RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

AUTOMATISATION DE LA GESTION DES CERTIFICATS AVEC ACME

LES FONDAMENTAUX

ANSSI-BP-106
10/09/2025

PUBLIC VISÉ :

Développeur Administrateur RSSI DSI Utilisateur

Informations

Attention

Ce document rédigé par l'ANSSI s'intitule **« Automatisation de la gestion des certificats avec ACME »**. Il est téléchargeable sur le site `cyber.gouv.fr`.

Évolutions du document :

VERSION	DATE	NATURE DES MODIFICATIONS
1.0	24/12/2024	Version Initiale
1.1	10/09/2025	Numérotation des recommandations

Table des matières

1
Préambule

Ce document liste des recommandations pour la mise en œuvre d'un service de gestion automatisée de certificats électroniques d'authentification de serveur web reposant sur le protocole ACME (*Automatic Certificate Management Environment*).
Dans la suite du document, le terme « certificat » sera utilisé en lieu et place du terme « certificat électronique d'authentification de serveur web ».
Pour appréhender au mieux ces recommandations, il est nécessaire d'avoir lu la RFC 8555 [13] sur le protocole ACME, qui décrit notamment les notions liées au protocole ACME évoquées dans ce document.

L'automatisation de la gestion des certificats assure un gain en efficacité et limite le risque d'indisponibilité des applicatifs métiers lorsqu'ils ne sont pas renouvelés. Étant donné que la durée de vie des certificats est de plus en plus courte, il peut s'avérer intéressant d'automatiser leur renouvellement, pour des raisons d'économie de charge de travail chez les demandeurs de certificats.

Attention

Cependant l'automatisation apporte de nouveaux risques, car elle implique notamment une plus grande exposition de l'autorité de certification avec l'ajout d'un serveur ACME exposé sur un réseau pas forcément maîtrisé par l'entité opérant l'AC (par exemple, dans le cas d'une AC publique, le serveur ACME est exposé sur Internet), et augmente la surface d'attaque côté demandeur de certificats avec la mise en œuvre d'un client ACME.

La mise en œuvre de l'automatisation de la gestion des certificats implique des changements techniques très importants sur la manière de délivrer les certificats.
Concernant le fournisseur de certificats, la mise en œuvre de l'automatisation ne devra pas être réalisée par le simple ajout d'un greffon (*plugin*) sur l'infrastructure de gestion des clés existante. En particulier, une autorité de certification intermédiaire dédiée à l'émission automatisée de certificats devra être créée. De plus, un serveur ACME devra être mis en œuvre, ainsi que la gestion de comptes externes d'administration ACME et des éléments de *binding* [1] associés.
Concernant le demandeur de certificats, l'utilisation d'ACME impose une délivrance décentralisée des certificats, ce qui implique un changement de rôles des parties prenantes à la gestion des certificats. En l'absence d'automatisation, les certificats sont délivrés au responsable des certificats (en charge de la demande et du suivi du cycle de vie du certificat) qui les distribue aux administrateurs des serveurs web concernés. Avec l'automatisation, le responsable du certificat ne recevra pas directement le certificat demandé, car celui-ci sera automatiquement reçu par le client ACME, à proximité du serveur web. L'émission des certificats reste quant à elle centralisée au niveau de l'autorité de certification.

1. MAC key et keyID de l'*external account* évoqué dans la RFC 8555. Voir la définition du compte externe d'administration ACME au chapitre 2.1.

Ces travaux doivent être réalisés quelle que soit l'architecture retenue par le fournisseur de certificats et celle retenue par le demandeur de certificats pour mettre en œuvre l'automatisation.

La mise en œuvre de l'automatisation de la gestion des certificats avec le protocole ACME entraine des risques côté fournisseur de certificats et côté demandeur de certificats (cf. 2.3), que les recommandations de ce document visent à atténuer.

2
Principes généraux

2.1 Définitions

Autorité de certification (AC) Le terme « autorité de certification » comprend ici notamment l'autorité d'enregistrement, la base de données associée et le service de génération de certificats du fournisseur de certificats.

AC publique ACME Le terme « AC publique ACME » désigne ici une AC mettant en œuvre l'automatisation de la délivrance de certificats en utilisant le protocole ACME et dont l'AC racine signataire de l'AC publique ACME est présente dans les magasins de confiance des certificats des navigateurs web. L'AC est ainsi reconnue sur Internet. Selon le service de gestion automatisée des certificats proposé par l'AC, la simple capacité à faire valider un défi ACME pour un domaine donné peut suffire à faire délivrer le certificat associé par cette AC (c'est le cas de LET'S ENCRYPT par exemple).

AC interne ACME Le terme « AC interne ACME » désigne ici une AC non reconnue publiquement, mettant en œuvre l'automatisation de la délivrance de certificats en utilisant le protocole ACME. L'AC racine signataire de l'AC interne ACME n'est pas présente par défaut dans les magasins de confiance des navigateurs web, sa présence nécessite un ajout explicite.

Comptes L'architecture proposée met en œuvre deux types de compte : les comptes externes d'administration ACME et les comptes ACME.

Compte externe d'administration ACME Ce compte sert à définir des paramètres afin de limiter et contrôler les actions réalisables par le ou les comptes ACME, comme par exemple, une liste des domaines autorisés. La RFC 8555 ne permet pas de définir de tels paramètres pour un compte ACME, d'où la nécessité de créer un compte externe d'administration ACME. Le compte externe d'administration ACME correspond à l'« *external account* » évoqué dans la RFC 8555.
Le compte externe d'administration ACME est créé auprès de l'autorité d'enregistrement, suite à l'authentification du demandeur de certificats (une personne physique ou morale). La création du compte externe d'administration ACME entraine la création d'éléments d'authentification spécifiques au compte externe d'administration ACME par l'AC (une clé secrète de MAC, appelé MAC key et son identifiant, appelé KeyID). Ces éléments (MAC key et KeyID) sont appelés éléments de

binding. Ces éléments de *binding* sont transmis au demandeur de certificats par l'AC. Les éléments de *binding* permettent au demandeur de certificats d'associer un ou plusieurs comptes ACME à un compte externe d'administration ACME, par le mécanisme nommé EAB (*External Account Binding*) dans la RFC 8555.
Lors de la création du compte externe d'administration ACME, ses paramètres (telle que la liste des domaines autorisés) pourront être définis, et pourront être mis à jour au cours du temps. Par exemple, lorsqu'un compte externe d'administration ACME définissant une liste des domaines autorisés est associé à un compte ACME, les demandes de certificat émises par ce dernier pour un nom de domaine absent de la liste seront refusées par l'AC.

Compte ACME Ce compte est créé par un client ACME, il correspond au *ACME account* de la RFC 8555. Un compte ACME est associé à un unique compte externe d'administration ACME par le mécanisme nommé EAB (*External Account Binding*) dans la RFC 8555 (l'EAB peut par exemple être mis en œuvre par le client ACME *certbot* lors de la création de compte ACME, avec les options *- -eab-kid* et *- -eab-hmac-key).* À chaque compte ACME est associé un bi-clé (composé d'une clé privée et d'une clé publique) JWK. Les requêtes du compte ACME à destination du serveur ACME du fournisseur de certificats sont authentifiées par une signature JWS réalisée par la clé privée du bi-clé du compte ACME.

Défi ACME Le défi ACME permet au demandeur de certificat de prouver sa possession du nom de domaine du certificat demandé, auprès du serveur ACME. Différents types de défi ACME sont définis par des RFC (HTTP-01 [13], DNS-01 [13], TLS-ALPN-01 [15]), ils sont abordés en 3.1.6 et 3.2.1. Par exemple, le défi HTTP-01 consiste à déposer un fichier contenant un aléa fourni par le serveur ACME sur un chemin prédéfini du serveur web, alors que le défi DNS-01 consiste à créer un enregistrement TXT contenant un aléa fourni par le serveur ACME auprès du serveur DNS faisant autorité sur la zone DNS à laquelle appartient le serveur web. La validation par le serveur ACME de la résolution du défi ACME est nécessaire à la délivrance du certificat.

Renouvellement de certificat Un renouvellement de certificat désigne la génération d'un nouveau certificat pour le même nom de domaine et éventuellement les mêmes champs ou extensions, mais avec la génération d'un nouveau bi-clé (composé d'une clé privée et d'une clé publique).

Pour les définitions d'autres termes spécifiques aux infrastructures de gestion de clés, se référer au CyberDico de l'ANSSI [2] ou au RGS et ses annexes A [9].

2.2 Architecture

Un exemple d'architecture est représenté sur le schéma 1. Les différents éléments intervenant dans l'automatisation de la gestion des certificats sont listés ci-dessous :

- un service de génération des certificats ;

- une autorité d'enregistrement pour la création des comptes externes d'administration ACME et la gestion des éléments de *binding* ;
- une zone de stockage des éléments de *binding* et les paramètres des comptes externes d'administration ACME (par exemple : base de données, système de fichier) ;
- un serveur ACME ;
- un client ACME ;
- un serveur web sur lequel le certificat sera installé ;
- un demandeur de certificats associé à un compte externe d'administration ACME.

