Abstract

This document describes a method of providing private DNS subdomains such that each subdomain can be shared among multiple devices of a single owner or group. A private subdomain can be used for sharing personal services while increasing privacy and limiting knowledge of scarce resources.

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 September 25, 2019.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.
1. Introduction

Section 6.6 of [RFC7558] highlights the privacy risks of DNS service announcements in clear text. While there has been a long focus on access control to private services including the use of encryption and authentication through TLS [RFC8446] for connections, the DNS-SD announcements [RFC6763] themselves may leak private information including but not limited to device types and versions, enabled services on the device subject to attack, personal names and identifiers used for tracking, etc.

Some services are meant to be advertised and used freely by devices on the link but other services are restricted to an owner or group and these services are announced publicly as a side effect of the current service discovery deployment.

This document defines a method for collaborating devices to share private services with one another but without revealing the existence of these services in a public way. This provides an additional layer of privacy protection for an individual’s devices or those of a defined group sharing a common purpose.

The additional privacy is achieved by creating private subdomains that require a private key for bidirectional access to DNS queries and responses for the zone.

This document defines a subdomain hierarchy for providers to enable this feature as well as a mechanism for interoperable transfers to and from the subdomain. This includes creating and destroying the subdomains, adding and removing records through DNS Update, and private authenticated queries.
2. Requirements Language

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. These words may also appear in this document in lower case as plain English words, absent their normative meanings.

3. Subdomain Operations

An administrative domain provider will enable private subdomains by creating a base subdomain at "_pvt.<domain>." In addition to the SOA and NS records, a public KEY record [RFC2535], [RFC3445] MUST be created at the apex which is openly available for queries. This public key will be used for message encryption relating to the maintenance of private subdomains.

The Zone bit for all KEY records used in this specification MUST be set to 0. The protocol value for the KEY record is set to DNSSEC (3) and the algorithm value is taken from the available algorithms defined in the IANA DNS Security Algorithm Numbers.

3.1. Zone Creation

A subdomain is created by the owner in an administrative domain for which the owner has a trusted relationship. For instance, if a user has services provided by an administrative domain and that user has been assigned a user name or account at that domain, the user could then uniquely claim ownership of the subdomain "<user>._pvt.<domain>." The administrative domain can use any means it finds sufficient to verify the trusted relationship with the user including RADIUS, AAA, email verification, or some other method not described here which may include enabling the service on a per-user basis.

The user can then create the subdomain by sending an UPDATE [RFC2136] to the MNAME of the SOA record for "_pvt.<domain>." containing a new KEY record for the zone "<user>._pvt.<domain>." The KEY record contains a public key that will later be used by the administrative domain to verify signed requests. If this zone already exists, the UPDATE fails with RCODE YXRRSet. If the zone does not exist, the user has successfully claimed the zone and all subsequent operations by the user will require knowledge of the private key associated with the registered public key in the KEY record. The user can distribute
this private key to any or all of its devices for access to the private subdomain.

In response, appropriate NS records for "<user>" will be created in the "_pvtr.<domain>." and a new SOA record "<user>._pvt.<domain>." with appropriate record fields will also be created along side the new KEY record submitted by the user. The authoritative servers for the new "<user>._pvt.<domain>." will be managed by the administrative domain provider.

At this point, the owner has knowledge of the public key of "_pvtr.<domain>." and the administrative domain has knowledge of the public key of "<user>._pvt.<domain>." All subsequent operations for the subdomain "<user>._pvt.<domain>." are signed with the private key of the sender. The administrative domain provider can verify the sender should have access to the records in the private zone and the owner can verify the received records are authentic and haven’t been tampered with.

3.2. Adding / Removing Resource Records

Once the zone is created, the user can begin adding or removing records to the "<user>._pvt.<domain>" subdomain through additional UPDATE messages for the zone.

To ensure zone additions and deletions are from the subdomain owner, the UPDATE message must be signed with the owner’s private key and the signature included in the additional data section in the form of a SIG(0) record [RFC2931]. More information about authenticating UPDATE messages can be found in [RFC3007].

