Network Working Group
Internet-Draft
Intended status: Informational
Expires: 3 September 2026

Wei Wang
CNNIC
Wenyong Wang
UESTC
Ting Yang
UESTC
Wenbin Luo
UESTC
Xingxing Yang
CNNIC

2 March 2026

Out-of-Band Discovery of Authentic Resolvers (ODAR)
draft-author-out-of-band-authentic-resolvers-00

Abstract

This document defines Out-of-Band Discovery of Authentic Resolvers (ODAR), a set of mechanisms for DNS clients to discover and authenticate a resolver’s identity via out-of-band channels. A resolver discovered in this manner is referred to as an "Authentic Resolver". These mechanisms can be used to authenticate a resolver when only its IP address is known, and to validate resolver identity information learned via other means. These mechanisms are designed for deployments in which the authenticity information is provided by the out-of-band channels, such as distributed systems, ARPA reverse domain name resolution systems, and InterPlanetary File System (IPFS). This document also clarifies the complementary relationship between ODAR and the Recursive-Identifier mechanism defined in RFC 9499, and specifies how the two mechanisms can be integrated to achieve end-to-end trusted identity transmission of recursive resolvers in the DNS system.

Table of Contents

1. Introduction

When DNS clients wish to rely on resolver identity, they often require information beyond the resolver's IP address, such as a stable resolver identifier, the resolver operator identity, and authenticated bindings between these identities and the resolver endpoints. However, common configuration mechanisms typically provide only an IP address, for example via DHCP [RFC2132] [RFC9915], IPv6 Router Advertisement (RA) options [RFC8106], or manual configuration. In such settings, identity information learned through the DNS resolution path can be unavailable or untrustworthy, since the client may need to depend on the very resolver it is trying to authenticate. ODAR addresses this gap by enabling clients to discover and authenticate resolver identity via out-of-band channels, including distributed systems and blockchains, as well as ARPA reverse domain name resolution systems [IANA-ARPA] and the InterPlanetary File System (IPFS) [IPFS] that are extended and customized for out-of-band authentication scenarios, and to use this information to validate resolver identity obtained through other means.

This document defines two mechanisms for clients to discover and authenticate Authentic Resolvers using out-of-band channels:

1. When only an IP address of a resolver is known, the client queries an out-of-band channel to obtain authenticated identity information and bindings for that resolver (Section 4).

2. When the name of a resolver is known, the client queries an out-of-band authenticity channel to obtain authenticated identity information and bindings for that named resolver. This can be used to validate resolver identity prior to selecting the resolver or establishing encrypted DNS (Section 5).

Both of these approaches allow clients to confirm that a discovered Authentic Resolver has identity information authenticated by the selected out-of-band channel. "Authentic" in this context means that the resolver identity is bound to the resolver endpoint by an authorized trust anchor for that channel; for example, the binding is attested by the resolver operator, or recorded in a verifiable distributed system such as a blockchain, or published in the customized ARPA reverse domain name resolution system or IPFS with signature authentication.

ODAR focuses on solving the trust establishment problem between DNS

clients and recursive resolvers through out-of-band channels, while the Recursive-Identifier mechanism defined in RFC 9499 [RFC9499] solves the node identification problem between recursive resolvers and authoritative servers through in-band EDNS0 extension. The two mechanisms are complementary and non-conflicting, and their integration can realize the full-link identity authentication and identification of recursive resolvers from clients to authoritative servers. This document specifies the integration principles and deployment methods of ODAR and RFC 9499 in Section 6.3.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

The following additional terms are used:

ODAR
: Out-of-Band Discovery of Authentic Resolvers. "ODAR" refers to the mechanisms defined in this document.

Authentic Resolver
: A resolver whose identity information and bindings to resolver endpoints are authenticated via an out-of-band authenticity channel. The authenticated bindings are provided under an authorized trust anchor for that channel.

Out-of-Band Authenticity Channel
: A channel independent of the DNS resolution path that provides verifiable authenticity information for resolver identity and endpoint bindings. Examples include verifiable distributed systems such as blockchains, customized ARPA reverse domain name resolution systems for out-of-band authentication, and the InterPlanetary File System (IPFS) with signature and content identifier (CID) verification mechanisms.