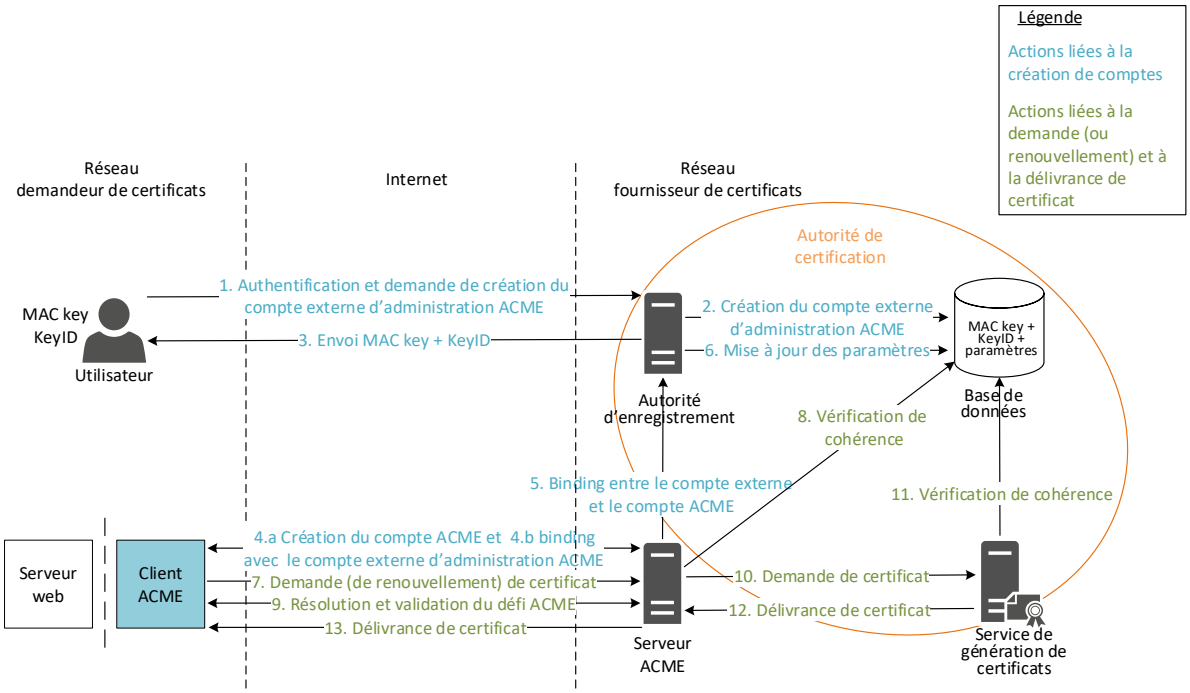


Schéma 1 – Architecture haut niveau

La création du compte externe d'administration ACME (étapes 1, 2 et 3), la création du compte ACME (étape 4.a) et l'association de ces deux comptes (étapes 4.b, 5 et 6) ne sont à réaliser qu'une seule fois pour un même couple de compte externe d'administration ACME et compte ACME. Une fois ces deux compte créés et associés, la demande (ou le renouvellement) de certificats (étape 7), la résolution de défi ACME (étape 9) et la réception de certificat peuvent être complètement automatisées pour le demandeur de certificats.

Par comparaison, un exemple de déroulement des étapes pour obtenir de manière automatisée un certificat auprès d'une AC publique ACME, est représenté sur le schéma 2.

Sur les schémas 1 et 2, ne sont pas représentées les briques de filtrage nécessaires à l'interconnexion sécurisée des trois réseaux représentés.

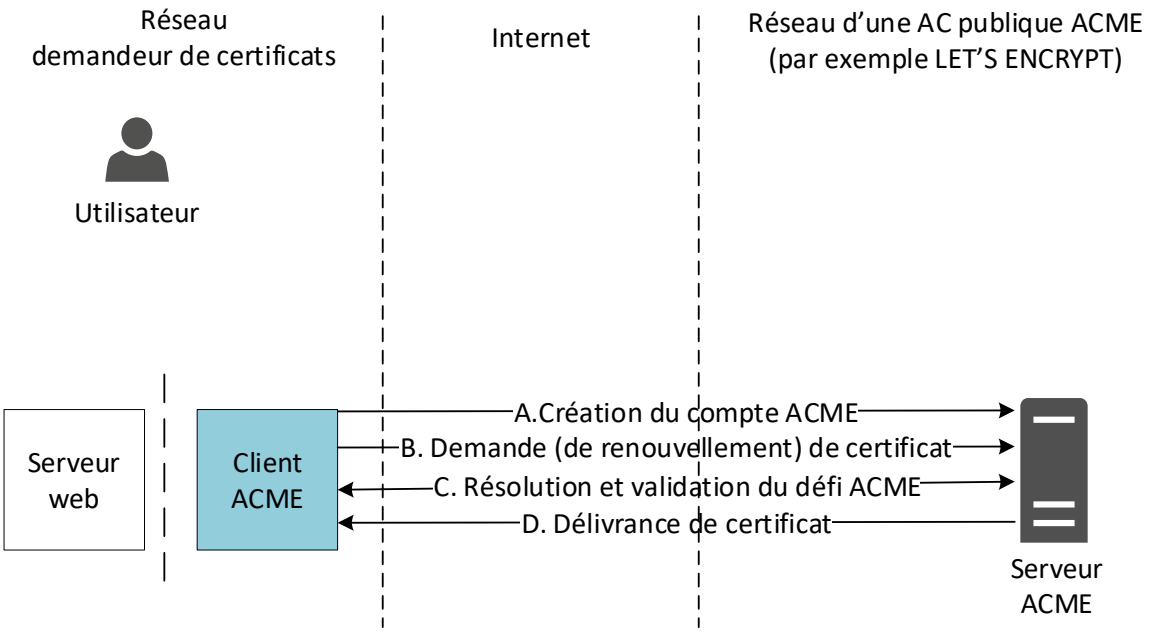


Schéma 2 – Exemple d'étapes à suivre pour l'obtention d'un certificat avec ACME, auprès d'une AC publique ACME

La délivrance de certificat par une AC publique ACME ne nécessite pas forcément un enrôlement du demandeur de certificats.
Excepté l'enrôlement, les demandes de certificats et de renouvellement sont similaires auprès d'une AC nécessitant un enrôlement (comme recommandé par ce document) et auprès des AC ne le nécessitant pas : ces demandes peuvent être complètement automatisées pour le demandeur de certificats.

Pour le cas d'une AC interne ACME, le client ACME et le serveur ACME ne sont pas nécessairement exposés sur Internet, ils peuvent être reliés par des réseaux internes. Leurs échanges ne transitent alors pas sur Internet.

2.3 Risques

Les risques présentés dans ce chapitre sont valables quel que soit le niveau d'exposition du service d'automatisation (exposition sur Internet ou exposition sur des réseaux internes). Les risques présentés ci-dessous ne sont pas exhaustifs.

2.3.1 Risques concernant le fournisseur de certificats

Compromission de l'autorité d'enregistrement
Impact : l'attaquant pourrait créer un compte externe d'administration ACME et y associer une liste arbitraire de domaines. L'attaquant serait ainsi en mesure de demander et d'obtenir des certificats auprès de l'AC, pour les domaines pour lesquels il est en mesure de faire valider un défi ACME.
Les éléments de *binding* associent au moins un compte ACME à un compte externe d'administration ACME. Toute demande de certificat étant liée à un compte ACME, lui-même associé à un compte externe d'administration ACME, la simple capacité à résoudre un défi ACME par un attaquant n'est pas suffisante à lui faire délivrer un certificat dont le nom de domaine n'appartient pas à la liste des domaines autorisés. Ainsi, les éléments de *binding* servent à éviter à l'AC d'émettre des certificats illégitimes en cas de compromission des serveurs (web ou DNS par exemple) résolvant des défis ACME.
La seule compromission des éléments de *binding* n'a pas d'impact si l'attaquant n'est pas en mesure de faire valider des défis ACME.
Les éléments de *binding* n'apportent pas de protection au demandeur de certificats contre un attaquant en mesure de faire valider un défi ACME car l'attaquant pourra alors se faire délivrer un certificat valide auprès d'une autre AC publique ACME.

Compromission du serveur ACME
Impact : l'impact est dépendant de l'architecture du service de gestion automatisée des certificats. En cas de cloisonnement entre le serveur ACME et l'autorité d'enregistrement, la base de données et le service de génération des certificats, l'impact est limité à des requêtes illégitimes auprès de l'AC (qui doivent être refusées par l'AC) et à une indisponibilité du service. A contrario, en cas d'absence ou de faible cloisonnement entre le serveur ACME avec l'AC, l'impact peut être équivalent à celui d'une compromission de l'AC.

