Verified-Hello SMTP extension
draft-vesely-vhlo-03

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on December 14, 2009.

Copyright Notice

Copyright (c) 2009 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents in effect on the date of publication of this document (http://trustee.ietf.org/license-info). Please review these documents carefully, as they describe your rights and restrictions with respect to this document.
Abstract

This memo defines an extension to the SMTP service that provides protocol support for weak authentication of SMTP clients. Weakly authenticated clients enjoy an intermediate level of trust: they have no relying privileges, but can attempt to deliver mail to local users, are whitelisted from some filters, and may receive DSNs as needed.

Note that this treatment is what SMTP recommends for all clients. However, most servers operate filters to limit spam, thereby affecting the reliability of the mail forwarding system. Verified-Hello recovers that reliability by providing for uncensored mail transmission in a framework where authenticated domains are responsible for the messages they send. In addition, support is provided for an extensible set of authentication mechanisms, so that they can be managed and branded.
Table of Contents

1. Introduction ................................................. 4
   1.1. Content filtering ........................................ 4
   1.2. Prime delivery ........................................... 4
   1.3. Domains, weak authorization, and branding ............... 5
   1.4. Requirements Language .................................... 7
2. Definition and Registration of the VHLO Extension ............ 7
3. Behavior of SMTP client and server ........................... 7
   3.1. Syntax of the VHLO command ............................... 8
   3.2. Server side checks on the Domain ....................... 9
      3.2.1. Greylisting check .................................... 9
      3.2.2. DNSBL check ......................................... 10
      3.2.3. SPF check ........................................... 10
      3.2.4. MX check ........................................... 10
      3.2.5. PTR and ‘iprev’ checks ................................ 10
      3.2.6. VBR check ........................................... 11
      3.2.7. DKIM check ........................................... 11
   3.3. Responses to the VHLO command ............................ 12
      3.3.1. Positive response .................................... 12
      3.3.1.1. VHLO parameter and MAIL FROM command ............ 12
      3.3.2. Transient error responses ............................ 13
      3.3.3. Negative responses .................................... 13
      3.3.4. Diagnosis of failed VHLO commands .................... 14
   3.4. Restrictions and further server side checks ............... 15
      3.4.1. MAIL FROM restriction ................................. 15
      3.4.2. VBR restriction ....................................... 15
      3.4.3. DKIM-Signature headers existence and verification .... 15
      3.4.4. Greylisting restrictions .............................. 16
4. Forwarding of messages accepted under VHLO .................... 16
5. Submission strategy ............................................ 17
6. IANA Considerations ............................................ 18
7. Security Considerations ........................................ 18
8. References ..................................................... 19
   8.1. Normative References ..................................... 19
   8.2. Informative References .................................... 20
Appendix A. Examples .............................................. 20
   A.1. Prime delivery message transfer .......................... 20
   A.2. Failure after DNSBL check ................................ 21
   A.3. Failure on the MAIL FROM restriction check ............... 21
   A.4. Automatically finding a common vouching service .......... 22
   A.5. Reattempting Greylisted transmission ...................... 22
Author’s Address .................................................. 23
1. Introduction

1.1. Content filtering

Email Service Providers have to resort to content filters to limit the amount of spam. Such filters apply heuristic criteria, such as statistical analysis of the words in the message body, for determining a message’s worthiness. Messages that are deemed not worth the recipient’s attention, may happen to be delivered inside hidden or junk folders, or quarantined, so that the recipients will not notice them. (Reporting a delivery failure is not an option when the sender is not trusted, because the Return-Path is most likely forged.)

There has been a time when content filtering was considered a panacea. Until machines will be unable to properly understand the content of mail message, that assumption is to be considered deceiving. Even if machines could understand human language, having to undergo their censorship may be inadvisable. In addition, the reasons why users may not want to read a mail message vary widely, and no definition of spam has been universally agreed upon. Hence, discarding spam conflicts with reliability, and using content filters to detect spam worsen that even more.

This is not to say that content filters are useless. There are several situations where they can be used without affecting overall reliability, e.g. to discern messages so as to deliver them to different persons in a given group, or to different folders in a user’s mailbox. The relevant point is that those filters fail every now and then, therefore their use is safe only when the recipients can easily cope with those failures. Content filtering can be safely used to determine which persons and/or folders a message is delivered to, because a human will eventually read the message and correct any filtering malfunction. When content filtering is used to reduce spam, it is important to be aware that the reliability of the channel is also reduced. As an alternative channel, Verified Hello is more reliable because it avoids content filtering.