Resolver Identity Information
: Information used to identify a resolver and its operator, and to authenticate bindings between that identity and one or more resolver endpoints. This can include a stable resolver identifier, operator identity, and associated credentials.

Recursive-Identifier
: A mechanism defined in RFC 9499 [RFC9499] that enables a recursive resolver to carry its own identity identifier in DNS query messages to authoritative servers through the EDNS0 OPT option (OPTION CODE=10), for the purpose of traffic limiting, scheduling, and security policy enforcement by authoritative servers.

3. Out-of-Band Authenticity Information

ODAR authenticity channels can advertise one or more Authentic Resolvers whose identities are authenticated by an authorized trust anchor for the channel.

When a client discovers Authentic Resolvers, it learns identity information such as a resolver identifier, the resolver operator identity, and authenticated bindings to one or more resolver endpoints. Endpoint information can include IP addresses and, when applicable, resolver hostnames and parameters needed to establish DNS. The formatting of the authenticity information and the verification procedure are defined by the specification of the selected out-of-band channel. For ARPA reverse domain name resolution and IPFS, the authenticity information shall be packaged in a standard structured format, and the verification procedure

shall include signature validation, CID matching (for IPFS), or PTR record and associated resource record validation (for ARPA).

The following is an example of an authenticity object describing a DoH resolver endpoint:

```
resolver-id: odar:resolver:example-1
operator: Example Resolver Operator
endpoints: [ "https://doh.example.net/dns-query" ]
alpn: h2
attestation: sig(op-key, resolver-id || endpoints || alpn)
```

3.1. ARPA Reverse Domain Name Resolution for Out-of-Band Authenticity

The customized ARPA reverse domain name resolution system for ODAR is an extended out-of-band channel that is independent of the standard DNS forward resolution path. Resolver operators SHALL publish the signed authenticity object of the resolver in the dedicated ARPA reverse zone for ODAR, and bind the resolver's IP address to the PTR record pointing to the resolver identity and the TXT record storing the structured authenticity object (including resolver-id, operator, endpoints, alpn, and attestation). The authorized trust anchor for the ARPA channel is the DNSSEC key of the ODAR dedicated ARPA zone, and clients MUST verify the DNSSEC signature of the PTR and TXT records when querying the ARPA channel to ensure the authenticity of the resolver identity information.

3.2. IPFS for Out-of-Band Authenticity

IPFS serves as an ODAR out-of-band channel by storing the encrypted and signed resolver authenticity object in the IPFS network, with the object generating a unique Content Identifier (CID). Resolver operators SHALL publish the mapping between the resolver's IP/name and the corresponding CID through a trusted index service, and the authenticity object stored in IPFS MUST be signed with the operator's private key. Clients first query the trusted index service to obtain the CID corresponding to the resolver's IP/name, then retrieve the authenticity object from IPFS nodes via the CID, and finally verify the signature of the object using the operator's public key (from the authorized trust anchor) to complete the identity authentication. The IPFS channel's trust anchor includes the public key of the resolver operator and the root key of the trusted index service for CID mapping.

4. Out-of-Band Discovery by IP Address

When a DNS client is configured with a resolver IP address, it SHOULD query the selected out-of-band authenticity channel before relying on that resolver for other DNS queries. This allows the client to obtain authenticated resolver identity information and endpoint bindings. If the ARPA reverse domain name resolution channel is selected, the client constructs the ODAR dedicated reverse ARPA domain name based on the resolver's IP address (IPv4 or IPv6), queries the dedicated ARPA zone for the PTR record and the associated TXT record storing the authenticity object, and verifies the DNSSEC signature of the records under the zone's trust anchor. If the IPFS channel is selected, the client queries the trusted IPFS index service with the resolver's IP address to obtain the corresponding CID, retrieves the authenticity object from IPFS via the CID, and verifies the object's signature and integrity.

The following is an example of an authenticity object returned for an IP-based lookup:

```
resolver-id: odar:resolver:example-1
operator: Example Resolver Operator
endpoints: [ "1.2.3.4", "https://doh.example.net/dns-query" ]
alpn: h2
attestation: signature(issuer-key, resolver-id || operator || endpoints\
```

```
    || alpn)
```

If the out-of-band channel has no authenticity information for the configured IP address, it SHOULD return an explicit negative result indicating that no Authentic Resolver is available for that IP address. For the ARPA channel, this means the absence of signed PTR/TXT records in the dedicated ODAR reverse zone for the IP address; for the IPFS channel, this means the trusted index service returns no CID mapping for the IP address or the retrieved object from IPFS is invalid or unsigned.

