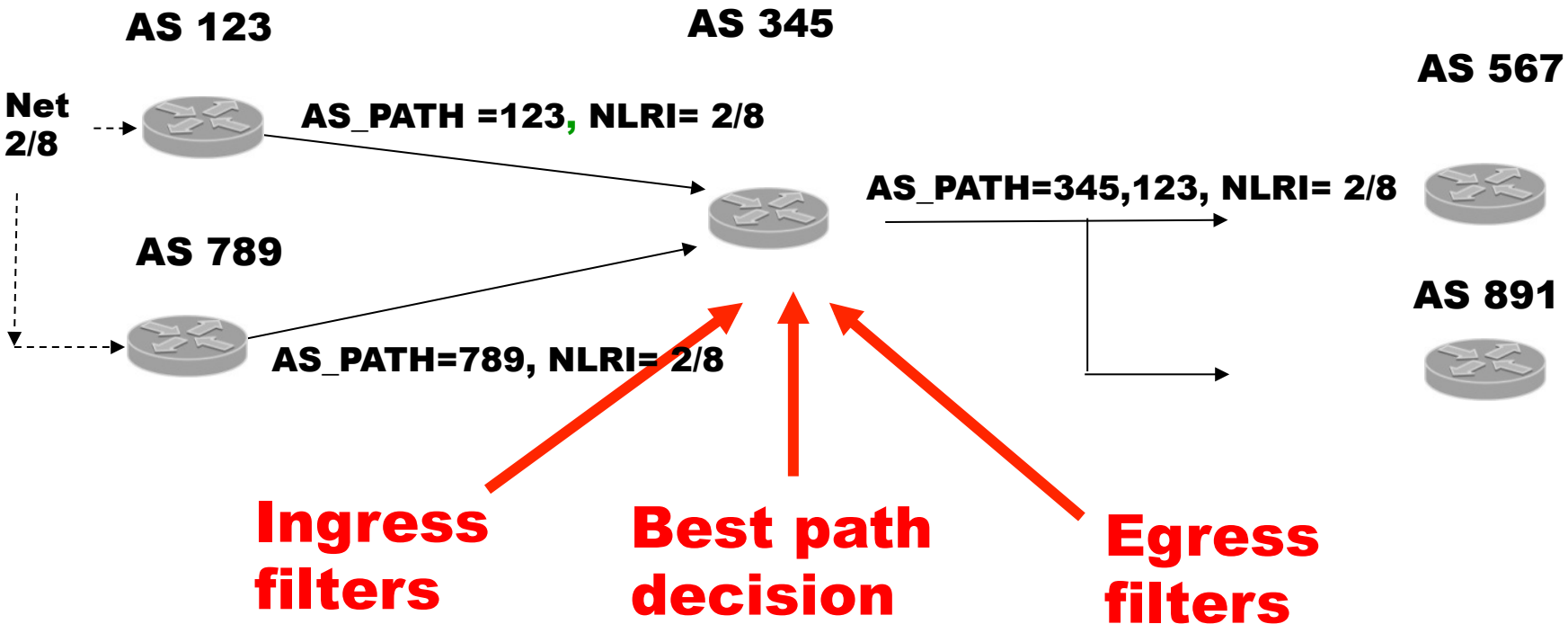
SIDR BGPSEC Doc Overview

- **draft-ietf-sidr-bgpsec-overview – overview of the set of documents related to BGPSEC** *(good summary)*
- Basis for BGPSEC work
  - **RFC7132** - Threat Model for BGP Path Security (basis for why)
  - **RFC7353** - Security Requirements for BGP Path Validation
- **draft-ietf-sidr-bgpsec-protocol-09 - BGPSEC Protocol Specification** *(obviously important to read)*
- **draft-ietf-sidr-bgpsec-ops-05 - BGPsec Operational Considerations** *(has languished, but explains thinking about operations)*
- Crypto stuff *(not crucial to understand BGP impact*)
  - draft-ietf-sidr-bgpsec-pki-profiles-08 - A Profile for BGPSEC Router Certificates, Certificate Revocation Lists, and Certification Requests
  - draft-ietf-sidr-bgpsec-algs-08 - BGP Algorithms, Key Formats, & Signature Format
- Crypto stuff *(about router crypto management, more than BGP impact)*
  - draft-ietf-sidr-rtr-keying - Router Keying for BGPsec