1.2. Prime delivery

The term "prime delivery" is used to indicate that a message is not tagged as spam, quarantined, silently dropped, or delivered in junk folders. A junk folder is one from where unread messages are normally deleted, or moved to another junk folder, without human intervention. In addition, prime delivery implies that the message is not edited by changing or altering its headers so as to make it less visible or discourage users from displaying its content.
Prime delivery implies strict [RFC5321] conformance, rather than mere acceptance of the message. In case the message has to be forwarded to another internal or external server, its transmission SHOULD attempt to preserve the trust and reputation that was granted on acceptance, as detailed in Section 4. Failure to relay MUST be reported as indicated by [RFC5321].

End users may operate their own content filtering. They can do so within their clients, or setting up their own filtering recipes within per-user sections of the Mail Delivery Agent configuration; there is a twilight zone here, between the delivery MTA and the end user. Of course, an MTA cannot control what each user does. Therefore, prime delivery only concerns stock filters that operate for all users. In case users can configure their mailboxes by making on/off decisions about specific content filters, implementing prime delivery involves dynamically turning off the relevant filters. For the sake of reliability, the delivery agent SHOULD ensure that prime delivery is consistently flagged by Authentication Status [RFC5451] headers or similar, and administrators should educate their users on how to appropriately whitelist messages flagged as such.

1.3. Domains, weak authorization, and branding

DNS domain names are delegated to organizations (or individuals) who control the relevant DNS setting. While in general a domain is not required for sending email messages, Verified Hello provides for a framework where only messages sent on behalf of an authenticated domain are accepted. In this respect, this extension is only useful for relaying messages across domain boundaries, thereby complementing the Message Submission [RFC4409] extension. To do email, an organization also controls a set of hosts connected to the Internet through one or more IP addresses. In this memo, we assume that the hosts operating for a given domain do so on behalf of the organization who owns the domain, and is responsible for the messages it sends. We also assume that these hosts share the same policies and are possibly coordinated with one another. In the simple cases, the relevant organization corresponds to the registrant name in whois databases records for both the domain name and the IP addresses. In general, privacy concealments and virtual hosts complicate this topic enough to discourage easy categorizations. At any rate, domain names can be used as a brand, and reputation records based on them last longer than those based on IP addresses.

Global communications require that SMTP servers accept mail coming from unknown hosts. This requirement rules out strong authentication schemes, because, by definition, it is not possible to authenticate unknown entities. Historically, Internet protocols granted some trust to any host, since sporting a global IP address was deemed a
sufficient credential. When more restrictive criteria became
required, a number of mechanisms have emerged for identifying the
sender. DNS and rDNS are used to check the relationship between the
sender’s IP address and its domain. However, using EHLO, the
sender’s domain can only be guessed at. Some mechanisms, e.g. rDNS,
are not universally available, and, although good senders try and
facilitate the identification of themselves by setting up DNS as well
as they can, receivers provide no feedback on their effort. Since
senders don’t know which mechanism, if any, would satisfy the
requirements of a given server, they can only follow generic
guidelines, outdated static policy pages, and rare support team’s
hints whose validity is not imperishable. This extension promotes
those identification mechanisms to weak authentication schemes by
explicitly requiring the domain name of the organization responsible
for sending, and providing feedback from the receiving server to the
sender.

Letting a sender know which mechanism failed is a risk only in case
of security through obscurity. Mechanisms that are secure by design
don’t have to be kept secret. The mechanisms considered in this memo
only involve DNSBL, SPF, MX, PTR, VBR, and DKIM. However, Verified
Hello provides for extensibility of this authentication/reputation
(auth-rept) mechanisms base. Giving feedback is important for
mechanism management, as it allows popular mechanisms to gain
potential. In addition, some mechanisms reference a different domain
that makes explicit assertions about the reputation of the sender’s
domain. This is where the branding practice comes into play. As the
number of domains that give reputation indications may grow much more
quickly than the number of mechanisms, feedback is specially
important for spreading their popularity. In this respect, Verified
Hello is not yet another authentication mechanism. It is a framework
for managing those mechanisms.