Usurpation de l'identité du titulaire du compte externe d'administration ACME
Impact : l'attaquant serait en mesure de modifier les paramètres du compte externe d'administration ACME (comme par exemple la liste des domaines autorisés).

Usurpation d'un nom de domaine par un demandeur de certificats légitime
Impact : un demandeur de certificats légitime, ayant un compte externe d'administration ACME, pourrait demander l'ajout de noms de domaine qu'il ne possède pas dans sa liste des domaines autorisés. Le demandeur de certificats serait ainsi en mesure de demander et d'obtenir des certificats par l'AC, pour les domaines présents dans sa liste des domaines autorisés et pour lesquels il est en mesure de faire valider un défi ACME.

Détournement du trafic émanant du serveur ACME
Impact : un attaquant serait en mesure de faire valider les défis ACME pour des domaines qu'il ne maîtrise pas, par détournement BGP. Il pourrait ainsi faire émettre par l'AC des certificats pour des domaines présents dans la liste de domaines autorisés de son compte externe d'administration ACME.

2.3.2 Risques concernant le demandeur de certificats

Compromission de la clé privée du compte ACME
Impact : un impact de la compromission du seul compte ACME est de rendre le compte ACME inutilisable par le demandeur de certificats légitime suite à l'altération de la clé privée du compte ACME (atteinte en disponibilité).
Les demandes de certificat à partir d'un compte ACME compromis n'aboutiront à la délivrance d'un certificat par l'AC ou par une autre AC publique ACME que pour les noms de domaines pour lesquels l'attaquant est en mesure de faire valider un défi ACME. L'attaquant ayant compromis un compte ACME pourrait demander et obtenir la révocation des certificats délivrés à partir de ce compte ACME (atteinte en disponibilité).

Compromission d'un serveur hébergeant un client ACME
Impact : identique à la compromission de la clé privée du compte ACME. De plus, selon l'architecture côté demandeur de certificats, le client ACME peut avoir des droits très élevés sur des serveurs web ou sur les serveurs DNS : un attaquant pourrait ainsi demander des certificats pour des noms de domaines pour lesquels il a suffisamment de droits pour faire valider les défis ACME.

Compromission du client ACME
Impact : identique à la compromission d'un serveur hébergeant un client ACME.

Compromission du compte externe d'administration ACME (éléments de *binding* : MAC key + keyID)
Impact : l'attaquant ayant compromis le compte externe d'administration ACME est en mesure de créer un compte ACME associé au compte externe d'administration ACME.
Les demandes de certificat à partir d'un compte ACME associé à un compte externe d'administration ACME compromis n'aboutiront à la délivrance d'un certificat par l'AC que pour les noms de domaines pour lesquels l'attaquant est en mesure de faire valider un défi ACME.

3
Recommandations

3.1 Recommandations concernant le fournisseur de certificats (AC)

3.1.1 Compte externe d'administration ACME

Pour le cas d'usage de certificats délivrés et renouvelés par une AC interne ACME, la mise en œuvre des recommandations concernant le compte externe d'administration ACME peut éventuellement être optionnelle si la bonne maîtrise des noms de domaine par l'AC est justifiée par une analyse des risques.

R1 Un compte externe d'administration ACME doit être créé pour l'utilisation du service de gestion automatisée des certificats et doit être associé à au moins une personne physique.

R2 Pour permettre la création du compte externe d'administration ACME, le demandeur de certificats doit s'authentifier au travers d'un mécanisme d'authentification multifacteur conforme au guide *Recommandations relatives à l'authentification multifacteur et aux mots de passe* [10], mis à disposition par le fournisseur de certificats.

R3 Un compte externe d'administration ACME peut avoir plusieurs comptes ACME associés.

R4 Une demande de mise à jour des paramètres du compte externe d'administration ACME (comme de la liste des domaines autorisés) doit être authentifiée au travers d'un mécanisme d'authentification multifacteur conforme au guide *Recommandations relatives à l'authentification multifacteur et aux mots de passe* [10].

R5 Les paramètres du compte externe d'administration ACME doivent notamment comprendre : la liste des domaines autorisés, la durée de validité du compte externe d'administration ACME, la liste des comptes ACME associés à ce compte externe d'administration ACME et leur statut (valide, suspendu, désactivé), et le nombre de regénération de la clé secrète du compte externe d'administration ACME (MAC key).

R6 L'alimentation de la liste des domaines autorisés doit être validée par une vérification humaine. Des contrôles automatiques peuvent être mis en œuvre mais validés, in fine, par un personnel du fournisseur de certificats.

R7 Lors de l'alimentation de la liste des domaines autorisés, l'AC doit vérifier s'il existe un enregistrement DNS *Certification Authority Authorization* (CAA) [2] pour le nom de domaine du certificat à émettre. Dans le cas où ce dernier existe, l'AC doit vérifier qu'elle fait bien partie des AC autorisées à émettre des certificats pour ce nom de domaine.

3.1.2 Compromission, suspicion de compromission et renouvellement du compte externe d'administration ACME

R8 Un compte externe d'administration ACME doit avoir une période de validité définie, d'au maximum trois ans.

R9 Les éléments de *binding* d'un compte externe d'administration ACME doivent être renouvelables à la demande du titulaire du compte externe d'administration ACME. Les secrets cryptographiques doivent être renouvelés périodiquement.

R10 En cas de compromission d'un des éléments de *binding* d'un compte externe d'administration ACME, le processus « Compromission d'un compte externe d'administration ACME » (cf. A.2), doit être mis en œuvre.

R11 En cas de suspicion de compromission d'un des éléments de *binding* d'un compte externe d'administration ACME, le processus « Suspicion de compromission d'un compte externe d'administration ACME » (cf. A.3) doit être mis en œuvre.

R12 La fin de validité d'un compte externe d'administration ACME doit impliquer le renouvellement du compte externe d'administration ACME, selon le processus « Renouvellement d'un compte externe d'administration ACME » (cf. A.1).

R13 Toute requête du demandeur de certificats liée à un processus de compromission, suspicion de compromission ou renouvellement du compte externe d'administration ACME doit être authentifiée au travers d'un mécanisme d'authentification multifacteur conforme au guide *Recommandations relatives à l'authentification multifacteur et aux mots de passe* [10].

3.1.3 Compte ACME

R14 Un compte ACME doit être associé à un unique compte externe d'administration ACME.

R15 Il est recommandé de pouvoir suspendre un compte ACME, par exemple en cas suspicion de compromission du bi-clé du compte ACME.

R16 En cas de compromission du bi-clé d'un compte ACME, le processus « Compromission d'un compte ACME » (cf. A.5) doit être mis en œuvre.

2. La CAA est une mesure de sécurité qui permet aux propriétaires de domaines de spécifier dans leurs serveurs de noms de domaine (DNS) quelles sont les AC autorisées à émettre des certificats pour ce domaine.Si une autorité de certification reçoit une commande de certificat pour un domaine avec un enregistrement CAA et que cette autorité de certification n'est pas répertoriée comme un émetteur autorisé, il lui est interdit d'émettre le certificat pour ce domaine ou tout sous-domaine. Les enregistrements CAA sont standardisés par l'IETF [14].

R17 En cas de suspicion de compromission du bi-clé d'un compte ACME, le processus « Suspicion de compromission d'un compte ACME » (cf. A.6) doit être mis en œuvre.

R18 Un compte ACME doit pouvoir être renouvelable, sur demande du demandeur de certificats. En cas de renouvellement d'un compte ACME, le processus « Renouvellement d'un compte ACME » (cf. A.4) doit être mis en œuvre.

3.1.4 Binding du (des) compte(s) ACME avec le compte externe d'administration ACME

R19 L'algorithme de MAC utilisé pour le *binding* d'un compte ACME à un compte externe d'administration ACME doit être conforme au guide des mécanismes cryptographiques [5] (par exemple, l'algorithme HMAC-SHA256).

R20 La clé secrète utilisée pour le *binding* d'un compte ACME (MAC key) à un compte externe d'administration ACME doit être générée par l'autorité d'enregistrement à partir d'un générateur aléatoire conforme au guide des mécanismes cryptographiques [5].

R21 La clé secrète utilisée pour le *binding* d'un compte ACME à un compte externe d'administration ACME (MAC key) doit être stockée protégée en confidentialité et en intégrité par des mécanismes conformes au guide des mécanismes cryptographiques [5].

R22 La transmission de la clé secrète d'un compte externe d'administration ACME (MAC key) doit être effectuée de manière à assurer sa confidentialité et son intégrité, avec des mécanismes conformes au guide des mécanismes cryptographiques [5]. Cette clé peut par exemple être envoyée dans un conteneur Zed!, ou via un canal TLS conforme aux recommandations de l'ANSSI [6].

R23 En cas de perte de la clé secrète du compte externe d'administration ACME (MAC key) par le demandeur de certificats, sans suspicion de compromission, soit le demandeur de certificats demande au fournisseur de certificats de lui transmettre à nouveau l'élément de *binding* (via une procédure comprenant une authentification multifacteur) si le fournisseur de certificats en a la capacité, soit le demandeur de certificats demande la mise en œuvre du processus « Renouvellement d'un compte externe d'administration ACME » (cf. A.1).

