



Vouch By Reference specification

The Domain Assurance Council
November 2007

Version pro-18, 04/05/2007

VBR Specification Overview

Vouch By Reference, or VBR, is a protocol for adding third-party certification to email.

Specifically, VBR permits independent third parties to certify the owner of a domain name that is associated with received mail. VBR may be performed anywhere along the email transit path, by any capable receiving module, either within the handling service or by end-user software.

VBR accomplishes this with a two-part protocol:

- In the first part, a sender affixes VBR information to email messages. The VBR information says which domain certification services the sender believes will vouch for email traffic associated with that sender.
- In the second part, the receiver queries one or more certification services to obtain information about the identity that has been associated with a received message. This latter protocol uses the DNS to distribute the certification information.

A sender provides certification attestations through the use of a new RFC 2822 mail header field, "VBR-Info:". This header field contains the names of services that the sender claims will vouch for them, and the particular type of content of the message. A queried, third-party, DNS-based certification service can respond with a list of the types of message content they will vouch for, such as "transactional mail from example.com" and/or "all mail from example.org".

A prerequisite for successful VBR operation is validation of the identity associated with the message. VBR is based on the use of domain names as identifiers, and permits multiple methods of obtaining and validating domain names. The validation methods are described in the "Obtaining a useful domain name" section below.

The sender performs two steps:

1. Adds a VBR-Info header field to its message
2. Protects the message, as appropriate

A sender uses VBR to say which domain certification services the sender believes will vouch for a particular piece of mail. The certification service uses VBR to state which signatures it will vouch for. This protocol uses the DNS to distribute the certification information.

Use of the VBR-Info Header

A message may have multiple VBR-Info header fields. This means that in 2822 terminology, VBR-Info is a "trace header field" and should be added at the top of the header fields.

The content of the VBR-Info header is a list of three elements:

- The accountable domain
- The type of content in the message
- A list of domain names of services that the sender expects to vouch for the sender for that kind of content

The accountable domain is given as `md=` followed by a domain name. The content type is given as `mc=` followed by a string; the defined values of that string are found below. The list of services is given as `mv=` followed by a colon-separated list of domain names.

The syntax of the header is defined below.

Validation process

A message receiver uses VBR to determine certification status by following these steps:

1. Extracts the domain to certify and the type of message content
2. Verifies legitimate use of that domain using one or more authentication mechanisms as described herein
3. Obtains the name of a vouching service that it trusts, either from among the set supplied by the sender or from another source
4. Queries the vouching service to determine whether the vouching service actually vouches for that type of content for that domain.

The VBR-Info Header

The `VBR-Info` header has the following format:

```
VBR-Info: md=<domain>; mc=<type-string>; mv=<certifier-list>;
```

where `<domain>` is the domain being vouched for, `<type-string>` is the content type of the message, and `<certifier-list>` is a list of domain names of certification providers that the sender asserts will vouch for this particular message. The structure of the `<certifier-list>` is one or more domain names, with a colon (":") between each.

For example, assume that the signer has two companies who are willing to vouch for its transactional notices: `certifier-a.com` and `certifier-b.com`. The signer would add the following to the header of its outgoing message:

```
VBR-Info: md=somebank.com; mc=transaction; mv=certifier-a.com:certifier-b.com;
```

All three fields in the VBR-Info header are mandatory. In particular, there is no default for the `md=` domain.

Upper and lower case characters in a VBR-Info header are equivalent, although conventionally the fields are all in lower case. For upward compatibility, verifiers should accept the fields in any order and should ignore any fields other than the three defined here.

If a message has more than one VBR-Info header, verifiers should check each in turn or in parallel until either a satisfactory certifier is found or all the headers have been checked. All of the VBR-Info headers in a single message should have identical `mc=` values. The semantics of a message with non-identical `mc=` categories are undefined.

DNS Query

When a recipient wants to check whether a message is vouched for, it compares the list in the message to the list of services it trusts. For each service that is on the intersection of the two lists, it creates a domain name to look up that consists of the following DNS labels (from left to right):

- the domain name which asserts it can be certified
- `_vouch` (a string literal)
- the host name of the vouching service This domain name is queried for a DNS TXT record.

For example, if a message signed by `somebank.com` contained the VBR-Info header above, the receiver might look up either or both of the following names, depending on which vouching service it trusts:

```
somebank.com._vouch.certifier-b.com
somebank.com._vouch.certifier-a.com
```

If the DNS TXT record exists, it contains a space-delimited list of all the types that the server certifies. For example, the contents of the TXT record might be

```
transaction list
```

In the example above, the receiver checks whether or not either certifier vouches for "transaction" mail. That would be indicated by either of the following types: `all` or `transaction` (`all` indicates that the certifier vouches for all message types sent by the domain in question). If either of those types appear in either TXT record, the message is vouched for. Of course, the recipient must ignore services that it does not trust; otherwise, a bad actor could just add an authority that it has set up so that it can vouch for itself.