Currently, there is a few number of giant ESPs who host the mailboxes
of roughly one half of the global email users community. Obviously,
they work hard for ensuring cute anti-spam filtering, and first class
deliverability. In order to avoid hassles, several small MTAs are
configured to use one of those giant ESPs Mail Submission Agents
(MSAs) as smart hosts. One collateral advantage of using Verified
Hello is that falling back to smart hosts can be confined to specific
cases, depending on the outcome of the weak authentication process.
The postmasters of a sending domain can resort to smart hosts while
they collect feedback. Then, for the increased privacy and
efficiency that direct delivery yields, they’ll have the ability to
select what combination of mechanisms and brands will satisfy the
majority of their targets, and decide to implement those
requirements.
Finally, Verified Hello attempts to ease Greylisting.

1.4.  Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

2.  Definition and Registration of the VHLO Extension

According to [RFC5321] provisions, the definition for this extension goes as follows:

- the textual name of this extension is "Verified Hello";
- the EHLO keyword associated with the extension is "VHLO";
- the parameter associated with the EHLO keyword is a random value up to 16 octets long (see Section 3.3.1.1);
- this extension defines one additional verb, VHLO, whose only mandatory parameter is the Domain name of the sender, possibly followed by one parameter for each reputation tag (see Section 3.1);
- VHLO is also defined as one additional parameter to the MAIL verb (see Section 3.3.1.1), no parameters are defined for the RCPT verb;
- supporting the extension affects the behavior of a server and client SMTP as described in Section 3; and
- the maximum length of the MAIL command is increased by 22 octets, while the RCPT command is not affected.

Finally, as required by [RFC4409], this extension is NOT RECOMMENDED on the Submission port.

3. Behavior of SMTP client and server

The VHLO command is used by a client to request prime delivery of messages. If the server accepts the command by giving a positive response (see Section 3.3.1), all messages transmitted thereafter until either the end of the session or a further successful VHLO command are considered in the framework of the former VHLO command.
An SMTP client MAY issue the VHLO command as part of a session
initiation, before initiating a mail transaction. That is to say,
right after the EHLO command, or instead of it. (In the latter case,
of course, the client has to infer that the server supports this
extension by some other means.) Clients MAY attempt the VHLO command
various times with different parameters, as long as the receiving
server allows further retries (see Section 3.3.3). Clients failing
to issue a successful VHLO command MAY rely on the EHLO command
instead. If the server supports VHLO and issued reply codes 550 or
553, and the client’s configuration includes a list of alternative
MSAs, the client SHOULD relay through an alternative MSA.

After successfully transmitting one or more messages in the framework
of a successful VHLO command, a client MAY issue another VHLO command
to transmit more messages. Changing framework is required when new
messages are transmitted on behalf of a different Domain, or with
different VHLO parameters.

The receiving server MUST ensure prime delivery of the messages
accepted in the framework of a successful VHLO command. These
messages are subject to MAIL FROM restriction, and, possibly, to
DKIM-Signature headers existence and verification, VBR restriction,
and Greylisting restrictions (see Section 3.4).

3.1. Syntax of the VHLO command

The only mandatory argument to VHLO is Domain. The syntax is as
follows:

vhlo            = "VHLO" SP Domain *( SP auth-rept-claim) CRLF
auth-rept-claim = auth-rept-tag [ ":" tag-spec-param ]
auth-rept-tag   = "GID" / "MX" / "PTR" / "VBR" / "DKIM" / further-tag
tag-spec-param  = gid-param / vbr-param / dkim-param / further-param

where the Domain is the fully-qualified DNS domain name delegated to
the entity or organization that is responsible for sending the
message(s) that will be transmitted in the framework of this command.
Note that, unlike the EHLO command, the Domain is not necessarily the
host name of the SMTP client.

The maximum line length of the VHLO command is 1000 octets, including
the terminating CRLF.

The GID auth-rept-tag and its associated gid-param SHOULD be supplied
in the special cases described in sections Greylisting check, and
Greylisting restrictions.

The remaining arguments MAY be supplied to authenticate the domain name or provide hints for its reputation. These arguments are supplied spontaneously by the client, up to the maximum line length.