R24 Le fournisseur de certificats doit sensibiliser le demandeur de certificats quant à sa gestion des comptes externes d'administration ACME et des comptes ACME. Il devra notamment mettre en lumière les risques liés à l'association de nombreux comptes ACME à un seul compte externe d'administration ACME (par exemple : grande exposition de la clé secrète du compte externe d'administration ACME, remédiation laborieuse en cas de compromission du compte externe d'administration ACME) et à l'opposé, les risques liés à l'utilisation d'un compte ACME pour un compte externe d'administration ACME (par exemple : la difficulté d'usage pour le demandeur de certificats, qui pourrait conduire à des mauvaises pratiques telles qu'une trop grande exposition de la clé secrète du compte ACME).

3.1.5 Protocole ACME

R25 Il est recommandé que les implémentations du serveur ACME et du client ACME soient conformes à la RFC 8555 [13]. Chaque différence avec la RFC 8555 doit être listée dans un document accessible aux utilisateurs du service de gestion automatisée des certificats.

R26 Le serveur ACME doit rejeter toute demande de création ou de renouvellement de certificat dont les domaines (précisés dans l'attribut *commonName* ou dans l'extension *SubjectAlternativeName*) n'appartiennent pas à la liste des domaines autorisés, définie au niveau du compte externe d'administration ACME.

R27 Le serveur ACME doit rejeter toute demande ou renouvellement de certificat pour les sous-domaines (précisés dans l'attribut *commonName* ou dans l'extension *SubjectAlternativeName*) des domaines appartenant à la liste des domaines autorisés si ces sous-domaines n'ont pas été explicitement autorisés.

R28 Le serveur ACME doit mettre en œuvre un mécanisme de validation multi-points des défis ACME [3]. Ainsi, le serveur ACME doit rejeter les demandes de certificat dont le défi ACME associé n'a pas pu être validé par plusieurs points de présence Internet.

R29 Toute demande de certificat doit être soumise à une limite d'échec de validation. Par exemple, il est recommandé d'imposer une limite d'échec de validation de cinq échecs par compte ACME, par nom de domaine et par heure.

3.1.6 Autorité de Certification

R30 Un certificat X.509 intermédiaire doit être exclusivement dédié au service de gestion automatisée des certificats. La limitation du certificat X.509 intermédiaire à la signature de certificats uniquement pour le service de gestion automatisée des certificats permet de limiter les impacts à ce seul service en cas de compromission de cette AC [4].

R31 L'infrastructure du service de gestion automatisée des certificats (autorité d'enregistrement, base de données, serveur ACME, service de génération des certificats) doit être dédiée à la gestion automatisée des certificats. De plus, cette infrastructure doit être cloisonnée, au moins logiquement, avec toute autre infrastructure de gestion des certificats.

R32 Les différents échanges entre le serveur ACME, le service de génération des certificats, l'autorité d'enregistrement, et la base de données qui stocke notamment les éléments de *binding* et les paramètres des comptes externes d'administration ACME doivent être protégés en confidentialité, intégrité et authenticité par des mécanismes conformes au guide des mécanismes cryptographiques [5].

3. Cette validation consiste à ce que la requête de validation du défi ACME soit effectuée depuis plusieurs points de présence Internet. Ceci implique le déploiement de plusieurs serveurs chargés de valider les défis ACME depuis plusieurs systèmes autonomes (ou *Autonomous System*, AS). Plus de détails sur les attaques de détournement de trafic peuvent être trouvés dans l'article suivant [11].

4. L'AC, par nature du service proposé, sera plus exposée qu'une AC ne proposant pas d'automatisation de la gestion des certificats et donc elle sera plus exposée aux menaces d'attaques provenant d'un réseau potentiellement non maîtrisé.

R33 Les droits d'accès à la base de données qui stocke notamment les éléments de *binding* et les paramètres des comptes externes d'administration ACME doivent être limités au strict minimum. En particulier, seule l'autorité d'enregistrement doit pouvoir écrire dans cette base de données.

R34 Avant de transmettre une demande de certificat d'un client ACME au service de génération des certificats, le serveur ACME doit vérifier auprès de la base de données que les paramètres du compte externe d'administration ACME associé au compte ACME à l'origine de la demande de certificat autorisent l'émission du certificat. En particulier, les domaines précisés dans l'attribut *commonName* ou dans l'extension *SubjectAlternativeName* du certificat doivent être présents dans la liste des domaines autorisés.

R35 Avant d'émettre un certificat, le service de génération des certificats doit vérifier auprès de la base de données que les paramètres du compte externe d'administration ACME associé au compte ACME à l'origine la demande de certificat autorisent l'émission du certificat. En particulier, les domaines précisés dans l'attribut *commonName* ou dans l'extension *SubjectAlternativeName* du certificat doivent être présents dans la liste des domaines autorisés.

R36 L'architecture du service de gestion automatisée des certificats doit respecter les bonnes pratiques des guides de l'ANSSI *Recommandations relatives à l'administration sécurisée des systèmes d'information* [7] et *Recommandations relatives à l'interconnexion d'un système d'information à Internet* [4].

R37 À chaque création ou renouvellement de certificat, un nouveau bi-clé associé à ce certificat doit être généré. La réutilisation de clés est proscrite.

R38 Les certificats émis par le service de gestion automatisée des certificats doivent notamment contenir les champs suivants :

- Le champ *Subject Alternative Name* doit être présent et contenir tous les noms de domaine couverts par le certificat (même s'il y a qu'un seul nom de domaine) ;
- Le champ *basicConstraints* doit être positionné à la valeur *CA :FALSE* et en mode critique ;
- Le champ *keyUsage* doit être positionné à la valeur *digitalSignature* et/ou *keyEncipherment* selon le type de clé du certificat, en mode critique ;
- Le champ *ExtendedKeyUsage* doit être positionné à la valeur *id-kp-serverAuth*.

R39 Il est recommandé que la période de validité des certificats émis par le service de gestion automatisée des certificats soit d'au plus 90 jours.

R40 Les certificats doivent pouvoir être renouvelés en amont de leur expiration.

R41 Le serveur ACME doit valider la résolution de défi ACME pour chaque entrée du champ *Subject Alternative Name* d'un certificat donnée.

R42 L'AC ne doit pas délivrer de certificats dits « *wildcard* [5] ».

R43 Il est recommandé de diffuser les informations de révocation des certificats par deux mécanismes distincts afin d'assurer leur redondance (CRL et OCSP par exemple).

R44 Il est recommandé de préciser à l'AC lors de la demande de révocation la raison de la révocation d'un certificat.

5. Un certificat *wildcard* est un certificat valide pour tous les sous-domaines d'un domaine, formulé généralement comme suit **.mondomaine.fr*.

R45 La présence de la raison de révocation dans la CRL et dans la réponse OCSP associées est recommandée.

R46 La demande de révocation d'un certificat doit être émise par un compte autorisé : le compte ACME ayant émis le certificat ou le compte externe d'administration ACME lié au compte ACME ayant émis le certificat. De plus, une demande de révocation signée par la clé privée du certificat à révoquer doit être considérée comme valide par le serveur ACME (uniquement si le champ *keyUsage* du certificat comprend la valeur *digitalSignature*).

R47 Le fournisseur de certificats doit permettre au titulaire du compte externe d'administration ACME de choisir le type de défi ACME parmi HTTP-01, DNS-01 et TLS-ALPN-01.

R48 Le fournisseur de certificats doit mettre à disposition du demandeur de certificats une analyse des risques auxquels le demandeur de certificats s'expose en ayant recours au service de gestion automatisée des certificats ainsi que des recommandations d'usage du service et des recommandations d'architecture. En particulier, le fournisseur doit soumettre au demandeur de certificats une analyse des risques concernant l'usage d'un des trois défis ACME par rapport aux autres. Le tableau 1 récapitule les différents avantages et défauts des défis ACME HTTP-01, DNS-01 et TLS-ALPN-01.

