Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: May 17, 2015

R. Van Rein
ARPA2.net

November 13, 2014

Kerberos Realm Descriptors in DNS (KREALM)
draft-vanrein-dnstxt-krb1-01

Abstract

This specification defines methods to determine Kerberos realm descriptive information for services that are known by their DNS name. Currently, finding such information is done through static mappings or educated guessing. 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 May 17, 2015.

Table of Contents

1. Introduction

When a Kerberos client contacts a service, it needs to obtain a service ticket, and for that it needs to contact the KDC for a realm under which the service is run. To map a service name into a realm name and then into a KDC, clients tend to use static mappings or educated guesses; the client's KDC may or may not be involved in this process. Through DNS, such mappings could be dynamically expanded, permitting more flexibility than under the current practice.

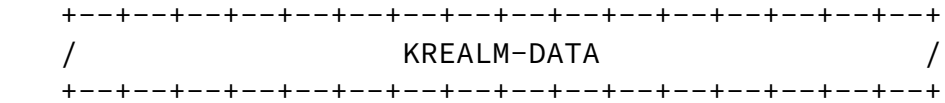
Two mappings are needed for the given scenario. One is a mapping from the FQDN of a service to its realm name; the other is a mapping from the realm name to the Kerberos-specific services such as the KDC. The latter mapping is published in SRV records [RFC4120] and such traffic is protected by the Kerberos protocol itself. The first mapping however, has hitherto not been standardised and is ill-advised over unsecured DNS because the published information is then neither validated by DNS nor does it lead to a protocol that could validate it.

With the recent uprise of DNSSEC, it is now possible to make a reliable judgement on the authenticity of such data in DNS, which enables the standardisation of the first mapping in the form of resource records in secured DNS.

This specification defines how to publish and process Realm Descriptors using a newly defined resource record type KREALM. Each of these records holds of a series of tagged string values. A few of these are defined below, others may be added by future specifications.

2. The KREALM Resource Record

This specification introduces a new DNS resource record that serves as a realm descriptor for Kerberos. The name for this DNS resource record type is KREALM, and its numeric value is TBD1. The corresponding RDATA format is as follows:



The syntax of KREALM-DATA is the DER encoding of the following ASN.1 syntax:

```
KREALM-DATA ::= SEQUENCE {
        versionNumber INTEGER (0..) DEFAULT 0,
        SET OF SEQUENCE {
            tag IA5String,
            value UTF8String
        }
    }
```

This specification makes the assumption that all values are represented as strings.

DISCUSS: RFC 4120 defines realm names with the KerberosString type which is a GeneralString, but it then advises to constrain it to IA5String or else risk interoperability problems. It is worth noting that the ESC "%" "G" prefix defined in ISO 2022 can be used to introduce an UTF8String in the KerberosString, and that

implementations even exist that insert UTF8String in KerberosString fields without even that escape. It's a jungle out there! Defining UTF-8 for this new field type does not seem to be such a stretch; it includes the IA5String subset and it also keeps the door ajar for future attempts at I18N of realm names and other Kerberos parameters. OTOH, OCTETSTRING would probably be too general, and place too much faith in wire representations to be suitable for comparison.

The advised format for the resource data in master zone files is the base64-encoded KREALM-DATA content in DER-encoding. Although most data will be printable string data, it need not adhere to an ASCII character set, may include NUL characters and have a somewhat complex

grammar; all these aspects would complicate master zone files and thus make them more error-prone.

Tags are registered with IANA, and this document defines the first few. A special range of tags starting with "x-" is available for local or experimental use. Implementations MAY safely ignore tags (and the corresponding value) that are not known to them. An application that does not recognise a tag name MUST silently discard it.

The versionNumber 0 is used as a version number for this specification; it is also the default versionNumber when absent from the encoding. Future updates to this specification MUST use another versionNumber IF they are invalidate any assumptions made in this specification. Such new applications SHOULD advise how to setup DNS in a backward-compatible manner; they might for instance publish both old and new styles of KREALM records.

Clients requesting KREALM records MUST ensure that the record uses proper syntax, including the string formats specified for tag and value fields and a versionNumber that the client understands.

Multiple KREALM 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.

In this general form, there are no constraints on the number of

permissible occurrences of a tag in one or more KREALM records, but tags MUST define whether multiple occurrences are permitted, and if so, what their interpretation is.