If the administrative domain provider can verify the signature with the subdomain owner’s public key, the records are added to, or removed from, the "<user>._pvt.<domain>." zone. See section 2.5.2 of [RFC2136] for the specifics of adding or removing records in the Update section.

In order to change the KEY record at the apex of the zone, the old KEY record should be added to the Prerequisite section and the new KEY record in the Update section. Then the message is signed with the subdomain owner’s private key.

This is useful for changing the algorithm or key length for the public/private key pair.

If instead the private key associated with the public key in the KEY record has been compromised, the user should contact the
administrative domain out of band to verify authenticity and replace the KEY record through a process established by the provider.

3.3. Zone Destruction

When the owner is ready to destroy the subdomain ", it can do so by deleting the KEY record at the apex through an UPDATE message. As above, the UPDATE message additional data section MUST contain a SIG(0) signature over the entire message. Once validated, the zone will be removed along with the NS records for "<user>" in the "_pvt.<domain>" zone.

The owner is free to destroy and re-create the subdomain as needed for as long as the relationship continues with the administrative domain.

4. Querying Resource Records

Only the owner and the administrative domain provider know the true contents of the records. Queries must be made through direct connections to an authoritative server for the subdomain over a TLS connection. If the authoritative server also provides connections over UDP or TCP without TLS, queries for records in private zones over non-TLS connections MUST return an RCODE containing REFUSED.

4.1. Signed Requests

All queries MUST be signed with the private key of the owner. The signature MUST be in the Additional records section in the form of a SIG(0) record. If a query is received that is not signed or cannot be verified with the public key in the KEY record at the apex of the "<user>._pvt.<domain>.", a response containing the question as received with an RCODE of REFUSED with no answers MUST be returned. The Authority section of the response MUST contain the SOA record for the "<user>._pvt.<domain>.".

Authoritative servers MUST verify the signature in the query before returning the results.

5. Responses

6. Security Considerations

The Strict Privacy Usage Profile for DNS over TLS is REQUIRED for connections to the authoritative name servers [RFC8310]. Since this is a new protocol, transition mechanisms from the Opportunistic Privacy profile are unnecessary.
See Section 9 of [RFC8310] for additional recommendations for various versions of TLS usage.

DNSSEC is RECOMMENDED for the authentication of authoritative DNS servers. TLS alone does not provide complete security. TLS certificate verification can provide reasonable assurance that the client is really communicating with the server associated with the desired host name, but since the desired host name is learned via a DNS query, if the DNS response is subverted then the client may have a secure connection to a rogue server. DNSSEC can provide added confidence that the response has not been subverted.

Deployment recommendations on the appropriate key lengths and cypher suites are beyond the scope of this document. Please refer to TLS Recommendations [RFC7525] for the best current practices. Consider that best practices only exist for a snapshot in time and recommendations will continue to change. Updated versions or errata may exist for these recommendations.

The authoritative server connection endpoint SHOULD be authenticated using DANE TLSA records for the associated DNS record used to determine the name (SOA, SRV, etc). This associates the target’s name with a trusted TLS certificate [RFC7673]. This procedure uses the TLS Sever Name Indication (SNI) extension [RFC6066] to inform the server of the name the client has authenticated through the use of TLSA records. Therefore, if the DNS record used to obtain the name passes DNSSEC validation and a TLSA record matching the target name is useable, an SNI extension must be used for the target name to ensure the client is connecting to the server it has authenticated. If the target name does not have a usable TLSA record, then the use of the SNI extension is optional. See Usage Profiles for DNS over TLS and DNS over DTLS [RFC8310] for more information on authenticating domain names.
7. References

7.1. Normative References


7.2. Informative References


Author’s Address

Tom Pusateri
Unaffiliated
Raleigh  NC 27608
USA

Phone: +1 (919) 867-1330
Email: pusateri@bangj.com