Défi ACME	**HTTP-01**	**DNS-01**	**TLS-ALPN-01**
Avantage	Facile à mettre en œuvre (écriture sur le serveur web)	Preuve de possession de nom de domaine forte (preuve de la maîtrise du DNS)	Facile à mettre en œuvre (supporté par les principaux serveurs web)
Défauts	■ Preuve de possession de nom de domaine faible car vulnérable aux attaques par téléversement de fichiers (*Arbitrary File Upload*) ■ Si le serveur web (ou l'applicatif web qu'il héberge) est vulnérable aux attaques par téléversement de fichiers, alors un attaquant pourra se faire délivrer un certificat pour ce serveur web par une AC ACME publique	■ Potentiellement difficile à mettre en œuvre (interactions entre les équipes DNS et les équipes certificats/serveur web nécessaires, droits fins en écriture à définir par l'intermédiaire d'une délégation de zone ou d'un enregistrement CNAME sur les sous-domaines réservés à la validation des défis ACME DNS-01) ■ Installation nécessaire d'un greffon (greffon non évalué et à maintenir) ■ En cas de mauvaise configuration (droits trop permissifs sur le DNS), l'impact d'une compromission du client ACME est très forte (potentiellement compromission intégrale du DNS)	■ L'extension TLS ALPN est supportée par les principaux serveurs web (Nginx, Apache HTTP Server, Microsoft IIS, etc.), mais pas par tous ■ Non supporté par l'ensemble des clients ACME ■ La résolution du défi TLS-ALPN-01 nécessite un contrôle de la pile logicielle TLS du serveur en charge de terminer le lien TLS du service web/HTTPS et portant les adresses IP issues de la résolution du nom de domaine du certificat demandé
Remarque	Des recommandations de ce document proposent des contre-mesures aux risques du défi HTTP-01 (notamment avec la création d'un compte externe d'administration ACME).	Le défi DNS-01 n'est à mettre en œuvre qu'en cas de maîtrise et maturité sur le sujet (maîtrise du DNS avec droits fins, maintien du greffon).	Adapté aux services de répartition de charge (*load balancers*), aux services de réseau de diffusion de contenu (*Content Delivery Network*) et aux serveurs web exposant du contenu Web exclusivement en HTTPS.

TABLEAU 1 – Tableau comparatif des défis ACME HTTP-01, DNS-01 et TLS-ALPN-01

R49 Des rapports sur les actions liées à un compte externe d'administration ACME donné doivent être envoyés hebdomadairement ou mensuellement au demandeur de certificats correspondant. Ces rapports doivent dresser un état des lieux, en listant notamment le nombre de certifi-

cats générés, révoqués, en cours de validité, ainsi que les évolutions des paramètres du compte externe d'administration ACME, comme par exemple la liste des domaines autorisés.

R50 Parallèlement à l'envoi régulier de rapports, un tableau de bord récapitulatif des actions liées à un compte externe d'administration ACME, mis à jour en temps réel doit être mis à disposition de chaque titulaire de compte externe d'administration ACME.

R51 L'AC doit enregistrer les certificats qu'elle émet parmi les registres du programme *Certificate Transparency*.

R52 L'AC doit vérifier que les registres du programme *Certificate Transparency* [6] ne présentent pas de certificats enregistrés par des AC publiques [7], pour les domaines présents dans les listes des domaines autorisés.
En cas d'émission de certificats pour les domaines présents dans les listes des domaines autorisés du demandeur de certificats de l'AC par une autre AC publique [8], le fournisseur doit en avertir le demandeur de certificats.

R53 Un service de test (« *staging* » en anglais) de gestion automatisée des certificats doit être proposé au demandeur de certificats à des fins de tests de fonctionnement.

R54 Les certificats délivrés par le service de « *staging* » ne doivent pas être émis par une racine de confiance et doivent être facilement identifiables comme certificats de test (en contenant par exemple le mot TEST dans le *Common Name* du certificat).

3.2 Recommandations concernant le client ACME et sa mise en œuvre

3.2.1 Fonctionnalités et caractéristiques du client ACME

R55 Il est recommandé que le client ACME soit conforme à la RFC 8555 [13].

R56 Un client ACME avec des éventuels greffons de confiance doivent être choisis. En particulier, le client ACME et ses éventuels greffons, doivent avoir fait l'objet d'évaluation apportant des garanties sur leur niveau de sécurité. Il est recommandé de mettre en œuvre un client ACME certifié ou qualifié par l'ANSSI, ou recommandé par un fournisseur de certificats.

R57 Le client ACME et ses éventuels greffons doivent faire l'objet d'un maintien en conditions opérationnelles et d'un maintien en conditions de sécurité (MCO et MCS) au même titre que les

6. Le programme *Certificate Transparency*, initié par GOOGLE [1] et standardisé par l'IETF [12], vise à créer des registres publics listant des certificats X.509. Ces registres permettent de surveiller l'apparition de nouveaux certificats. La vérification se fait par l'intermédiaire de *Signed Certificate Timestamp* (SCT) qui, horodatés et signés par les administrateurs des registres, constituent des assurances d'insertion du certificat. Pour les domaines présents dans les listes des domaines autorisés du demandeur de certificats, dans les cas où l'AC constaterait la présence de certificats signés par une autre AC, elle doit prévenir le demandeur de certificats afin qu'il puisse contrôler la légitimité ou non de ces certificats.
7. Excepté les AC publiques renseignées par le demandeur de certificats.
8. Excepté les AC publiques renseignées par le demandeur de certificats.

autres composants logiciels du SI, comme par exemple le serveur web sur lequel sera installé le certificat délivré par le service de gestion automatisée des certificats.

R58 Les droits du client ACME et des éventuels greffons associés doivent être limités au strict minimum pour assurer un fonctionnement nominal. En particulier, les clés privées et les certificats ne doivent être accessibles en lecture et écriture qu'aux comptes de service le nécessitant.

- **Exemple de déploiement du client ACME à proscrire :** Il est courant de rencontrer de la documentation officielle invitant à exécuter le client ACME avec les privilèges de super-utilisateur (*root* sur les systèmes Unix ou Linux), afin que le client ACME puisse écrire les fichiers de certificats et de clé privée et recharger ou redémarrer les services faisant usage des certificats nouvellement émis. Cependant, cette pratique est à proscrire, car elle va à l'encontre du principe de moindre privilège. Le protocole ACME n'exige pas de droits aussi élevés et aussi larges sur le système que les droits du super-utilisateur. Seul le déploiement des certificats sur le système local peut justifier, ponctuellement et de manière isolée, de tels droits.

- **Exemple de déploiement du client ACME recommandé :** Il est recommandé de dédier un compte de service propre au client ACME via le mécanisme de contrôle d'accès du système (la ségrégation en utilisateurs et groupes par exemple). Ce compte de service doit être configuré afin d'être autorisé à écrire les fichiers de certificats lors des renouvellements automatisés, sans pour autant bénéficier des droits d'administration avancés sur le système. Seul ce compte de service propre au client ACME doit avoir les droits d'écriture sur les certificats et les clés privées.

R59 Il est recommandé de limiter les droits des services faisant usage des certificats nouvellement émis (le serveur web par exemple), à la lecture de ces certificats et des clés privées associées.

- **Exemple 1 d'installation des certificats :** L'installation (ou le rechargement) des certificats sur le système local peut être effectuée par le client ACME, avec la mise en œuvre d'une commande d'administration (par exemple avec *sudo* ou *doas* sur les systèmes Unix ou Linux) permettant une élévation de privilèges locale et restreinte du compte de service du client ACME, afin d'autoriser ce dernier à recharger ou redémarrer (via le système d'exploitation) les services faisant usage des certificats nouvellement émis.

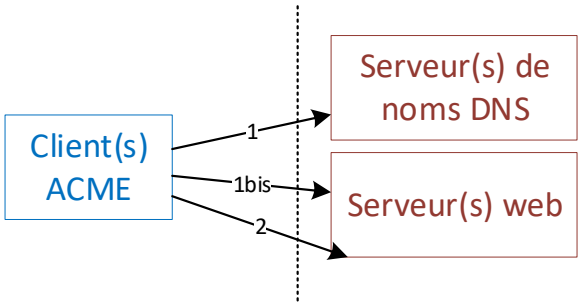
- **Exemple 2 d'installation des certificats :** L'installation (ou le rechargement) des certificats sur le système local peut être effectuée par une tâche périodique indépendante du client ACME, mise en œuvre avec un service de type *crontab* ou *timer systemd* sur les systèmes Unix ou Linux, permettant de recharger ou redémarrer les services faisant usage des certificats nouvellement émis.

R60 Les privilèges du client ACME sur les serveurs assurant la résolution des défis ACME (les serveurs de noms DNS dans le cas du défi DNS-01 et les serveurs web dans le cas du défi HTTP-01) doivent être limités au strict minimum pour assurer un fonctionnement nominal. En particulier, le client ACME ne doit pas s'exécuter avec les mêmes privilèges systèmes que le serveur web ou le serveur DNS.

R61 Sur les serveurs mettant à disposition les réponses aux défis ACME (serveur DNS pour le défi DNS-01 et serveur web pour le défi HTTP-01), le client ACME ne doit avoir les droits d'écriture que sur les périmètres des services concernés (dossier */.well-known/acme-challenge/* du dossier racine exposé par le serveur web pour le défi HTTP-01, sous-domaine *_acme-challenge* du domaine du certificat demandé pour le défi DNS-01).

R62 Pour le défi DNS-01, il est recommandé d'écrire un enregistrement de type CNAME placé sur les sous-domaines *_acme-challenge.domaines.tld* des domaines visés par les demandes de certificats, pointant sur un domaine tiers moins sensible (tel que *domaine-tiers.tld* et situé en dehors de la zone contenant *domaines.tld*). Il est recommandé de dédier ce domaine tiers au défi DNS-01.

