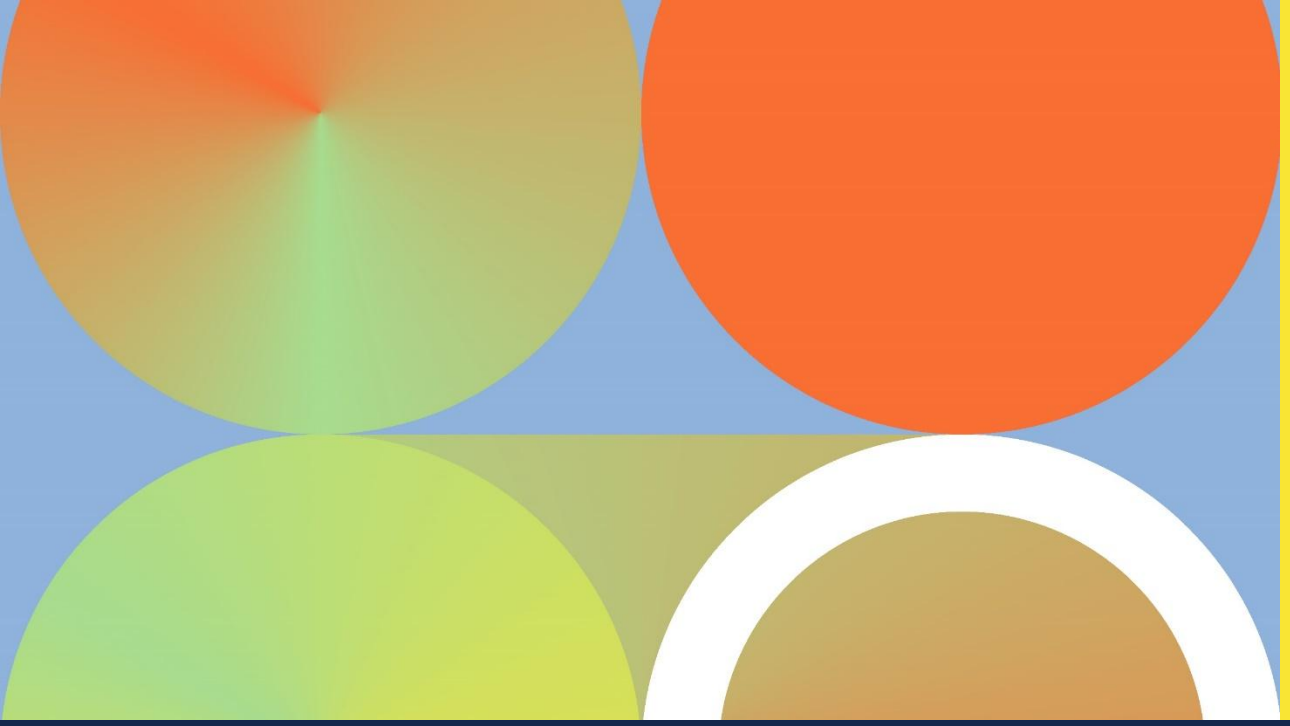


Internet
made in France

Webinaire Afnic

DNSSEC : prévenez le détournement des réponses DNS

25 septembre 2025

Bienvenue à toutes et tous !

Internet
made in France

Stéphane Bortzmeyer

Ingénieur Expert R&D,
Afnic

Michaël Timbert

Ingénieur R&D,
Afnic

Lotfi Benyelles

Responsable de l'offre
Conseil et Formation,
Afnic

L'Afnic : l'Association Française pour le Nommage Internet en Coopération

- Association française à but **non lucratif**
- **Gestionnaire du .fr** depuis plus de 25 ans et de 20 extensions géographiques et de marques
- **Opérateur de service essentiel**, certifié ISO 27001
- **Organisme certifié Qualiopi® pour les actions de formation** (DNS, noms de domaine, cybersécurité)

