Network Working Group
Internet-Draft
Intended status: Experimental
Expires: April 22, 2015

R. Van Rein
ARPA2.net

October 19, 2014

Finding the Kerberos Realm of a Service in DNS
draft-vanrein-dnstxt-krb1-00

Abstract

This specification defines methods to determine realm names for services being contacted by their DNS name. Currently, finding realm names is done through guessing or local configuration. DNS can make this process more dynamic, provided that DNSSEC is used to ensure authenticity of resource records.

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 http://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 April 22, 2015.

Copyright Notice

Table of Contents

1. Introduction

When a client contacts a Kerberised service, it needs to obtain a service ticket, and for that it needs to contact the realm under which the service is run. To map a service name into a realm name and then into a KDC, the client uses local mappings, or it can contact its KDC which look into its local mappings. Through DNS, such mappings could be dynamically expanded, thus permitting more flexibility without explicit configuration.

There are two important mappings that are needed for the given scenario. One is a mapping from the FQDN of a service to its realm name; the other is a mapping from the realm name to the Kerberos5-specific services such as the KDC. The latter mapping is published in SRV records [RFC4120] and the traffic is protected by the protocols themselves. The first mapping however, has never been standardised and are ill-advised because unsecured DNS cannot be considered a reliable source.

With the recent rise of DNSSEC however, it is possible to make a reliable judgement on the authenticity of such data, which enables

the standardisation of the first mapping in the form of TXT records in DNS. This specification defines how to publish and process such records.

Each TXT record holds of a series of tagged string values. A few of these are defined below, others may be added by future specifications.

2. Kerberos TXT record syntax

The TXT record for Kerberos is a simple sequence of ABNF terminals:

"v" "=" "krb1" *(";" tag "=" value)

The initial v=krb1 is used as a hint to applications that this specification is followed. Space and tab character sequences after terminals are ignored; a tag is a sequence of letters, digits, dashes and underscores; a value is anything but whitespace or semicolons. Note that the entire TXT record is case-insensitive. TODO: Really? "The ASCII case insensitivity conventions only apply to ASCII labels" [Section 3.2 of [RFC4343]]

When a TXT record does not adhere to this syntax, it MUST NOT be processed as described in this specification, but this MUST NOT be fatal to the processing of other TXT records. When the initial v=krb1 matches the syntax but the rest does not, then a processing application MAY release a warning message.

Tags are registered with IANA, and this document defines the first few. New additions are always optional. An application that does not recognise a tag name MUST silently discard it.

Multiple TXT records may be supplied under a queried name, and there may be multiple that adhere to this syntax; these present alternatives that can be tried. Since DNS does not supply them in any order, the DNS client can choose freely in what order to process these records. When no TXT record adheres to this syntax, then no alternative is available through DNS.

3. Defining Home Records and Home Tags

The TXT records defined here may be used to define realm names that do not look similar to the FQDN at which it is found. Other TXT records may define one domain-styled [Section 6.1 of [RFC4120]] realm name that translates back to the FQDN at which the TXT record was found. The latter category of TXT record is called a "home record" in this specification.

TXT records which are not home records can be used to reference from a DNS name to a realm that maps onto another DNS name. The use of DNSSEC makes this safe; the same party that masters the server settings also determines the authentication service to use.

Some tags may be defined to be used in home record only. Such tags are defined by the term "home tags". Specification whether a tag is a home tag is intended to avoid claims about realms being made outside its control.

4. Querying Realm Descriptions

The following subsections define two procedures for finding a Kerberos realm. One procedure starts from a domain name, the other starts from the hostame of a server.

When dealing with services found through DNS SRV [RFC 2782], a choice between the use of a domain name or hostname is possible. In these situations, the FQDN of the SRV queries MUST be used in the procedure for domain name queries.

Since DNS in general cannot be considered secure, the client MUST dismiss any DNS responses that are not Insecure, Bogus or Indeterminite [Section 5 of [RFC4033]]. Only Secure responses are taken into account. This specification does not prescribe that the client validates the responses by itself, but the deployment used SHOULD NOT accept validation states of DNS responses from a reliable validating source over unreliable communication channels.

The result may contain TXT records that do not adhere to the syntax of this specification; such TXT records MUST be removed from the result. Within the syntax, there may be tags that are unknown; such tags and their value MUST be ignored when further processing the results. Finally, some tags are defined as "home tags", and those

MUST be ignored if the TXT record is not a home record.

When no Secure DNS responses are received, this procedure MUST be terminated without extracting realm descriptive information from DNS. Such termination need not be fatal; other procedures may exist to find a realm name.

4.1. Querying a Domain's Realm Descriptions

To find the Kerberos realm definition for a domain name, a DNS client conducts a TXT query targeted at the domain name.

Where this specification speaks of querying a domain, its interpretation of a domain is that of a name space, which may or may not have a host attached, but which is likely to have services attached, for instance through MX or SRV records. Domain names also occur in many naming schemes after an optional username and @ symbol, such as the domain name (that also happens to be termed "realm", but

without connection to Kerberos realms) in a Network Access Identifier [RFC4282].

