Gestion des identités

La collection de fiches « ReCyF en pratique » a pour objectif d'éclairer les principales mesures de gestion de risque issues du Référentiel Français de Cybersécurité (ReCyF). Ce référentiel a pour vocation de devenir le socle de la réglementation cyber française.

La collection de fiches « ReCyF en pratique » ne se substitue pas au référentiel. Les fiches ne sont pas prescriptives et ne visent pas l'exhaustivité. Sur la base des objectifs de sécurité fixés dans Référentiel Cyber France (ReCyF), ces fiches expliquent en pratique les effets recherchés, présentent des exemples concrets d'implémentation et proposent des références utiles pour aider les entités à mettre en œuvre ces objectifs et mesures de sécurité.

Elles s'adressent à un public technique chargé de la mise en œuvre de ces objectifs de sécurité au sein des entités concernées.

Cet ensemble de fiches est organisé en cinq rubriques: Défense, Protection, Gouvernance, Résilience et Obligations NIS 2, les quatre premières constituant les piliers essentiels des mesures de gestion des risques.

Rubrique Protection
Adoptez un ensemble de mesures essentielles pour éviter la compromission de vos SI.

INDICATION DE LECTURE

Pour distinguer les passages du texte destinés aux entités importantes (EI), de ceux destinés aux entités essentielles (EE), les marques suivantes ont été placées en marge du texte:

Ce texte (sans repère en marge) est à destination des EI et des EE

Ce texte (avec repère bleu en marge) est à destination des EE uniquement

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

Effets recherchés

L'objectif principal est d'empêcher tout utilisateur illégitime d'accéder aux ressources du système d'information.

Pour cela, chaque action effectuée sur le système doit pouvoir être attribuée de manière univoque à l'utilisateur ou au processus automatique qui l'a réalisée. Cette imputabilité repose sur la combinaison de trois fonctions de sécurité : identification, authentification et gestion des droits d'accès, auxquelles s'ajoute la traçabilité en fonction complémentaire.

Par ailleurs, la gestion du cycle de vie des comptes permet de limiter les risques d'accès non autorisés. Ainsi, les comptes dont l'utilisation n'est plus justifiée doivent être désactivés sans délai, afin qu'ils ne puissent plus ouvrir de session. La désactivation d'un compte entraîne la suppression globale des droits d'accès qui lui étaient attribués, et cette mesure doit être systématique pour tout compte n'ayant plus vocation à être utilisé.

Approche générale

Mesures ReCyF	**Objectif de sécurité 10** Gestion des identités et des accès des utilisateurs aux systèmes d'information ▸ Identification : 10.A.1-EI/EE, 10.A.2-EI/EE, 10.A.3-EI/EE, 10.A.4-EI/EE, 10.A.5-EI/EE, 10.A.6-EI/EE

L'entité doit attribuer un compte différent à chaque utilisateur ou processus automatique qui accède au système d'information.

Ces comptes doivent avoir des identifiants spécifiques à l'utilisateur ou au processus automatique concerné.

Il s'agit donc :

- de comptes individuels : dans ce cas, un compte correspond à une seule personne physique, identifiable par son nom ou par un identifiant unique ;

- de comptes techniques : ils sont rattachés à des processus automatiques (un programme, une application, un service, un script, etc.) dont les secrets ne doivent pas être connus et utilisés par des utilisateurs physiques afin de faciliter l'interprétation des évènements de traçabilité. Il est possible pour ces comptes de limiter les droits (voir section « Droits d'accès »), par exemple en retirant les sessions interactives.

Le cas particulier des comptes partagés

Un compte est dit « partagé » s'il est commun à plusieurs personnes ou plusieurs processus automatiques.

L'utilisation de comptes partagés se justifie dans certains cas d'usage, par exemple :

- Pour des raisons techniques :
  → l'équipement n'offre pas de mécanisme de gestion de comptes et n'utilise qu'un seul compte, voire pas de compte du tout. Il ne permet donc pas de créer un compte pour chaque utilisateur ;
  → l'équipement doit maintenir dans la durée une même session active. Dans ce cas, les utilisateurs ne peuvent pas recourir à des sessions différentes, ouvertes avec leurs comptes individuels respectifs. C'est le cas au sein de systèmes industriels ou de calculateurs, dont le temps d'opération peut être plus long que le temps de présence d'un utilisateur unique.