R63 Comme alternative équivalente à la précédente recommandation, il est aussi recommandé pour le défi DNS-01 de mettre en œuvre d'une délégation de zone vers un serveur de noms faisant autorité uniquement sur la (ou les) zone(s) *_acme-challenge.domaines.tld* des domaines visés par les demandes de certificats.



Le client ACME ne doit avoir que les droits 1 ou 1bis selon le type de défi ACME utilisé, et 2 sur chacun des serveurs web.
1. Droits permettant la résolution du défi ACME DNS-01 : droits d'écriture sur le sous-domaine *_acme-challenge* au domaine du certificat demandé pour le défi DNS-01
1bis. Droits permettant la résolution du défi ACME HTTP-01 : droits d'écriture sur le dossier */.well-known/acme-challenge/* du dossier racine exposé par le serveur web
2. Droits nécessaires à l'installation du certificat sur le serveur web : droits à la commande de rechargement des certificats ou droits au redémarrage du service.

SCHÉMA 3 – Schéma sur les droits nécessaires et suffisants du client ACME sur les serveurs web et DNS

R64 Après validation du défi ACME par le serveur ACME, il est recommandé de supprimer les fichiers déposés dans le dossier */.well-known/acme-challenge/* et les enregistrements TXT [9] écrits sur le sous-domaine *_acme-challenge* nécessaires à la résolution du défi ACME.

R65 Les clés cryptographiques générées côté client, en particulier par le client ACME [10], doivent être générées à partir d'un générateur aléatoire conforme au guide des mécanismes cryptographiques [5].

9. Le format des enregistrements TXT du challenge DNS-01 fait qu'il n'est pas possible de distinguer des enregistrements les uns des autres (par exemple il n'y a pas de précision dans le format de l'enregistrement permettant de distinguer si l'enregistrement est pour un nom de domaine spécifique ou un certificat dit « *wildcard* »).

10. Le client ACME est généralement en charge de deux types de clés : les clés des comptes ACME et les clés des certificats. Dans le cas où certaines de ces clés ne seraient pas créées par le client ACME mais importées dans celui-ci, il est important de s'assurer de leur bonne génération.

R66 À chaque création ou renouvellement de certificat, de nouvelles clés doivent être générées [11]. Il est proscrit de réutiliser des clés ayant déjà été utilisées.

R67 En tant que mesure d'hygiène, il est recommandé de supprimer régulièrement les anciennes clés des anciens certificats (hors clés de certificats utilisées pour du recouvrement).

R68 Les certificats dits « *wildcard* » sont à proscrire.

R69 Il est recommandé que chaque certificat soit utilisé pour un unique service TLS.

R70 En cas de transfert de clés privées de certificats (entre deux serveurs par exemple), ces clés privées doivent être protégées en confidentialité et en intégrité durant leur transport.

R71 Le transport sécurisé des certificats et clés privées sur les autres serveurs doit également s'assurer du maintien des droits d'accès en lecture et/ou écriture à destination sur les espaces de stockage de ces serveurs.

R72 Le client ACME doit produire des journaux d'évènements (notamment les créations de nouveaux comptes, les créations et renouvellements de certificats, etc).

3.2.2 Mise en œuvre du client ACME

R73 Dans le cas d'une implémentation du client ACME intégrée au serveur web (par l'usage d'un greffon par exemple), il est recommandé de s'assurer que les fonctionnalités ACME ne s'exécutent pas avec les mêmes privilèges système que le service web. Cette recommandation vise à prévenir toute éventuelle latéralisation (et inverse) d'un attaquant si le client ACME venait à être compromis. Des exemples de mise en œuvre sont donnés en **R58**.

R74 Concernant la mise en œuvre du défi HTTP-01, il est recommandé de limiter l'exposition du chemin */.well-known/acme-challenge/* au seul client ACME, afin que d'autres services ne puissent pas y accéder.

R75 Concernant la mise en œuvre du défi DNS-01, il est recommandé de limiter l'exposition du sous-domaine *_acme-challenge* du domaine du certificat demandé au seul client ACME, afin que d'autres services ne puissent pas y accéder.

R76 Une analyse des risques relative au déploiement, à l'architecture et à la configuration du client ACME doit être réalisée par le demandeur de certificats. L'objectif de cette recommandation est de responsabiliser l'utilisateur du service de gestion automatisée des certificats. Un point d'attention doit être porté à la protection du serveur hébergeant le client ACME. En effet, la compromission de ce serveur pourrait amener à la compromission du compte ACME. Des exemples d'architecture sont fournis dans la section 3.3.

R77 L'architecture du système d'information auquel est intégré le client ACME doit respecter les bonnes pratiques des guides de l'ANSSI *Recommandations relatives à l'administration sécurisée des systèmes d'information* [7] et *Recommandations relatives à l'interconnexion d'un système d'information à Internet* [4].

11. À chaque certificat émis doit être associé un bi-clé n'ayant pas servi au préalable. Cette fonctionnalité est nativement présente dans la plupart des clients ACME disponibles en opensource.

R78 Le maintien en condition de sécurité (MCS) du client ACME doit être assuré.

R79 Les mises à jour de sécurité doivent être appliquées rapidement après leur publication.

R80 Le client ACME doit être intégré dans la politique de maintien en condition de sécurité du système d'information sur lequel il est installé.

R81 La collecte des journaux d'évènements sur le client ACME doit être activée et ces journaux doivent être centralisés dans la mesure du possible en respectant les recommandations du guide *Recommandations de sécurité pour l'architecture d'un système de journalisation* [8]. L'analyse des journaux permet une investigation post-mortem en cas d'incident de sécurité, voire de détecter un incident de sécurité avant que l'attaquant ne parvienne à réaliser son objectif. La centralisation des évènements de sécurité contribue d'une part à sécuriser la collecte des évènements et d'autre part à faciliter les opérations de détection et d'analyse en cas d'incident. Étant donné que le client ACME va générer des certificats sans contrôle humain, il est important d'analyser régulièrement les évènements collectés afin de s'assurer par exemple que le client ACME ne génère des certificats que pour des noms de domaine légitimes.

R82 Limiter la diversité logicielle des clients ACME installés sur un même SI.

R83 Il est recommandé de limiter le nombre de briques technologiques utilisées au sein d'un même SI afin de minimiser la présence de vulnérabilités et de faciliter le MCO/MCS du SI. Ainsi, il est proposé de ne mettre en œuvre qu'un type de client ACME, développé par un éditeur.

R84 Renouveler les certificats en amont de leur expiration. Il est recommandé de renouveler le certificat d'un serveur web avec une marge de sécurité, afin de pouvoir traiter un éventuel problème lié au renouvellement. Il est ainsi recommandé de procéder au renouvellement des certificats au 2/3 de leur durée de validité, c'est-à-dire tous les 60 jours pour des certificats émis avec une durée de validité de 90 jours [12].

R85 Réaliser des tests de fonctionnement avec les services de test (« *staging* » en anglais) des fournisseurs de certificats sur les environnements de préproduction. L'objectif des tests de fonctionnement est de vérifier le bon déroulement des processus de délivrance et de renouvellement des certificats. Il s'agit en particulier de s'assurer que les défis soient bien réalisés par le client ACME et que le serveur ACME soit en mesure de les vérifier (vérifier que les flux de résolution de défis sont bien ouverts, vérifier la bonne installation de la clé sur le serveur web etc.).

3.2.3 Environnement d'installation et protection des clés

R86 Configurer une authentification multifacteur sur l'interface de gestion des certificats mise à disposition par le fournisseur de certificats. L'interface de gestion des certificats mise à disposition du demandeur de certificats par le fournisseur de certificats permet potentiellement la réalisation d'actions sensibles (le renouvellement de la clé secrète d'un compte externe d'administration ACME (MAC key) par exemple). Ainsi, l'accès à cette interface doit être protégé de façon robuste.

12. À noter que ces plages de temps sont les pratiques courantes à date de rédaction de ce document pour les autorités de certification ACME mais sont susceptibles d'évoluer, notamment à la baisse, dans le futur.

R87 Les rapports envoyés régulièrement par le prestataire du service de gestion automatisée des certificats doivent être analysés par le demandeur de certificats dans une démarche de détection d'anomalie concernant l'utilisation de ce service.

R88 Les serveurs web dont les certificats sont gérés avec le protocole ACME doivent être à jour et respecter les recommandations du guide *Recommandations pour la sécurisation des sites web* [3]. [13]

R89 Il est recommandé de publier un enregistrement DNS Certification Authority Authorization (CAA) afin de définir la ou les AC autorisées à émettre un certificat pour un domaine donné. Cette recommandation permet notamment d'exclure explicitement des AC publiques des AC autorisées à émettre un certificat pour des domaines précis, et ainsi empêcher l'émission automatique de certificats par ces AC publiques pour les domaines pour lesquels un attaquant serait en mesure de résoudre un défi ACME.

