NRIセキュアテクノロジーズ

DNSSEC.JP プロトコル理解SWG

DNSSEC Key Timing Considerations (draft-ietf-dnsop-dnssec-key-timing-00)

2010年08月26日

NRIセキュアテクノロジーズ株式会社
MSS事業本部
ネットワークセキュリティサービス部

中島　智広

〒105-7113
東京都港区東新橋1-5-2 汐留シティセンター

おことわり

- 本ドキュメントはDNSSEC.JP プロトコルSWGの活動として
  メンバーを対象としたInternet Draftの輪講のために作成した資料です
- 内容には十分配慮していますが正確性については保証できません
- Internet Draftの話であり実際の運用スキームと異なる場合があります
- 原文が更新される可能性がありますので必ず原文を確認してください
- 重大な誤りに気づいた場合は下記までご連絡いただけると幸いです
  ※修正をお約束するものではありません

nakashima@nri-secure.co.jp

本Internet Draftで扱われている内容

- DNSSECにおける鍵の状態遷移
- ロールオーバ方式の長所/短所
- ロールオーバと初回登録の違い
- 緊急ロールオーバ用の準備鍵
- アルゴリズムが違う場合の考慮

- 考慮されている時間
  - RRのTTL
  - ネガティブキャッシュのTTL
  - 署名に要する時間
  - 署名の有効期限
  - 運用ポリシ上の鍵の有効期限
  - スレーブサーバへのゾーン転送時間
  - DS更新のために必要な待ち時間
  - バリデータとの時計のずれ

1.1 Key Rolling Consideration

- DNSSECを導入したゾーン管理者は署名に用いる鍵の交換を鍵の危殆化や鍵の管理ポリシに則って実施しなければならない
- DNSにはキャッシュの概念があるためキャッシュの考慮が必要(バリデータは別々に入手した鍵と署名で検証を行うかもしれない)
- UDPパケットのサイズは限られているため、使われていない鍵は適切なタイミングで削除されなければならない. 同様の理由で事前公開される鍵も適切なタイミングで登録されなければならない
- 初回導入時に大量のゾーンに対して鍵の登録を行う際には、手順をうまく考えて実施する必要がある
- 緊急時に迅速に鍵の交換を行うためには事前に公開された鍵が必要
- ライフサイクルを含む鍵のマネジメントポリシを決める必要がある

1.2 Type of Keys

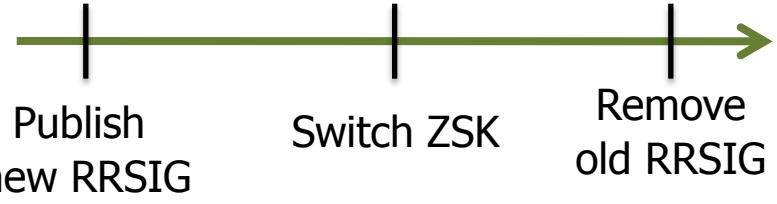
- DNSKEYはZSKとKSKの二つが存在する
- ロールオーバの際は一貫した方法をとる必要がある
- ZSKとKSKのロールオーバには類似性があるが、
  違う点もあるので本ドキュメントでは別々のものとして扱う

(ZSKロールオーバにおけるRRSIG(RR)をDNSKEYに、
DNSKEYをDSに取り替えて考えるとZSKとKSKのロールオーバは同じ)

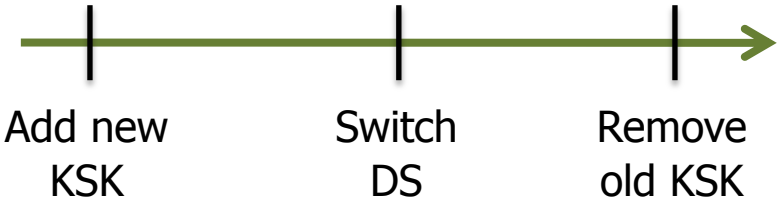
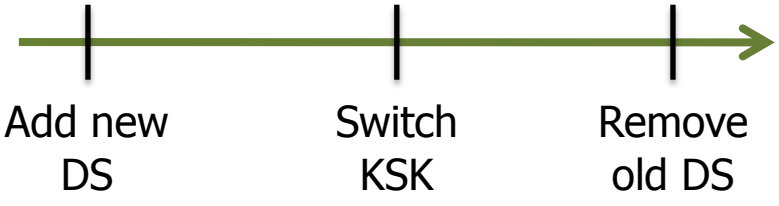
1.3 Terminology