L'expert français du DNS et des noms de domaine

afnic

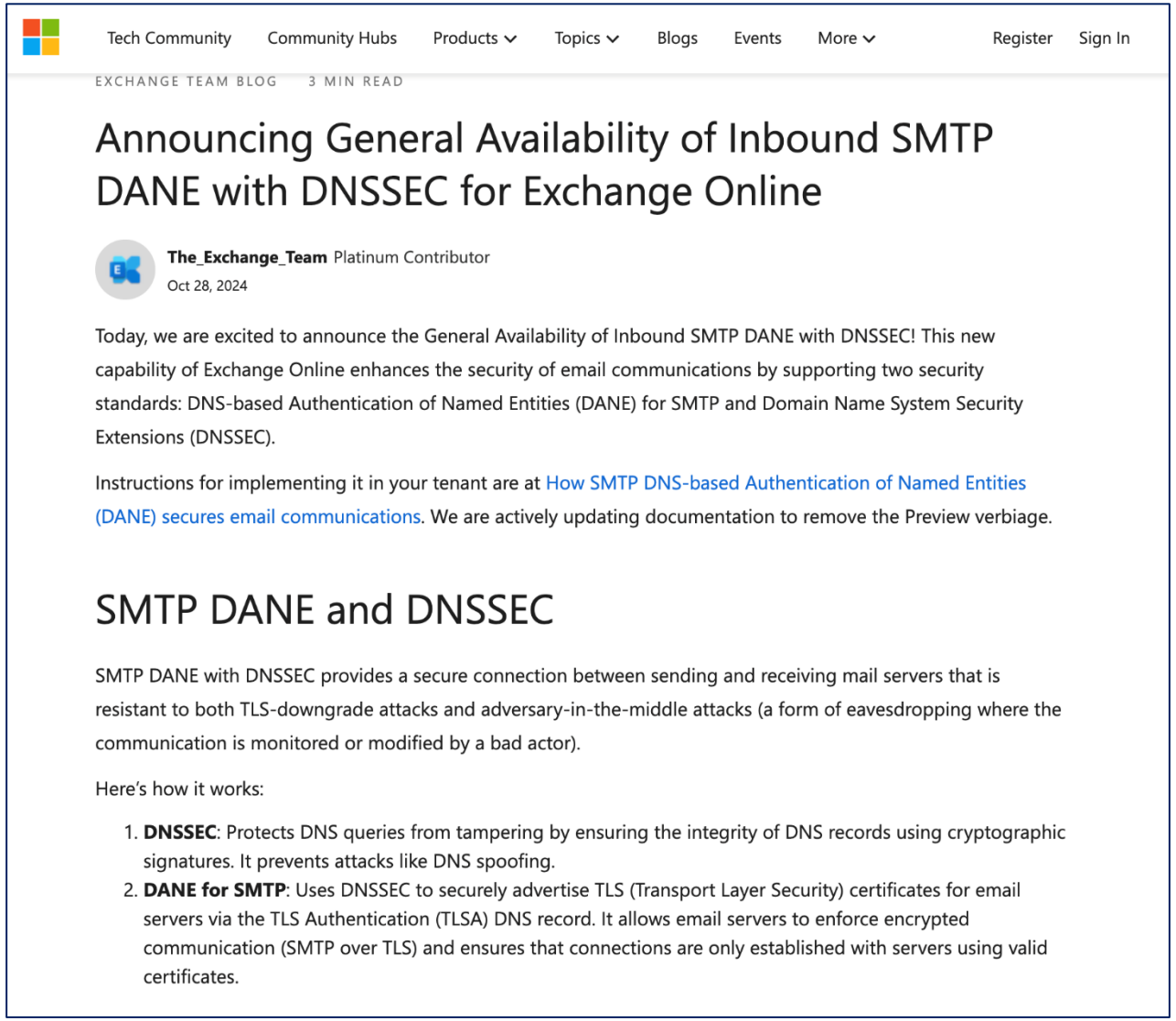
Au programme de ce webinaire

- Point d'actu sur le protocole DNSSEC
- Le fonctionnement du DNS
- DNSSEC : Domain Name System Security Extensions
- La mise en place de DNSSEC
- Les erreurs les plus fréquentes à éviter

1

Point d'actu sur le protocole DNSSEC

DNSSEC : quelques actualités



Tech Community Community Hubs Products Topics Blogs Events More Register Sign In

EXCHANGE TEAM BLOG 3 MIN READ

Announcing General Availability of Inbound SMTP DANE with DNSSEC for Exchange Online

The_Exchange_Team Platinum Contributor
Oct 28, 2024

Today, we are excited to announce the General Availability of Inbound SMTP DANE with DNSSEC! This new capability of Exchange Online enhances the security of email communications by supporting two security standards: DNS-based Authentication of Named Entities (DANE) for SMTP and Domain Name System Security Extensions (DNSSEC).

Instructions for implementing it in your tenant are at How SMTP DNS-based Authentication of Named Entities (DANE) secures email communications. We are actively updating documentation to remove the Preview verbiage.

