

BGP L3VPN origin validation (draft-ymbk-l3vpn-origination-02)

November 2012

Problem Statement

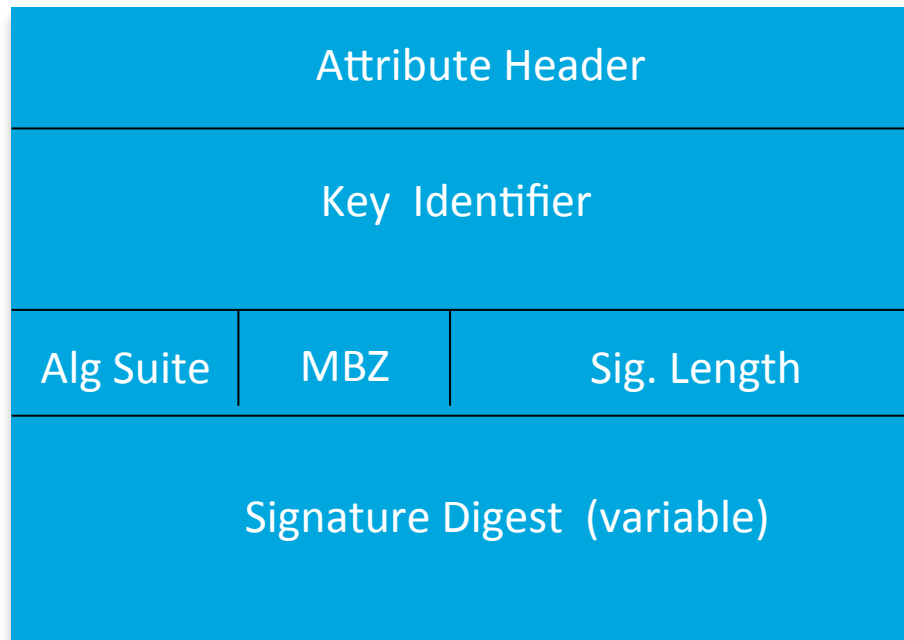
- ❑ It is currently possible for BGP based L3VPN routes to accidentally be sourced in a unintended manner in transit.
 - ❑ This is usually due to unintentional mis-configuration in a transit service provider (SP) resulting in VPN prefixes originating from the transit SP
 - ❑ Malicious attacks are also possible.
- ❑ No mechanism in place to authenticate VPN prefixes in terms of origin validation.
- ❑ The draft (draft-ymbk-l3vpn-origination-02) attempts to define one such scheme.

BGP L3VPN origin validation– Scheme Description

- ❑ Originator of the VPN route signs BGP update using a secret key
- ❑ The scheme does not mandate a PKI, though one may be used, and symmetric or asymmetric keys may be used
- ❑ The originator and validator have a trust agreement where they agree upon a secret key and associated Key Identifier.
- ❑ Key Identifier is a opaque value used to identify the context of the key in the BGP update. Often the VPN-ID can be used as the Key Identifier.
- ❑ The signature digest generated from the associated key is carried in a new BGP attribute and is validated at the receiver end by retrieving the key from the key Identifier context and computing the equivalent signature digest.