R90 La clé secrète d'un compte externe d'administration ACME (MAC key) doit être protégée en confidentialité et en intégrité avec des mécanismes conformes au guide des mécanismes cryptographiques [5]. Sa disponibilité doit être assurée.

R91 La présence de la clé secrète d'un compte externe d'administration ACME (MAC key) sur les serveurs hébergeant les clients ACME doit être limitée aux opérations d'association de comptes ACME à ce compte externe d'administration ACME.

R92 Une fois les comptes ACME associés à ce compte externe d'administration ACME, la clé secrète du compte externe d'administration ACME doit être supprimée du serveur hébergeant les clients ACME. La clé secrète d'un compte externe d'administration ACME donné (MAC key) n'est utilisée que lors de l'association d'un nouveau compte ACME à ce compte externe d'administration ACME [14].

R93 Il est recommandé de limiter l'exposition de la clé secrète d'un compte externe d'administration ACME lorsqu'elle n'est pas utilisée. Par exemple, il n'est pas recommandé de stocker la clé secrète d'un compte externe d'administration ACME donné sur le client ACME une fois les comptes ACME associés à ce compte externe d'administration ACME.

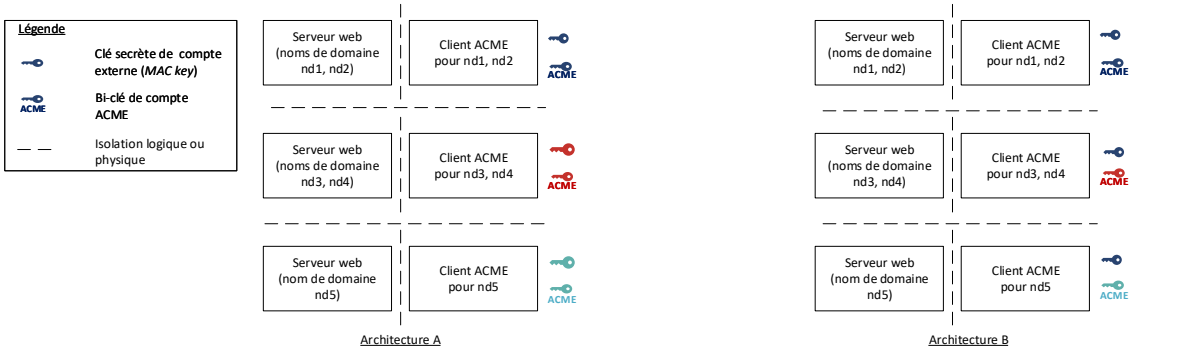
R94 La clé privée d'un compte ACME doit être protégée en confidentialité et en intégrité avec des mécanismes conformes au guide des mécanismes cryptographiques [5].

13. La présence d'une vulnérabilité de type « téléversement de fichier arbitraire » (*Arbitrary File Upload*) dans l'applicatif web permettra à un attaquant à faire valider un défi ACME HTTP-01 légitime et donc recevoir illégitimement un certificat valide pour le domaine du site web vulnérable.

14. En cas de révocation d'un compte externe d'administration ACME suite à une compromission de sa clé secrète (MAC key), tous les comptes ACME qui lui sont associés seront automatiquement révoqués (cf. A.2). Ainsi, les impacts opérationnels du renouvellement d'un compte externe d'administration ACME et des comptes ACME qui lui sont associés doivent être pris en compte pour le choix du nombre de comptes ACME à associer au compte externe d'administration ACME.
L'architecture des services nécessitant des certificats doit également être prise en compte pour le choix du nombre de comptes ACME à associer à un compte externe d'administration ACME donné.

3.3 Exemples d'architectures côté demandeur de certificats

3.3.1 Exemples d'architectures recommandées côté demandeur de certificats



La gestion automatisée des certificats est répartie sur plusieurs clients ACME.
Les clients ACME ne peuvent résoudre de défis ACME (HTTP-01 ou DNS-01) que pour certains noms de domaine (par exemple : le client ACME pour nd1 et nd2 peut résoudre un défi ACME pour nd1 et nd2 mais pas pour nd3).
Plusieurs comptes externes sont créés.
Chaque client ACME est lié à un compte externe différent des autres clients ACME. Pour chaque client ACME, un compte ACME dédié est créé.
(A noter (ce n'est pas représenté sur le schéma) qu'il pourrait y avoir plusieurs comptes ACME liés à un même compte externe.)
Les authentifiants du/des utilisateur(s) des clients ACME doivent être distincts pour chaque client ACME.

Avantages :
- Les clients ACME sont isolés entre eux, ainsi la compromission d'un client ACME n'impacte pas les autres clients ACME
- Cloisonnement par compte externe : l'impact de la compromission d'un compte externe est limitée
- Cloisonnement par compte ACME : l'impact de la compromission d'un compte ACME est limitée
- Facilité d'usage car création d'un nouveau compte ACME sur chaque machine (pas besoin de copier/coller les clés du compte ACME)

Inconvénients:
- Difficulté d'usage dû au cloisonnement par compte externe

La gestion automatisée des certificats est répartie sur plusieurs clients ACME.
Les clients ACME ne peuvent résoudre de défis ACME (HTTP-01 ou DNS-01) que pour certains noms de domaine (par exemple : le client ACME pour nd1 et nd2 peut résoudre un défi ACME pour nd1 et nd2 mais pas pour nd3).
Un seul compte externe est créé.
Pour chaque client ACME, un compte ACME dédié est créé.
Les authentifiants du/des utilisateur(s) des clients ACME doivent être distincts pour chaque client ACME.

Avantages :
- Les clients ACME sont isolés entre eux, ainsi la compromission d'un client ACME n'impacte pas les autres clients ACME
- Cloisonnement par compte ACME : l'impact de la compromission d'un compte ACME est limitée
- Facilité d'usage car création d'un nouveau compte ACME sur chaque machine (pas besoin de copier/coller les clés du compte ACME)

Inconvénient :
- Remédiation lourde en cas de compromission du compte externe

SCHÉMA 4 – Exemples d'architectures recommandées côté demandeur de certificats

3.3.2 Exemples d'architectures non recommandées côté demandeur de certificats

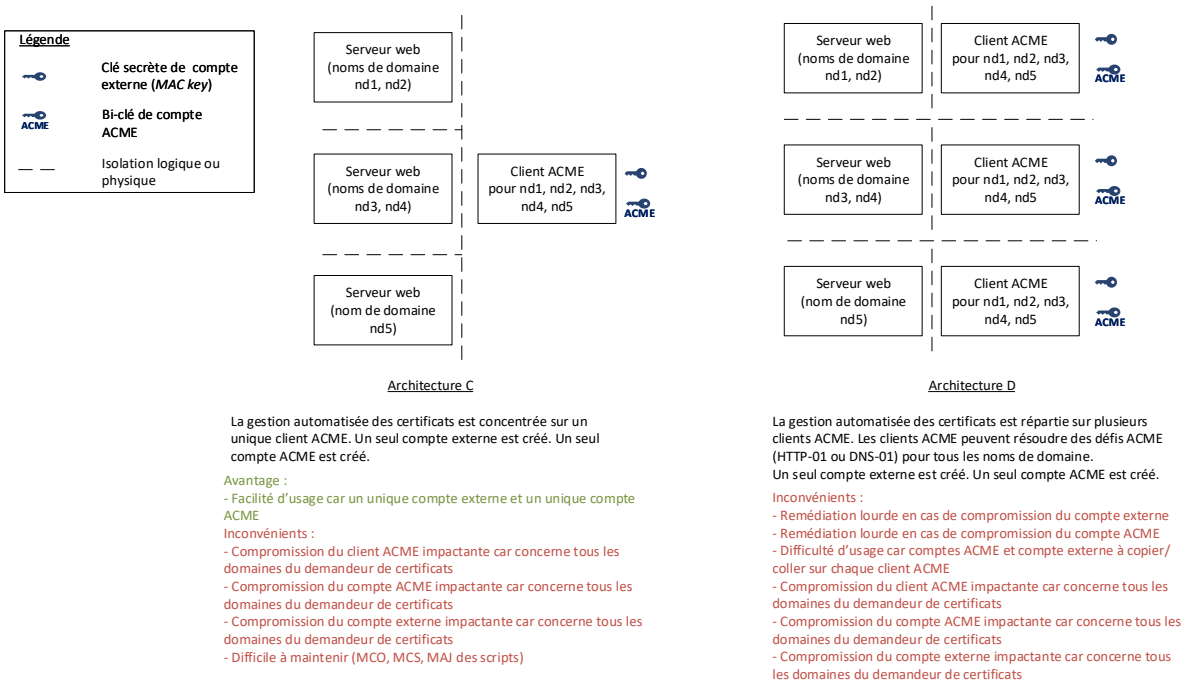


SCHÉMA 5 – Exemples d'architectures **non recommandées** côté demandeur de certificats

Annexe A
Processus à suivre en cas de renouvellement, compromission ou suspicion de compromission d'un compte externe d'administration ACME ou d'un compte ACME

Les actions décrites sont à réaliser soit par le fournisseur de certificats soit par l'utilisateur des certificats.