Idea of BGPSEC

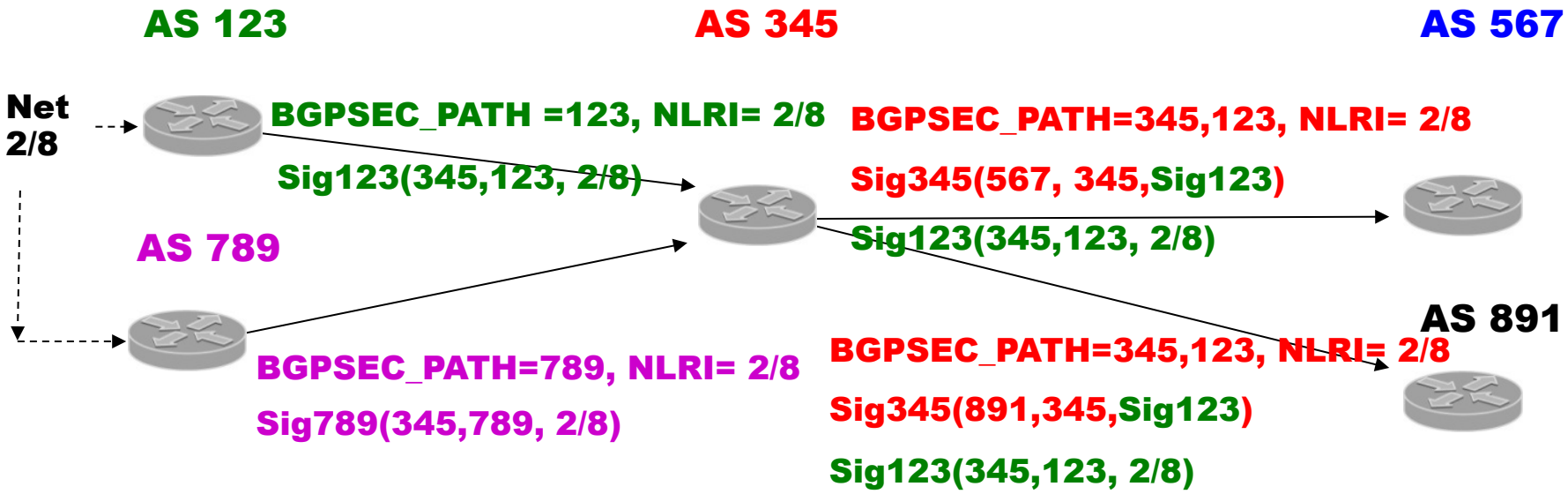
- Need to protect the formation of the AS_PATH
  - Prevent grafting valid origin on path
  - Prevent path poisoning
- So sign everything you receive to prove you didn't invent the path
  - Include the AS you are sending to, to prevent cut-and-paste creation of a signed path
- New attribute
- New capability – only send new attribute to neighbors who can handle it

BGP Process



- BGP receives many routes to the same prefix
- Ingress filter decides what routes to consider
- Decision process picks just one best route
- Egress filter decides what neighbors receive an update

BGPSEC Process



- Each update has a signature for each AS in the BGPSEC_PATH
  - Each signature covers BGPSEC_PATH to that point and the "sent-to" AS
- At ingress, check all signatures
- At egress, add a new signature to the list when you add your AS, and include the AS you are sending to in the signature
- Routers have keys tied to their AS in the RPKI

Other Diff from BGP

- AS_PATH – it is encoded in the BGPSEC_Path Attribute.
  - It is not present as a separate attribute
  - Another reason for the capability negotiation
- There's an algorithm to extract the usual AS_PATH from the BGPSEC_Path attribute
  - Could be used internal to an implementation
    - I.e., to compute path length
  - Must be used at a boundary with a non-BGPSEC speaking neighbor

