Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: 2 September 2026

J. Haas
HPE
B. Beck
OpenSSL
Y. Qu
Futurewei Technologies

1 March 2026

TLS Authentication for BGP
draft-hbq-bgp-tls-auth-00

Abstract

The Border Gateway Protocol, Version 4 (BGP-4) (RFC 4271) uses TCP (RFC 9293) as its transport layer protocol. There are proposals to run BGP over TLS-based transport protocols, including QUIC. This document discusses authentication considerations for running BGP over TLS protocols and defines a PKI framework to provide for authenticating BGP peering sessions.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 2 September 2026.

Copyright Notice

Table of Contents

1. Introduction

The Border Gateway Protocol, Version 4 (BGP-4) [RFC4271] uses TCP [RFC9293] as its transport layer protocol. TCP provides a sequenced, reliable byte stream for BGP to deliver its PDUs for a BGP session. BGP is provides its own framing layer. TCP provides no security mechanisms, including authentication, data integrity, or privacy, for its users. (See [RFC4949] for definitions of these properties.)

Attacks against BGP running over TCP lead to the development of TCP-MD5 [RFC2385] and later the TCP Authentication Option (TCP-AO) [RFC5925]. These mechanisms protect against disrupting the TCP stream. In particular, it provides for data integrity of the TCP stream and also provides a form of authentication via using shared secrets needed to implement these mechanisms. Section 1.2 of [RFC5925] discusses how TCP-AO is not intended to replace the use of IPsec [RFC4301] or TLS [RFC8446].

There are proposals to run BGP over alternative transport protocols, including QUIC [I-D.draft-retana-idr-bgp-quic] [RFC9000]. QUIC leverages TLS version 1.3 [RFC9001], which provides for authentication and also privacy. Data integrity is also a property of TLS, however when TLS is carried over TCP, it does not provide protection of the TCP stream.

TLS makes use of certificates as part of its authentication infrastructure. This document defines a public key infrastructure (PKI) [RFC5280] profile for authenticating BGP peering sessions when carried over TLS transport.

2. Conventions and Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

AS: Autonomous System.

ASN: Autonomous System Number.

CA: Certificate Authority.

RPKI: Resource Public Key Infrastructure.

3. A History of Securing BGP Transport Sessions

Modernly, BGP-4 [RFC4271] doesn’t provide for authentication of its sessions within the protocol. An earlier version of BGP-4 defined in [RFC1771] attempted to define an authentication mechanism, however it was problematic and not deployed.

BGP’s security issues using TCP were noted in [RFC1773] and later as part of [RFC4272]. By that time, the use of TCP-MD5 - even with its deficiencies - were part of best current operational practice.

Securing BGP using IPsec has been offered as an option, as was typical of IETF routing protocols carried over TCP. However, the general deployment of routing protocols using IPsec has been problematic for various reasons. While many implementations offer IPsec as an authentication option, it is not commonly deployed.

Mechanisms such as TCP-MD5, TCP-AO, and IPsec provide for authenticating a BGP session through the use of shared secrets. These are used to provision their mechanisms for a given BGP peering session and are tied to a pair of IP addresses for the session.

4. Why Authenticate BGP

Pair-wise authentication of BGP session endpoints provide assurance that each side of the BGP session is the expected party. However, this authentication only provides assurance that each side has provided the necessary credential for the mechanism and that it is associated with the BGP speaker’s IP address.

Validating that each party supplying this information is a trusted party requires additional scrutiny. Nothing in the BGP protocol or IP address assignment for a BGP speaker attests to whether that party is legitimate or not. For example, a fraudulent party claiming to be the trusted party could be supplying the credentials to secure the session. This permits the fradulent party to participate in BGP routing in the same role as the trusted party for devious reasons.

A trusted channel for distributing these security credentials is thus needed.

5. Using TLS Certificates for BGP

TLS 1.3 is leveraged by many protocols to provide for authentication, data integrity, and privacy. It leverages PKI certificates to validate the TLS session. Some of the details for validating certificates are left to applications using those certificates.

The web PKI is inappropriate for validating TLS sessions protecting BGP. Many resources addressed by web PKI certificates are particular to websites and a certificate validation model where a large number of trust anchors are distributed to web browsers and other HTTPS clients for validation of TLS sessions.