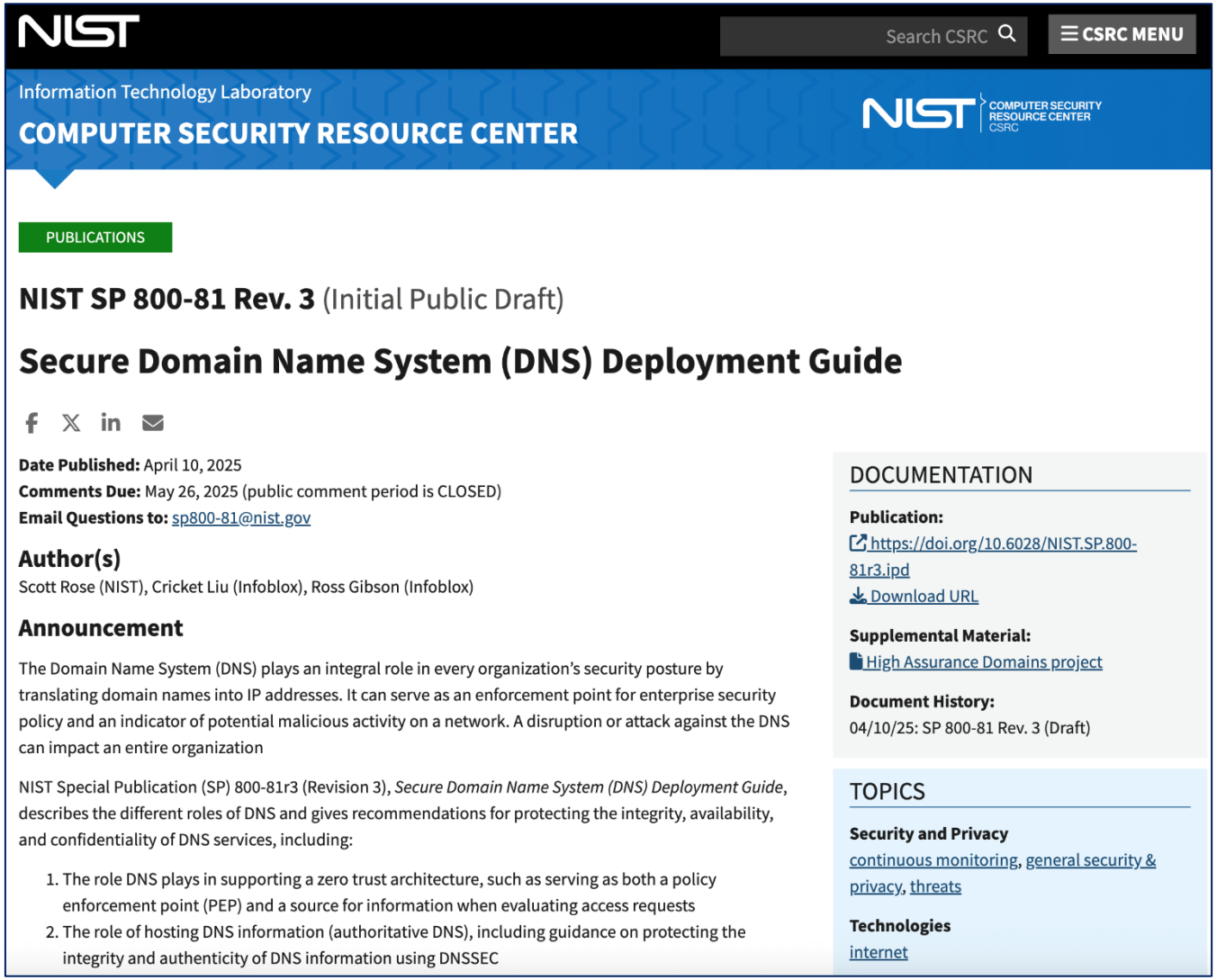
SMTP DANE and DNSSEC

SMTP DANE with DNSSEC provides a secure connection between sending and receiving mail servers that is resistant to both TLS-downgrade attacks and adversary-in-the-middle attacks (a form of eavesdropping where the communication is monitored or modified by a bad actor).

Here's how it works:

1. **DNSSEC**: Protects DNS queries from tampering by ensuring the integrity of DNS records using cryptographic signatures. It prevents attacks like DNS spoofing.
2. **DANE for SMTP**: Uses DNSSEC to securely advertise TLS (Transport Layer Security) certificates for email servers via the TLS Authentication (TLSA) DNS record. It allows email servers to enforce encrypted communication (SMTP over TLS) and ensures that connections are only established with servers using valid certificates.

DNSSEC : quelques actualités



NIST

Search CSRC

CSRC MENU

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

NIST COMPUTER SECURITY RESOURCE CENTER CSRC

PUBLICATIONS

NIST SP 800-81 Rev. 3 (Initial Public Draft)

Secure Domain Name System (DNS) Deployment Guide

Date Published: April 10, 2025
Comments Due: May 26, 2025 (public comment period is CLOSED)
Email Questions to: sp800-81@nist.gov

Author(s)

Scott Rose (NIST), Cricket Liu (Infoblox), Ross Gibson (Infoblox)

Announcement

The Domain Name System (DNS) plays an integral role in every organization's security posture by translating domain names into IP addresses. It can serve as an enforcement point for enterprise security policy and an indicator of potential malicious activity on a network. A disruption or attack against the DNS can impact an entire organization

NIST Special Publication (SP) 800-81r3 (Revision 3), *Secure Domain Name System (DNS) Deployment Guide*, describes the different roles of DNS and gives recommendations for protecting the integrity, availability, and confidentiality of DNS services, including:

1. The role DNS plays in supporting a zero trust architecture, such as serving as both a policy enforcement point (PEP) and a source for information when evaluating access requests
2. The role of hosting DNS information (authoritative DNS), including guidance on protecting the integrity and authenticity of DNS information using DNSSEC

DOCUMENTATION

Publication:
https://doi.org/10.6028/NIST.SP.800-81r3.ipd
Download URL

Supplemental Material:
High Assurance Domains project

Document History:
04/10/25: SP 800-81 Rev. 3 (Draft)

TOPICS

Security and Privacy
continuous monitoring, general security & privacy, threats

Technologies
internet

2

Le fonctionnement du DNS (Domain Name System)

Toutes vos activités internet passent par le DNS

Fonction → traduire un nom en adresse IP utilisable :

- chaque service en ligne (site, messagerie, application) est identifié par un nom de domaine
- ce nom est l'identité unique de votre organisation ou de vos services sur internet

Le DNS publie les informations techniques nécessaires à cette identification

- Adresse IP (A, AAAA) pour accéder au site
- Serveurs de messagerie (MX, SPF, DKIM, DMARC)
- Services spécifiques comme la messagerie instantanée, HTTPS, SSH, vérification de domaine : (SRV, SVCB, SSHFP, TXT…)

→ Le DNS est donc critique

Les acteurs du DNS

1. www.pik.bzh ?