Other Diff from BGP

- One neighbor per update
  - You are including your neighbor in the signature, so can only send to one neighbor
- One NLRI per Update
  - If multiple NLRI, signature would cover them all, so real hard to choose just one NLRI from the group to propagate
- Route servers
  - Route servers typically hide their AS from AS_PATH
  - Their AS will be included in BGPSEC_Path attribute, but extraction of AS_PATH does not include route server (specially marked) – so does not affect path length

Can also handle

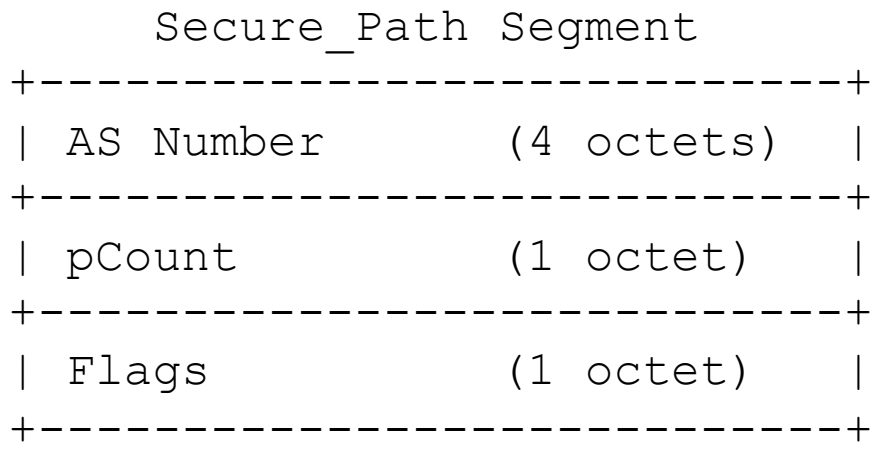
- Prepending
  - Don't want N signatures for N prepends
  - pcount field in the BGPSEC_PATH attribute
- Confederations
  - A flag to note when neighbor is in the same confederation (like AS_CONFED_SEQUENCE)
- Migration
  - BGPSEC attributes can behave just like "local AS", "replace AS" in current BGP.

The Details

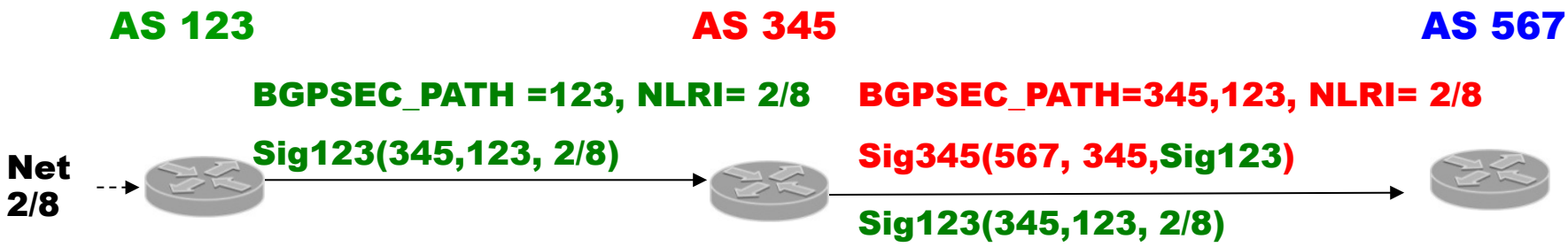
- Optional non-transitive attribute BGPSEC_Path attribute
  - Secure Path and Signature block
  - Secure Path is 1 or more SecurePathSegments