The resources appropriate for validation in the BGP protocol include the Autonomous System (AS) number for the peering session, and the IP address for the peering session.

6. Authenticating BGP Using TLS Certificates

Authenticating BGP peering sessions needs only to be done in a pair-wise fashion between two BGP speakers. Authentication of BGP sessions using this profile rely upon end entity certificates carried in TLS that contain the following fields:

* One or more "ASIdentifer" fields for that BGP speaker's local AS numbers.

* Optionally, one or more "IPAddress" fields for that BGP speaker's local IP address endpoints for the BGP session.

6.1. High Level Validation Procedure

1. The local BGP speaker receiving the end entity certificate from the remote BGP speaker validates the TLS certificate; details of this validation are described in subsequent sections.

2. If the certificate has been successfully validated, the received ASIdentifier is checked against the expected remote AS for the BGP session.

3. If the ASIdentifier successfully validates, and an IPAddress field is present, the IPAddress prefix is validated against the remote peer's expected IP endpoints.

4. If all of these procedures have succeded, the peer has been authenticated and the BGP protocol may use this TLS session. Otherwise, the session should be closed.

6.2. AS-level Trust Anchors

Since BGP sessions are pair-wise, in principle the peering session could be provisioned with the local end entity certificate and the expected remote end entity certificate. This is somewhat similar to provisioning per-session shared secrets for other mechanisms. In the absence of additional validation, it also is no better from a trust perspective: How did you get this end certificate in the first place and why do you trust it?

Consider the case where the end entity certificates are issued by a certificate authority that is operating at the BGP AS level. If all end entity certificates protecting BGP peering sessions are issued by their AS-level CA, and the AS's CA certificate is used as the trust anchor for the session, then all that is required to be installed on a BGP speaker is the remote peer's AS-level CA certificate.

Unlike per-session end entity certificates, the AS-level CA certificate may be made available through channels where validation of authenticity of the certificate is easier. This permits service providers to have a higher degree of confidence that the end entity certificate supplied during the TLS handshake has been issued by the service provider.

6.3. Trusted Third Party Trust Anchors

An option that may appeal to some service providers to validate AS-level certificates is to permit a trusted third party to be a mutual parent in the validation hierarchy. One such example might include the Regional Internet Registries (RIRs) that are already issuing AS numbers to service providers for BGP use. While RIRs appear at first glance to be a natural fit for such mutual trusted third parties, any party that has the trust of two parties participating in validation can serve this purpose.

The core proposition to this model is that the third party is trusted. Such a party can issue certificates that would permit validation to proceed in a pair-wise fashion for a service provider using this trust relationship.

7. Issuing End Entity Certificates

In models where an AS-level CA exists, end entity certificates protecting BGP peering sessions are created on an as-needed basis and provisioned onto the protected systems.

This may be "push" model where a centralized provisioning system creates and distributes the end entity certificates and associated BGP peering configuration for each BGP speaker.

Another possible model is a "pull" model where sufficient trust exists between the requesting BGP speaker and the AS-level certificate infrastructure. Such a model has some resemblance to the use cases enabled by the ACME protocol [RFC8555].

8. BGP TLS Certificate Profile

8.1. Introduction

This document defines a profile for X.509 Public Key Certificates intended for use in identifying BGP autonomous systems (ASes) by their registered Autonomous System Number (ASN) for purposes of TLS authentication. This profile specifies the use of a new Subject Alternative Name (SAN) extension type to carry the ASN, facilitating the verification of the certificate holder’s identity as a legitimate

holder of the AS and supporting cryptographic authentication in routing and network security protocols. It defines a new Other Name for inclusion in the X.509 Subject Alternate Name (SAN) to carry an AS number.

The intention of this document is to define a certificate profile for use in a TLS handshake for transport connections used by protocols to exchange routing information.

X.509 certificates are a foundational element of public key infrastructure (PKI), providing cryptographic binding between a public key and an identity. In the context of network routing and infrastructure security, such as RPKI (Resource Public Key Infrastructure) or future secure routing mechanisms, it is essential to cryptographically bind a public key to an AS's unique identifier— the Autonomous System Number (ASN).

This profile specifies the minimal requirements and constraints for X.509 certificates used to identify an AS solely by its ASN. It leverages existing X.509 standards, primarily [RFC5280], and defines a specific approach for ASN inclusion in the Subject Alternative Name extension.