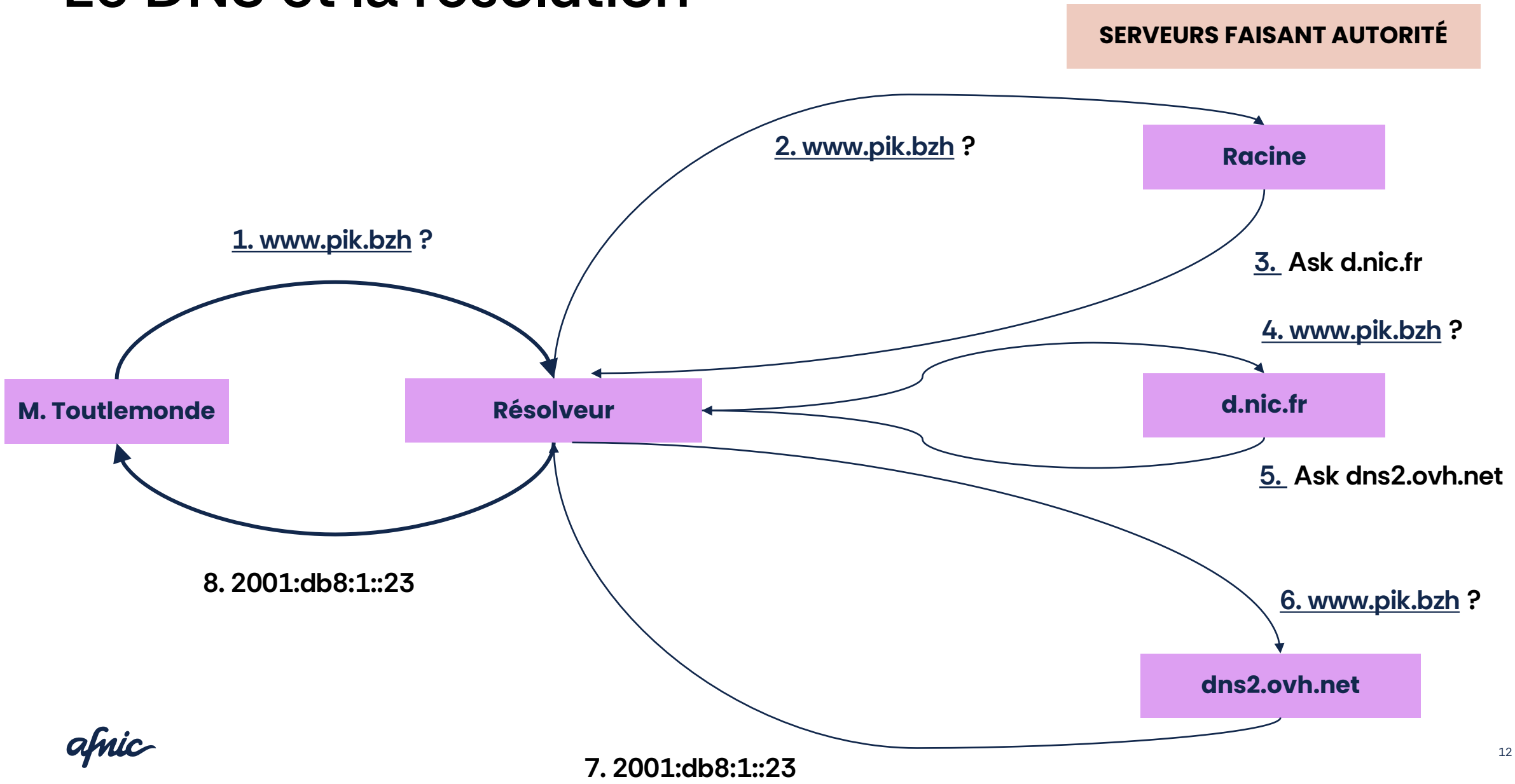
Le **résolveur** va répondre avec l'adresse IP (un enregistrement **A** ou **AAAA**), sauf s'il ne l'a pas…

Exemple : FAI (Orange, Free, Bouygues), résolveur public (Cloudflare, Google, DNS4EU), résolveur d'entreprise.

Le **serveur faisant autorité** (ou hébergeur DNS) va la lui fournir ou lui indiquer où la trouver.

Exemple : Bureaux d'enregistrement, Entreprises, Associations, Universités, Particuliers