- 用語は[RFC4033]と[RFC5011]に定義されているものを使用
- そのほかについてはAppendixに記載

2.1 ZSK Rollover Method

方式	長所	短所
Pre-Publication  	DNSSECのデータ量を最小にとどめることができ、パフォーマンスへの影響を抑えることができる	鍵の事前登録を行う点で3つの方式の中では複雑
Double-Signature  	3つの方式の中で最も手順が少なくシンプル	DNSSECのデータ量が大きくなる
Double-RRSIG  	なし ※記述の完全性のためモデルとして記載しているに過ぎない	Pre-PublicationとDouble-Signatureの両方の短所を併せ持つ

2.2 KSK Rollover Method

方式	長所	短所
Double-Signature  	親ゾーンの更新が1回で済む	2つのKSK RRsetが含まれるためパケットサイズが大きくなる
Double-DS  	KSK RRsetのパケットサイズを最小にできる	親ゾーンの更新が2回
Double-RRset  	短い手順と期間で効率的に実施できる	2つのKSK RRsetが含まれるためパケットサイズが大きくなる

2.3 Summary

Method	ZSK	KSK	Description
Pre-Publication	○	×	DNSKEYをRRSIGよりも先に公開する
Double-Signature	○	○	DNSKEYとRRSIGを同時に更新する
Double-RRSIG	○	×	DNSKEYよりも先にRRSIGを公開する
Double-DS	×	○	DSをDNSKEYよりも先に公開する
Double-RRset	×	○	DNSKEYとDSを同時に公開する

