



Vouch By Reference Guide for Certification Providers

The Domain Assurance Council
November 2007

The Vouch By Reference (VBR) protocol allows certification providers to serve as sources of certification information for mail senders. For this certification information to be available to receivers, two things must happen:

- The sender must include a VBR header in outgoing messages that include information on the certification providers who vouch for it
- The certification provider must make vouching information available through the DNS This document describes the second item.

Important note: Certification providers who use VBR must fully understand the semantics defined in the protocol. These are the definitions that your customers will expect you to adhere to.

Overview

The VBR protocol specifies that a recipient verifies incoming mail by doing a DNS lookup based on the information in the `VBR-Info` header of messages they receive. Those lookups go to the DNS servers of the vouching services the receivers trust.

Each DNS record used for VBR validation has the structure:

```
<vouched-for>._vouch.<provider>
```

where `<provider>` is the domain name of the certification provider, `<vouched-for>` and is the domain name.

The verifier sends a DNS request for a TXT record. If it receives a response, it looks for a string that matches the type that was specified in the `VBR-Info` header.

TXT Record Contents

The response is a TXT record that is a text string that is a space-delimited list of types that the certification provider vouches for. The types are listed in the protocol.

The order of the types in the text string is not important.

Using BIND to Distribute VBR Records

Different DNS server systems use different methods to add DNS records. The commonly-used BIND system uses text configuration files for each zone. This section shows two different methods for using BIND with VBR. Both sections have the exact same result to DNS users, but have different tradeoffs for the tools that you use to populate the files and possibly for the speed at which BIND reloads when you add or remove DNS entries.

Domain Assurance Council Vouch By Reference Guide for Certification Providers

In this section, the certification provider has the domain name "exampletrust.com".

Large named.conf, Small Zone Files

One way to set up BIND is to have a record for each requested name in the `named.conf` file. For example:

```
zone "somebank.com._vouch.exampletrust.com" { type master;
    file "db.somebank.com"; };
zone "newyork.biggrocery.com._vouch.exampletrust.com" { type master;
    file "db.newyork.biggrocery.com"; };
zone "atlanta.biggrocery.com._vouch.exampletrust.com" { type master;
    file "db.atlanta.biggrocery.com"; };
zone "phoenix.biggrocery.com._vouch.exampletrust.com" { type master;
    file "db.phoenix.biggrocery.com"; };
```

The zone files would then each have a single TXT record in them. For example, the `db.newyork.biggrocery.com` file would contain just one DNS record:

```
newyork.biggrocery.com._vouch.exampletrust.com. IN TXT "list"
```

Small named.conf, Large Zone Files

A second option is to have only a single entry in `named.conf`, but then have many records in each zone file. The `named.conf` file would have just a single line for the parent zone:

```
zone "exampletrust.com" { type master; file "db.exampletrust"; };
```

and many lines in the `db.exampletrust` file:

```
somebank.com._vouch.exampletrust.com. IN TXT "all"
newyork.biggrocery.com._vouch.exampletrust.com. IN TXT "list"
atlanta.biggrocery.com._vouch.exampletrust.com. IN TXT "list"
phoenix.biggrocery.com._vouch.exampletrust.com. IN TXT "list"
```

Best Practices

Certification providers must have reliable DNS servers that will respond to recipients' requests at all times. This means that a provider should have multiple DNS servers in geographically distant locations, and that each DNS server should be resilient enough, and have sufficient processing power and bandwidth, to adequately respond to senders' queries.

Be sure to match the time-to-live (TTL) of the TXT record with the amount of time you guarantee certification for the sender. Setting the TTL to a long value causes recipients to trust a sender during the entire life of that record, even if you later change the record (such as if a sender becomes untrustworthy). However, setting the TTL to a very short value causes recipients to have to come to your DNS server much more often, putting both a higher load on the server and needing more bandwidth. Thus, determining the tradeoff of TTL duration is important for any certification provider.