Registration Extensions (REGEXT)
Internet-Draft
Intended status: Informational
Expires: 5 June 2026

Z. AlBanna
J. Gould
S. Hollenbeck
Verisign

2 December 2025

Extended Key Usage and Mutual TLS in EPP
draft-albanna-regext-eku-mtls-in-epp-00

Abstract

This document describes the state of the Mutual Transport Layer Security (mTLS) client authentication mechanism in the Extensible Provisioning Protocol (EPP) with respect to a recent change in the client certificates published by some Certificate Authorities (CAs). The issue is described and options are presented to address the operational impact of the change.

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 5 June 2026.

Table of Contents

1. Introduction

Recent changes to policies related to Mutual Transport Layer Security (mTLS) client certificates are presenting operational challenges for the Extensible Provisioning Protocol (EPP) client authentication process. This document describes the changes, the challenges associated with these changes, and suggested approaches to continue to implement mTLS authentication in EPP.

2. Conventions used in this document

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.

3. Background and Problem Overview

As described in RFC 5734 [RFC5734], the Extensible Provisioning Protocol (EPP) can be transported over the Transmission Control Protocol (TCP). This transport requires use of the Transport Layer Security (TLS) protocol, specifically the Mutual Transport Layer (mTLS) option within TLS to protect information exchanged between an EPP client and an EPP server. Section 9 of RFC 5734 [RFC5734] states that mutual client and server authentication using the TLS Handshake Protocol is REQUIRED, but it does not provide specific implementation requirements. This process requires both the EPP client and the EPP server to possess X.509 [RFC5280] digital certificates, specific to each, that is trusted by the other party. These certificates include X.509 standard extensions, including the Extended Key Usage (EKU) extensions for the client and the server.

While not a requirement of EPP, some server implementations of TLS require that a client certificate include the Extended Key Usage (EKU) extension with the id-kp-clientAuth key usage purpose (clientAuth EKU), defined in section 4.2.1.13 of RFC 5280 [RFC5280]. Similarly, some client implementations of TLS require that a server certificate include the EKU extension with the id-kp-serverAuth key usage purpose (serverAuth EKU). The clientAuth EKU and the serverAuth EKU are registered with IANA as described in Section 3.6 of RFC 7299 [RFC7299], for world wide web (WWW) client applications and world wide web (WWW) server applications, respectively. There are EKU entries registered for other protocols or applications, such as email, SCVP and SSH, but none are registered for EPP.

4. Current State

Several Certificate Authorities (CAs) [ref_1],[ref_2], [ref_3] are planning on discontinuing support for TLS certificates that include the clientAuth EKU extension. Deployments that rely on the clientAuth EKU as a part of EPP session establishment face an immediate problem. When TLS certificates stop including the clientAuth EKU extension, EPP mTLS authentication in the EPP servers will fail when the clientAuth EKU extension is required. To establish an EPP session, the EPP mTLS connection must be complete and the client must successfully complete the EPP login command as described in RFC 5730 [RFC5730]. Some EPP servers implement multi-factor authentication in the EPP login command that uses the client certificate subjectAltName extension of the dNSName [RFC4985] to match with the client account to establish the EPP session.

Due to local policy and implementation-specific needs, RFC 5734 [RFC5734] does not provide specific recommendations for X.509 certificates and EKU extensions for use in mTLS authentication. In

practice, EPP clients and EPP servers use EKU extensions intended for world wide web applications because those certificates have been easy to acquire from popular Certificate Authorities (CAs). Removal of the clientEKU extension from client-used certificates can cause mTLS authentication to fail, making it necessary to explore alternative approaches.

5. Potential Solutions

There are multiple solutions the community can consider in addressing this issue as listed in Section 5.1. These solutions can include supporting mechanisms to enhance performance and security of client authentication. These mechanisms are summarized in Section 5.2.

5.1 Solutions to Consider

5.1.1 CA issued certificates:

Continuing with the status quo, registrars can subscribe to a CA service that provides client certificates with the client EKU extension included.

The advantage of this approach is that it matches the current state where server can continue to validate the clientAuth EKU extension.

The disadvantage of this approach is the availability of CA’s issuing certificates with the clientAuth EKU setting and continue to have the EPP protocol be dependent on an EKU setting that is meant for a different application with the continued risk of EPP being impacted by WWW policy changes.

5.1.2 Registry issued certificates:

Setting up a CA through open-source software options is an achievable but sizable engineering task. A CA can be setup privately by a Registry or publicly for the EPP industry. The effort to create a CA for the EPP industry that needs to be publicly trusted is a considerable undertaking that will require serious expertise and resources as the CA/Browser Forum Baseline Requirements illustrates [ref_4]. A registry that chooses to perform the CA function should consider using client’s "reference identity" and server’s "presented identity" association, as described in RFC 9525 [RFC9525] and similar to RFC 7469 [RFC7469], for added security.