5. Out-of-Band Discovery by Resolver Name

When a DNS client is configured with a resolver name, it SHOULD query the selected out-of-band authenticity channel before relying on that resolver to obtain authenticated resolver identity information and endpoint bindings. This can be used to validate resolver identity prior to selecting the resolver or initiating subsequent interactions with the resolver. If the ARPA reverse domain name resolution channel is selected (with the resolver name bound to a fixed IP address), the client first resolves the resolver name to the corresponding IP address (via a trusted minimal DNS resolver), then performs the ARPA reverse query as specified in Section 3.1. If the IPFS channel is selected, the client queries the trusted IPFS index service directly with the resolver name to obtain the corresponding CID, then retrieves and verifies the authenticity object from IPFS as specified in Section 3.2.

The following is an example of an authenticity object returned for a name-based lookup:

```
resolver-name: doh.example.net
resolver-id: odar:resolver:example-1
operator: Example Resolver Operator
endpoints: [ "https://doh.example.net/dns-query", "1.2.3.4" ]
alpn: h2
attestation: signature(issuer-key, resolver-name || resolver-id\
  || operator || endpoints || alpn)
```

If the out-of-band channel has no authenticity information for the configured resolver name, it SHOULD return an explicit negative result indicating that no Authentic Resolver is available for that resolver name. For the ARPA channel, this means the resolver name maps to an IP address with no signed PTR/TXT records in the ODAR dedicated reverse zone; for the IPFS channel, this means the trusted index service returns no CID mapping for the resolver name.

6. Deployment Considerations

Resolver deployments that support ODAR are advised to consider the following points.

6.1. Forwarders and Intermediaries

A DNS forwarder or intermediary SHOULD NOT attempt to substitute its own identity for that of an upstream resolver when ODAR is in use. In particular, if clients are provisioned with the forwarder’s IP address but the out-of-band authenticity information binds identities to upstream resolver endpoints, clients may fail to authenticate the intended resolver or may authenticate the wrong endpoint.

Operators that deploy forwarders SHOULD ensure that the out-of-band authenticity channel reflects the actual resolver endpoint that the client will rely on. If the forwarder is the intended trust target, the channel SHOULD publish bindings for the forwarder. If the upstream resolver is the intended trust target, the forwarder SHOULD behave transparently and operators SHOULD provision clients in a way that is consistent with the published bindings. For the

ARPA channel, operators SHALL ensure that the ODAR dedicated reverse zone publishes the correct IP-resolver identity bindings for the actual resolver endpoint (forwarder or upstream resolver) and maintains the validity of the DNSSEC signature for the zone records. For the IPFS channel, operators SHALL update the CID mapping in the trusted index service in a timely manner when the resolver endpoint changes, and ensure the new authenticity object is re-signed and stored in IPFS with a new CID.

6.2. Trust Anchor and Attestation Management

Resolver operators that support ODAR need to maintain the trust anchor material required by the selected out-of-band authenticity channel and to publish timely authenticity information, including updates and revocation when bindings change. This may pose challenges for deployments with frequent endpoint changes, large numbers of resolver endpoints, or multiple administrative domains.

Operators SHOULD ensure that clients can obtain and validate the out-of-band authenticity information without depending on the resolver being authenticated. Deployments SHOULD also consider how clients obtain revocation status or freshness guarantees for attestations provided by the channel. For the ARPA channel, operators SHALL maintain the DNSSEC key pair of the ODAR dedicated reverse zone, perform timely key rotation and signature renewal for the zone records, and publish the revocation status of the resolver identity via CAA or dedicated DNS records in the ARPA zone. For the IPFS channel, operators SHALL maintain the validity of the operator’s private key for signing authenticity objects, update the CID mapping in the trusted index service for revoked resolver identities (marking the CID as invalid), and ensure clients can query the revocation status of the CID via the index service. Additionally, IPFS-deployed authenticity objects SHOULD include a freshness timestamp, and clients SHALL reject objects with expired timestamps according to local policy.