3. Key Rollover Timelines

■内容

- Section2で分類されたロールオーバ方式について
  時間軸に着目し詳細に流れの整理を行ったもの

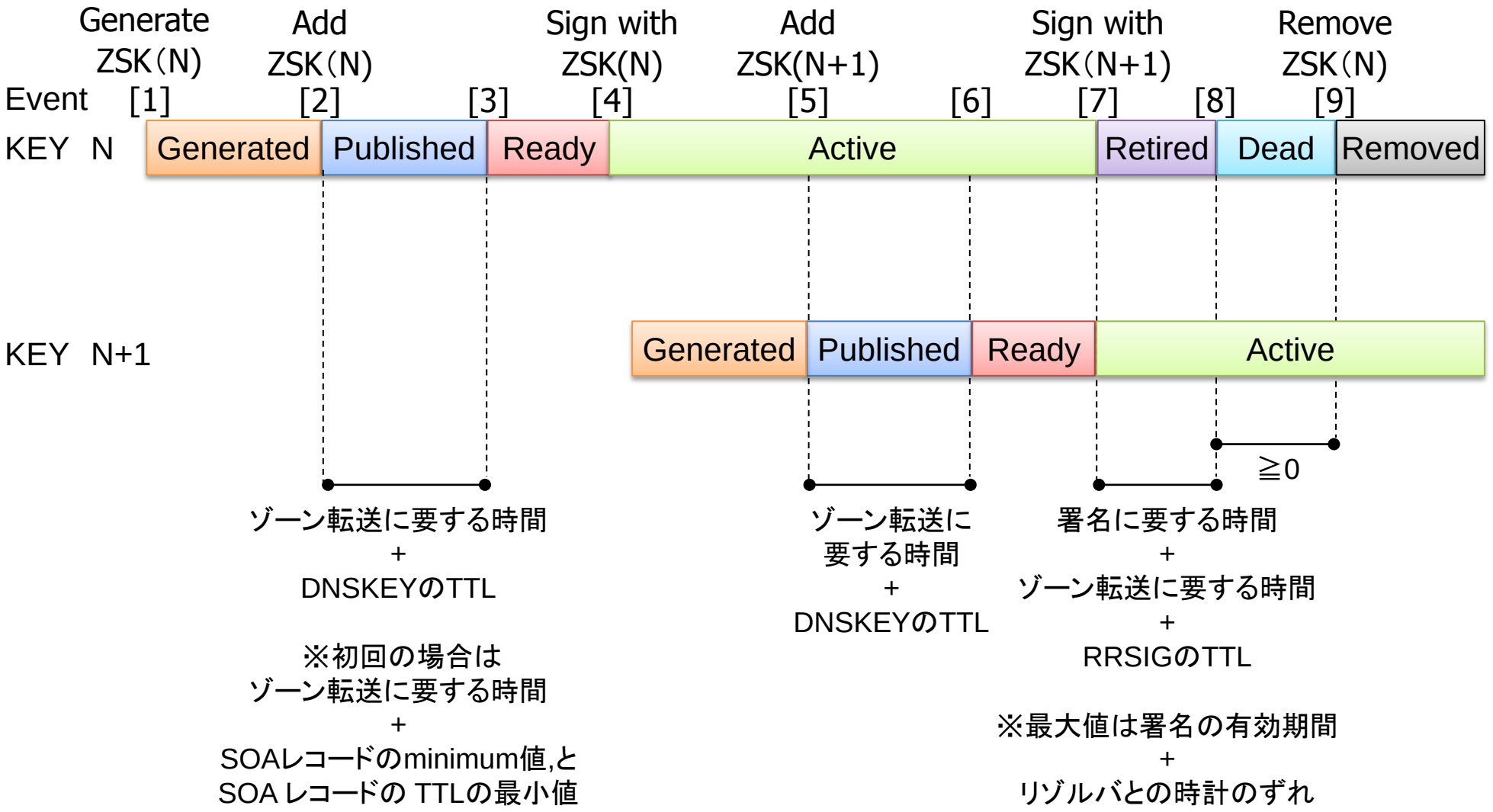
■注意事項

- 鍵の状態に基づいて記述されているが一部正しくない部分がある
  (原文の記述に厳密に従っているため)
- Event番号は原文に準拠
- Event番号に紐付くアクションを記述
  (アクションが記述されていないEventは時間の経過による変化を表す)
- 鍵Nと鍵N+1とその署名が説明の主体であり
  鍵N-1とその署名の扱いは明記されていない部分がある
  例：鍵N-1とそれを用いて作られた署名の削除タイミング