Advantages of running a private CA include providing total control over infrastructure, security, and cost, customized certificate policies, instant issuance, and revocation.

Some of the disadvantages could include significant operational overhead related to acquiring proper expertise, infrastructure setup and maintenance, maintaining compliance with standards, and high liability exposure in case of a security compromise.

5.1.3 Self-signed certificates:

This option is dependent on registry policies and methods of operation. A registry that chooses to accept a self-signed client certificate to establish an EPP session should verify Domain Name System (DNS) Transport Layer Security Authentication (TLSA) records published by the client to enhance efficiency. Registries should also consider using client's "reference identity" and server's "presented identity" association, as described in RFC 9525 [RFC9525] and similar to RFC 7469 [RFC7469], for added security.

An advantage of this approach is the EPP session establishment between the client and the server becomes independent of third parties.

A disadvantage of this approach is a dependency on implementing certificate pinning in the client and the server, which includes managing the self-signed certificates by the client, provisioning the self-signed certificates by the client in the server, and implementing certificate pinning verification in the server. On the server-side, there is work to be done to map the self-signed certificates to the client accounts, which could be done with Service Identity association RFC 9525 [RFC9525]. This could require new support for infrastructure needed to issue and track certificates plus the effort needed to introduce TLSA, client's "reference identity", and server's "presented identity" association processes to enhance performance and security.

5.2 Mechanisms:

5.2.1 EPP without an EKU:

The EPP RFCs do not require Extended Key Usage (EKU) extension with the id-kp-clientAuth key usage purpose for client certificates and with the id-kp-serverAuth key usage purpose for server certificates, which are registered with IANA for the world wide web applications and not EPP. EPP clients and servers can configure a unique set of trusted CA certificates that are not dependent on validating the EKU values in either the client or the server. By not validating the id-kp-clientAuth and id-kp-serverAuth key usage purpose in client and server certificates, this mechanism enables EPP to be independent from world wide web applications.

This mechanism provides a fast implementation time since the registry could accept a broader set of CA issued certificates and the registry could define explicitly what CA certificates to trust. However, this mechanism will still maintain a dependency on world wide web applications, such as reducing the maximum validity period of TLS certificates to 47 days by 2029 [ref_5]. CAs continue to adjust to WWW application policies that may or may not apply to the EPP protocol.

5.2.2 EPP specific EKU:

Establish EPP-specific client and server EKUs in the SMI Security for PKIX Extended Key Purpose Registry, defined in RFC 7299 [RFC7299]. This process will follow the guidelines as specified in RFC 8126 [RFC8126].

This mechanism provides a scalable and a long-term independence for the EPP operating environment. Specifically, it is an effective mechanism for the registry issued EPP client certificates. However, given this would be a new EKU setting, CAs may not be inclined to support this approach for a market as small as the EPP market.

5.2.3 Service Identity association (CA issued certificate or Self-signed Certificate):

Service Identity, RFC 9525 [RFC9525] association, is a security mechanism that enhances a client’s ability to verify that the server’s presented identity matches its identity. This mechanism is the server verifying the client certificate against a set of certificates set in the client’ s account as part of authenticating EPP client-server connections, which is like Service Identity

association defined in RFC 9525 RFC 9525 [RFC9525] and certificate pinning defined in RFC 7469 [RFC7469]. Its purpose is to enhance the security of the connection by ensuring that the client presents a certificate from a set of certificates in their account leveraging the certificate fingerprint. There are a few, not mutually exclusive, options to Service Identity association such as harvesting via TLSA, EPP extensions which allow the registrar to provision the certificates for their account, Web User Interface (UI), and manually via customer support.

This mechanism is effective but it does have some challenges in the areas of maintenance complexity, scalability, inflexibility, and risks of breaking connectivity due to pinned certificate becoming compromised or expired. This mechanism may also be outdated relative to newer technologies such as Online Certificate Status Protocol (OCSP), and Certificate Transparency (CT) [ref_6].

5.2.4 Transport Layer Security Authentication (TLSA) Record:

DNS TLSA records associate a TLS certificate with its domain name. They are an extension of DNSSEC and can be leveraged for stronger authentication. This approach requires the client to follow a number of steps which include obtaining a CA issued certificate, or a self signed certificate, that is published using TSLA records for harvesting offline and validating when establishing the EPP session. This certificate is added to a zone that is DNSSEC signed. The client needs to ensure that the TLSA records include the client certificates passed in the mTLS connection to the registry. The registry needs to know the domain name of the TLSA zone to harvest the certificates for each of the client accounts to update the list of pinned certificates.

