ACCÈS

qui est qui, qui peut quoi, et qui l'a vraiment fait

La gestion des comptes, des mots de passe et des droits, d'après le référentiel de l'ANSSI

Livre blanc by ChallengeMyProject

À qui s'adresse ce document ?

À toute personne qui décide, dans son organisation, qui a accès à quoi : dirigeant, responsable administratif ou RH, chef de projet. Les attentes de l'ANSSI en matière de comptes, de mots de passe et de droits, traduites en décisions concrètes. Aucun prérequis technique.

01

Le problème : savoir qui a fait quoi

Pourquoi un compte par personne n'est pas un détail

Dans une entreprise, tout le monde a des accès : une messagerie, un logiciel de comptabilité, un espace de fichiers partagés, parfois l'outil de paie. Chacun de ces accès repose sur un compte.

Le jour où un dossier disparaît, où une facture est modifiée, où des données clients sortent de l'entreprise, une seule question compte : qui l'a fait ? Si trois personnes utilisent le même identifiant, la réponse n'existe pas. Ni pour vous, ni pour votre assureur, ni pour une éventuelle enquête.

C'est ce que l'ANSSI appelle l'imputabilité : la capacité à rattacher chaque action à une personne précise. Elle ne s'improvise pas au moment de l'incident. Elle se prépare avant, en organisant les comptes.

Ce livre blanc reprend les attentes de l'ANSSI sur ce sujet, telles qu'elles figurent dans la fiche « Gestion des identités » du Référentiel Cyber France (ReCyF), version 1.0, septembre 2026. Il les traduit en décisions accessibles sans compétence technique.

02

Trois verrous

Identification, authentification, droits d'accès

Toute sécurité d'accès repose sur trois fonctions distinctes, souvent confondues dans le langage courant. Les séparer est le premier réflexe à acquérir.

Concrètement, une action met en jeu trois fonctions, dans cet ordre.

L'identification : annoncer qui l'on est. Il s'agit de l'identifiant, du nom d'utilisateur, de l'adresse e-mail. Il désigne une personne, mais ne prouve rien : n'importe qui peut le saisir.

L'authentification : le prouver. C'est le mot de passe, le code reçu sur le téléphone, l'empreinte digitale. Sans cette étape, un identifiant valide suffirait à entrer. L'ANSSI demande qu'au moins un des éléments en jeu soit toujours secret.

Les droits d'accès : définir ce que l'on peut faire. Une fois entré, tout ne doit pas être ouvert. Le comptable accède à la comptabilité, pas aux dossiers du personnel. C'est la configuration des droits qui trace cette frontière, et elle seule.

À ces trois fonctions s'ajoute la traçabilité : garder la trace de qui a fait quoi, et quand. Sans elle, les trois premières restent invérifiables.

03

Un compte par personne, un compte par machine

La règle de base, et ce qu'elle implique

Première règle, et la plus structurante : l'ANSSI demande que chaque utilisateur et chaque programme automatique dispose de son propre compte, avec un identifiant qui lui est propre.

Les comptes individuels correspondent à une personne physique, identifiable par son nom ou par un identifiant unique. C'est le cas général : un salarié, un compte.

Les comptes techniques sont rattachés à un programme, une application, un service, un script — pas à un être humain. Leur secret ne doit être connu d'aucun utilisateur. Si une personne s'en sert, les traces deviennent ininterprétables : on ne sait plus si l'action vient du programme ou d'elle. Ces comptes gagnent aussi à être bridés, par exemple en leur interdisant d'ouvrir une session comme le ferait un humain.

Cette règle a une conséquence directe sur les habitudes d'entreprise. Le compte « accueil », le compte « compta » ou le compte « direction » partagés entre plusieurs personnes deviennent des exceptions à justifier, et non des commodités.

À retenir : **un identifiant qui ne désigne qu'une seule personne, voilà ce qui rend une trace exploitable.**

04

Le compte partagé : quand il est inévitable

Comment rester capable de dire qui a agi

Certains équipements n'offrent qu'un seul compte, certaines activités exigent une session unique à plusieurs. Le partage se justifie parfois — il se compense toujours.

Habituellement, un compte a un titulaire unique. Il est dit partagé lorsqu'il est commun à plusieurs personnes — l'ANSSI reconnaît deux familles de situations où cela reste légitime.

Les raisons techniques : l'équipement ne sait pas gérer plusieurs comptes, ou il doit garder une même session ouverte plus longtemps qu'une personne n'est présente — automates industriels, calculateurs.

Les raisons opérationnelles : plusieurs personnes doivent travailler simultanément dans la même session — un poste d'accueil du public, une saisie de données à plusieurs mains.

Dans ces cas, l'imputabilité n'est plus assurée par le compte. Elle doit l'être autrement.