3.2. Server side checks on the Domain

The receiving server SHOULD check that the supplied domain is valid and reckon its reputation.

The server is not limited by the checking methods indicated in the parameters. In particular, it is RECOMMENDED that DNSBL, 'iprev', and SPF checks are carried out anyway. While this section indicates circumstances for the failure of each single check, it is up to the local policy to establish what combinations of successful checks yield positive responses.

Some circumstances may require to terminate a VHLO framework and start a new one, with varied Domain or parameters. Typically, only a part of the checks need to be carried out again.

3.2.1. Greylisting check

The GID auth-rept-tag provides the value of a VHLO framework that had been given by this same server or a related MX during a previous SMTP session:

\[
\text{gid-param} = \text{original-vhlo-string}
\]

The receiving server SHOULD check that the original-vhlo-string corresponds to the value that it or a related MX has given as random-string in response to a successful VHLO command. Use of the GID auth-rept-tag is reserved for retrying the transmission of messages that suffered a transient failure in the framework of the corresponding VHLO command, as described in section Section 3.3.1.1.

If the server applies Greylisting, it MAY use the provided gid-param, if supplied, as an additional key to a group of messages, besides other data items used to implement Greylisting. If using this parameter, the server MUST still check that the other data items correspond, and that the sender accomplishes the directives described in Greylisting restrictions.

The server SHOULD NOT issue a negative response for improper usage of this parameter. However, if bad faith can be ascertained, the server MAY add that knowledge to the sending Domain’s reputation. On the other hand, using this parameter eases the task of verifying that a
Domain’s servers adopt a regular retrying behavior. Such knowledge MAY also be added to the Domain’s reputation. It is RECOMMENDED that Domains with enough reputation are whitelisted from Greylisting.

3.2.2. DNSBL check

The server SHOULD check any relevant DNSBL, and, if a DNSBL that the server, according to its policy, considers trustworthy for either rejecting messages or degrading their worthiness, gives a positive match, then the server SHOULD issue a negative response. See [I-D.irtf-asrg-dnsbl] for details on this check.

3.2.3. SPF check

If the server carries out SPF checks, it SHOULD check the supplied Domain using the method described in [RFC4408], and, if that results in a "fail", the server SHOULD issue a negative response. According to its policy, the server MAY issue a negative response when the result is anything but "pass".

Note that the so-called "helo check" often gets a result of "none" because [RFC4408] does not provide for SPF (or TXT) RRs to be valid for a whole zone, and many hostmasters omit to define an SPF policy for each host. Unlike EHLO, the Domain argument taken by VHLO points to the sending domain, not the host. Because of the MAIL FROM restriction, no further SPF checks are required for transactions in the framework of this VHLO command.

3.2.4. MX check

The MX auth-rept-tag suggests that the client is connecting from an IP address that belongs to one of the Domain’s MX servers. The receiving server SHOULD lookup the MX records of the given Domain and successively lookup the addresses (A or AAAA depending on the connection) of each of the hosts listed therein, until it finds a matching address or the list is exhausted. If no match was found, the server SHOULD issue a negative response.

3.2.5. PTR and ‘iprev’ checks

The PTR auth-rept-tag suggests that the client is connecting from an IP address that can be resolved backward to an host name under the given Domain’s hierarchy. Note that this also works for Top Level Domains or branches of ccTLDs who run no mail services, hence the added delegation check.

The receiving server SHOULD lookup the PTR records for the connecting address and verify that at least one of the returned RRs contains a
host name whose rightmost part matches the Domain. In addition, the
authoritative Name Server for the Domain must match the NS for the
host name thus found; that is, the Domain and the sending host share
the same NS. If no match was found, the server SHOULD issue a
negative response.

The server SHOULD also check that the name found thereby resolves
forward, possibly through a CNAME, to the connecting address, as
indicated by the ’iprev’ Authentication Method described in
[RFC5451].

3.2.6. VBR check

The VBR auth-rept-tag provides a list of vouching services:

vbr-param       = [ "mc=" type-string ";" "mv=" ] certifier-list
certifier-list  = domain-name *( ":" domain-name )

The receiving server SHOULD carry out the VBR validation process as
it would be done for a VBR-Info header containing the corresponding
elements, see [RFC5518].