3. Defining Home Realms and Home Records

One of the tags defined by this specification is the "realm" tag [Section 6.1] that specifies a realm name. Realm names can be mapped [Section 7.2.3 of [RFC4120]] to DNS names. Those realm names in "realm" tags of KREALM records that that map to the FQDN at which that KREALM record was found, are hereby defined as "Home Realms".

KREALM records of which all realm name tags are Home Realms, are hereby defined as "Home Records". Note how KREALM records are not defined to be Home Realms when they contain a mixture of Home Tags and "realm" tags that are not Home Tags.

In general, the DNS name to which a realm name maps can hold information about the location of a KDC [Section 7.2.3 of [RFC4120]]

and other realm-specific services. This does not change; but for Home Realms, the same FQDN is the basis for finding the KREALM record and the KDC and other services; for other KREALM records that Home Records, the KREALM tag is a reference to a realm that translates to another DNS name, which in turn serves as the basis for finding the KDC and other realm services.

The following specifications are strict about their reliance on DNSSEC for KREALM records. The reason for this is to ensure that both the pointer to the actual service and its containing realm are inserted into DNS by the same responsble party. When combined with cryptographic ensurance of reaching the proper KDC for a realm, this provides a secure mechanism for access to realms can be created, whether or not they are the realm into which a user logged on.

Mechanisms for cryptographic ensurance of reaching realms is standard in Kerberos implementations; based on DNSSEC this may even be extended with more dynamic mechanisms, but that is not defined in this specification. A result that this specification may have is that the user knows the realms to ask for, even if it is a realm that was hitherto unknown. In that sense, the KREALM record may be a stepping stone in loosely connected links between Kerberos realms.

4. Querying Realm Descriptors

The following subsections define two procedures for finding Kerberos realm descriptors for the DNS name of a service. One procedure starts from a domain name, the other starts from the host name of a service.

When dealing with services found through DNS SRV [RFC2782], a choice between the use of a domain name or host name is possible. In these situations, the FQDN of the SRV queries, without the _Service._Proto prefix, MUST be used in the procedure for domain name queries, and the procedure for querying a domain should be followed rather than the procedure for a host name.

Since DNS in general cannot be considered secure, the client MUST dismiss any DNS responses that are Insecure, Bogus or Indeterminate [Section 5 of [RFC4033]]. Only the remaining Secure responses are taken into account. This specification does not require that the client validates the responses by itself, but a client deployment SHOULD NOT accept DNS responses from a trusted validating DNS resolver over untrusted communication channels.

To give one possible implementation, a Kerberos client may send DNS queries with the DNSSEC OK bit [RFC3225] set to enable DNSSEC, and require that the Authenticated Data bit [RFC3655] is set in the

response to indicate the Secure state for answer and authority sections of the response. When the DNS traffic to and from the validating resolver is protected, for instance because that resolver is reached over a loopback interface, then the Kerberos client has implemented the requirements for Secure use of the answer and authority sections in DNS responses.

The result may contain KREALM records that do not adhere to the syntax of this specification; such KREALM records MUST be removed from the result. In the sequence of tag-and-value pairs, there may be tags that are unknown; such tags and their value MUST be ignored when further processing the results. Finally, some tags are specifically registered with IANA for use in Home Tags, and those MUST be ignored if the KREALM 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; non-DNS procedures may exist to find a realm name.

4.1. Querying a Domain's Realm Descriptors

To find Kerberos realm descriptors for a domain name, a DNS client conducts a KREALM query targeted directly 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 Descriptors

To find a realm descriptor for a host name, a KREALM query is performed to the same FQDN as that of the host name. If this fails with a secure denial, a fallback KREALM query is done on the FQDN of the zone apex. The reason to use the zone apex in this role is that it signifies the start of administrative control over a zone, generally making it cover a larger DNS name range than a single host name, while still residing under the same operational control as the host name itself -- which is valuable from a security viewpoint.

Without a signed denial, no fallback query is performed; this mitigates denial of service attacks on that host name's FQDN. With a signed denial, evidence of non-existence of the KREALM record is

returned, and part of that is a field named the Signer's Name. This field must contain the zone name [Section 3.1.7 of [RFC4034]], and this value is used as the FQDN of the zone apex for the fallback query. The querying client MUST ensure that this property holds; that is, it MUST NOT proceed with the fallback query if the Signer's Name does not have the original host name as a subordinate name.