Vous devez rétablir autrement le lien entre l'action et la personne. Ces mesures peuvent être techniques — un badge d'accès à la salle où se trouve la machine dit qui était présent — ou organisationnelles : un cahier où chacun inscrit la date et l'heure d'utilisation du compte suffit à retrouver, plus tard, qui agissait.

Trois précautions complètent le dispositif. Réserver le compte partagé à la seule activité qui l'impose. Encadrer techniquement son usage : plages horaires, postes autorisés. Et changer le secret dès qu'une personne entre dans le groupe ou le quitte — sinon elle en garde la clé.

Le compte partagé dégrade la sécurité. Il ne devrait exister que là où rien d'autre n'est possible.

05

Les mots de passe

Ce qui les rend solides,
et ce qui les rend tenables

Le mot de passe reste le moyen d'authentification le plus répandu. Les règles qui l'entourent ont beaucoup évolué, et certaines habitudes d'entreprise sont aujourd'hui contre-productives.

La longueur prime sur les caractères compliqués. La solidité d'un mot de passe se mesure par son entropie, exprimée en bits : elle combine sa longueur et la variété des caractères autorisés par le système. Plus l'entropie est élevée, plus le nombre de combinaisons à essayer est grand. Une phrase longue et facile à retenir vaut donc mieux qu'une suite courte de symboles impossibles à mémoriser. La CNIL met à disposition un calculateur d'entropie et un générateur de mots de passe construits à partir d'une phrase.

La réutilisation est le vrai danger. Un mot de passe volé sera systématiquement essayé ailleurs : c'est le premier réflexe de l'attaquant, qui reprend le couple identifiant / mot de passe et le teste sur tous les services qu'il peut atteindre. D'où la règle unique à retenir : jamais le même mot de passe deux fois.

Mémoriser des dizaines de mots de passe différents est hors de portée. L'outil prévu pour cela est le coffre-fort numérique : une base de données chiffrée qui les stocke, les génère aléatoirement et les saisit à votre place. Il n'en reste plus qu'un seul à retenir, celui qui ouvre le coffre — et celui-là doit être long : **quelque chose comme 128 bits d'entropie.**

06

L'authentification multifacteur

Trois familles de preuves, quatre niveaux de sécurité

Un facteur d'authentification appartient à l'une de trois familles : ce que je sais (un mot de passe, un code PIN), ce que je possède (un téléphone, une carte à puce), ce que je suis (une empreinte digitale, un visage).

L'authentification multifacteur combine des facteurs d'au moins deux de ces familles. Un mot de passe suivi d'une question secrète n'en est donc pas : les deux relèvent de ce que je sais.

Attention à une confusion fréquente : un facteur n'est pas forcément un secret. Votre visage est un facteur d'authentification, mais il n'a rien de secret — vous l'exposez toute la journée. L'ANSSI demande qu'au moins un des facteurs repose toujours sur un élément réellement secret.

À retenir : un mécanisme se juge à quatre niveaux. Le multifacteur avec facteur fort résiste à presque tout, hameçonnage compris. L'authentification forte à un seul facteur arrête les attaques automatisées. Le multifacteur sans facteur fort convient au risque modéré. L'authentification simple ne protège presque de rien.

07

Les droits d'accès

Ouvrir ce qui est nécessaire, et rien de plus

Être authentifié ne veut pas dire avoir le droit. La troisième fonction décide de ce que chacun peut réellement faire une fois entré.

Quatre principes gouvernent l'attribution des droits, et aucun n'est technique.

Raisonner par profils, jamais par personnes. Les droits s'attachent à des profils correspondant aux métiers — comptabilité, commerce, direction, administration — et non à des individus. Accueillir un salarié consiste alors à lui donner le bon profil, pas à recopier les droits d'un collègue.

Limiter à ce qui est nécessaire. Vos droits doivent borner les actions possibles et les données visibles au besoin réel du profil. Le profil « utilisateur » d'un logiciel permet de s'en servir ; le profil « administrateur » permet de le configurer. Très peu de personnes ont besoin du second.

Refuser l'accès plutôt que le tolérer. Lorsqu'une personne parvient à s'authentifier sur une ressource dont elle n'a pas besoin, l'accès doit lui être refusé par les droits. Le cas est fréquent avec l'authentification unique (SSO), qui ouvre plusieurs applications après une seule connexion : le chef de projet accède à l'outil de planification, pas à celui de la paie.

Ne jamais conserver les secrets d'usine. Les mots de passe et clés installés par défaut par un fournisseur doivent être changés avant la mise en service. Et le fournisseur ne doit pas rester le seul à pouvoir les modifier ensuite.

Ce que devient un compte au fil du temps

Un compte n'est pas un objet qu'on crée et qu'on oublie. Trois moments décident de la sécurité de l'ensemble.