3.2.7. DKIM check

The DKIM auth-rept-tag asserts that all messages transmitted in the
framework of this VHLO command (in case it is successful) have a
DKIM-Signature header whose domain (d) or identity (i) tag matches
the Domain in the VHLO command. The parameter contains additional
properties of such signatures:

See [RFC4871] for imported ABNF

dkim-param      = sig-s-tag *( ";" sig-tag )

where the sig-s-tag is the s=selector string, while the optional sig-
tag’s are selected parts of the DKIM-Signature header. Note that the
parameter MUST NOT contain any whitespace, although it is allowed in
the signature header. At least the sig-s-tag for the selector (and
the sig-q-tag if a query method different than "dns/txt" is used)
MUST be provided. The algorithm (a) and the header list (h) tags
might also possibly be used by the server to reckon reputation.

The receiving server MAY fetch the public key required to verify the
DKIM signatures. If the key does not exist, the server SHOULD issue
a negative response.
3.3. Responses to the VHLO command

An organization’s servers accept incoming mail messages according to some policies. The requisites for according a positive reply to a VHLO command SHOULD NOT be less strict than those for accepting an incoming message. In particular, if a policy states that certain conditions imply that a message would be accepted with some reserves, it should likely state that VHLO is denied under the same conditions.

When processing the optional auth-rept-claim’s parameters, the server MUST ignore any parameter whose tag it does not support or understand.

In case of unsuccessful response, the server retains its previous state.

3.3.1. Positive response

If the checks carried out on the Domain and the connection indicate that the server will wholeheartedly accept messages from the client, the server returns a 250 reply code. The response is a multi-line response with the same format as the EHLO response (ehlo-ok-rsp in [RFC5321]), with the keywords for all the SMTP extensions available as a consequence of entering this VHLO framework.

Upon a positive response, the client MUST reset any flags and variables associated to SMTP extensions that it may have since previous EHLO or VHLO commands in the same session.

3.3.1.1. VHLO parameter and MAIL FROM command

The server response to the VHLO and EHLO commands includes the VHLO keyword along with a randomly generated token of up to 16 octets. The format of the relevant line is as follows:

```
ehlo-line       = "VHLO" SP random-string
random-string   = 1*16( %d33-60 / %d62-126 )
                ; any CHAR excluding ";", SP, and control
                ; characters.
```

The random string supplied by the server MUST be repeated by the client as the value of the VHLO parameter to the MAIL command, for each transaction in the framework of this VHLO command. This is meant to guard against blind attacks and to ease Greylisting checks.
3.3.2. Transient error responses

If the server is temporarily unable to carry out any required check on the Domain, it SHOULD return the 451 reply code. Then, the client SHOULD quit the session and retry at a later time.

The server MAY return the 450 reply code to indicate that it is not able or willing to reckon the client’s reputation during this section, irrespectively of any parameter supplied. In this case, the client MAY try an EHLO command instead, to transmit messages outside of any VHLO framework.

The server MAY return the 455 reply code to indicate that it is temporarily unable to carry out the checks implied by one or more specific parameters. It is possible that a positive response is given if the client repeats the command using different auth-rept-claim’s or different tag-spec-param’s. The text of the response SHOULD indicate the missing parameters as described in Section 3.3.4.

3.3.3. Negative responses

If the server cannot grant prime delivery because of a missing parameter or parameter’s value in the VHLO command, it SHOULD return the 555 or 550 reply codes indicating the missing parameters and arguments as described in Section 3.3.4.

The server MAY return the 553 reply code to indicate that it will never grant prime delivery for the given Domain to the current client, whatever auth-rept-claim’s the client may supply.

The server MUST return the 503 reply code (bad sequence of commands) if a VHLO command is issued while a transaction is active.

The server MAY also return the 500 or 502 reply codes to indicate that it does not support this extension.

After a 555 reply code, the client MAY retry a VHLO command with the parameters modified accordingly. Otherwise, if it is unable to satisfy the server requirements, the client SHOULD proceed as if it obtained a 500 reply code. It is RECOMMENDED that the client application logs the missing requirements, so that administrators know how to gain access to the given server.