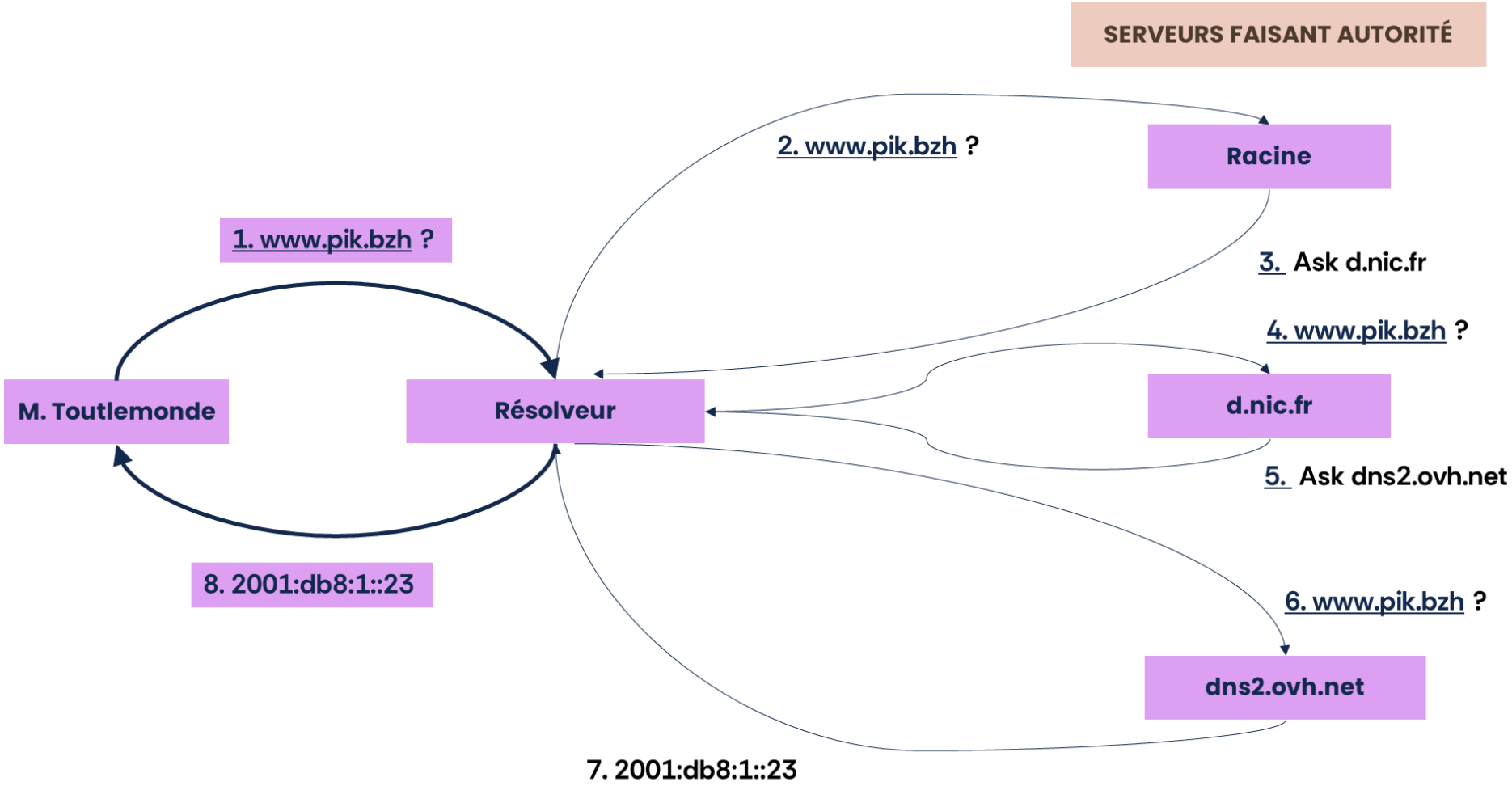
Le DNS et la résolution



3

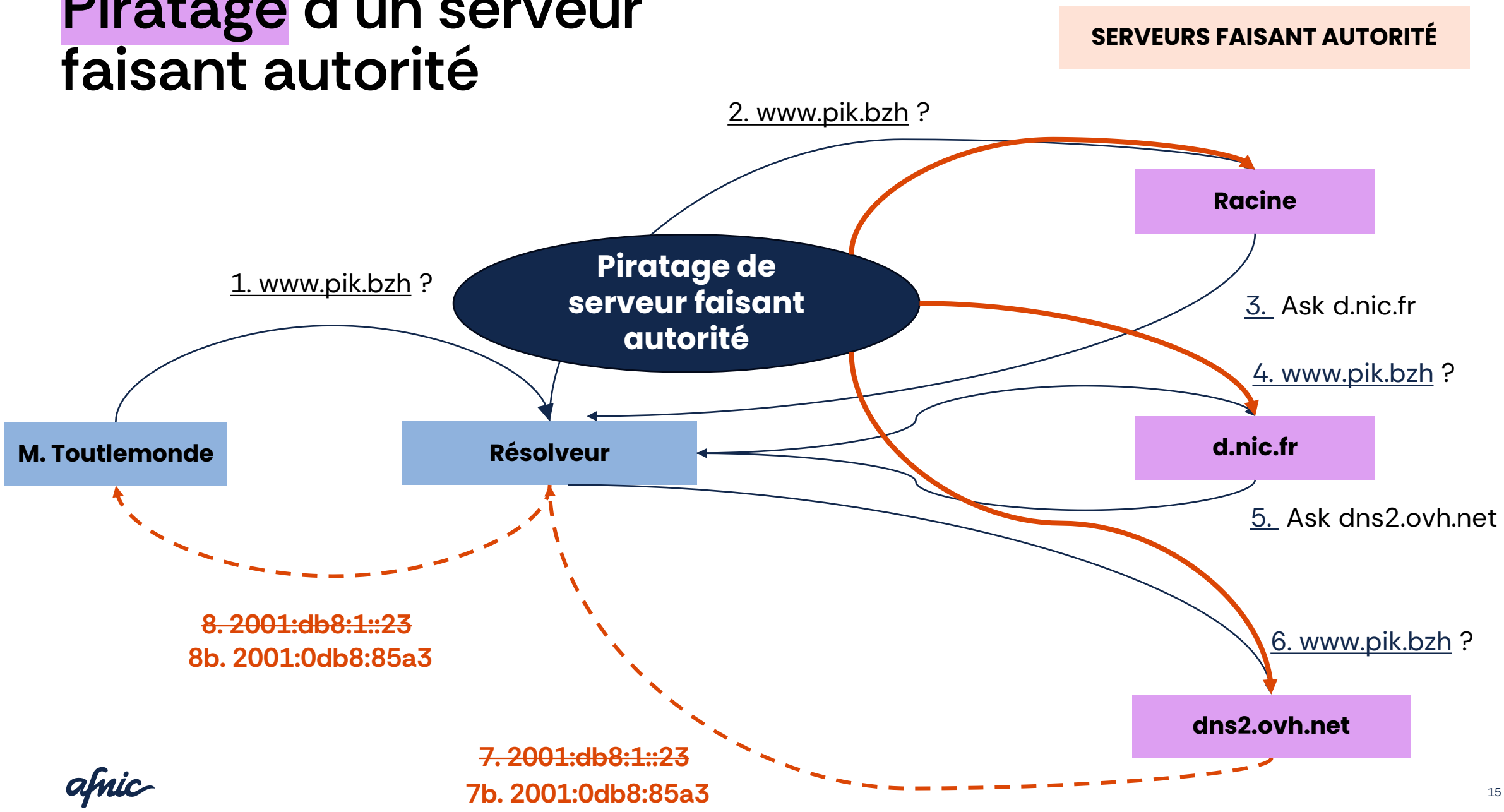
DNSSEC : les risques auxquels ce protocole répond