La création. Le compte est ouvert avec le bon profil dès le départ, correspondant au besoin réel du poste. C'est le moment où bien faire coûte le moins cher, et celui qu'on rattrape le plus difficilement.

Le changement de poste. Une mobilité interne ajoute des droits — et, trop souvent, n'en retire aucun. Au bout de quelques années, certains salariés cumulent les accès de tous les postes qu'ils ont occupés. Le profil doit être remplacé, pas complété.

Le départ. L'ANSSI demande la désactivation « sans délai » des comptes dont l'usage n'est plus justifié. Sans délai suppose deux choses : une procédure qui signale le départ — le plus souvent déclenchée par les ressources humaines — et une action rapide, automatisée si possible. À défaut, il faut au moins un responsable désigné et un délai écrit.

La désactivation, préférable à la suppression

Supprimer un compte efface aussi ses traces et les données qui lui sont rattachées — clés de chiffrement, certificats, historique. La désactivation, elle, empêche toute connexion tout en préservant ce qui pourrait servir plus tard, en cas d'enquête ou de litige, et dans le respect des règles de protection des données.

Elle vaut aussi pour les absences longues : congé sabbatique, congé maternité, arrêt maladie. Le compte est simplement réactivé au retour.

Enfin, parce que des oublis se produisent toujours, l'ANSSI recommande une revue périodique des comptes et des droits : comparer, profil par profil, ce qui est réellement attribué à ce dont le poste a besoin. Cette revue s'appuie sur des informations issues des ressources humaines, tenues à jour — c'est souvent là que tout se joue, bien plus que dans l'outil informatique.

08

Les pièges les plus courants

Ce que l'on croit réglé et qui ne l'est pas

Un dispositif d'identités échoue presque toujours sur les mêmes points. Aucun n'est technique, et c'est précisément ce qui les rend faciles à négliger.

Il reste des comptes génériques « bien pratiques ». Vous en avez sûrement un : un compte « accueil » ou « atelier » partagé par commodité, sans nécessité technique. Il annule l'imputabilité de tout ce qui passe par lui.

Il arrive qu'un départ ne soit jamais signalé. Ce jour-là, le compte reste actif parce que personne n'a prévenu l'informatique. C'est un problème de procédure, pas de logiciel.

Il y a les droits qui s'empilent. Sans revue périodique, une carrière interne se transforme en cumul d'accès que plus personne ne sait justifier.

Il y a le mot de passe réutilisé. Le même sur l'outil interne et sur un service grand public : une fuite ailleurs devient une intrusion chez vous.

Il reste des secrets d'usine en service. Des équipements mis en service avec le mot de passe du fabricant, connu de tous et parfois publié en ligne.

Il y a enfin les prestataires sans fin. Les comptes ouverts pour un intervenant extérieur survivent souvent des années à la fin de sa mission.

En résumé : aucun de ces pièges ne se résout par un achat. Tous se résolvent par une décision d'organisation, écrite, avec un responsable et un délai.

09

Checklist : vos comptes et vos accès

Onze points à vérifier dans votre organisation

- [ ] **Chaque personne dispose de son propre compte nominatif**
- [ ] **Les comptes partagés sont listés, justifiés et compensés**
- [ ] **Aucun humain n'utilise un compte technique**
- [ ] **Un mot de passe unique par service**
- [ ] **Un coffre-fort numérique est fourni, et réellement utilisé**
- [ ] **Le multifacteur protège les accès sensibles**
- [ ] **Les droits sont attribués par profil métier**
- [ ] **Les secrets installés par défaut ont tous été changés**
- [ ] **Le départ d'un salarié déclenche la désactivation sans délai**
- [ ] **Les comptes des prestataires ont une date de fin définie**
- [ ] **Une revue des comptes a lieu chaque année**

Conclusion

Une question d'organisation avant tout

La gestion des identités tient dans une phrase : savoir qui est qui, décider qui peut quoi, et pouvoir le prouver ensuite. Rien de tout cela ne s'achète.

Les mesures attendues par l'ANSSI sont, dans leur immense majorité, des décisions d'organisation : un compte par personne, un profil par métier, une procédure qui relie un départ à une désactivation, une revue annuelle. Elles coûtent peu et se mettent en place progressivement.

Ce que ce dispositif vous rend le jour d'un incident n'est pas une protection absolue — c'est une réponse. Celle qui manque presque toujours : qui a fait quoi, et quand.

C'est ce que ce document visait à vous donner : de quoi décider, et de quoi commencer.

Ce livre blanc a été rédigé par les équipes de ChallengeMyProject.

David Patiashvili

Fondateur, président & CTPO

E-mail :
david.patiashvili
@challengemyproject.com

Téléphone :
+ 33 (7) 69 40 60 43

Visio / RDV :
challengemyproject.com

David Patiashvili
Fondateur | Directeur technique

+33 (0)7 69 40 60 43
david.patiashvili@challengemyproject.com