A.1 Renouvellement d'un compte externe d'administration ACME

A. Renouvellement des éléments de *binding* du compte externe d'administration ACME et envoi de ces nouveaux éléments de *binding* au demandeur de certificats après authentification ou vérification de son identité.

B. Désactivation (au sens de la RFC 8555) de tous les comptes ACME associés au compte externe d'administration ACME.

C. Création de nouveaux comptes ACME et association au compte externe d'administration ACME. **Attention : pas de nécessité de révoquer les certificats émis par les comptes ACME désactivés en B.**

A.2 Cas de compromission d'un compte externe d'administration ACME

A. Désactivation du compte externe d'administration ACME (refus de toute action à l'initiative de l'utilisateur liée à ce compte, notamment l'association de nouveau compte ACME, la modification de la liste des domaines autorisés etc., et désactivation (au sens de la RFC 8555) des comptes ACME associés au compte externe d'administration ACME).

B. Création d'un nouveau compte externe d'administration ACME, en respectant la procédure de création initiale. Les éléments de *binding* de ce nouveau compte externe d'administration ACME doivent être différents de ceux du compte externe d'administration ACME compromis.

C. Analyse des comptes ACME :

   a. Pour les comptes ACME « suspects », qui auraient pu être créés et associés malicieusement au compte externe d'administration ACME, avant la désactivation des comptes ACME : révocation des certificats générés par ces comptes, idéalement dans les 24h après la détection de compromission.

   b. Pour les comptes ACME suspectés de compromission, si le bi-clé du compte ACME est stocké au même endroit que la MAC key par exemple : mise en œuvre du processus « Suspicion de compromission d'un compte ACME ».

   c. Pour les comptes ACME non suspects : création de nouveaux comptes ACME et réassociation des comptes ACME au nouveau compte externe d'administration ACME, créé en b.
   Attention : pas de nécessité de révoquer les certificats émis par ces comptes ACME non suspects.

La désactivation d'un compte ACME implique le refus de toutes les actions en cours impliquant ce compte ACME, ainsi que le refus de toute nouvelle action l'impliquant.
Ces actions sont notamment : le binding avec un compte externe d'administration ACME, la demande ou le renouvellement d'un certificat lié à ce compte, la demande de révocation d'un certificat.
Cette définition reprend la notion de « deactivated account » de la RFC 8555. La désactivation d'un compte ACME est irréversible.

A.3 Cas de suspicion de compromission d'un compte externe d'administration ACME

A. Suspension du compte externe d'administration ACME le temps de l'investigation de la suspicion de compromission : suspension de toutes les actions en cours impliquant ce compte externe d'administration ACME comme l'association de nouveau compte ACME, la modification de la

liste des domaines autorisés, etc., ainsi que la mise en tampon de toute nouvelle action à l'initiative de l'utilisateur de certificat l'impliquant, et suspension des comptes ACME associés.

B. Si la compromission est avérée (ou que le doute persiste), mise en œuvre du processus « Compromission du compte externe d'administration ACME ». Sinon, réactivation des comptes ACME suspendus et reprise des actions liées au compte externe d'administration ACME.

La suspension d'un compte ACME implique la suspension de toutes les actions en cours impliquant ce compte ACME, ainsi que la mise en tampon de toute nouvelle action l'impliquant.
Ces actions sont notamment : le binding avec un compte externe d'administration ACME, la demande d'un certificat lié à ce compte, la demande de révocation d'un certificat. Un compte ACME suspendu peut revenir à un état non suspendu. Lors du retour à un état non suspendu, les actions suspendues et mises en tampon lors de la suspicion de compromission peuvent reprendre.

A.4 Renouvellement d'un compte ACME

A. Renouvellement du bi-clé du compte ACME avec la procédure « *account key rollover* », définie par la RFC 8555 (sans impact sur les certificats déjà générés avec ce compte ACME).

B. Si l'étape A. n'est pas possible :

   a. Désactivation du compte ACME, selon la RFC 8555 ;

   b. Création d'un nouveau compte ACME (avec un bi-clé différent du précédent compte ACME) ;

   c. Association du compte ACME au compte externe d'administration ACME du précédent compte ACME (avec les éléments de *binding*).
   Pas de révocation des certificats émis par le compte ACME désactivé en B. a.

A.5 Cas de compromission d'un compte ACME

A. Désactivation du compte ACME, au sens de la RFC 8555.

B. Révocation des certificats émis par ce compte ACME (au moins depuis la date estimée de la compromission du compte ACME).

C. Création d'un nouveau compte ACME.

D. Association du nouveau compte ACME au compte externe d'administration ACME avec les éléments de *binding* existants.

E. Demande de nouveaux certificats avec le nouveau compte ACME.

A.6 Cas de suspicion de compromission d'un compte ACME

A. Suspension du compte ACME, le temps de l'investigation de la suspicion de compromission.

B. Si la compromission est avérée, mise en œuvre du processus « Compromission d'un compte ACME ».

C. Sinon, retour à un état non suspendu du compte ACME.

	État du compte externe d'administration ACME	État d'un compte ACME associé au compte externe d'administration ACME
Suspicion de compromission d'un compte externe d'administration ACME	Suspendu (réversible)	Suspendu (réversible)
Compromission d'un compte externe d'administration ACME	Désactivé (irréversible)	Désactivé (irréversible)
Suspicion de compromission d'un compte ACME	Nominal	Suspendu (réversible)
Compromission d'un compte ACME	Nominal	Désactivé (irréversible)

Tableau 2 – Tableau synthétisant les états des comptes en fonction du processus

Bibliographie

[1] *Certificate Transparency*.
Page web.
https://certificate.transparency.dev.

[2] *CyberDico de l'ANSSI*.
Publication anssi, 2024.
https://cyber.gouv.fr/publications/cyberdico-quest-ce-que-cest.

[3] *Recommandations pour la sécurisation des sites web*.
Note technique DAT-NT-009/ANSSI/SDE/NP v1.1, ANSSI, août 2013.
https://cyber.gouv.fr/guide-sites-web.

[4] *Recommandations relatives à l'interconnexion d'un système d'information à Internet*.
Guide ANSSI-PA-066 v2.0, ANSSI, juin 2019.
https://cyber.gouv.fr/guide-interconnexion-si-internet.

[5] *Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques*.
Guide ANSSI-PG-083 v2.0, ANSSI, janvier 2020.
https://cyber.gouv.fr/publications/mecanismes-cryptographiques.

[6] *Recommandations de sécurité relatives à TLS*.
Guide ANSSI-PA-035 v1.2, ANSSI, mars 2020.
https://cyber.gouv.fr/guide-tls.

[7] *Recommandations relatives à l'administration sécurisée des systèmes d'information*.
Guide ANSSI-PA-022 v3.0, ANSSI, mai 2021.
https://cyber.gouv.fr/guide-admin-si.

[8] *Recommandations de sécurité pour l'architecture d'un système de journalisation*.
Guide DAT-PA-012 v2.0, ANSSI, janvier 2022.
https://cyber.gouv.fr/guide-journalisation.

[9] *Référentiel général de sécurité (RGS)*.
Référentiel Version 2.0, ANSSI, juin 2012.
https://cyber.gouv.fr/rgs.

[10] *Recommandations relatives à l'authentification multifacteur et aux mots de passe*.
Guide ANSSI-PG-078 v1.0, ANSSI, octobre 2021.
https://cyber.gouv.fr/guide-authentification.

[11] *Bamboozling Certificate Authorities with BGP*.
Henry Birge-Lee, Yixin Sun, Anne Edmundson, Jennifer Rexford, and Prateek Mittal.
27th USENIX Security Symposium (USENIX Security 18), pages 833–849, Baltimore, MD, août 2018. USENIX Association.
ISBN 978-1-939133-04-5.
https://www.usenix.org/conference/usenixsecurity18/presentation/birge-lee.

[12] *Certificate Transparency*.
RFC, juin 2013.
https://www.rfc-editor.org/info/rfc6962.

[13] *Automatic Certificate Management Environment (ACME)*.
RFC, mars 2019.
https://www.rfc-editor.org/info/rfc8555.

[14] *DNS Certification Authority Authorization (CAA) Resource Record*.
RFC, novembre 2019.
https://www.rfc-editor.org/info/rfc8659.

[15] *Automated Certificate Management Environment (ACME) TLS Application Layer Protocol Negotiation (ALPN) Challenge Extension*.
RFC, février 2020.
https://www.rfc-editor.org/info/rfc8737.

Version 1.1 - 10/09/2025 - ANSSI-BP-106

ISBN : 978-2-11-167177-5 (papier)
ISBN : 978-2-11-167178-2 (numérique)

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI - 51 boulevard de La Tour-Maubourg, 75700 PARIS 07 SP
cyber.gouv.fr / conseil.technique@ssi.gouv.fr

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité