RFC 4431 プロトコル理解 SWG

1. Introduction

- このドキュメントは、DNS の正常な信頼の連鎖外のTrust Anchor を発行するために、新しいリソースレコードを定義します

- DNSSEC バリデータによるこれらのレコードの使用は、このドキュメントの範囲外です。しかし、これらのレコードは、署名されていないゾーンまたは DS レコードを発行しないゾーンからの DNSSEC データの検証する助けになると期待されます

2. DLV Resource Record

- DLV リソースレコードは RFC 4034 の Section 5 で定義された
  DS リソースレコードと同一の wire と表示形式
- DLV レコードは、IANA が指定した DS レコードと同じ値を
  アルゴリズムと digest type のフィールドで使います
- DLV レコードは正常な DNS レコードタイプであり、特別な処理を
  要しません
  - DLV レコードは、RFC 4035 Section 3.1.4.1 で規定されている DS レコードタイプの特別な処理を必要としません (受け継がない)
  - DS レコードと異なって、DLV レコードは親側のゾーンカット側に表示されないかもしれません
  - DLV レコードは、ゾーンの Apex に表示されるかもしれません

3. Security Considerations

- DLV RR を DNSSEC 検証の一部として使わない権威サーバにとって、特定のセキュリティの懸念はありません
  - DLV RR は他の DNS データと同じです
- DNSSEC 検証の一部として DLV RR を使用するソフトウェアは、使用に当たり規制を課すべきです
  - しかし、これらの規制はこれらのレコードをどう使うか詳細に述べられているドキュメントに従うのがベストです
  - 最低限として、何かしらの暗号を使った認証していないレコードを使うことはお薦めしません
  - 多くの場合、DNSSEC 自身が DLV RR を認証するのに使用されます
  - DLV RR がどう使用されるかによって、適切に認証が行われていない場合、DNS データのなりすまし検出の失敗などを含むセキュリティ上の問題につながる可能性があります

3. Security Considerations

- RFC 4034 Section 8 で解説されている DS RR の Security Consideration は DLV RR に適用可能です
  - 特に key tag field は、DNSKEY RR の選択を効率良くするために
    使用されるが、一つの DNSKEY RR を特定するわけではない。
    二つの異なる DNSKEY RR が同じ owner name, algorithm type
    および key tag を持っていることがあります。Key Tag のみを使用して、DNSKEY RR を選択している実装は間違った公開鍵を選択する
    可能性があります。

4. IANA Considerations

- IANA は Specification Required 部分に DNS type code 32769 を割り当てました

- DLV リソースレコードはDS リソースレコードのための同じアルゴリズムと既に使用されているダイジェストタイプを再利用します