Unlike the Autonomous System identifier delegation extension from [RFC3779], this profile is not intended to reflect the association of routing ip addresses to AS numbers for purposes of validating routing decisions. This profile is intended for use cases in which an endpoint is to be identified as a specific ASN endpoint of a TLS connection, for securing routing control connections, such as BGP.

This profile is intended to provide a mechanism whereby an AS can reliably generate short lived end entity certificates to reliably identify TLS connection endpoints.

TLS can be used with fixed certificates or pre-shared keys, and may be very appropriate to use in that model for certain uses in this space where the two relying parties at each end of a connection have decided to trust each other by some out of band mechanism. The focus of this draft is to establish a certificate profile for a PKI that enables the ability to establish trust via either a mutually operated, or third party CA in a reliable manner, with short lived end-entity certificates provisioned automatically from an intermediate certificate dedicated to this purpose for an ASN.

8.2. Certificate Fields and Extensions

This profile extends the base X.509 certificate profile defined in [RFC5280]. The following table specifies the requirements for critical fields and extensions.

8.2.1. Version

Field	Requirement	Specification
version	MUST	Set to 2 (meaning X.509 version 3).

Table 1

8.2.2. Temporal Validity

End entity certificates using this profile MUST NOT be valid for more than two weeks. Revocation methods SHOULD NOT be used to verify the continued validity of end entity certificates. Automated methods SHOULD be used to provision end entity certificates to devices that use them.

Intermediate certificates using this profile MUST NOT be valid for more than one year. Revocation methods SHOULD be used to verify the continued validity of intermediate certificates.

8.2.3. Subject and Subject Public Key Info

Field	Requirement	Specification
subject	SHOULD NOT	Certificates in this profile are primarily identified by the ASN in the SAN extension. The subject field SHOULD be empty (an empty sequence of RDNs).
subjectPublicKeyInfo	MUST	Contains the public key associated with the AS.
subjectKeyIdentifier	MUST	Contains the subjectKeyIdentifier for the public key.

authorityKeyIdentifier	SHOULD	Contains the authorityKeyIdentifier for the public key of the certificate's issuer, if the certificate is not self-signed.

Table 2

8.2.4. Extensions

The following extensions are mandatory or critical for this profile:

8.2.4.1. Basic Constraints

Field	Requirement	Specification
basicConstraints	MUST	MUST be present. If the certificate is an End-Entity certificate (AS identity), CA MUST be set to FALSE. If the certificate is for a CA that issues AS Identity Certificates, CA MUST be set to TRUE.

Table 3

8.2.4.2. Key Usage

Field	Requirement	Specification
keyUsage	MUST	MUST be present. For End-Entity AS Identity Certificates, digitalSignature MUST be asserted.

Table 4

8.2.4.3. Extended Key Usage (EKU)

Field	Requirement	Specification
extKeyUsage	MUST	EKU values SHOULD be one or both of TLS client authentication, and TLS server authentication. Other EKU values SHOULD NOT be present.

Table 5

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

Table 6

Other SAN names SHOULD NOT be present.

8.2.4.5. RFC 3779 Extensions

[RFC3779] extensions used for validating the RPKI SHOULD NOT be present.

Field	Requirement	Specification
id-pe-ipAddrBlocks	SHOULD NOT	This profile is deliberately separate from RPKI.
id-pe-autonomousSysIds	SHOULD NOT	This profile is deliberately separate from RPKI.

Table 7

8.3. AS Identifier Encoding in Subject Alternative Name

The ASN SHALL be included in the Subject Alternative Name extension using the otherName choice of the GeneralName type.

The specific OID for the AS Identifier is:

```
id-pe-ASIdentifier OBJECT IDENTIFIER ::= {
    iso(1) identified-organization(3) dod(6)
    internet(1) private(4) enterprise(1) {IANA-Assigned-Oid}
}
```

NOTE: A specific OID MUST be obtained from IANA for this profile before final standardization. For this draft, we use the placeholder id-pe-ASIdentifier.