6.3. Integration with RFC 9499 Recursive-Identifier Mechanism

ODAR and the RFC 9499 [RFC9499] Recursive-Identifier mechanism target different stages and participants in the DNS resolution process, with no technical conflicts and natural complementary attributes. Resolver deployments that support both mechanisms can achieve a closed loop of resolver identity authentication-identification-verification across the entire DNS link (client -> recursive resolver -> authoritative server). This section specifies the core integration principles, identity identifier unification requirements, and deployment implementation methods for the two mechanisms.

6.3.1. Core Integration Principles

1. Layered Responsibility Separation: ODAR is responsible for the out-of-band identity authentication of recursive resolvers by DNS clients, establishing the initial trust relationship between clients and resolvers; RFC 9499 is responsible for the in-band identity identification of recursive resolvers to authoritative servers, providing accurate resolver node information for authoritative server traffic control and security policies. The two mechanisms shall not interfere with each other’s functional implementation, and their trust anchors and verification processes shall be independently maintained.

2. Identity Information Consistency: The resolver identity identifier used in the RFC 9499 Recursive-Identifier mechanism SHALL be consistent with the resolver-id defined in the ODAR authenticity object. This ensures the uniqueness and traceability of resolver identity across the entire link, and enables authoritative servers to associate the Recursive-Identifier with the authenticated identity information in the

ODAR channel for further validity verification.

3. Dual Mechanism Mutual Enhancement: ODAR provides authenticated resolver identity information for the RFC 9499 mechanism, solving the problem that authoritative servers can only identify resolver nodes but cannot verify the legality of their identities; the RFC 9499 mechanism enables authoritative servers to map the in-band Recursive-Identifier to the out-of-band ODAR authenticated identity, realizing fine-grained access control and traffic scheduling based on legitimate resolver identities. At the same time, clients can use the ODAR-authenticated resolver identity to verify whether the Recursive-Identifier carried by the resolver in subsequent DNS interactions is consistent with the pre-authenticated identity.

6.3.2. Resolver Identity Identifier Unification Requirements

1. Unified Identifier Specification: Resolver operators SHALL use the ODAR-defined resolver-id (e.g., odar:resolver:example-1) as the identity identifier for the RFC 9499 Recursive-Identifier mechanism. The identifier SHALL be a fixed, non-modifiable string that uniquely identifies the resolver instance or cluster, and SHALL be published in the ODAR authenticity object and the Recursive-Identifier configuration of the resolver at the same time.

2. Dual Publication and Synchronization: When the resolver identity changes (e.g., operator reorganization, resolver cluster merge), the operator SHALL first update the resolver-id and corresponding authenticity information in the ODAR out-of-band channel, and then synchronously update the Recursive-Identifier configuration of the resolver. The update process SHALL ensure atomicity to avoid identity inconsistency between the out-of-band channel and the in-band message.

3. Identifier Format Compatibility: The unified resolver-id SHALL comply with the format requirements of the RFC 9499 Recursive-Identifier mechanism for custom string identifiers, avoiding special characters that are not supported by EDNS0 OPT option data, and ensuring that the identifier can be correctly carried in DNS query messages and parsed by authoritative servers.

6.3.3. Deployment Implementation Methods

1. Resolver Side Deployment: Recursive resolver operators that support both ODAR and RFC 9499 SHALL: (1) Publish the signed authenticity object containing the unified resolver-id to the selected ODAR out-of-band channel (ARPA/IPFS/blockchain); (2) Configure the resolver to carry the same resolver-id in the EDNS0 OPT option (OPTION CODE=10) when sending DNS query messages to authoritative servers, in accordance with the RFC 9499 specification; (3) Maintain the real-time synchronization between the ODAR-published resolver-id and the RFC 9499 configured identifier, and provide a mechanism for real-time detection and alarm of identity inconsistency.

2. Client Side Deployment: DNS clients SHALL first complete the out-of-band authentication of the resolver via ODAR and cache the authenticated resolver-id and corresponding endpoint information. When the client initiates a DNS query through the resolver, it MAY verify the consistency between the Recursive-Identifier carried in the resolver’s subsequent DNS interaction messages and the pre-authenticated resolver-id (if the client can parse the EDNS0 option of the DNS message), to prevent resolver identity spoofing and middleman tampering.