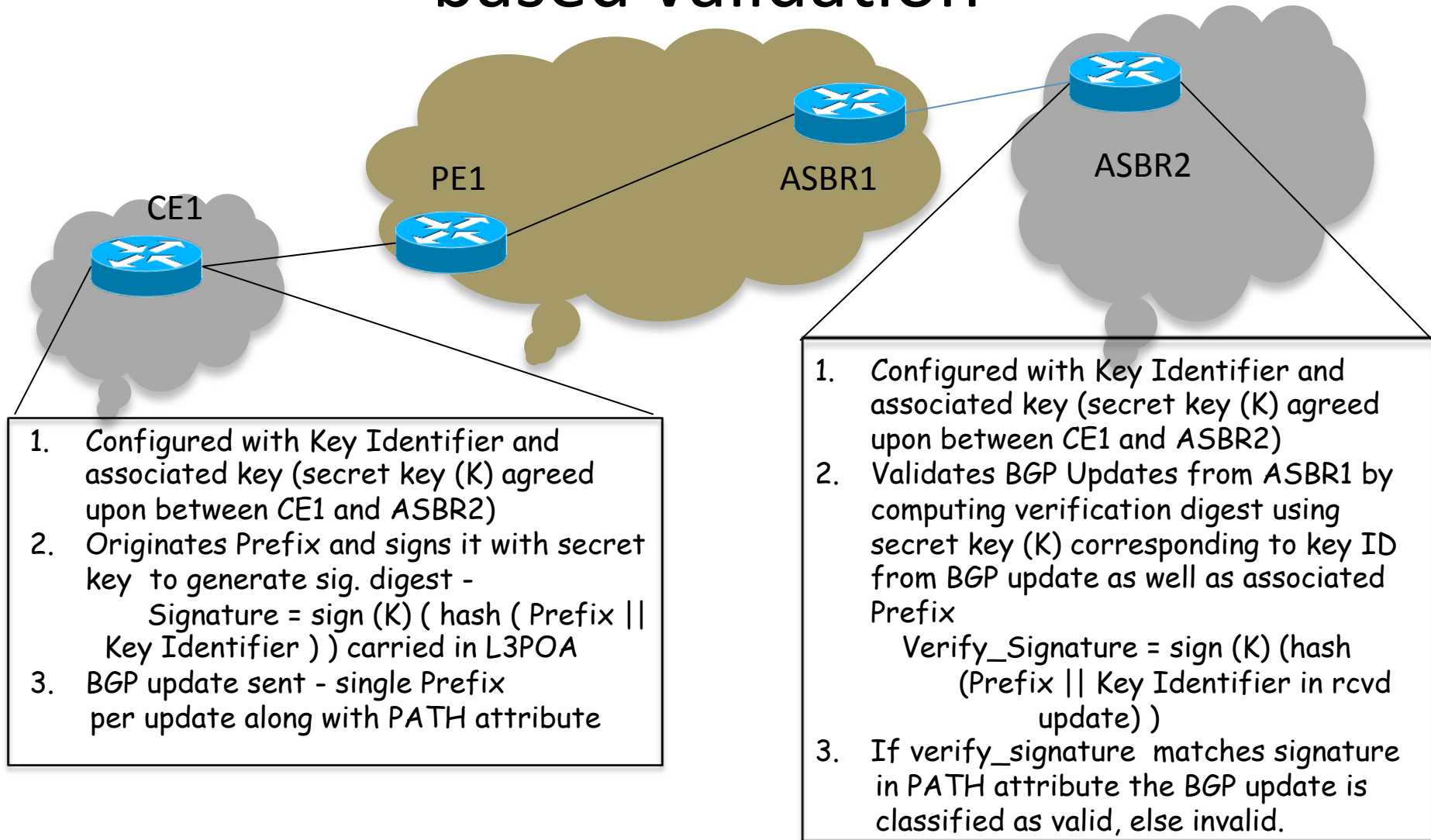
BGP L3VPN origin validation – BGP extensions

- ❑ A new optional transitive attribute defined in BGP to carry the signature digest.

