# draft-schwartz-add-ddr-forwarders-02

## Reputation Verified Selection of Upstream Encrypted Resolvers

Chris Box & Ben Schwartz, IETF 114

# You said, we listened

There were indications of support in the April adoption call, but also some valid points made that we agree needed thinking about:

*“Structure and flow quite confusing”*

*“Needs a normal introduction that explains what implementations should do”*

*“Defining a ‘relaxed validation’ policy that just says to ignore everything without telling people to read the functional/privacy/security problems and mitigations is very problematic”*

*“Using the network’s resolver without encryption would be better than … unverifiable upgrade alternative”*

*“I’d like to see more revision and clarity in what this document is actually proposing”*

*“Having trusted resolvers … far stronger than the ‘check again every five minutes’ approach”*

# The response: a significantly changed -02 draft

- No longer informational.
- Now proposes what clients should do.
- Requires the use of a reputation system to give an opinion on the discovered upstream resolver.
- Leaves the choice of reputation system to the client.
- Upgrades only occur if a green light is given.
- Hence has a new name: Reputation Verified Selection of Upstream Encrypted Resolvers

# How it works

1. The client begins DDR discovery, querying for _dns.resolver.arpa.
2. The legacy DNS forwarder, since it does not understand DDR, forwards this query upstream.
3. The upstream recursive resolver, which supports DDR, replies with details of how to access its encrypted DNS service.
4. The client receives this response and performs Reputation Verified Selection.
    - This verifies the identity of the offered encrypted service
    - And checks the reputation of this confirmed identity
        - For example checking an embedded list of known trusted resolvers
5. If the determined reputation meets the client's criteria, it may commence using encrypted DNS towards the upstream resolver. This is known as Cross-Forwarder Upgrade.

# Common issues with Cross-Forwarder Upgrade

If the local forwarder provides an essential blocking function (e.g. for malware), it should also be told to block cross-forwarder upgrade. Denying resolver.arpa achieves this.

Clients should be capable of detecting which names are part of a split horizon on the local network, so they can exempt those queries from cross-forwarder upgrade. For example .local, .home.arpa, and those learned via local domain hint mechanisms and validated. NXDOMAIN fallback can also be used.

# So RVS is entirely dependent on a built-in list then?

Embedding a list of known trusted resolvers in a client is only one possible model for assessing the reputation of a resolver.

In future a range of online reputation services might be available to be queried, each returning an answer according to their own specific criteria. These might involve answers on other properties such as jurisdiction, or certification by a particular body.

It is out of scope for the draft to define these query methods, other than to note that designers should be aware of bootstrapping problems.

It is the client's decision as to how to combine these answers, possibly using additional metadata (e.g. location), to make a determination of reputation.

# Why should I be interested in implementing this?

A large fraction, perhaps a majority, of residential internet users in the United States and Europe rely on local DNS forwarders that are not compatible with DDR because they are accessed via a private IP address. Many such devices also face significant hurdles in being upgraded to support encrypted DNS, so it is likely that a large installed base of legacy DNS forwarders, providing Do53 on a private IP address, will remain for some years.

DDR results in no encryption when a legacy DNS forwarder is present. This leaves the user's query activity vulnerable to passive monitoring [RFC7258], either on the local network or between the user and the upstream resolver.

It’s considerably quicker to enable encrypted DNS for a handful of ISP core network sites than to enable it for millions of legacy forwarders. Reputation Verified Selection enables the use of encrypted transport in these configurations, reducing exposure to a passive surveillance adversary for those running clients supporting this functionality.

# Some open questions we noted regarding the design

Would it be better to use the SVCB TargetName to select a single Resolver Identity? This would avoid the need to enumerate the certificate's names, but it would require the use of SNI (unlike standard DDR), and would not be compatible with all upstream encrypted resolvers.

Can we simplify the resolver identity to just a domain name? This would make reputation systems easier, but it would not allow distinct reputation for different colocated resolution services, so reputation providers would have to be sure that no approved resolver has other interesting co-located services.

# Questions for the working group:

- Is this draft better?
- Would it be beneficial to users?
- Can the design be improved?

# Backup slide: the detailed RVS procedure

Clients MAY use RVS when (a) the local DNS server is identified by a Private IP address and (b) the DDR SVCB resolution process does not produce any Encrypted DNS endpoints that have this IP address in their A or AAAA records. RVS then proceeds as follows:

1. The client connects to one of the indicated Encrypted DNS endpoints.
2. The client receives a certificate, which it verifies to a suitable root of trust.
3. For each identity (e.g. SubjectAltName) in the certificate, the client constructs a Resolver Identity:
    - For DNS over TLS and DNS over QUIC, the Resolver Identity is an IP address or hostname and the port number used for the connection.
    - For DNS over HTTPS, the Resolver Identity is a URI Template in absolute form, containing the port number used for the connection and path indicated by dohpath.
4. The client determines the reputation of each Resolver Identity derived from the certificate.
5. The maximum (i.e. most favorable) reputation is the reputation of this connection.