- Pour des raisons opérationnelles :
  → une activité nécessite l'utilisation d'une même session par plusieurs utilisateurs simultanément. Cela peut être le cas de personnes chargées d'accueil du public dans un bâtiment ou de personnes entrant des données dans un laboratoire.

Dans tous ces cas particuliers où l'imputabilité d'une action à un utilisateur unique n'est plus assurée par l'utilisation d'un compte individuel, l'entité met en place des mesures permettant d'atteindre un niveau d'imputabilité équivalent :

- Ces mesures peuvent être **techniques**, comme l'utilisation d'autres traces techniques permettant de rattacher de façon fiable une action à une personne. Par exemple, sur certains systèmes de type Unix, il est nécessaire de faire certaines opérations avec des privilèges *« root »* : l'emploi de la commande *« sudo »* permet ainsi d'identifier quel utilisateur a fait usage des privilèges *« root »* en consultant les journaux du système. Ou encore, la mise place d'un contrôle d'accès individuel par badgeuse pour accorder l'accès à une salle contenant un robot industriel permet de savoir qui effectue des opérations sur le robot industriel.

- Ces mesures peuvent également être **organisationnelles**. À titre d'exemple, l'utilisation d'un cahier d'enregistrement décrivant précisément la date et l'heure d'utilisation d'un compte partagé permet de retrouver l'utilisateur responsable d'une action datée. L'objectif est de pouvoir savoir a posteriori quelles personnes utilisaient un compte partagé à un moment donné.

L'usage de comptes partagés implique une dégradation de la sécurité. Ceux-ci ne devraient être utilisés que lorsqu'ils sont strictement nécessaires. Par exemple, un utilisateur devant utiliser un compte partagé pour une certaine activité ne devrait l'utiliser qu'à cette fin, et utiliser un compte individuel pour ses autres activités. Enfin, des mesures techniques peuvent aussi encadrer l'utilisation des comptes partagés, notamment en limitant la plage horaire d'utilisation ou la liste des équipements sur lesquels ils sont utilisés. Les mesures disponibles dépendent fortement des équipements ou logiciels concernés.

Désactivation des comptes

Dans les cas où l'utilisation d'un compte n'est plus justifiée, sa désactivation est souvent préférable à sa suppression, pour permettre de conserver la traçabilité des actions associées dans le temps, ou pour conserver des données liées au compte de l'utilisateur (clés de chiffrement, certificats, etc.) en cas de besoin d'investigations futures et dans le respect des règles sur la protection des données.

La désactivation du compte doit aussi se faire en cas d'absence prolongée de la personne titulaire du compte (congé sabbatique, congé maternité, congé maladie, etc.), ou lorsque le compte n'est plus nécessaire (départ de l'entité, suppression du service, etc.). Un compte désactivé pourra être réactivé au retour de son titulaire.

La notion de désactivation « sans délai » implique une procédure permettant d'identifier qu'un compte n'est plus nécessaire et une action rapide pour désactiver le compte. La procédure peut être déclenchée par les RH lors d'un départ, par exemple. L'action doit être, si possible, automatisée. À défaut, la responsabilité et le délai de la désactivation doivent être clairement établis.

Afin de pallier d'éventuels oublis, l'entité est encouragée à mettre en place une revue régulière des comptes. Cette partie traitant du cycle de vie d'un compte est abordée de façon plus détaillée dans la section « Droits d'accès ».

AUTHENTIFICATION

Mesures ReCyF

Objectif de sécurité 10
Gestion des identités et des accès des utilisateurs aux systèmes d'information
- Authentification : 10.B.1-EI/EE, 10.B.2-EI/EE, 10.B.3-EI/EE, 10.B.4-EI/EE, 10.B.5-EI/EE, 10.B.6-EI/EE, 10.B.7-EE

Principes fondamentaux de l'authentification

Cette section présente les principes fondamentaux qui guident la conception, le choix et la mise en œuvre des mécanismes d'authentification (voir glossaire) au sein d'un système d'information.

L'accès à une ressource d'un système d'information doit être conditionné par un mécanisme d'authentification mettant en jeu l'utilisation d'au moins un élément secret pour que l'utilisateur prouve son identité. Sans cette authentification, n'importe qui pourrait accéder à une ressource en utilisant un identifiant valide.