After reply codes 500, 502, 550, and 553, the client MUST NOT attempt more VHLO commands during the current session. In addition, after reply codes 550 and 553, the client SHOULD NOT ever attempt any further VHLO command to an MX server of the current target for the given Domain; this implies caching the domains pair in a buffer that
will be cleared by either configuration updates or overrun.

After reply codes 500, 502, 550, 553, and 555, the client MAY quit the session and send the message through an alternative relay as described in Section 5. Alternatively, the client MAY try an EHLO command instead, to transmit messages outside of any VHLO framework.

3.3.4. Diagnosis of failed VHLO commands

Normally, a client supplies all the claims that can possibly result in increased reputation, except for line length limitations. VBR’s certifier-list’s, for example, might grow quite long and clients may be unable to store them on a single line. However, servers can issue multi-line responses containing the complete list, so that a client can select the correct certifiers to include in the next attempt. As some failures can be worked around automatically, failure responses SHALL contain both human readable text and machine readable text. Formally:

```
Failure-resp    = *( Failure-code "-" [ diag-text ] CRLF )
Failure-code    = %x34-35 %x30-35 %x30-39
diag-text       = [ hread-text ] [ ":" mread-text ]
head-text       = *( %d09 / %d32-57 / %d59-126 )
; regular characters except "":"
mread-text      = auth-rept-claim / check-failed
check-failed    = check-keyword ":" check-spec-info
cHECK-keyword   = "DNSBL" / "VBR"
check-spec-info = hread-text
; a domain name for VBR,
; a domain name, or URL replacing any "":"", for DNSBL
```

A server SHOULD NOT vary its requirements during a given session.

If a client manages to issue a successful VHLO command for a given Domain after a previous attempt failed, it MAY store the parameters for future reuse. However, the server requirements MAY be changed in future sessions.
3.4. Restrictions and further server side checks

Messages transmitted in the framework of a successful VHLO command are subject to the restrictions detailed in this section. Clients MUST NOT attempt to break these restrictions. Servers SHOULD check that clients comply.

3.4.1. MAIL FROM restriction

Non-empty arguments of the MAIL FROM commands are restricted to addresses whose domain part is compatible with the Domain given in the relevant VHLO command. Compatible here means that either the two domains names are identical, or they share at least one primary mail exchanger.

Formally, the two domain names match a caseless comparison; or one [or both] of them is a CNAME label of a DNS RR whose value eventually refers to the other [or, respectively, a common canonical name]; or the two domain names, after resolving any CNAME aliasing, both have MX RRs and the respective lists of primary (lowest preference) hosts have a common element, i.e. two host names that match a caseless comparison. Note that no IP address comparison is involved.

In addition, the server MUST check that the VHLO parameter is included and that the corresponding value matches the random string that the server generated on giving the positive response to the VHLO command.

3.4.2. VBR restriction

If the VHLO command in whose framework the message is received contained a VBR tag, the message MAY have a VBR-Info header. If that header is present, it MUST be compatible with the given vbr-param. Compatible here means that it mentions at least the certifier that the server trusts and verified before accepting the relevant VHLO command.

If a VBR-Info header is not present, the receiving server MAY add one based on the Domain given, the certifiers it trusts and verified, and its guess of the type of content.

3.4.3. DKIM-Signature headers existence and verification

If the VHLO command in whose framework the message is received contained a DKIM tag, the message MUST have a DKIM-Signature header compatible with the given dkim-param. Compatible here means that the domain (d) of the DKIM-Signature is the same, the selector (s) is the same one given in the parameter, the signed header fields in the
DKIM-Signature contain at least the ones given in the parameter, and the signing algorithm given in the parameter, if any, matches the one actually used.

In addition, if the server verifies signatures on the fly, the verification fails, and such failure would prevent the message from having a prime delivery, the server SHOULD reject the message instead.

3.4.4. Greylisting restrictions

If transmission of a message in the framework of a VHLO command fails due to transient conditions (4xx reply codes), and the transmission was not itself a retry, the sending server SHOULD annotate the current VHLO parameter in the message’s meta data while it queues the message for further retries. We refer to this piece of data as original-vhlo-string. Typically, a message’s meta data includes the envelope and possibly the failure reason, and is used by a server to devise a sending strategy as described in section 4.5.4.1 of [RFC5321]. (Note that we are talking about transient failures in the transmission of a message, i.e. after MAIL, RCPT, DATA, or data completion by <CRLF>.<CRLF>; not the VHLO command.)

