Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: March 18, 2016

R. Van Rein
ARPA2.net

September 15, 2015

Declaring Kerberos Realm Names in DNS (KREALM)
draft-vanrein-dnstxt-krb1-05

Abstract

This specification defines a method to determine Kerberos realm names for services that are known by their DNS name. Currently, such information can only be found in static mappings or through educated guesswork. DNS can make this process more flexible, 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 March 18, 2016.

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 guessing; the client's KDC may or may not be involved in this process. Through DNS, the static mappings could be made more dynamic, and be moved from local client configuration into the hands of the party administrating a server's presence in DNS. This permits more flexibility than under the current practice.

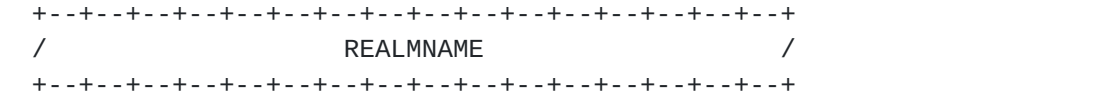
Two mappings are needed for the given scenario. One is a mapping from the FQDN of a service to its realm name; the other is a mapping from the realm name to the Kerberos-specific services such as the KDC. The latter mapping is published in SRV records [RFC4120] and such traffic is protected by the Kerberos 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 provide end-to-end validation for it.

With the recent uprise of DNSSEC, it is now possible to make a reliable judgement on the authenticity of 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 Kerberos realm names using a newly defined resource record type KREALM. These records hold a case-sensitive string with the realm name. Multiple KREALM records may be defined as alternatives and suggest iterating over them until a ticket can be procured.

2. The KREALM Resource Record Type

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



The REALMNAME is represented as a <character-string> [RFC1035] which starts with a single-byte length, followed by as many bytes of realm name as the length byte's value. The RDATA field therefore has a length of 1 up to 256 bytes, to hold a realm name of 0 up to 255 bytes. For instance, a realm EXAMPLE.ORG would be represented with the same RDATA as the following generic RDATA section that is also used for unkonwn resource record types [RFC3597]:

```
\# 12 ( 0b 45 58 41 4d 50 4c 45 2e 4f 52 47 )
```

The REALMNAME represents a Kerberos realm name, not a DNS name. As a result, there cannot be a trailing dot unless it is actually part of the Kerberos realm name. The realm name is never relative to the DNS name at which the KREALM record was found. Finally, there is no required relationship (such as partial overlap) between the realm name and the DNS name at which the KREALM record was found.

Realm names in Kerberos are often domain-styled [Section 6.1 of [RFC4120]], in which case they look like DNS names but are case sensitive; unlike the DNS names used as lookup keys in the DNS hierarchy, the REALMNAME format follows the <character-string> format in being case-sensitive.

In fact, the <character-string> format is a binary format, and DNS notation \DDD [Section 5.1 of [RFC1035]] exists to put arbitatrary bytes in the string notation, including even interior NUL bytes. This binary format leaves the door ajar for future internationalisation of Kerberos realm names. Realm names are defined with the KerberosString type [Section 5.2.1 of [RFC4120]] which is an ASN.1 GeneralString, but its specification currently advises to constrain the use of this string type to an IA5String (basically using only the first 128 codes of the ASCII table) to avoid interoperability problems. After the <character-string>'s length byte, the REALMNAME holds the value of the GeneralString, but not the corresponding ASN.1 tag and length.

It is worth noting that the ESC "%" "G" prefix [TODO:xref target="ISO2022"/] can be used to introduce an UTF8String in a GeneralString, and that implementations exist that insert UTF8String values in KerberosString fields without even that escape. All this precedes formal standardisation of internationalisation, but it suggests that the RDATA definition for KREALM can be supportive of future internationalisation of realm names, even if its current advised use is limited to the value of an IA5String.

The format for the resource data in master zone files is the same as for TXT records, which also have the same RDATA representation. The vital difference of KREALM lies its different record type, which declares that its RDATA has a well-defined meaning as a realm name, and can therefore be automatically processed without risking arbitrary coincidences that could lead to security problems. An example declaration of realm name EXAMPLE.ORG for a server named imap.example.org would be:

```
imap.example.org.  IN KREALM  "EXAMPLE.ORG"
```

The RDATA for this KREALM record has already been shown above, in the generic RDATA section notation.

