

# TLS Authentication for BGP

## draft-hbq-bgp-tls-auth

Jeffrey Haas, Bob Beck, Yingzhen Qu

# Motivation

- BGP, and several other IETF control plane protocols, run over TCP today.
- Most transport security considerations for such protocols hand-wave addressing transport security by saying, “We can use IPsec”.
  - IPsec is mostly not used. It is operationally cumbersome for the control plane.
- BGP provides transport security using TCP-AO (and previously, TCP-MD5) which provides integrity. Authentication is incidentally addressed through pre-shared keys.

# Motivation (2)

- There are many proposals to run BGP and other control plane protocols over QUIC.
  - We're not going to talk about these here. See prior talks in RTGAREA in IETF-123/124.
- QUIC uses the **TLS handshake** to get started.
- TLS uses certificates.
  - Most people are familiar with the web PKI when discussing TLS.
  - Web PKI is inappropriate for control plane protocols.
- Today, we're discussing a proposal for a BGP PKI.
  - **(This is really about the TLS handshake... and that's about it.)**

# Why are we here at SAAG/SIDROPS?

- To socialize this idea among the security smart part of IETF.
- This work is difficult to dispatch:
  - TLS? We're using TLS? **Boring**.
  - IDR? BGP is getting new security? Interesting, but IDR doesn't specialize in security.
  - SIDROPS? Lots of expertise about BGP security and certificates, but mostly about RPKI.
- The work is hybrid. It lands between SEC and RTG. We're chatting with both sets of ADs.

# Operations

- BGP has an “Autonomous System Number” that represents the network in the protocol.
- BGP is typically (manually) provisioned between routers by the remote (neighbor) IP address for the session.
  - Current security mechanisms are provisioned per-neighbor.

# High Level PKI

- A leaf (end-entity) “BGP session certificate” is created for each BGP session. Such a certificate has the AS and (optionally) IP as SAN names.
  - This binds the AS with the IP addresses for the session together.
- Leaf certificates may be generated **on demand** by the AS, using an intermediate certificate also with the AS SAN name.
- The AS intermediate may be distributed to your neighbor AS to be used as a trust anchor for your BGP session, or trusted via its issuer.

# Certificate Lifetimes

- The lifetime of the AS intermediate should be reasonably long. For example, a year.
- BGP session certificates *SHOULD* be short-lived. Perhaps two weeks. Such certificates *SHOULD* be automatically provisioned.
  - As with any TLS session, the operator might choose to ignore expired session certificates when operationally necessary.
- A goal is to avoid problematic revocation issues when the CRL might not be reachable when establishing BGP session.
  - After all, this is getting your Internet working in the first place!

# Establishing Trust

- The desired model is to establish trusted “introducers” for the BGP AS intermediate.
  - An ideal “introducer” is a mutually trusted third party CA.
  - A third party may decide to sign an AS intermediate by validating proof of possession of a key already present in the RPKI (as proof of “AS control”)
    - We are not trying to put these certificates in the RPKI itself!
    - We are not trying to re-use RPKI keys!
- The “introducer” could then be used as a trust anchor itself, or, once validated, the AS intermediates could be trusted directly (Intermediate elision).

# Main certificate details

## 8.2.4.4. Subject Alternative Name (SAN) - Critical

The ASN is carried within the GeneralName type using a specific OID.

Field	Requirement	Specification
subjectAlternativeName	<b>MUST</b>	<b>MUST</b> be present and <b>MUST</b> be marked as CRITICAL.
ASIdentifier	<b>MUST</b>	The ASN <b>MUST</b> be carried in a GeneralName of type otherName. The OID and structure of this otherName are defined below.
IPAddress	<b>MAY</b>	One or more IP addresses <b>MAY</b> be carried in the certificate.

Table 6

# Validation Procedure

- Rtr-A with AS-X and IP address a.b.c.1  
peers with  
Rtr-B with AS-Y and IP address a.b.c.2
- Rtr-A trusts AS-Y's AS intermediate.  
Rtr-B trusts AS-X's AS intermediate.
- During the TLS handshake, the BGP session certificate is  
verified and the remote AS number is checked along with the  
remote IP address.

... that's it.

# Next Steps

- Find a home for this BGP work.
  - ... Ideally without starting a whole new Working Group.
    - The core proposal here is small and mostly operationally simple.
      - ... but operational tooling can create a lot of nice-to-haves, such as an ACME-like extension for managing session certificates
        - ... and certificate-anything related to BGP is likely to create a “land grab” to manage an overly complex ecosystem. It’s important that the simple use case can be used on its own, without gaining cross-protocol security concerns.
- Realize that the non-BGP use cases will interest others looking to solve similar transport security issues.
  - ... and thus the simple idea may be a “victim of its own success”.
  - (See the appendix of the draft.)

Questions?