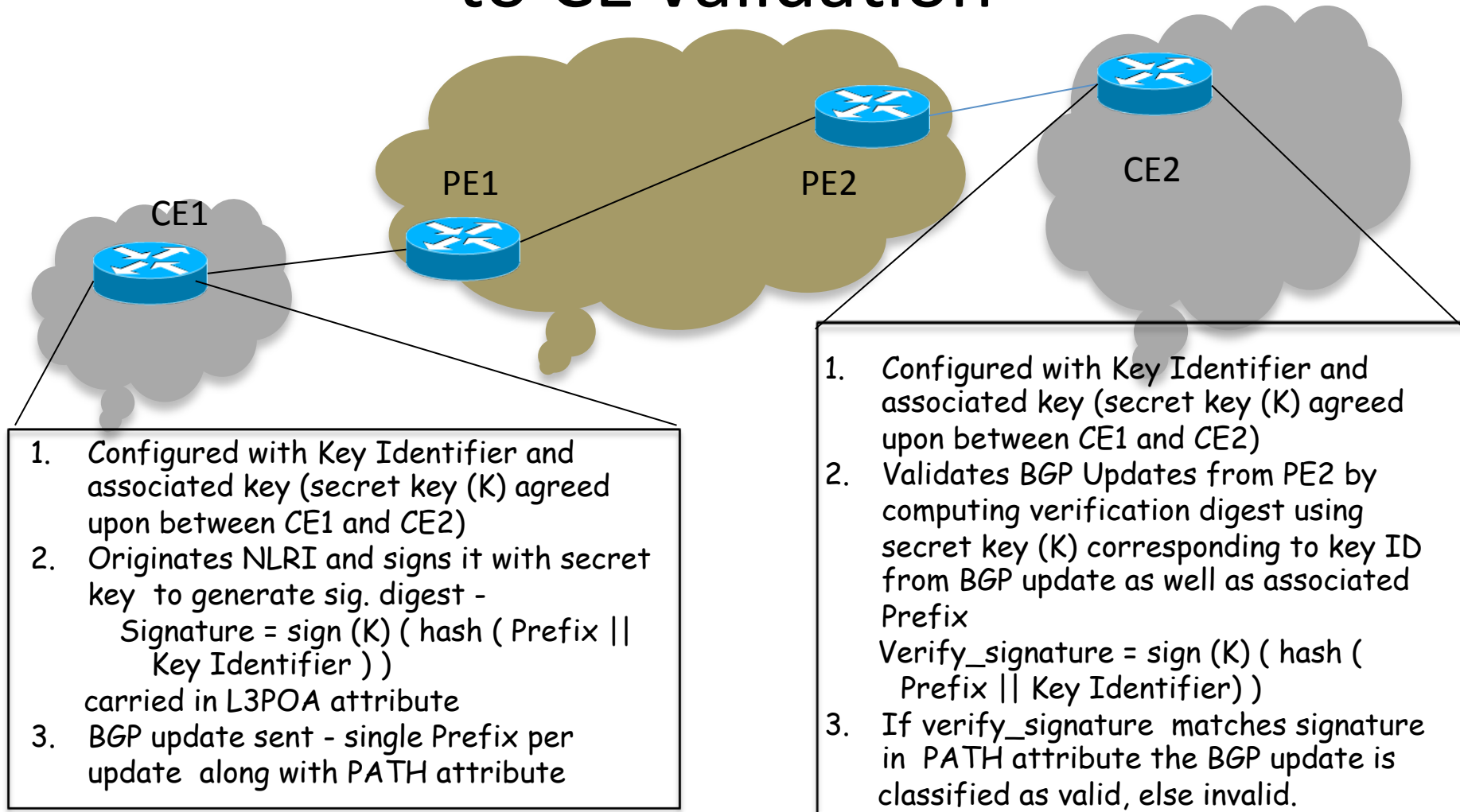


- ❑ Signature digest is generated as
 - ❑ $\text{Signature} = \text{sign}(\text{hash}(\text{Prefix/Len} || \text{Key Identifier}))$
- ❑ Single BGP Prefix per update to maintain integrity of signature.

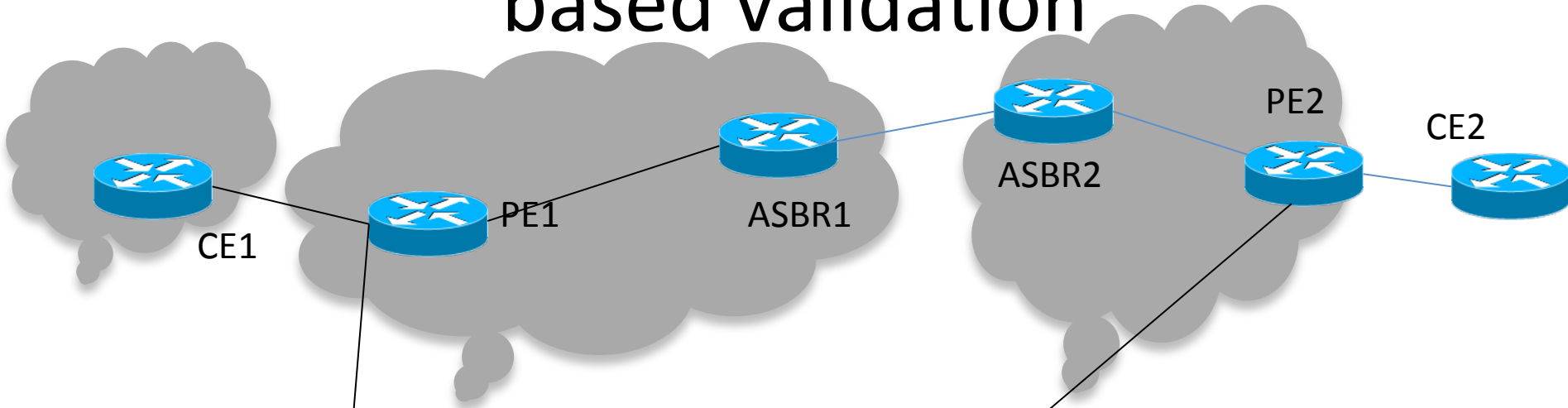
BGP L3VPN origin validation – Provider based validation



BGP L3VPN origin validation – End CE to CE validation



BGP L3VPN origin validation– PE - PE based validation



1. Here PEs, possibly across ASes, agree on the keying.
2. The Key Identifier and associated keys would normally be configured on a per VPN basis, with the PE1 signing and PE2 validating similarly
3. Here we are protected against route originating from unauthorized PEs.

BGP L3VPN origin validation - Advantages

- Origin validation for common L3VPN scenarios (inclusive of InterAS) – Provider based and CE based validation
- Does not mandate a PKI and can provide for lightweight authentication.
- Only end routers need to be aware of the new mechanism. Intermediate speakers do not need to be aware/upgraded so incrementally deployable