Les réponses DNS peuvent être falsifiées



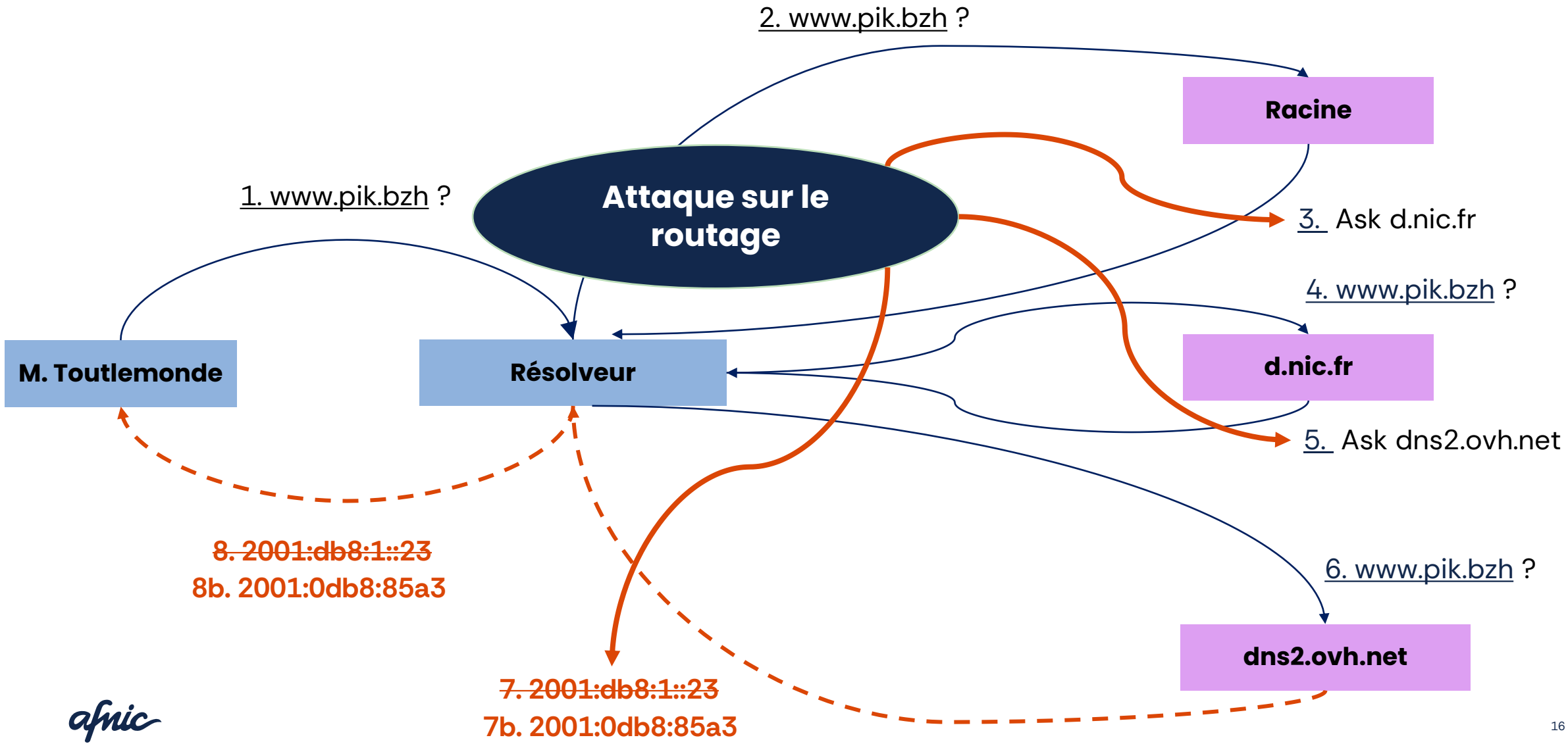
Les mécanismes de sécurité du DNS sont insuffisants, un attaquant peut injecter de fausses réponses.