3. Authoritative Server Side Deployment: Authoritative server operators SHALL: (1) Support the parsing of the RFC 9499

Recursive-Identifier option and extract the unified resolver-id; (2) Provide an optional interface to query the ODAR out-of-band channel (ARPA/IPFS/blockchain) to verify the legality of the extracted resolver-id and obtain the corresponding resolver operator identity, endpoint information and other authenticated data; (3) Based on the verified resolver identity information, implement fine-grained security policies such as traffic limiting, query permission control, and abnormal behavior detection, and reject query requests from resolvers with invalid or revoked resolver-id.

4. Cross-Channel Trust Anchor Collaboration: For deployments where the ODAR out-of-band channel is an ARPA reverse domain name resolution system, the authoritative server of the ODAR dedicated ARPA zone SHALL use the same DNSSEC trust anchor as the authoritative server of the forward domain name system to ensure the consistency of signature verification; for IPFS or blockchain-based ODAR channels, authoritative servers MAY pre-cache the root trust anchor of the channel to reduce the performance overhead of real-time out-of-band channel queries.

7. Privacy Considerations

ODAR requires a client to query an out-of-band authenticity channel using a resolver IP address or resolver name, which can reveal information about a client’s configured resolver, network environment, and resolver selection behavior. Following the guidance in [RFC6973], this section focuses on linkability and exposure on the path to the out-of-band channel, as well as mitigations that reduce unnecessary disclosure.

Such queries can reveal a client’s configured resolver, network environment, and resolver selection behavior to the operator of the out-of-band channel and to any on-path observers between the client and that channel. This information can enable correlation of client activity across time or across different access networks.

To limit such exposure, clients SHOULD minimize the information sent to the out-of-band channel to what is strictly necessary for the lookup. Clients SHOULD cache validated authenticity objects according to local policy and respect their freshness limits, in order to reduce repeated queries that increase observability. When available, clients SHOULD access the out-of-band channel over encrypted transports, and MAY use privacy-enhancing access methods such as proxies or relay services to reduce linkability. For the ARPA channel, clients SHOULD query the ODAR dedicated reverse zone via encrypted DNS transport (e.g., DoT/DoH) to prevent on-path observers from snooping on the reverse query content, and cache the signed PTR/TXT records with the DNSSEC signature validity period as the freshness limit. For the IPFS channel, clients MAY access IPFS nodes via private gateways or encrypted P2P connections, cache the CID and corresponding validated authenticity object locally, and avoid repeated queries to the trusted index service; additionally, clients SHOULD NOT send any unnecessary client-specific information to the IPFS index service or nodes during the lookup process.

If the out-of-band channel returns multiple endpoints for a resolver identity, endpoint selection can introduce distinguishable client behavior. Clients SHOULD apply local policy that avoids unnecessary variation in endpoint choice, and deployments SHOULD avoid publishing endpoint sets or selection guidance that would cause clients to reveal additional information beyond what is required to establish the intended DNS service. This requirement applies equally to the ARPA and IPFS channels; operators SHALL ensure that multiple endpoints published in the ARPA TXT records or IPFS authenticity objects are in a standardized order, and avoid including endpoint selection rules that may lead to client behavior

differentiation.

When integrating with the RFC 9499 [RFC9499] Recursive-Identifier mechanism, additional privacy considerations shall be taken into account: (1) Resolver operators SHALL avoid carrying sensitive information (e.g., internal cluster ID, operator private information) in the unified resolver-id to prevent information leakage via DNS query messages; (2) Authoritative server operators SHALL NOT collect or analyze the Recursive-Identifier carried in DNS query messages for irrelevant purposes, and SHALL delete the collected resolver identity information in a timely manner in accordance with data privacy laws and regulations; (3) Clients SHALL not send the authenticated resolver-id to any third-party services except for the necessary DNS interaction verification, to prevent the linkability of client resolver selection behavior and other network activities.

8. Security Considerations

ODAR relies on out-of-band authenticity channels, which introduces failure and attack modes that differ from in-band discovery. Following the guidance in [RFC3552], this section discusses denial-of-service and downgrade risks, verification requirements for authenticity objects, and endpoint-selection pitfalls when multiple bindings are published.