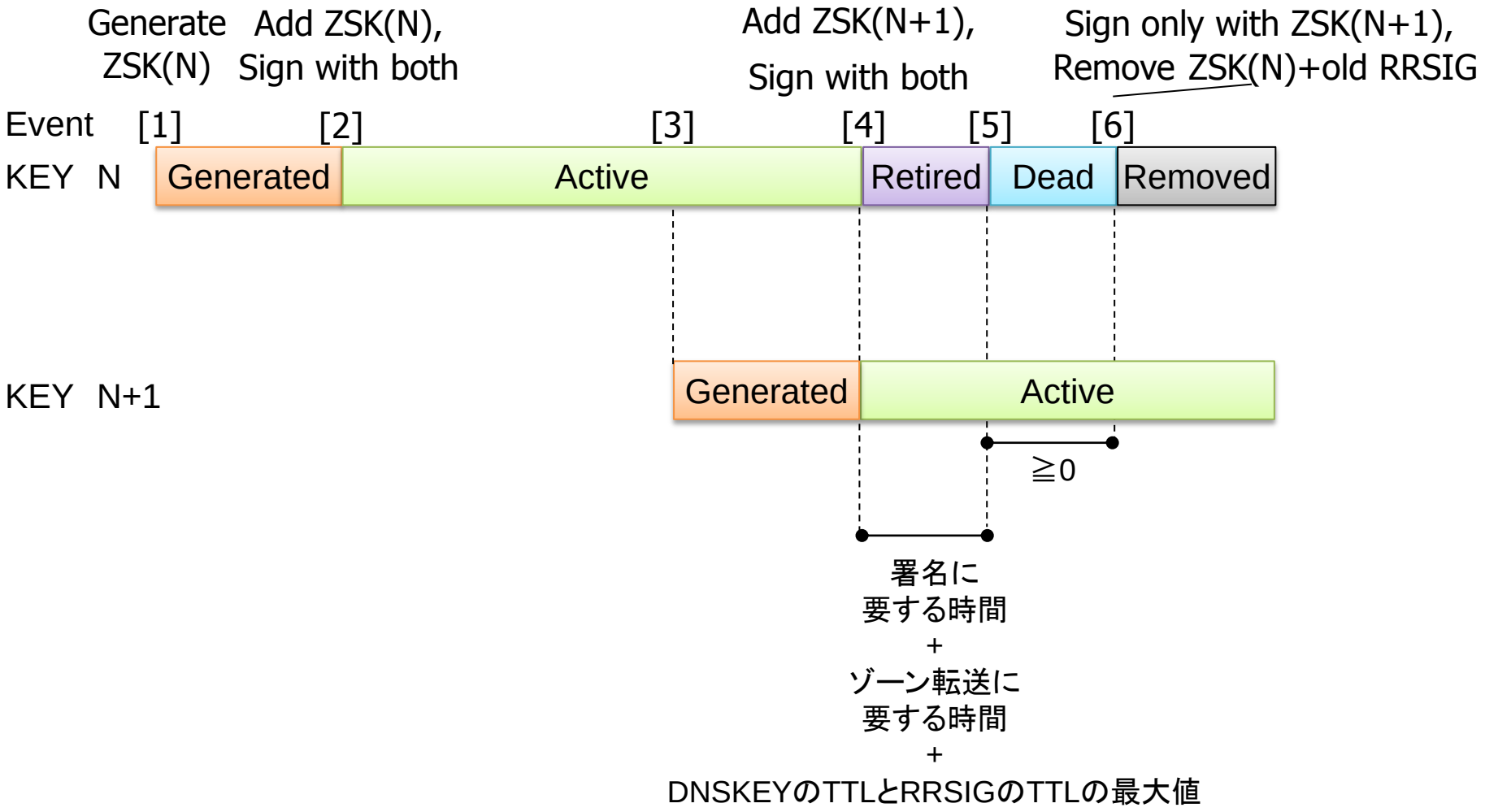
3.1 Key States

Generated	新しい鍵が生成されただけの状態 (鍵は何の用途にも利用されていない)
Published	生成された鍵がゾーンファイルに公開された状態 RRSIGやDSが最初に公開され次いでDNSKEYが変更される方式の場合、 RRSIGやDSを公開した状態もPublished と定義する。 (古いRR setがリゾルバでキャッシュされている可能性がある)
Ready	十分なPublished期間を経て、 リゾルバキャッシュが新しい状態のキャッシュを保持している状態
Active	鍵がゾーンの署名に用いられている状態(鍵視点と署名視点が混在)
Retired	さらに次の新しい鍵がActiveとなった状態 (リゾルバキャッシュには古いRRsetが残っているかもしれない状態)
Dead	DNSKEY RRSetに鍵は登録されているが 署名の検証には用いられていない状態 (リゾルバキャッシュに古いRRsetは残っていない状態)
Removed	鍵がゾーンファイルから削除された状態
Revoked	Revoke bit がたてられた状態