The ASIdentifier structure, defined by this OID, SHALL be an ASN.1 INTEGER representing the AS Number. AS Numbers range from 1 to 4,294,967,295.

```
ASIdentifier ::= INTEGER (1..4294967295)
```

The ASN.1 structure within the SAN extension will look like this:

```
SubjectAlternativeName ::= GeneralNames

GeneralNames ::= SEQUENCE SIZE (1..MAX) OF GeneralName

GeneralName ::= CHOICE {
    ... (other choices)
    otherName [8] OtherName,
    ... (other choices)
}

OtherName ::= SEQUENCE {
    type-id    OBJECT IDENTIFIER (id-pe-ASIdentifier),
    value      [0] EXPLICIT ANY DEFINED BY type-id
}
```

When encoding the ASN:

1. The type-id is set to id-pe-ASIdentifier.

2. The value is the ASN.1 INTEGER representation of the AS Number (e.g., AS 64496 would be encoded as the integer 64496).

8.4. End Entity Certificate Issuance

Any intermediate certificates used to issue end entity certificates using this profile MUST include all id-pe-ASIdentifier names as the end entity certificate. Such intermediate certificates MAY include SAN IP address name constraints as per [RFC5280] and if present they MUST be marked critical

8.5. Intermediate CA Issuance

The intermediate certificate for an AS can sign any leaf certificate for that AS that will then be able to authenticate a connection.

Out Of Band Trust Anchor Exchange Relying parties using this model exchange trust anchors out of band. Relying parties using this model may decide to validate mutual trust out of band. Appropriate care should be taken in any such scenario which is out of scope of this document. With trust mutually established, they may exchange trust anchors which will in turn be trusted to sign end entity certificates for each of them. This could take the form of a self signed intermediate certificate that is elided as a trust anchor by each party. Each party in this case must take appropriate care that such a trust anchor is not considered trusted in other places.

Third Party Trusted Certificate Authority Third party certificate authorities SHOULD validate requests for intermediate certificates using this profile by the following method:

For every AS in an intermediate certificate request:

* Validate a CMS message containing the public key of the certificate is signed by the corresponding key for the AS in a currently validated RPKI tree.

* This signature is considered to be “proof of control of the AS” for these purposes.

9. Operational Considerations

In circumstances where a BGP session’s certificate validation may not be possible - for example, the validating trust anchors are not installed - operators may have need to permit BGP sessions to be established without validating the authenticity of the session. Implementations MUST provide a mechanism to permit sessions to establish in the absence of such validation. One mechanism may be to make use of "Trust of First Use (TOFU)". Another may be to disable validation altogether.

While such practices are not recommended, operators have the option to do after the fact validation of the sessions that have been expediently trusted in this fashion. Implementations MUST provide operational access to the running session’s certificates used for the running sessions. Similarly, implementations MUST provide logging facilities for when BGP sessions are permitted to be established when validation either cannot be done or is permitted even though validation has failed.

End entity certificates are recommended to have a life time no longer than two weeks. Implementations SHOULD validate certificates used for the first use of a BGP session are valid within the expected life time. Implementations MAY ignore end entity certificate life time expiration that otherwise validates for sessions that have previously been seen to be established.

Ignoring life time validation errors is a balance for the security stance of the operator and a desire for BGP resiliency in the face of tardy certificate updates.

10. Security Considerations

10.1. Certificate Validation Security Considerations

The security of this profile relies on:

1. Strong Identity Verification: The CA MUST strictly verify the applicant's control of the ASN before issuance of an intermediate. Flaws in this process can lead to impersonation.

2. Criticality of SAN: Marking the subjectAlternativeName extension as critical ensures that relying parties that do not understand the id-pe-ASIdentifier OID will reject the certificate, preventing misinterpretation of the certificate's identity.

10.2. BGP Security Considerations

Implementations MUST provide granular control over the certificate trust anchors used to authenticate individual BGP sessions.

Use of this certificate profile for protecting BGP sessions carried over TLS have the opportunity to reduce impersonation of authorized parties peering with the BGP speaker. Correct provisioning of the trust anchors used for validating certificates is necessary to prevent such impersonation.

Trusted third party trust anchors provide opportunities for reduced operational complexity and fewer certificates necessary for BGP speakers. However, they introduce the opportunity for impersonation attacks to be enabled by the these parties. Beware of who you trust.

11. IANA Considerations

This document requests that IANA assign a unique OID under the SMI Security Private Extensions arc for id-pe-ASIdentifier to be used within the otherName field of the Subject Alternative Name extension.