Prepending count – just one signature covers a list of prepended ASs

Flag to denote confederation



BGPSEC_Path Attribute

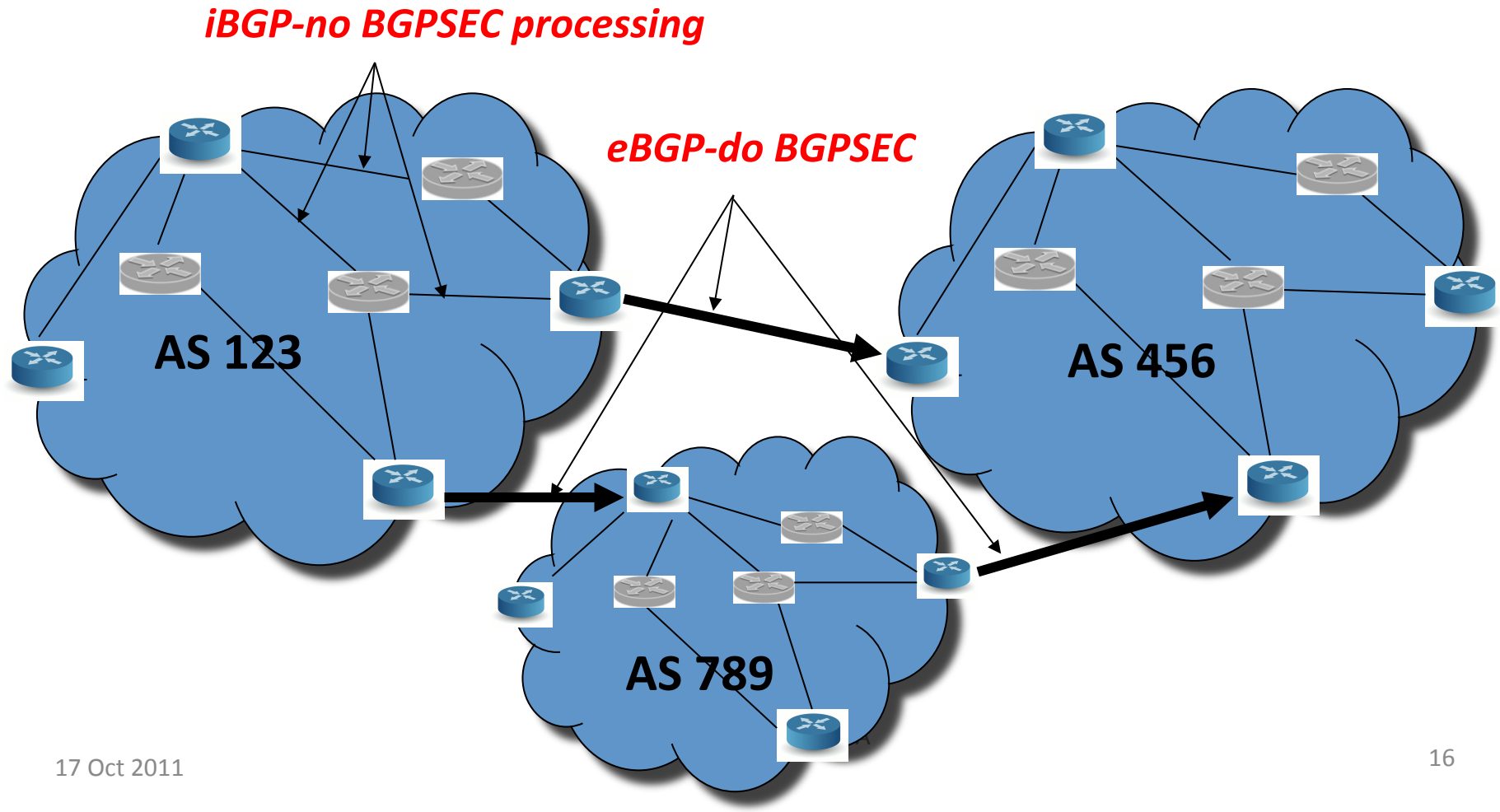


AS Number 123
pCount 1
Flags 0
signature (345,123,1,0)*[sigA]*

AS Number 345
pCount 1
Flags 0
AS Number 123
pCount 1
Flags 0
signature (567,345,1,0,*sigA*)
signature (345,123,1,0)*[sigA]*