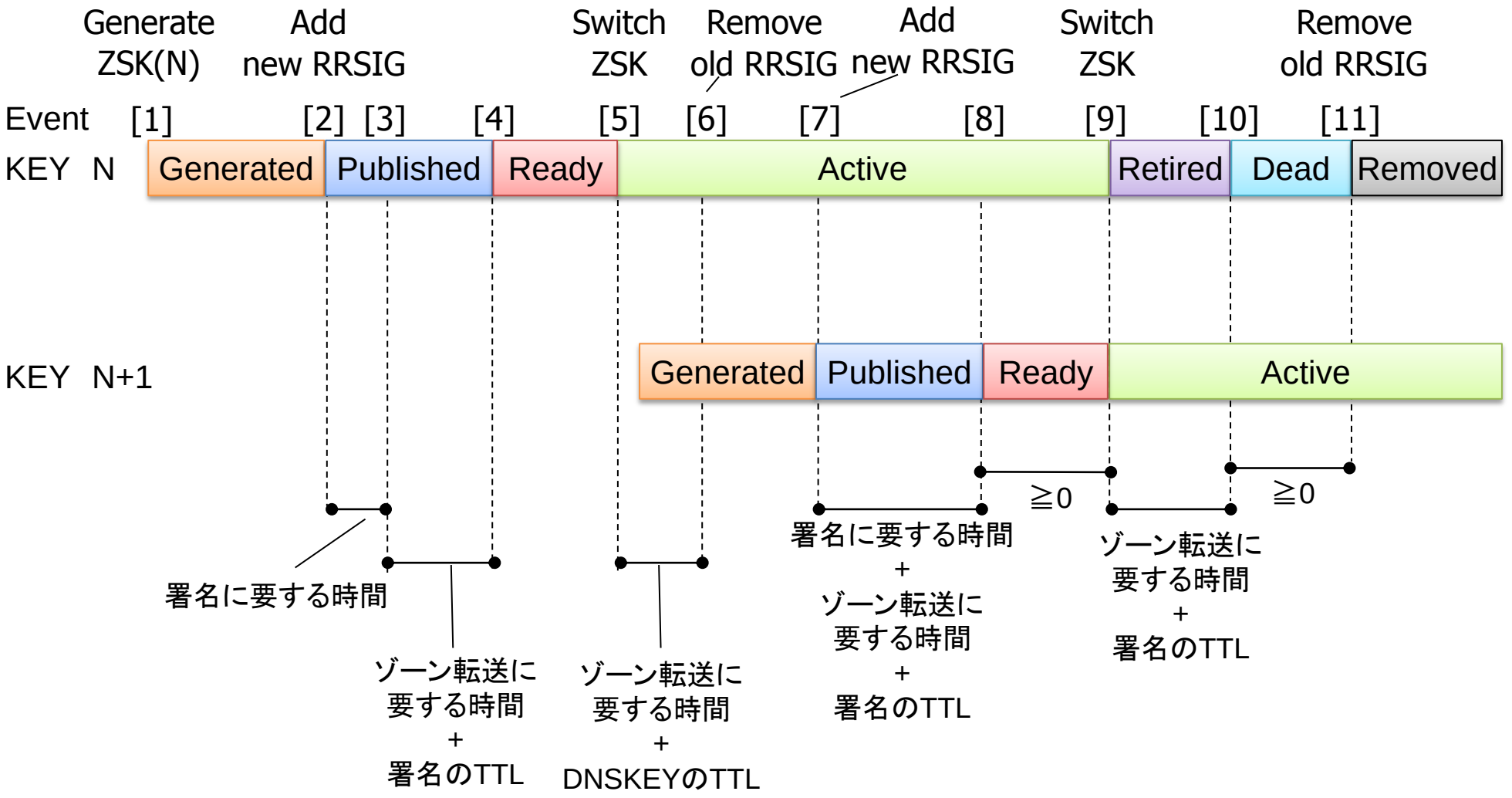
3.2.1 Pre-Publication Method



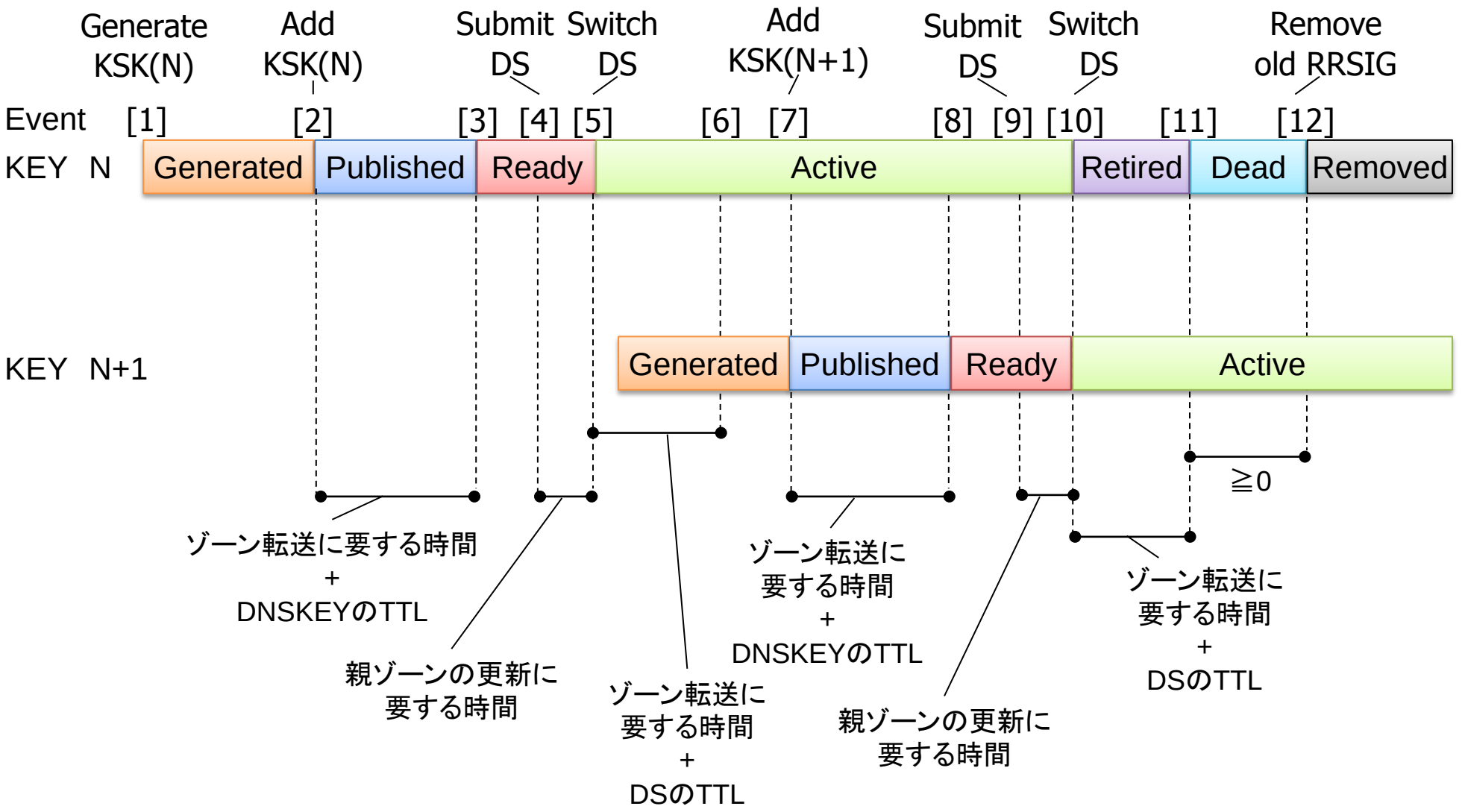
3.2.2 Double-Signature Method (ZSK)