Because ODAR relies on out-of-band authenticity channels, an on-path attacker on the DNS path can still prevent successful use by blocking access to the out-of-band channel or by causing clients to fall back to unauthenticated resolver selection. Clients should be aware that it might not be possible to distinguish between the absence of published authenticity information and an active blocking attack. To limit the impact of such blocking, clients MAY re-query the out-of-band channel periodically according to local policy. For the ARPA channel, attackers may attempt to block access to the ODAR dedicated reverse zone's authoritative servers or forge unsigned ARPA records; clients MUST only accept signed DNSSEC records from the authorized ARPA zone trust anchor and reject any unsigned or invalidly signed records. For the IPFS channel, attackers may attempt to block access to the trusted index service or IPFS nodes, or forge fake authenticity objects with invalid CIDs; clients MUST verify the CID integrity and the object's signature before accepting, and MAY use multiple IPFS nodes and index service replicas to mitigate blocking attacks.

Clients MUST verify authenticity objects under the trust anchor of the selected out-of-band channel before using any identity information or endpoint bindings. Clients MUST NOT rely on unauthenticated fields, and MUST ignore any authenticity object that contains mandatory elements the client does not understand. For the ARPA channel, this means clients MUST verify the DNSSEC signature of the PTR and TXT records in the ODAR dedicated reverse zone against the zone's trust anchor, and ignore any records with invalid signatures or unrecognized fields in the TXT-stored authenticity object. For the IPFS channel, clients MUST verify the signature of the retrieved authenticity object against the resolver operator's public key (from the trust anchor), check that the CID of the object matches the one obtained from the trusted index service, and ignore any objects with invalid signatures, mismatched CIDs, or unrecognized mandatory elements.

If the out-of-band channel provides bindings that associate a resolver identity with multiple endpoints, an attacker might attempt to steer clients toward an endpoint that is less protected or easier to intercept. Clients SHOULD apply local policy that prefers endpoints that provide endpoint authentication appropriate to the intended interaction, and deployments SHOULD avoid publishing

bindings that would cause clients to select endpoints without such protections unless explicitly intended. This requirement is enforced for the ARPA and IPFS channels; operators SHALL only publish endpoints with valid authentication mechanisms in the ARPA TXT records or IPFS authenticity objects, and clients SHALL prioritize endpoints with DoT/DoH or other encrypted DNS mechanisms according to local policy.

If the out-of-band channel supports updates or revocation, deployments SHOULD ensure timely publication of changes, and clients SHOULD consider freshness and revocation status when validating authenticity information. For the ARPA channel, deployments SHALL update the DNSSEC-signed records in the ODAR dedicated reverse zone in a timely manner when resolver bindings change, and publish revocation status via dedicated DNS records; clients SHALL check the record's signature timestamp and revocation status before using the information. For the IPFS channel, deployments SHALL update the CID mapping in the trusted index service for updated/revoked resolver identities, and add a revocation flag and expiration timestamp to the IPFS-stored authenticity object; clients SHALL query the index service for the latest CID and check the revocation and freshness status of the object before use.

8.1. Additional Security Considerations for RFC 9499 Integration

When integrating ODAR with the RFC 9499 [RFC9499] Recursive-Identifier mechanism, the following additional security risks and mitigation measures shall be considered to ensure the security of the full-link resolver identity transmission:

1. Recursive-Identifier Spoofing Attack: Attackers may forge the Recursive-Identifier option in DNS query messages to impersonate a legitimate resolver and bypass the authoritative server's security policies. Mitigation: Authoritative servers MUST verify the legality of the resolver-id in the Recursive-Identifier via the ODAR out-of-band channel before executing any policy based on the identifier, and reject requests with unauthenticated or revoked resolver-id. Recursive resolvers SHOULD use transport layer encryption (e.g., DoT/DoH) when sending DNS queries to authoritative servers to prevent the Recursive-Identifier option from being tampered with by on-path attackers.

2. Resolver Identity Inconsistency Risk: Human error or system failure may lead to inconsistency between the resolver-id published in the ODAR out-of-band channel and the Recursive-Identifier carried in the DNS message, which may cause the authoritative server to reject legitimate resolver requests or the client to fail identity verification. Mitigation: Resolver operators SHALL deploy an automated detection mechanism to periodically check the consistency of the two identifiers, and trigger an alarm and automatically rectify the inconsistency in a timely manner.