Multiple KREALM records may be supplied for the same DNS name; these represent alternatives that can be tried by the DNS client. Since DNS delivers the resource records as a set without any particular order, the DNS client can choose freely in what order to process these records.

It is possible to create a KREALM record for any DNS name, but this specification only provides query procedures for host names and domain names. The use with a domain name had the additional use of denoting the precise spelling for a realm name under its DNS-mapped name. DNS-mapped names currently would not modify more than the case of a DNS name, and even that is only done as the result of DNS compression [RFC4343]; but in a future with internationalised realm names there might be more to guess, in which case this facility is likely to be helpful. Since KREALM records in general pose no constraints on the relation between the contained realm name and the DNS name at which it is found, it is advised for this one application to map the realm name back to a DNS name and compare the result.

3. Querying Kerberos Realm Names

This sections defines a procedure for finding Kerberos realm names for the servers, as well as for a DNS-mapped realm name.

When applications directly know their server host name, perhaps because it is mentioned in a ticket as a service principal name, they will lookup the KREALM record at the same name as the server host name.

When applications locate their servers through a domain name, for example via MX [RFC1035] or SRV records [RFC2782], a choice between the use of the domain name or the appointed server host names is to be made. In these situations, the KREALM query MUST use only the domain name, without adding prefixes such as _Service._Proto for SRV records. The appointed servers for a domain service MUST NOT be queried for KREALM records, since these may reside under operational control foreign to the service domain. In addition, their possible shared use by many domains would mean that they may have to specify a long list of realms, most of which would be unusable to the client. The domain name is closer to the client's context and can provide a better-targeted list of KREALM records.

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 to be 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 or its KDC may send DNS queries with the Authentic Data (AD) bit set to enable DNSSEC [Section 5.7 of [RFC6840]], and require that the Authenticated Data bit is set in the response to indicate [RFC3655] 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 the validating resolver is reached over a loopback interface, then the Kerberos client or its KDC has implemented the requirements for Secure use of the answer and authority sections in DNS responses.

When no Secure DNS responses are received when DNS timesout, then the KREALM query MUST be terminated without extracting realm names from DNS. This termination MAY be done immediately upon receiving Secure denial for the requested KREALM record. KREALM query termination need not be fatal; non-DNS procedures may exist to find a realm name, including the current practice of static mappings and educated guessing.

4. Publishing Kerberos Realm Names

KREALM records should generally be published at the domain names and server host names that a Kerberos application may want to approach.

As an exception to this general rule, server host names may be exempted if they are always looked up through a domain name. Note however, that most query mechanisms that lookup domain names through special resource record types have fallbacks to plain server host name lookups. When such direct server host names are supported in a deployment of those applications, usually meaning that these server host names may occur in Kerberos service principal names, and when the realm name cannot be detected through a preferred mechanism for such server host names, then an additional KREALM record located at the server name is also going to be helpful.

There may be situations where a domain represents a Kerberos realm, but uses domain-style references such as MX and SRV records to point to foreign server host names. Such foreign server host names are often unsuitable to accompany with a KREALM record, so it is advisable to either not refer to the server host names directly in service tickets, or to see to it that a realm name is always attached by the KDC.

These instructions are somewhat flexible, as a result of the pre-existing mechanisms for finding a realm name for a given service principal name. Assuming that the more flexible approach of KREALM records is preferred, a suitable test would be to run the targeted applications from an unconfigured Kerberos client.

Zones that intend to provide applications with Kerberos realm names through KREALM records MUST be protected by DNSSEC to make them usable to those applications.

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, even when querying a non-existent KREALM record.

5. 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.

The lookup of KREALM records can be done by a KDC, which can send back Cross-Realm Routing suggestions [Section 9 of [RFC6806]] to Kerberos clients that enable canonicalization. The cached DNS records, their validation and possibly realm-crossover caching at the KDC can all benefit fast responses for future lookups by all Kerberos clients.