The current VHLO parameter should be added to meta data only after the very first failure; in particular, not if a previous attempt to transmit the message has happened before, whether in the framework of a VHLO command or not. This implies that use of VHLO is restricted to hosts who are able to discern new messages from retried attempts.

When attempting to retransmit a queued message that has this original-vhlo-string in its meta data, the sending client SHOULD transmit such string using the GID auth-rept-tag with

\[
gid-param = \text{original-vhlo-string}
\]

Only messages that share the same original-vhlo-string may be transmitted in the framework of a VHLO command that used the GID auth-rept-tag with that value. This implies that the sending client MUST terminate the current VHLO framework in case the next message’s original-vhlo-string differs from the gid-param used to establish it (where no gid-param matches an empty original-vhlo-string.)

4. Forwarding of messages accepted under VHLO

A message accepted in the framework of a VHLO command deserves prime delivery. However, the receiving server possibly does not host the mailboxes of the relevant recipients directly. For example, it may
be a boundary or secondary exchanger, a vanity address server, or it may be following user-specific forwarding instructions. For this specification, we just distinguish if the message is forwarded within the same organization or to an external domain.

If the message is forwarded internally, all hosts MUST be configured so as to honor the promise of prime delivery that border or secondary exchangers grant on their behalf. If, for whatever reason, prime delivery is not possible, a failure notification MUST be sent to the Return-Path address, if any. Even if sending notifications is expected to be fairly safe at this point, it is RECOMMENDED that any organization-wide policy that can be applied on acceptance produces an on-line rejection rather than a delayed failure notification.

If the message is forwarded to an external domain, the SMTP client MUST attempt to issue a VHLO command, unless either it can determine that the target host does not implement this SMTP extension, or it has some other arrangement with the target host that grants prime delivery (e.g. using \[ff\]). Note that, if VHLO is used for forwarding, unless the forwarder is an authorized sender for the original Domain, the Return-Path MUST be changed (e.g. using \[srs\]).

5. Submission strategy

Small and medium organizations may lack the global reputation that would ensure high deliverability to their SMTP relays. To increase the deliverability of their messages, they may use an MSA from a larger organization. However, privacy concerns and mail flow optimization would suggest to resort to external MSAs only when that is necessary for message deliverability.

The VHLO command, by allowing to check deliverability in advance, enables clients to use smart hosts optionally. Rather than configuring a fixed mail out path for certain target domains, relays can dynamically adjust their strategy according to the target host’s response to the VHLO command. The list of preferred VBR certifiers provided by a negative response may be used as keys to build a corresponding list of smart hosts that can be used as Mail Submission Agents, provided that the certifiers of each smart host are known.

To implement this strategy, a relay’s configuration needs a list of alternative MSAs, consisting in one or more entries containing a host name, a username/password pair, and an optional list of VBR certifiers of that MSA. Other means to dynamically select an MSA, and how to determine the default one should also be provided for.
6. IANA Considerations

This extension will have to be inserted in the mail-parameters assignments IANA registry. The keyword VHLO may appear

- as a service type (possibly),
- as an SMTP extension keyword, and
- as an SMTP extension keyword that has a parameter.

(Apparently, there is no registry of the MAIL command parameters that are used by various extensions.)

A registry is needed for tracking the auth-rept-tag / check-keyword that must be unique in the diagnostic text. This document defines

- DKIM
- DNSBL
- GID
- MX
- PTR
- SPF
- VBR

7. Security Considerations

This document proposes an intermediate level of trust. An SMTP client is being authenticated based on weak evidence, originating from the DNS and the TCP layer:

- The IP address of the remote client is known from the TCP layer. Verification of the random string implies it is fairly difficult to forge it.
- Any of the MX, PTR, or SPF checks confirms that the IP address is somehow authorized by the organization who owns the Domain.
- The DNSBL check implies that the IP address is not that of a known attacker.
The two remaining checks, DKIM and VBR, may provide two additional characterizations of the messages being transmitted. DKIM ensures that messages have passed through the domain’s signing process, which presumably implies that any sender’s local policy has been enforced. In this respect, DKIM is most useful if the sending organization does not have a fine grained control on their PTR, MX, or SPF settings.