Piratage d'un serveur faisant autorité

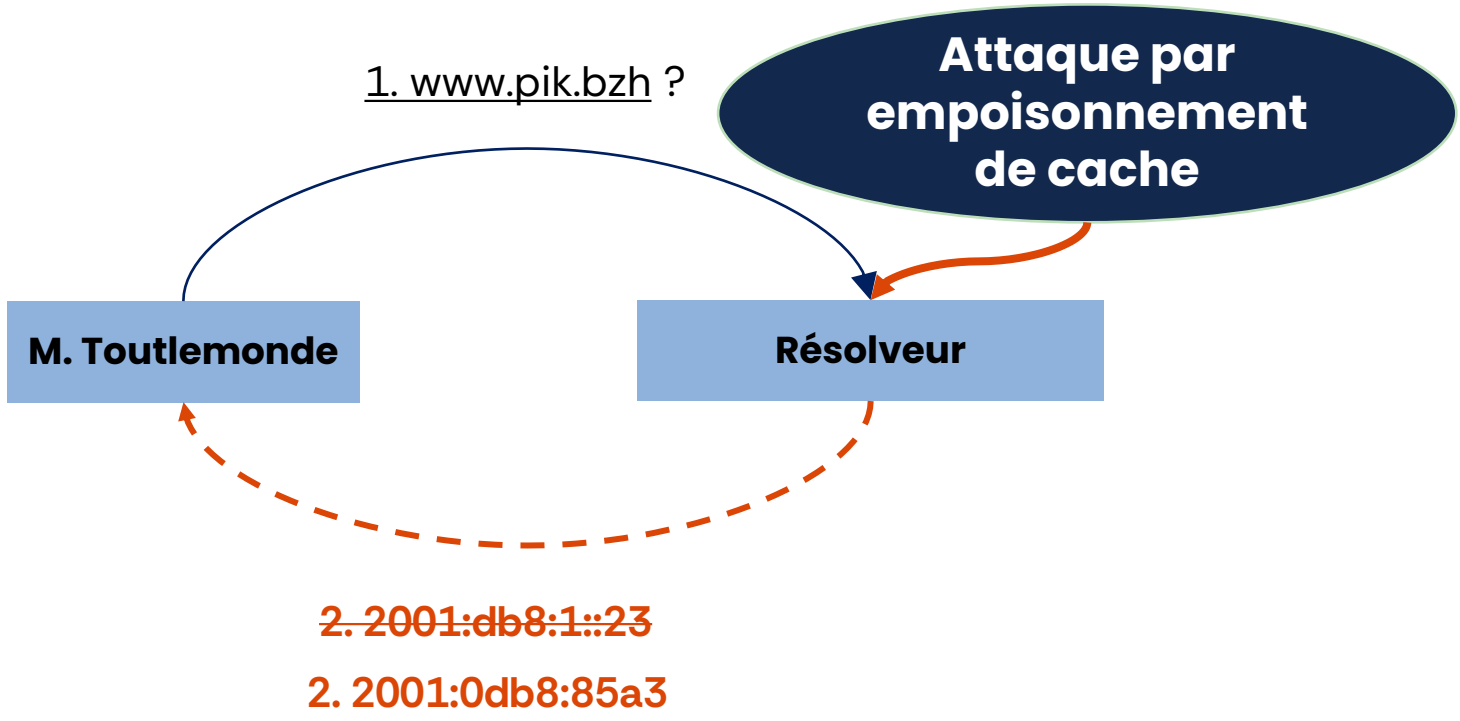


Attaque sur le routage

SERVEURS FAISANT AUTORITÉ



Empoisonnement de cache



SERVEURS FAISANT AUTORITÉ

Racine

d.nic.fr

dns2.ovh.net

Ce qu’il faut en retenir

→ Toutes ces attaques ont un point commun : elles exploitent l’absence de garantie d’authenticité du DNS

→ Tout ce qui est critique est signé cryptographiquement de nos jours : le DNS doit l’être aussi

4

Les principes de DNSSEC

Le principe de DNSSEC

- DNSSEC signe cryptographiquement les enregistrements DNS
- Cryptographie standard
- Peu importe le serveur répondant : la signature peut être vérifiée