3. Out-of-Band Channel Query Attack: Attackers may launch a DDoS attack on the ODAR out-of-band channel by forging a large number of resolver-id verification requests from authoritative servers, resulting in the unavailability of the channel and the failure of the RFC 9499 mechanism's identity verification. Mitigation: ODAR out-of-band channel operators SHALL deploy anti-DDoS protection mechanisms, and limit the frequency of resolver-id verification requests from a single authoritative server IP address. Authoritative servers SHALL cache the verified resolver-id and its validity period to reduce the number of real-time out-of-band channel queries.

4. Trust Anchor Compromise Risk: If the trust anchor of the ODAR

out-of-band channel is compromised, attackers may forge resolver authenticity information, leading to the failure of both ODAR authentication and RFC 9499 identity verification. Mitigation: Operators SHALL strengthen the security protection of the ODAR trust anchor, adopt multi-party custody and regular key rotation mechanisms, and publish the trust anchor compromise information in a timely manner to enable clients and authoritative servers to update the trust anchor and reject fake authenticity information.

9. IANA Considerations

This document has no IANA actions. If the ODAR dedicated ARPA reverse zone is standardized in subsequent versions of this document, IANA actions for ARPA zone allocation and DNS record type registration may be required; additionally, if a dedicated IPFS index service for ODAR is standardized, IANA actions for relevant parameter and identifier registration may be proposed. For the integration with RFC 9499 [RFC9499], this document does not require additional IANA actions, as it reuses the existing EDNS0 OPT option code (10) defined in RFC 9499 and does not propose new option codes or parameter registrations.

10. References

10.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC2132] Alexander, S. and R. Droms, "DHCP Options and BOOTP Vendor Extensions", RFC 2132, DOI 10.17487/RFC2132, March 1997, <https://www.rfc-editor.org/info/rfc2132>.

[RFC8106] Jeong, J., Park, S., Beloeil, L., and S. Madanapalli, "IPv6 Router Advertisement Options for DNS Configuration", RFC 8106, DOI 10.17487/RFC8106, March 2017, <https://www.rfc-editor.org/info/rfc8106>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC9915] Mrugalski, T., Volz, B., Richardson, M., Jiang, S., and T. Winters, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", STD 102, RFC 9915, DOI 10.17487/RFC9915, January 2026, <https://www.rfc-editor.org/info/rfc9915>.

[RFC9499] Chen, T., et al., "EDNS0 Recursive-Identifier Option", RFC 9499, DOI 10.17487/RFC9499, <https://www.rfc-editor.org/info/rfc9499>.

10.2. Informative References

[RFC3552] Rescorla, E. and B. Korver, "Guidelines for Writing RFC Text on Security Considerations", BCP 72, RFC 3552, DOI 10.17487/RFC3552, July 2003, <https://www.rfc-editor.org/info/rfc3552>.

[RFC6973] Cooper, A., Tschofenig, H., Aboba, B., Peterson, J., Morris, J., Hansen, M., and R. Smith, "Privacy Considerations for Internet Protocols", RFC 6973, DOI 10.17487/RFC6973, July 2013, <https://www.rfc-editor.org/info/rfc6973>.

[IPFS] IPFS Project, "InterPlanetary File System (IPFS) Specification", <https://specs.ipfs.tech/>, accessed 2026.

[IANA-ARPA] IANA, "ARPA Domain Name Registry",
<https://www.iana.org/domains/arpa>, accessed 2026.

Authors' Addresses

Wei Wang
CNNIC
Building 4, No. 9, Beijing Auto Museum West Road
Fengtai District, Beijing 100070
China
Email: wangwei@cnnic.cn

Wenyong Wang
University of Electronic Science and Technology of China
No. 2006, Xiyuan Ave, West Hi-Tech Zone
Chengdu, Sichuan 611731
China
Email: wangwy@uestc.edu.cn

Ting Yang
University of Electronic Science and Technology of China
No. 2006, Xiyuan Ave, West Hi-Tech Zone
Chengdu, Sichuan 611731
China
Email: yting@uestc.edu.cn

Wenbin Luo
University of Electronic Science and Technology of China
No. 2006, Xiyuan Ave, West Hi-Tech Zone
Chengdu, Sichuan 611731
China
Email: 202421080108@std.uestc.edu.cn

Xingxing Yang
CNNIC
Building 4, No. 9, Beijing Auto Museum West Road
Fengtai District, Beijing 100070
China
Email: yxx@cnnic.cn