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 KREALM records helps both the Kerberos client and its KDC to focus on those realms for which a service ought to have a name defined. This limits the list of potential realm names 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.

The definition of KREALM records under a domain rather than under a server host name (for cases where a choice exists, such as for applications that use SRV or MX records) should give less potential realm names, because the domain is closer to the client's domain/ realm than the server might be.

Limiting the length of the list of possible ticket requests to try 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.

6. Privacy Considerations

The information contained in a KREALM record for a domain is barely more than the domain's DNS name already holds; the KREALM record spells out the case-sensitive realm name, and implies the use of Kerberos. The use of Kerberos is usually also implied by the presence of certain SRV records.

The KREALM records also mark the names of Kerberised servers. Internal use may prohibit such disclosure, but in those use cases it is often possible to rely on existing mechanisms for guessing a realm name, including simply using the realm name under which a client logged on with Kerberos.

7. Security Considerations

There is no restriction for KREALM records to mention realm names that map back to DNS names in a disjoint part of the DNS hierarcy. The records could therefore specify realm names for a service even if the service is not recognised by the realm. The KDC for the appointed realm would be very clear about that when trying to procure a service ticket, so there is no security issue with such misguided use of KREALM records.

The general point is that the use of DNSSEC makes us rely on the party that publishes the KREALM record, and that party could specify improper realm names or drop realm names that are vital to the client. This is not expected to be a security risk either; the party publishing the KREALM record is the same party that publishes the service's records, namely the DNS operator. By publishing the service's record in DNS, this operator already has potential control over service denial and other MITM-type attacks, so the KREALM record does not add any new abusive powers.

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 strictly requiring DNSSEC for all KREALM records.

8. IANA Considerations

This specification defines a new "Resource Record (RR) Type", to be registered in the 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 name".

9. References

9.1. Normative References

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, DOI 10.17487/RFC1035, November 1987, <http://www.rfc-editor.org/info/rfc1035>.

[RFC2782] Gulbrandsen, A., Vixie, P., and L. Esibov, "A DNS RR for specifying the location of services (DNS SRV)", RFC 2782, DOI 10.17487/RFC2782, February 2000, <http://www.rfc-editor.org/info/rfc2782>.

[RFC3597] Gustafsson, A., "Handling of Unknown DNS Resource Record (RR) Types", RFC 3597, DOI 10.17487/RFC3597, September 2003, <http://www.rfc-editor.org/info/rfc3597>.

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, DOI 10.17487/RFC4033, March 2005, <http://www.rfc-editor.org/info/rfc4033>.

[RFC4120] Neuman, C., Yu, T., Hartman, S., and K. Raeburn, "The Kerberos Network Authentication Service (V5)", RFC 4120, DOI 10.17487/RFC4120, July 2005, <http://www.rfc-editor.org/info/rfc4120>.

[RFC4343] Eastlake 3rd, D., "Domain Name System (DNS) Case Insensitivity Clarification", RFC 4343, DOI 10.17487/RFC4343, January 2006, <http://www.rfc-editor.org/info/rfc4343>.

[RFC6806] Hartman, S., Ed., Raeburn, K., and L. Zhu, "Kerberos Principal Name Canonicalization and Cross-Realm Referrals", RFC 6806, DOI 10.17487/RFC6806, November 2012, <http://www.rfc-editor.org/info/rfc6806>.

9.2. Informative References

[RFC3655] Wellington, B. and O. Gudmundsson, "Redefinition of DNS Authenticated Data (AD) bit", RFC 3655, DOI 10.17487/RFC3655, November 2003, <http://www.rfc-editor.org/info/rfc3655>.

[RFC4592] Lewis, E., "The Role of Wildcards in the Domain Name System", RFC 4592, DOI 10.17487/RFC4592, July 2006, <http://www.rfc-editor.org/info/rfc4592>.

[RFC6840] Weiler, S., Ed. and D. Blacka, Ed., "Clarifications and Implementation Notes for DNS Security (DNSSEC)", RFC 6840, DOI 10.17487/RFC6840, February 2013, <http://www.rfc-editor.org/info/rfc6840>.

Author's Address

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

Email: rick@openfortress.nl