4.2. Querying a Host's Realm Descriptions

The query of a hostname may be done at two levels, namely the hostname itself and the apex of the zone holding the hostname. The latter requires a signed denial for the hostname; the signature of this denial holds a field named the "Signer's Name" which must contain the zone name [Section 3.1.7 of [RFC4034]], which is used for the second query if the name differs from the initial hostname.

Note that most name servers will also return a SOA record with a negative response; this addition however, is not guaranteed and it may be removed from the response due to frame size constraints. This is why the SOA record is not preferred for finding the secondary description.

5. Publishing Realm Descriptions

The default position for realm-descriptive TXT records is in the apex of a zone. These may be home records, but that is not a requirement;

it is possible to authenticate multiple domain names with a single Kerberos realm.

It is possible to override entries underneath the zone apex. This may be done for individual host names, or through a wildcard that catches a range of undefined names. Note that wildcards receive special treatment [RFC4592] when used with DNSSEC, but that they are supported.

The various entries in DNS override each other in a particular order; the zone apex is the fallback default; wildcards cator to unspecific subordinate names, and an accurately matched hostname has the highest priority.

Note that a domain is not always the same as a zone apex. So, when querying a domain name as specified in Section 4.1, there will be no fallback to a zone apex. An entry similar to the one in a zone apex should then be defined; and similarly, it may be overridden with wildcards and hostnames that define subordinate DNS names.

The syntax supports TXT records that define no realm at all. These are interpreted as the absense of Kerberos for the given name.

6. Realm Descriptor Tags

The names of tags fall apart in two types:

- "General tags" can be used in any v=krb1 TXT records;
- "Home tags" can only be used in TXT records that describe a realm that matches the FQDN of the TXT record.

When home tags occur in a TXT record that does not define a realm name that matches the FQDN of the TXT record, then these home tags MUST be ignored.

6.1. Realm Descriptor Tag "realm"

The tag "realm" MAY be present in all TXT records that adhere to this specification, and it MUST be processed by implementations of this specification.

The value of a "realm" tag names a realm connected to the TXT record's FQDN. Since the content of a TXT record is case-insensitive, a mapping to case-sensitive realm names is needed. In this mapping, a realm-value letter is mapped to a lowercase letter if it is preceded by an equals sign and mapped to an uppercase letter if not; equals signs are not mapped to realm characters; all other characters are mapped without modification. The result MUST be a domain-style realm name [Section 6.1 of [RFC4120]] to be accepted for further processing along the lines of this specification.

When multiple "realm" tags occur in one TXT record, then they present alternative suggestions to combine with all other tags in the same TXT record. Note that a TXT record with multiple "realm" tags is never a home record.

The absense of a "realm" tag in a TXT record conforms to this specification; it does not provide any realm names for the given FQDN in DNS. One such TXT record can be used to specify the absense of Kerberos tickets for the FQDN of that TXT record; this can be used to override TXT records in a wildcard or at the zone apex.

An example use of the "realm" tag in a TXT record is

example.com. IN TXT "v=krb1; realm=EXAMPLE.COM"

Since the FQDN of this TXT record is example.com, this TXT record may also hold home tags.

In addtion to the previous example, the following tag indicates that there is no realm, and so it is useless to lookup a Kerberos ticket for ftp.example.com:

ftp.example.com. IN TXT "v=krb1"

6.2. Realm Descriptor tag "service"

The tag "service" MAY be present in any TXT record that adheres to this specification, and it SHOULD be recognised by implementations of this specification. The tag is optional.

The value of a "service" tag is the name of a service, as used in principal names. This can be used as a hint to clients that need to match service tags. The occurrence of a service tag and a realm tag in the same TXT record may be read to suggest that a principal ticket for the combination exists. Since service names are used to match, and act as a hint, their representation without case in DNS is not a problem; they are matched through case-insensitive comparison.

The purpose of this tag is to enable clients an early selection between alternatives that it may wish to pursue; adding a service tag may improve the speed of resolution when multilple alternatives are listed in DNS, especially when future initatives would require public key cryptography for realm crossover. Since the tag is optional and its presence may not lead to a single combination of realm, service and FQDN, clients must still be prepared to iterate over alternatives.

When multiple "service" tags occur in one TXT record, then they present alternative suggestions to combine with all other tags in the same TXT record. The set is then to be considered complete; that is, when one or more "service" tags occur but none matches to a service that a client requires, then the realm description in that TXT record does not apply.

An example use of this tag in a TXT record is

www.example.com. IN TXT "v=krb1; realm=example.com; realm=example.org; service=http; service=ftp"

This would match with the following principal names:

- HTTP/www.example.com@EXAMPLE.COM
- HTTP/www.example.com@EXAMPLE.ORG
- ftp/www.example.com@EXAMPLE.COM

- ftp/www.example.com@EXAMPLE.ORG

A service named "krbtgt" is not offered for this service name, as far as this TXT record is concerned.