The name for the label `_vouch` was chosen because any domain name that includes it as one of its labels cannot be a valid host name. There will never be any accidental overlap with a valid domain name. Further, it is safe to create a rule that says that a TXT DNS record that comes from a domain name that includes a `_vouch` label will always have the structure defined in this document.

This query method relies on the considerable advantages of existing DNS efficiencies, reliability and experience. The lookup is very efficient, and certifiers can add and delete client records as quickly as they want. The lookup also leverages the DNS's negative caching (RFC 2308).

Types of message content

This section describes the types of content that can be vouched for. While the rest of the VBR specification is mostly technical and precise, describing the types of contents in mail messages is inherently open to interpretation. Thus, this section makes distinctions in as specific a way as possible, but the reader must understand that these semantic definitions can be interpreted in very different ways by different people.

Note that the values in the `mc=` element is self-asserted. The purpose of this element is for auditing. There will likely be cases where a certifier will vouch for one type of a sender's mail (such as transactional mail) but not another type (such as advertising). A sender who cannot get anyone to certify their advertising mail, but has a certifier for their transactional mail, might be tempted to cheat and mislabel it as transactional. The `mc=` element creates an the audit trail to help their certifiers catch such cheating and allow the removal of the certification for the transactional mail.

Currently, three types of content are defined. The Domain Assurance Council (DAC) may add additional types in the future, including adding vendor-specific types. DAC controls the names used in the VBR specification.

All

`all` means all mail from the sender.

List

`list` is the category for email sent to multiple recipients where each piece of mail is identical or is very similar to the others.

Transaction

`transaction` is the category for transactional messages. This is a response to a specific action of the user's, or a notice about an event in the user's account at the sender.

Vendor-specific types

Members of the Domain Assurance Council (DAC) can also create their own vendor-specific types with their own semantics. Members define their own semantics for their own types.

DAC expects that most mail will use the standard types of categories, but that some systems will use the vendor-specific types for particular mail between known parties. Recipients who do not care about the vendor-specific categories can just use the generic types, while recipients who want to use the vendor-specific types can do so as well.

The list of assigned vendor-specific types will be listed on the DAC membership list as they are assigned.

Obtaining a useful domain name

VBR relies on having a domain name that specifies "a party that is accountable for the message." This requires obtaining the domain name and possessing a strong basis for believing that the use of the domain name is valid, that is, that it has not been spoofed.

There are different ways to achieve this and this section discusses the allowed mechanisms.

DKIM

DomainKeys Identified Mail (DKIM, RFC 4871) defines an accountable identity by associating a domain name with the message. It provides assurance that the association is valid through a public-key-based authentication mechanism.

- When DKIM is the validation mechanism, VBR's `md=` must match the domain name taken from one of the DKIM-Signature header fields. If the DKIM signature contains an `i=` field, the domain name from that field is used; otherwise, the domain name from the DKIM signature `a=` field is used.
- The VBR-Info header field should be included in the set of header fields protected by DKIM to prevent a malicious party from changing the contents of the VBR-Info header or adding bogus VBR-Info headers.
- The VBR-Info header field should be added at the header immediately below the corresponding DKIM-Signature header field.

If the DKIM signature validates, the domain name taken from that signature is valid for use with VBR.

DomainKeys

DomainKeys (DK, RFC 4870) defines an accountable identity by associating a domain name with the message in the `a=` tag of the DomainKey-Signature header field. It provides assurance that the association is valid through a public-key-based authentication mechanism.

- When DomainKeys is the validation mechanism, VBR's `md=` must be the same value as the domain name found in the DomainKey-Signature `a=` parameter.
- The VBR-Info header field should be included in the set of header fields protected by DK to prevent a malicious party from changing the contents of the VBR-Info header or adding bogus VBR-Info headers.
- The VBR-Info header field should be added at the header immediately below the corresponding DomainKey-Signature header field.

If the DomainKeys signature validates, the domain in the `a=` tag is valid for use with VBR.

SPF

Sender Policy Framework (SPF) defines an accountable identity by using an existing message address and querying the DNS to discover whether it is valid for SPF use.

When SPF is the validation mechanism, VBR's `md=` must be the same value as the domain name in the `<reverse-path>` address that is in the SMTP MAIL command.

A domain is valid for use with VBR when the SPF process produces a "pass" result, but not when it produces a "neutral", "none", "softfail", or other result.

Sender ID

Sender ID defines an accountable identity by using an existing message address known as the Purported Responsible Address and querying the DNS to discover whether it is valid for Sender ID use.

When Sender ID is the validation mechanism, VBR's `md=` must be the same value as the domain name in the Purported Responsible Address in the message.

A domain is valid for use with VBR when the Sender ID process produces a "pass" result, but not when it produces a "neutral", "none", "softfail", or other result.