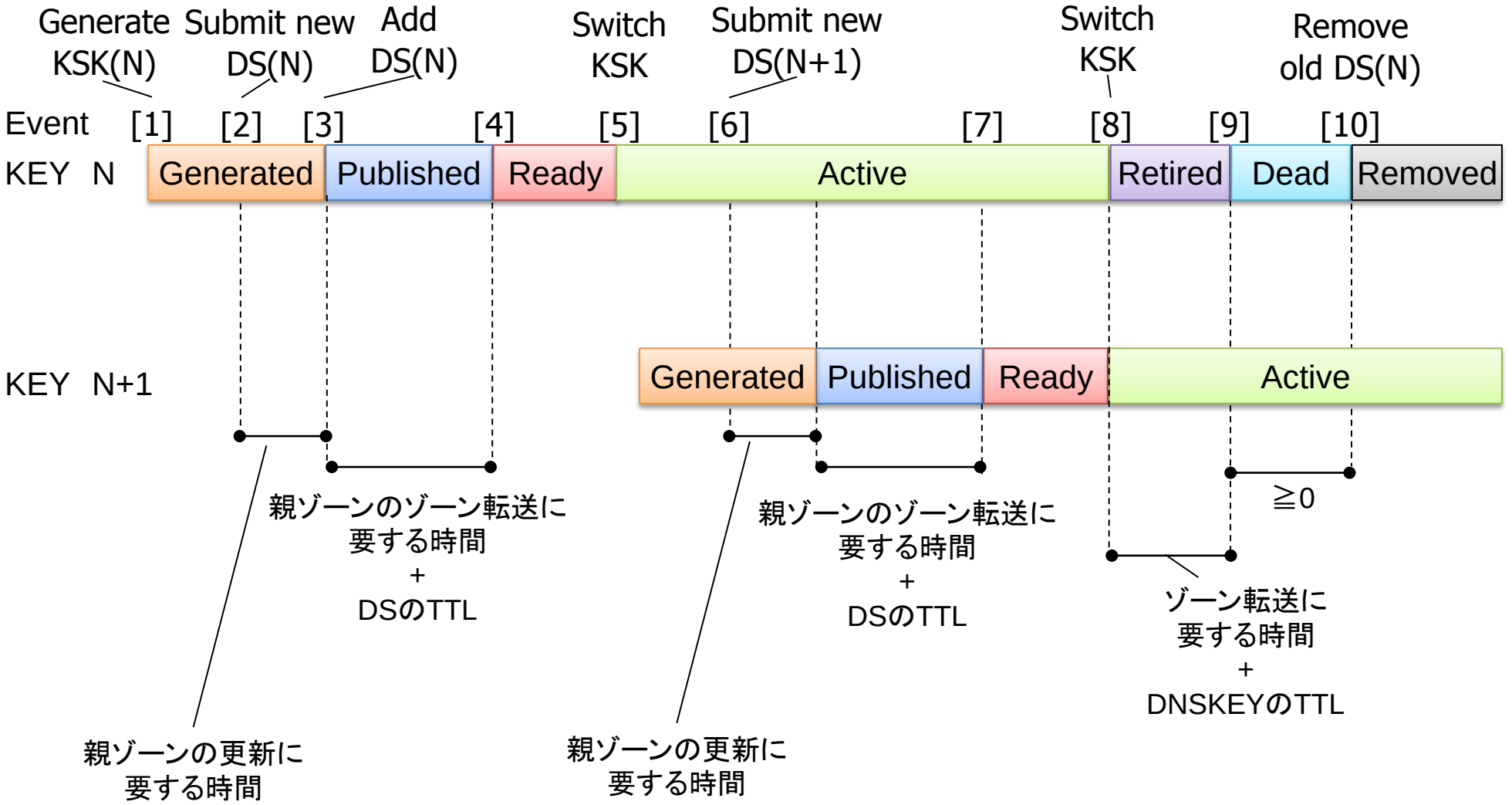
3.2.3 Double-RRSIG Method