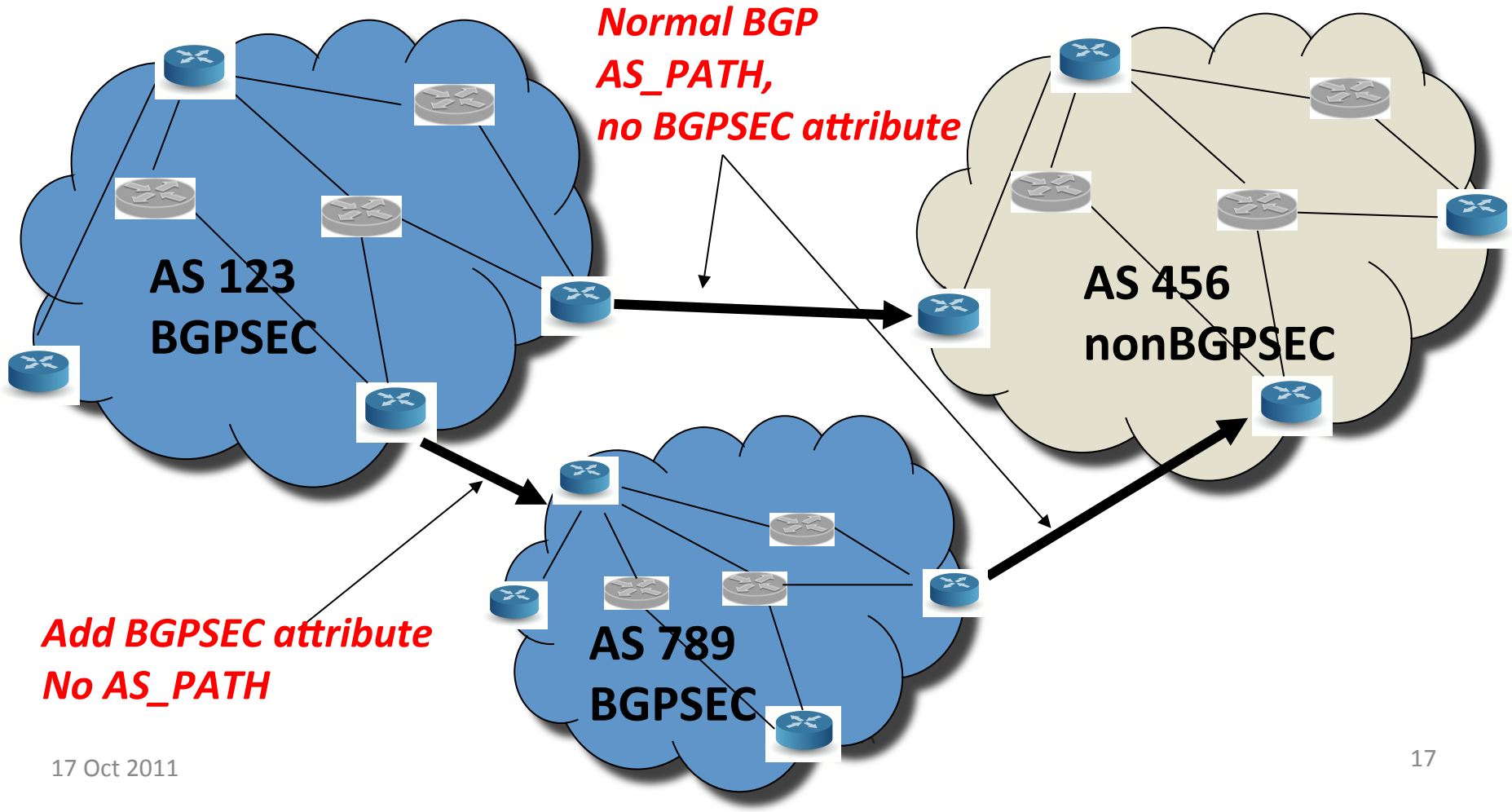
BGPSEC – Internal and External

BGPSEC signing and validation occurs only on eBGP connections
BGPSEC attributes are carried but not produced or checked on iBGP connections