DISCUSS: 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 Descriptors

The default position for KREALM records that describe a realm is in the apex of a zone. Such KREALM records may be Home Records, but that is not a requirement, because on Kerberos realm may cover any number of DNS zones.

When a KREALM record is published in the zone apex, it will cover all SRV records for that domain name, as well as all host names defined in the same zone. SRV records for subordinate names to the zone apex need a separate KREALM record. If a host name requires overridden KREALM record, then this may be specified in a KREALM record with the same FQDN as the host name.

One form of overriding KREALM definitions worth noting is one that does not define a Kerberos realm at all; such a record can be used to undefine any realm names that are defined in the zone apex.

Note that KREALM records with wildcard names will not work. All host names and most domain names define at least one resource record (of any type) with the name that the wildcard should cover. These defined names cause the wildcards to be suppressed [RFC4592] from DNS responses.

6. Tags in Realm Descriptors

The names of tags are partitioned into two types:

- General Tags can be used in any KREALM records;
- Home Tags can only be used in Home Records.

Any Home Tags that occur in other KREALM records than Home Records MUST be ignored.

6.1. Realm Descriptor Tag "realm"

The tag "realm" MAY be present in all KREALM records, and it MUST be recognised and processed by implementations of this specification; in other words, the tag is not optional.

The value of a "realm" tag provides a realm name for the queried FQDN. The permissible values of this tag conform to the permissible names of realm names [Section 6.1 of [RFC4120]], which a conforming application MUST validate before processing the value. This includes, but is not limited to, domain-style realm names. Since the value field is a general UTF8String, it is to be treated as a case-sensitive string [RFC4343], just like realm names.

It is possible to define zero "realm" tags in a KREALM record. This indicates that no realm is defined by that record. This is not an invalid condition; other KREALM records, if any, or other service-to-realm mappings may still be used.

When multiple "realm" tags occur in one KREALM record, then they present alternative suggestions to combine with all other tags in the same KREALM record.

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

example.com. IN KREALM "MBgxFjAUFgVyZWFsbQwLRVhBTVBMRS5DT00="

Written out, the RDATA holds the following DER representation:

```
SEQUENCE
   SET
      SEQUENCE
         IA5STRING    realm
         UTF8STRING   EXAMPLE.COM
```

Since the value of all "realm" tags map to the FQDN of this KREALM record, this KREALM record is a Home Record. As a result, tags that are registered as Home Tags may be added to this realm descriptor.

In addition to the previous example, the following tag indicates that there is no realm, and so it is useless to request a service ticket for ftp.example.com, as far as this domain descriptor in DNS is concerned:

ftp.example.com. IN KREALM "MAIxAA=="

The RDATA for this KREALM record encodes no tags and no values at all:

```
SEQUENCE
   SET
```

6.2. Realm Descriptor Tag "service"

The tag "service" MAY be present in any KREALM record, 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 KREALM record is a hint that a service ticket for the combination probably exists. Note that the value of this tag is a general UTF8String, and that it is case-sensitive [RFC4343].

The purpose of this tag is to enable clients to locally select alternatives that it may wish to pursue; adding a "service" tag may improve the speed of resolution when multiple alternatives are listed in DNS, which is especially fruitful when future initiatives would require public key cryptography for realm crossover.

When no "service" tag is defined in a KREALM record, then no hint for selection is available; processing must then continue under the assumption that any desired service name may be available for the realm description. In contrast, when one or more "service" tags are defined in a KREALM record, then this set may be considered a complete specification of available services. Note that multiple KREALM records may exist, each of which may or may not define "service" tags.

When multiple "service" tags occur in one KREALM record, then they present alternative suggestions to combine with all other tags in the same KREALM record.

An example use of this tag in a KREALM record is

```
www.example.com.  IN KREALM "ME8xTTAOFgdzZXJ2aWNlDANmdHAwDxYHc2Vydmlj
ZQwESFRUUDAUFgVyZWFsbQwLRVhBTVBMRS5DT00wFBYFcmVhbG0MC0VYQU1QTEUuT1JH"
```

This RDATA contains the following data structure:

```
SEQUENCE
   SET
      SEQUENCE
         IA5STRING    service
         UTF8STRING   ftp
      SEQUENCE
         IA5STRING    service
         UTF8STRING   HTTP
      SEQUENCE
         IA5STRING    realm
         UTF8STRING   EXAMPLE.COM
      SEQUENCE
         IA5STRING    realm
         UTF8STRING   EXAMPLE.ORG
```

This matches the following principal names, found by iterating over all combinations of "server" and "realm" values:

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

Apart from the case-insensitivity of the DNS name "www.example.com", this list is a complete list of principal names matched by the KREALM record. For instance, a service named "krbtgt" is not described by this KREALM record.