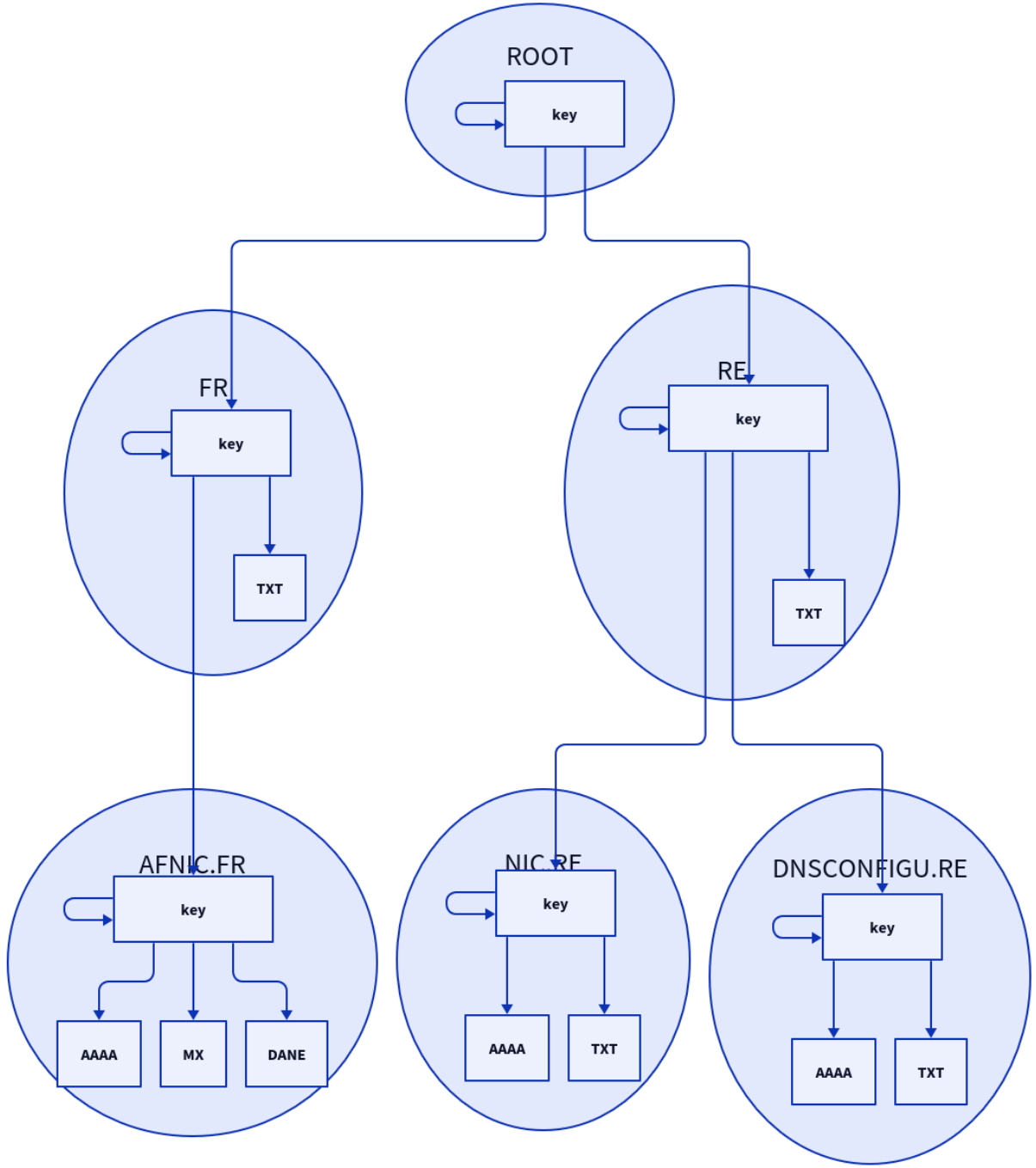
Une chaîne de confiance

- La clé publique du domaine est signée par le domaine parent
- Il suffit donc de connaître la clé de la racine

→ DNSSEC n'ajoute pas une nouvelle couche d'acteurs : il s'appuie sur la hiérarchie DNS existante (racine, TLD, domaine)

DNSSEC bien déployé

DNSSEC est une chaîne de confiance qui est la même que celle du DNS, sans introduire de nouveaux acteurs.



Déploiement

Deux types d'acteurs doivent agir.

- Le domaine est signé par le gestionnaire choisi par le titulaire
- Les résolveurs valident les enregistrements récupérés

Ce qu'il faut en retenir

Le protocole DNSSEC :

- **Garantit l'authenticité des réponses**
- **Représente la seule protection contre l'empoisonnement de cache**

Ce que le protocole DNSSEC ne garantit pas :

- **La confidentialité**
- **Il ne protège pas contre un détournement du nom de domaine dû à un manque de sécurisation de ce dernier** (ex : mot de passe de l'interface bureau d'enregistrement trop faible ou partagé avec plusieurs personnes)

5

Mettre en place DNSSEC

Les étapes clés

Dans un premier temps :

- Création des clés
- Génération des signatures
- Servir les clés et les signatures

Dans un deuxième temps :

- Publication du DS dans la Zone parente
  - Aucun risque tant que le DS n'est pas publié !

Ce qu’il faut bien garder en tête

- Comme tout projet de sécurité, DNSSEC demande une montée en compétences
- Automatisez la signature de zone
- Surveillez activement vos serveurs DNS
- Protégez vos clés

5

Conclusion

Un point sur la situation actuelle

- Le déploiement de DNSSEC progresse mais lentement
- Et tous les résolveurs ne valident pas

Nos ressources complémentaires pour approfondir vos connaissances sur DNSSEC

- Article de blog sur la Cryptographie post-quantique (PQC et DNSSEC), par Stéphane Bortzmeyer : lien

- Et pour aller encore plus loin dans le renforcement de votre expertise

L'Afnic dispense une formation dédiée sur 2 jours

« Sécuriser votre infrastructure DNS grâce à DNSSEC » pour :

- Acquérir la connaissance technique de l'extension DNSSEC
- Pouvoir opérer un résolveur (Unbound) pour valider les réponses avec DNSSEC
- Construire une infrastructure DNSSEC avec OpenDNSSEC et gérer les clés BIND pour servir les zones signées

Programme complet et inscriptions sur : https://www.afnic.fr/produits-services/formations/dnssec/

Prochaines sessions :
Du 20 au 21 nov. 2025 – du 2 au 3 avril 2026 – du 22 au 23 juin 2025

Merci pour votre participation !

Des questions ?

Internet
made in France

Contacts :

Stéphane Bortzmeyer
Ingénieur Expert R&D
stephane.bortzmeyer@afnic.fr

Michaël Timbert
Ingénieur R&D
michael.timbert@afnic.fr

Lotfi Benyelles
Responsable formation
lotfi.benyelles@afnic.fr

Association Française pour le Nommage Internet en Coopération

7 Avenue du 8 mai 1945, 78280 Guyancourt - France
Tel. +33 (0)1 39 30 83 00

www.afnic.fr | contact@afnic.fr | Facebook : facebook.com/afnic.fr