12. References

12.1. Normative References

[I-D.draft-retana-idr-bgp-quic]
Retana, A., Qu, Y., Haas, J., Chen, S., and J. Tantsura, "BGP over QUIC", Work in Progress, Internet-Draft, draft-retana-idr-bgp-quic-08, 7 January 2026, <https://datatracker.ietf.org/doc/html/draft-retana-idr-bgp-quic-08>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

[RFC3779] Lynn, C., Kent, S., and K. Seo, "X.509 Extensions for IP Addresses and AS Identifiers", RFC 3779, DOI 10.17487/RFC3779, June 2004, <https://www.rfc-editor.org/rfc/rfc3779>.

[RFC4271] Rekhter, Y., Ed., Li, T., Ed., and S. Hares, Ed., "A Border Gateway Protocol 4 (BGP-4)", RFC 4271, DOI 10.17487/RFC4271, January 2006, <https://www.rfc-editor.org/rfc/rfc4271>.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <https://www.rfc-editor.org/rfc/rfc5280>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/rfc/rfc8446>.

[RFC9000] Iyengar, J., Ed. and M. Thomson, Ed., "QUIC: A UDP-Based Multiplexed and Secure Transport", RFC 9000, DOI 10.17487/RFC9000, May 2021, <https://www.rfc-editor.org/rfc/rfc9000>.

[RFC9001] Thomson, M., Ed. and S. Turner, Ed., "Using TLS to Secure QUIC", RFC 9001, DOI 10.17487/RFC9001, May 2021, <https://www.rfc-editor.org/rfc/rfc9001>.

[RFC9293] Eddy, W., Ed., "Transmission Control Protocol (TCP)", STD 7, RFC 9293, DOI 10.17487/RFC9293, August 2022, <https://www.rfc-editor.org/rfc/rfc9293>.

12.2. Informative References

[RFC1771] Rekhter, Y. and T. Li, "A Border Gateway Protocol 4 (BGP-4)", RFC 1771, DOI 10.17487/RFC1771, March 1995, <https://www.rfc-editor.org/rfc/rfc1771>.

[RFC1773] Traina, P., "Experience with the BGP-4 protocol", RFC 1773, DOI 10.17487/RFC1773, March 1995, <https://www.rfc-editor.org/rfc/rfc1773>.

[RFC2385] Heffernan, A., "Protection of BGP Sessions via the TCP MD5 Signature Option", RFC 2385, DOI 10.17487/RFC2385, August 1998, <https://www.rfc-editor.org/rfc/rfc2385>.

[RFC4272] Murphy, S., "BGP Security Vulnerabilities Analysis", RFC 4272, DOI 10.17487/RFC4272, January 2006, <https://www.rfc-editor.org/rfc/rfc4272>.

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, DOI 10.17487/RFC4301, December 2005, <https://www.rfc-editor.org/rfc/rfc4301>.

[RFC4949] Shirey, R., "Internet Security Glossary, Version 2", FYI 36, RFC 4949, DOI 10.17487/RFC4949, August 2007, <https://www.rfc-editor.org/rfc/rfc4949>.

[RFC5925] Touch, J., Mankin, A., and R. Bonica, "The TCP Authentication Option", RFC 5925, DOI 10.17487/RFC5925, June 2010, <https://www.rfc-editor.org/rfc/rfc5925>.

[RFC8555] Barnes, R., Hoffman-Andrews, J., McCarney, D., and J. Kasten, "Automatic Certificate Management Environment (ACME)", RFC 8555, DOI 10.17487/RFC8555, March 2019, <https://www.rfc-editor.org/rfc/rfc8555>.

Appendix A. Use of this Profile for Non-BGP Purposes

Astute readers will note that while this document is written with a focus on BGP operational matters that similar security considerations apply for all other control plane protocols standardized by IETF that use TCP. The primary difference between the BGP use case and the more general-purpose control plane use case is the lack of a protocol-recognized "AS" as the party used both for protocol validation and as the identity for the CA certificates issuing end entity certificates.

The authors will consider a future general-purpose "TLS for routing" profile in the future based on experience in discussing this more specific use case.

Acknowledgments

TODO

Authors' Addresses

Jeffrey Haas
HPE
Email: jeffrey.haas@hpe.com

Bob Beck
OpenSSL
Email: beck@obtuse.com

Yingzhen Qu
Futurewei Technologies
Email: yingzhen.ietf@gmail.com