7. Efficiency Considerations

KREALM records are useful to define realm names for servers whose DNS information is not statically mapped in a Kerberos setup. This may simplify operative control of such static mappings. It may also introduce more dynamicity, which may be useful for such things as realm crossover.

Since realm names cannot be derived directly from DNS names, clients tend to construct various principal names by appending all the realm names that they are aware 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 principal names that may be considered can be relatively long.

The use of "realm" tags help the client to focus on those realms for which a service has a name defined. This limit the list of realm names to attempt to those realm names that the service suggests. The client does not need to guess as heavily. Similarly, the combined use of "service" tags helps to select only those KREALM records that further constrain the scope to search.

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

The combined publication of multiple "realm" tags with multiple "service" tags enables a compact representation of variations that a client should iterate over, without the 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 [Section 6.2], is optional.

Similarly, internal applications may still prefer local definitions for realm names that a client should consider; this specification does not enforce the KREALM record in those situations.

For situations which crossover between realms, the choice between static configuration in files and KDC configuration versus a dynamic configuration in DNS is still a choice; the dynamic option based on DNS publishes more information, but dynamic applications are more likely to desire such information to be publicly and securely

available.

9. Security Considerations

This specification defines a mechanism to redirect from a FQDN to a realm name that may not map to that same FQDN, or that define that no realm name exists for the originating FQDN. Publishing such a realm descriptor is the prerogative of the DNS administrator who is also in charge of publishing the location of the service that is protected by Kerberos. This administrator is generally trusted not to attack the security of a zone; DNSSEC makes this assumption even stronger than unsecured DNS, and this specification does not reduce or expand on that assumption.

When an external attacker would be permitted to spoof a KREALM record in a victim's DNS, then it could be possible for that attacker to

convince the client that the attacker is the authentic provider for the service. Additional spoofing of host name references could then complete the attack. This has been mitigated by requiring DNSSEC for all such KREALM records.

Another angle of attack could be due to suppression of KREALM records, specifically the ones for a host name which have a fallback option at the zone apex. Such attacks could direct a client to rely on information that may form a alternative of lesser security. 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 the zone apex is taken is validated by the signature field of the RRSIG record that holds it. This field is necessarily part of a signed denial under DNSSEC.

The ability to create a KREALM 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 IANA registry for tags, problems that this may cause 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 defines a new "Resource Record (RR) Type", to be registered in IANA registry of Domain Name System (DNS) Parameters". The name of the RRType is KREALM, its value is TBD1 and its meaning is "Kerberos realm descriptor".

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 "DNS KREALM Tag Registry". Each entry must provide a Yes/No flag to indicate if the tag is a Home Tag, meaning that it may only be interpreted as part of Home Records.

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

Tag name	Home Tag?	Definition
realm	No	[TBD:THIS-SPEC]
service	No	[TBD:THIS-SPEC]

Tag names are case-sensitive. Registration of new tags is subject to expert review, and a specification must be created as part of its definition.

DISCUSS: Suggestions on the submission process for new tags are requested.

In addition to the foregoing, tag names starting with "x-" are reserved for local and experimental use, for which registration is neither possible nor required. These unregistered tags will not be protected from name clashes.

11. References

11.1. Normative References

[RFC2782] Gulbrandsen, A., Vixie, P., and L. Esibov, "A DNS RR for specifying the location of services (DNS SRV)", RFC 2782, February 2000.

[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.

11.2. Informative References

[RFC3225] Conrad, D., "Indicating Resolver Support of DNSSEC", RFC 3225, December 2001.

[RFC3655] Wellington, B. and O. Gudmundsson, "Redefinition of DNS Authenticated Data (AD) bit", RFC 3655, November 2003.

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

[RFC4592] Lewis, E., "The Role of Wildcards in the Domain Name System", RFC 4592, July 2006.

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

6806, November 2012.

Author's Address

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

Email: rick@openfortress.nl