6.3. Realm Descriptor Tag "user"

TODO: Also define a "user" tag? RFC 3645 uses DNS@ krb4-style names, but in general I doubt if users should occur in DNS?

7. Efficiency Considerations

The TXT records introduced in this specification are useful to define realm names for servers whose DNS information is not statically configured in a Kerberos setup. This may release the pressure on such local configurations, and it may introduce more dynamicity, which may be useful for such things as realm crossover.

Since realm names cannot always be derived from DNS names, clients tend to construct various principal names by attaching all the realm names that they can think of, and attempting to obtain a service ticket for each in turn, until one is found. The KDC may also perform such actions, and return a reference [RFC6806] to a realm for consideration. In general, the list of service ticket names that may be considered can be relatively long.

Limiting the length of the list of ticket requests is going to be especially useful for situations with realm crossover when this involves public-key cryptography, as such algorithms are much slower than the symmetric algorithms normally used for Kerberos.

The use of "realm" tags can help the client to focus on those realms for which a service has a name defined. Similarly, the use of "service" tags is helpful to select only those TXT records that hold the service name sought by an application. The presence of multiple "realm" and/or multiple "service" tags in one TXT record enables iteration over multiple combinations, without a need to store the resulting cartesian product in DNS.

8. Privacy Considerations

It is common to spread service information in DNS, but for internal use this may be considered less desirable. This is why the "service" tag, as specified in Section 6.2, is optional.

9. Security Considerations

This specification defines a mechanism to redirect from a FQDN to a realm that may be located elsewhere, or to indicate that no realm is available for that FQDN. Publishing such a realm definition is the prerogative of the service administrator, and is therefore well-positioned in a DNS record at the same FQDN as the service, or at its zone apex.

However, when an attacker would be permitted to spoof such a record in a victim's DNS, then it could be possible for the attacker to convince the client that the attacker is the authentic provider for the service. Additional spoofing of hostname references could then complete the attack. This has been mitigated by requiring DNSSEC for all such TXT records.

Another angle of attack could be due to suppression of a TXT record, for instance for a hostname. Such attacks could direct a client to rely on the information stored in the zone apex, which may differ from an overridden value that is less desirable to the attacker. Such attacks have been mitigated by insisting on signed denials, and by stating that a non-responsive DNS server should not lead to the assumption that one can move up in the DNS hierarchy.

The process of finding the zone apex relies on a strict prescription in DNSSEC standards. The field from which it is taken is incorporated into the RRSIG record that holds it TODO:check, so this does not provide an opening to redirect the TXT queries to a domain of choice either.

The ability to create a TXT record that references a realm operated under another DNS name introduces a potential of setting flags for that remote realm that may be counter-productive. Given the open-endedness of the registry for these, problems due to this are mitigated by ignoring unknown tags, and treating known tags differently when they are registered as "home" tags; such tags are not processed for references to realms operated under another DNS name.

10. IANA Considerations

This specification establishes a new registry with IANA, whose entries are subject to expert review and whose definition must be described in a publicly available specification. The new registry will be known as the "Kerberos DNS TXT Tag Registry". Each entry must provide a flag to indicate if the tag may only be interpreted in

home tags.

The initial entries for this new registry introduced by this specification are:

Tag name	Home tag?	Definition
v	N/A	Not to be used [TBD:THIS-SPEC]
realm	No	[TBD:THIS-SPEC]
service	No	[TBD:THIS-SPEC]

Tag names are case-insensitive. The tag name "v" is reserved, and shall not be assigned.

In addition to the foregoing, tag names starting with "x-" are reserved for experimental use, for which no registration is possible, or required. For these unregistered tags there will be no protection from name clashes.

11. References

11.1. Normative References

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, March 2005.

[RFC4034] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Resource Records for the DNS Security Extensions", RFC 4034, March 2005.

[RFC4120] Neuman, C., Yu, T., Hartman, S., and K. Raeburn, "The Kerberos Network Authentication Service (V5)", RFC 4120, July 2005.

[RFC4343] Eastlake, D., "Domain Name System (DNS) Case Insensitivity Clarification", RFC 4343, January 2006.

[RFC4592] Lewis, E., "The Role of Wildcards in the Domain Name

System", RFC 4592, July 2006.

11.2. Informative References

[RFC6806] Hartman, S., Raeburn, K., and L. Zhu, "Kerberos Principal Name Canonicalization and Cross-Realm Referrals", RFC 6806, November 2012.

[RFC4282] Aboba, B., Beadles, M., Arkko, J., and P. Eronen, "The Network Access Identifier", RFC 4282, December 2005.

Author's Address

Rick van Rein
ARPA2.net
Haarlebrink 5
Enschede, Overijssel 7544 WP
The Netherlands

Email: rick@openfortress.nl