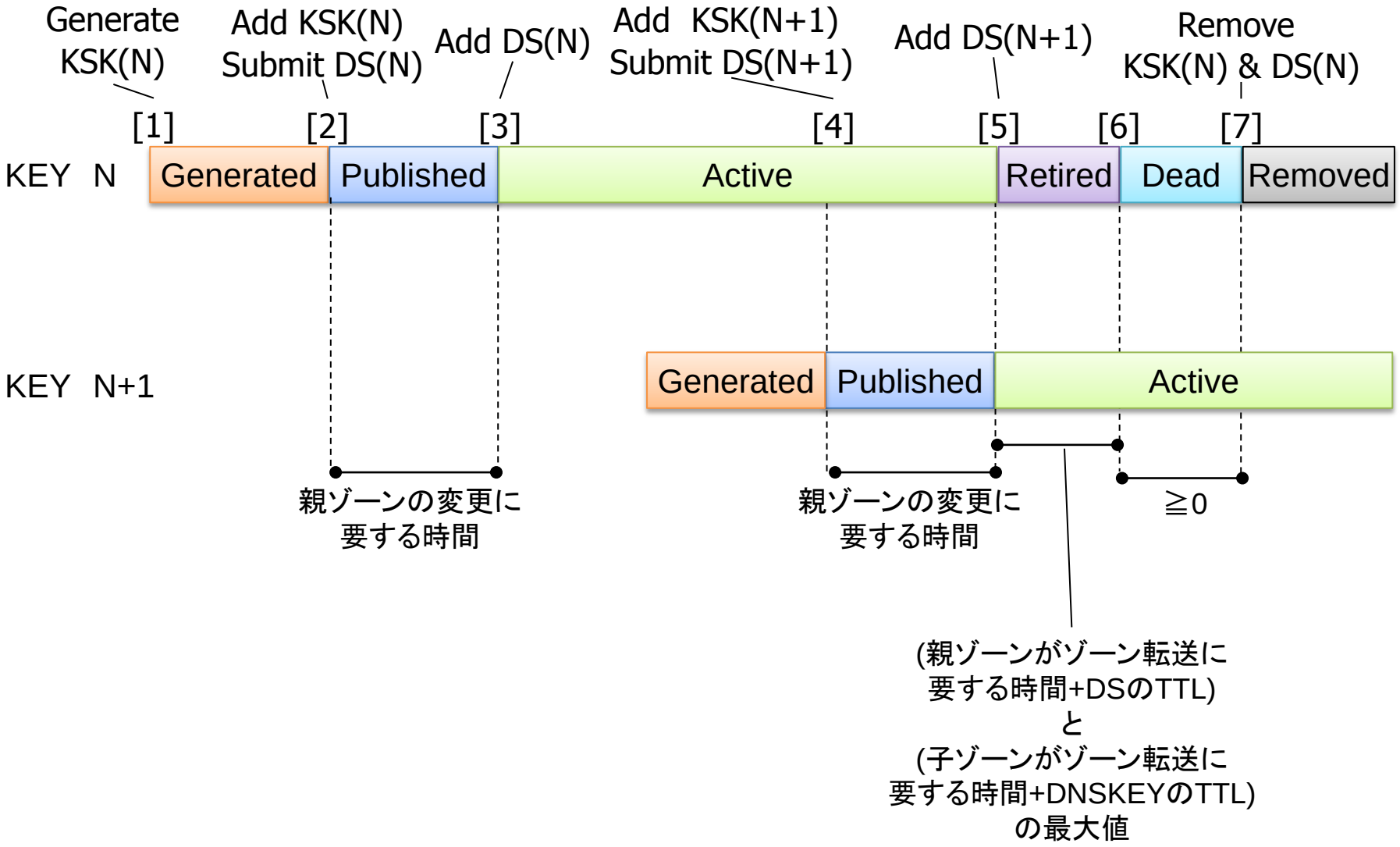
3.3.1 Double-Signature Method (KSK)