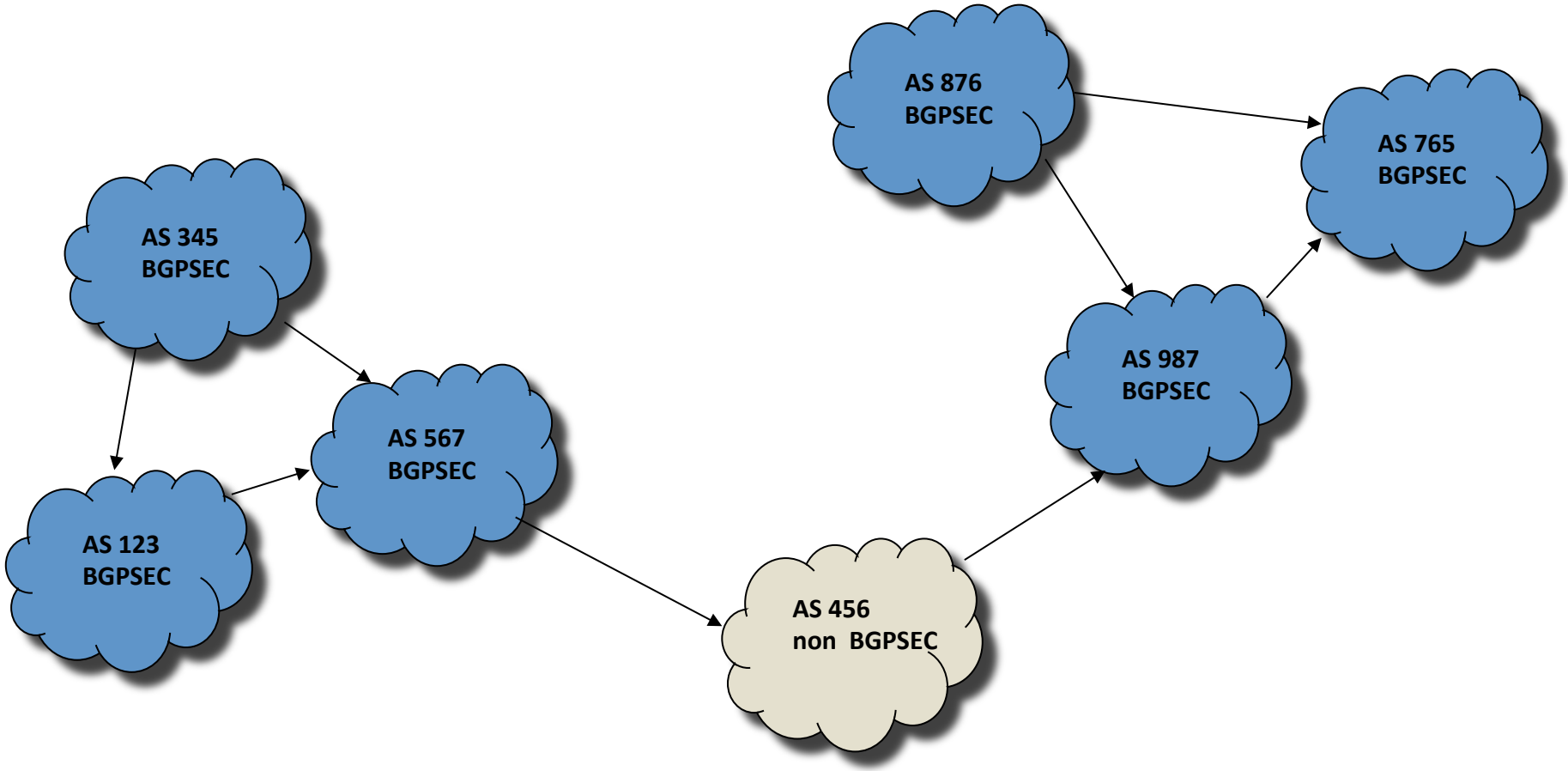


BGPSEC vs. nonBGPSEC

BGPSEC attribute only used with BGPSEC speaking neighbor
BGPSEC attributes in an Update get stripped for nonBGPSEC neighbor



Islands of BGPSEC



Non BGPSEC speaker can't pass BGPSEC attributes – keeps islands apart