VBR, depending on the certifier’s policy, may generically ensure that the sending domain is well behaved. A vouching service may scrutinize the DNS settings of a given domain, check their spam rate using honeypots, investigate the domain’s users, or otherwise establish the domain reputation. The possibility to communicate the preferred vouching services may work as an incentive for the advertised service providers.

The authentication provided by this extension is weaker than SMTP Authentication [RFC4409]. Therefore, it SHOULD NOT be used instead of it.

Diagnostic messages provided with negative responses to the VHLO command may disclose acceptance policies of the target domain. This is not considered harmful, since such policies are usually public. However, in case the security structure depends on keeping that information secret, the server should carefully consider what diagnostic messages it provides to what clients. It is possible to provide VHLO services to selected domains only, and discarding the rest with the reply code 553.

8. References

8.1. Normative References


8.2. Informative References

[I-D.irtf-asrg-dnsbl]
Levine, J., "DNS Blacklists and Whitelists",
draft-irtf-asrg-dnsbl-08 (work in progress),
November 2008.

[ff] FixForwarding.org, "solution proposed", 2009,


[srs] Libsrs2.org, "libsrs2 - Home", 2004,
<http://www.libsrs2.org/>.

Appendix A. Examples

Some examples showing the relevant snippet of client-server dialog.

A.1. Prime delivery message transfer
Complete example where the client successfully transfers a message

S: 220 example.com SMTP server ready
C: VHLO example.net
S: 250-example.com greetings example.net
   250 VHLO 0123456789ABCDEF
C: MAIL FROM:<author@example.net> VHLO=0123456789ABCDEF
S: 250 Ok
C: RCPT TO:<dest@example.com>
S: 250 Ok
C: DATA
S: 354 Go ahead
   This is transmitted with prime delivery!
   .
S: 250 Ok
C: QUIT
S: 221 Bye

A.2. Failure after DNSBL check

Colons have been replaced in the automatic message to formally
preserve machine readability

C: VHLO example.net
S: 555-You are blacklisted
   555 :DNSBL:see http://www.dnsbl.example/query/bl?ip=192.0.2.3
C: QUIT
S: 221 Bye

A.3. Failure on the MAIL FROM restriction check

In this snippet, the domain names are mismatched

C: VHLO example.net
S: 250-example.com greetings example.net
   250 VHLO 0123456789ABCDEF
C: MAIL FROM:<user@example.org> VHLO=0123456789ABCDEF
S: 550 Domain origin mismatch
C: QUIT
S: 221 Bye
A.4. Automatically finding a common vouching service

In this snippet, the client finds a valid VBR name

C: VHLO example.net MX VBR:vouch1.example:vouch2.example
S: 555-we only accept these :VBR:vouch97.example:vouch98.example
     555-:VBR:vouch99.example:vouch100.example:vouch101:example
     555 :VBR:vouch102:example:vouch103:example:vouch104:example
C: VHLO example.net MX VBR:vouch100.example:vouch101.example
S: 250-example.com greetings example.net
   250 VHLO 0123456789ABCDEF

A.5. Reattempting Greylisted transmission
On a first attempt the client got greylisted

S: 220 example.com SMTP server ready
C: VHLO example.net
S: 250-example.com greetings example.net
   250 VHLO FirstTime
C: MAIL FROM:<author@example.net> VHLO=FirstTime
S: 250 Ok
C: RCPT TO:<dest@example.com>
S: 450 You are greylisted, retry after 5 mins.
C: QUIT
S: 221 Bye

... 5 minutes later ...

S: 220 example.com SMTP server ready
C: VHLO example.net GID:FirstTime
S: 250-example.com greetings example.net
   250 VHLO SecondTime
C: MAIL FROM:<author@example.net> VHLO=SecondTime
S: 250 Ok
C: RCPT TO:<dest@example.com>
S: 250 Ok
C: DATA
S: 354 Go ahead
S: From: author@example.net
   To: dest@example.com
   Subject: test

   This is transmitted after greylisting delay!

S: 250 Ok
C: QUIT
S: 221 Bye

Author’s Address

Alessandro Vesely
v. L. Anelli 13
Milano, MI 20122
IT

Email: vesely@tana.it