This mechanism is reliable but it could have some challenges related to issues such as TLSA RRsets fail to match the server certificate chain or TLSA records cannot be validated due to internally signed domains that lack a signed delegation (DS records) in the parent zone [ref_7].

6. IANA Considerations

No action by IANA is necessary for this document at this time. As some of the ideas above suggested, there could be a future need to register the EPP specific EKU values, such as id-kp-eppClient and id-kp-eppServer.

7. Security Considerations

This document presents general solutions to mitigate the problem discussed. Each of the mentioned solutions have security considerations associated with them that will be addressed at the time of presenting the solutions specifications.

8. Acknowledgments

The following individuals have provided feedback and contributions to the content and direction of this document: TBD.

9. References

9.1. Normative References

[RFC5734] Hollenbeck, S., "Key words for use in RFCs to Indicate Requirement Levels", STD 69, RFC 5734, DOI 10.17487/RFC5734, August 2009, <https://www.rfc-editor.org/info/rfc5734>.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Key words for use in RFCs to Indicate Requirement Levels", RFC 5280, DOI 10.17487/RFC5280, May 2008, <https://www.rfc-editor.org/info/rfc5280>.

[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/info/rfc2119>.

[RFC9525] Saint-Andres, P. and R. Salz, "Service Identity in TLS", RFC 9525, DOI 10.17487/RFC9525, November 2023, <https://www.rfc-editor.org/info/rfc9525>.

[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/info/rfc8174>.

[RFC8126] Cotton, M., Leiba, B., and T. Naren, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 8126, DOI 10.17487/RFC8126, June 2017, <https://www.rfc-editor.org/info/rfc8126>.

[RFC7299] Housley, R., "Object Identifier Registry for the PKIX Working Group", RFC 7299, DOI 10.17487/RFC7299, July 2014, <https://www.rfc-editor.org/info/rfc7299>.

[RFC5730] Hollenbeck, S., "Extensible Provisioning Protocol (EPP)", STD 69, RFC 5730, DOI 10.17487/RFC5730, August 2009, <https://www.rfc-editor.org/info/rfc5730>.

[RFC7469] Evans, C., Palmer, C., and R. Sleevi, "Public Key Pinning Extension for HTTP", RFC 7469, DOI 10.17487/RFC7469, April 2015, <https://www.rfc-editor.org/info/rfc7469>.

[RFC4985] Santesson, S., "Internet X.509 Public Key Infrastructure Subject Alternative Name for Expression of Service Name", RFC 4985, DOI 10.17487/RFC4985, August 2007, <https://datatracker.ietf.org/doc/html/rfc4985>.

9.2. Informative References

[ref_1] Google Trust Services, "May 2025 - Client Authentication Certificates (clientAuth) Deprecation", May 2025, <https://pki.goog/updates/may2025-clientauth.html>.

[ref_2] digicert, "Sunsetting the client authentication EKU from DigiCert public TLS certificates", September 2025, <https://knowledge.digicert.com/alerts/sunsetting-client-authentication-eku-from-digicert-public-tls-certificates>.

[ref_3] SSL.com, "Removal of the Client Authentication EKU from TLS Server Certificates What You Need to Know", April 2025, <https://www.ssl.com/blogs/removal-of-the-client-authentication-eku-from-tls-server-certificates-what-you-need-to-know>.

[ref_4] CA/Browser Forum, "Latest Baseline Requirements", August 2025, <https://cabforum.org/working-groups/server/baseline-requirements/requirements/>.

[ref_5] digicert.com, "TLS Certificate Lifetimes Will Officially Reduce To 47 Days", May 2025, <https://www.digicert.com/blog/tls-certificate-lifetimes-will-officially-reduce-to-47-385days#:~:text=The%20three%20years%20for%20the,reused%20is%20only%2010%20days.>.

[ref_6] ssl.com, "What Is Certificate Pinning?", October 2023, <https://www.ssl.com/blogs/what-is-certificate-pinning/>.

[ref_7] isi.edu, "DANE in SMTP— the sky is not falling", March 2020, <https://dnssec-stats.ant.isi.edu/~viktor/test.html>.

Authors' Addresses

Zaid AlBanna
Verisign
12061 Bluemont Way
Reston, VA 20190
United States of America
Email: zalbanna@verisign.com

James Gould
Verisign
12061 Bluemont Way
Reston, VA 20190
United States of America
Email: jgould@verisign.com

Scott Hollenbeck
Verisign
12061 Bluemont Way
Reston, VA 20190
United States of America
Email: shollenbeck@verisign.com