



Vouch By Reference Guide for Software Vendors

The Domain Assurance Council
November 2007

Vouch by Reference (VBR) is intended to be straightforward for software vendors to implement. In this document, we assume that the reader is familiar with the protocol specification and with whichever method they use to obtain a useful domain name (such as DKIM).

Message Sending Software

Most importantly, mail transfer agent (MTA) software that sends mail must be able to apply accountability to outgoing messages, such as by signing outgoing mail with DKIM.

Outgoing messages must also contain a `VBR-Info` header in each message. If the sender is using DKIM or DomainKeys, this header should be covered by the signature. If the software that prepares the mail doesn't provide the `VBR-Info` header, the MTA may have to add it. Note that all messages in a batch will typically have the same `VBR-Info` header.

Message Receiving Software

Mail receiving software that supports VBR, whether an MTA or mail user agent (MUA) must be able to look for a `VBR-Info` header, and if it finds one, check the VBR. The software needs to be configured with two things:

- The list of domain names of vouching services to use, and
- The list of message categories, which may be the same for all services or may be specific to each vouching service.

Depending on the application, it may treat all mail with valid VBR the same, or it may treat it differently depending on the vouching service and the mail category. For example, if one vouching service might authenticate senders of any opt-in marketing mail, while another might only authenticate transactional mail from banks, a user application might display different icons next to messages vouched by the different services.

Vouching Software

Vouching services publish their VBR authentication information in the DNS. They may use a standard DNS server such as BIND or tinydns, or might use a specialized server that used a database of vouching information to answer queries.

Since the query traffic provides a rough estimate of the amount of mail traffic the service is vouching for, it would also be useful if the server logged or counted the traffic for analysis.

It is important to be able to add and remove entries quickly, in case a client is found to be sending mail out of compliance. It's also important to be able to adjust the time to live (TTL) for entries. The TTL can depend on the likeli-

hood that the entry may need to be changed, the load the server can support, and the desired granularity of logging.