3.3.2 Double-DS Method



3.3.3 Double-RRSet Method



3.3.4 Interaction with Configured Trust Anchor

- トラストアンカーの更新はRFC5011で取り扱われている
- Double-Signature及びDouble-RRSetに適合する
- 3.3.4.1 Additon of KSK
  RFC5011のadd hold-down timeの定義に基づき
  - Double-Signature Methodの場合
    鍵のPublished期間は「30日と鍵のTTLのうち大きい値」以上
  - Double-RRSet Method※の場合
    鍵のPublished+Ready期間は「30日と鍵のTTLのうち大きい値」以上
    ※原文ではDouble-RRSIGと記述されているが
    文脈からDouble-RRSetが正しいと考えられる
- 3.3.4.2 Removal KSK
  RFC5011のRemove hold-down timeの定義に基づき
  - Revoke状態の鍵は30日以上維持する必要がある

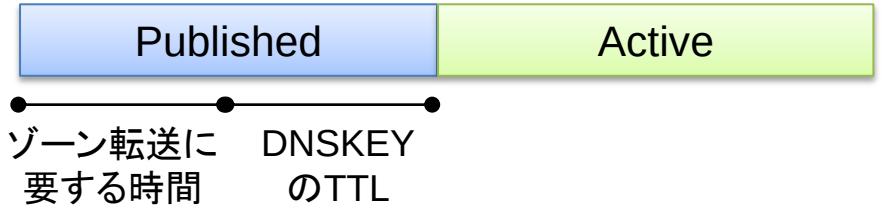
3.3.5 Introduction of First KSK

■KSKを最初に登録する際には考慮しなければならない点がある

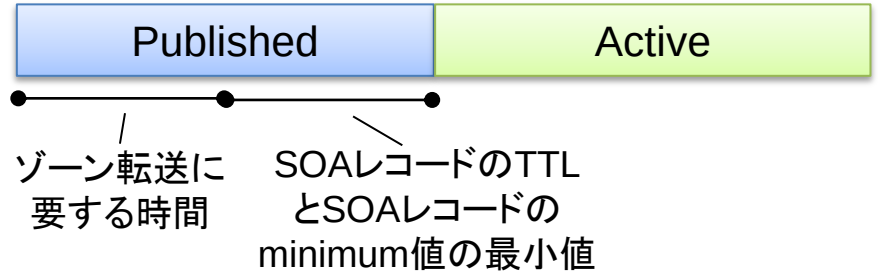
- ケース1: 親ゾーンがDNSSECで署名されておりセキュアな場合
  ➔自ゾーンのDSが親ゾーンに存在しないことがを約束される
- ケース2:親ゾーンがDNSSECで署名されておらずセキュアでない場合
  ➔自ゾーンのDSが新しいトラストアンカーとなる可能性がある

どちらの場合も

- 前のDNSKEY RRsetが子ゾーンに存在する場合



- 初めてDNSKEY RRset子がゾーンに出現する場合



4. Standby Keys

■通常、鍵は定期的なスケジュールに沿って更新されることになるが
緊急で鍵のロールオーバが必要となる場合があるかもしれない
その際、Standby keyがある場合に対応時間を最短にすることができる

■ZSKの場合

- Pre-Publication Methodの場合のみStandby keyの意味がある
(Double-SignatureやDouble-RRSIGでは、Standby keyを用意すると
署名が常に2セット必要となり大きなゾーンではパフォーマンスの影響が出る)
- 方法：ZSKをロールオーバした直後に次のZSKをPublishする

■KSKの場合

- Double-Signature Methodと Double-DS Methodの場合に利用可能
(Double-RRset Methodでは2つのActive Keyが使われている)
- 方法：新しいKSKを自ゾーンに登録せず親ゾーンに新しいDSを登録する

5. Algorithm Considerations

- 先述のセクションではすべての鍵と署名がただ一つのアルゴリズムを使用することを暗黙的に仮定していた
- アルゴリズムのロールオーバを行う場合を除き、アルゴリズムの異なる鍵との間に関係性はない、これは鍵のアルゴリズム毎に独立してロールオーバが可能なことを意味する
- ロールオーバは鍵のアルゴリズム毎に別々に行われるべきである

6.Summary

- ZSKでは"Pre-Publication"がよい方法であると考えられる
- KSKでは"Double-RRset"が最も効率的な方式
- KSK更新に要する時間は親ゾーンのポリシーに依存する
- 緊急時の鍵交換はすべてのロールオーバ方式において
  事前に予備鍵を公開しておくことで簡素化される

下記省略

- 7.IANA Consideration
- 8.Security Considerations
- 9.Acknowledgements
- 10.Change History
- 11.Reference

NRIセキュアテクノロジーズ