Il est important de comprendre la différence entre un secret et un facteur d'authentification. Par définition, un secret est un élément qui est connu par un nombre restreint de personnes nécessitant de le connaître. Les facteurs d'authentification regroupent l'ensemble des éléments permettant d'effectuer une authentification, que ceux-ci soient secrets ou non. Par exemple, dans le cadre de la reconnaissance faciale, le visage est considéré comme un facteur d'authentification mais n'est pas un secret.

Les facteurs d'authentification sont regroupés en trois familles de facteurs d'authentification :
- les facteurs de connaissance (« ce que je sais ») : un mot de passe, un code PIN, etc. ;
- les facteurs de possession (« ce que je possède ») : une carte à puce, un téléphone, un certificat électronique, etc. ;
- les facteurs inhérents (« ce que je suis ») : une empreinte digitale, une empreinte rétinienne, etc.

Les secrets sont en grande majorité des facteurs de connaissance ou sont contenus dans des facteurs de possession. Dans le cadre de ReCyf, que l'authentification soit simple ou multifacteur, au moins un des facteurs d'authentification doit nécessairement reposer sur un élément secret.

Mécanismes d'authentification

L'efficacité des mécanismes d'authentification dépend fortement du contexte (cas d'usage, nature des menaces et paramètres techniques).

En revanche, il est possible de décrire leur niveau de sécurité relatif et les types de menaces auxquelles ils répondent :
- **Authentification multifacteur forte** (un des facteurs permet une authentification forte) : ce mécanisme offre une protection renforcée contre la plupart des menaces, notamment les attaques par vol de mot de passe, l'hameçonnage ou l'usurpation d'identité. Il est particulièrement adapté aux environnements sensibles ou exposés à des risques élevés.

- **Authentification forte** (un seul facteur d'authentification) : ce mécanisme est efficace contre les attaques opportunistes ou automatisées, mais peut être vulnérable à des attaques ciblées (ingénierie sociale, vol de matériel, etc.). Il convient aux contextes où les menaces sont modérées et où une authentification multifacteur n'est pas réalisable.

- **Authentification multifacteur sans authentification forte :** bien qu'elle combine plusieurs facteurs, l'absence de facteur fort limite sa résistance aux attaques sophistiquées. Elle peut être adaptée à des contextes où le risque est modéré, mais ne doit pas être considérée comme équivalente à une authentification forte.

- **Authentification simple :** ce mécanisme est vulnérable à la plupart des menaces (vol de mot de passe, attaques par force brute, etc.). Il ne doit être utilisé que dans des contextes à très faible risque ou en complément d'autres mesures de sécurité.

En pratique, le choix du mécanisme d'authentification doit être guidé par une analyse des risques spécifiques au système et aux données protégées.

Complexité des secrets

Les recommandations vis-à-vis de la complexité des secrets sont disponibles :

- Pour les mots de passe : dans le guide ANSSI des recommandations relatives à l'authentification multifacteur et aux mots de passe (voir bibliographie).

- Pour les mécanismes cryptographiques : dans l'annexe B1 du Référentiel Général de Sécurité (RGS) qui contient les règles et recommandations concernant le choix et le dimensionnement de mécanismes cryptographiques (voir bibliographie).

Ces recommandations sont mises à jour régulièrement afin de s'adapter à l'évolution de la sécurité des mécanismes d'authentification.

La complexité des mots de passe dépend du système d'authentification dans lequel les mots de passe sont utilisés. En effet, si un système d'authentification autorise des mots de passe contenant seulement des lettres minuscules et 5 caractères minimum, alors les mots de passe utilisables seront potentiellement moins complexes que ceux d'un système d'authentification qui force l'utilisation de lettres minuscules et majuscules, de chiffres, de caractères spéciaux, et avec une longueur minimale de 12 caractères.

La complexité des mots de passe d'un système d'authentification s'exprime via l'entropie, mesurée en bits. L'entropie met en relation la longueur d'un mot de passe et la variété du jeu de caractères autorisés pour un mot de passe du système d'authentification. Cette complexité peut être également vue comme une difficulté accrue à prévoir un mot de passe, car une entropie élevée correspond à un nombre de combinaisons plus important et donc plus résistant aux attaques par force brute. La Commission nationale de l'informatique et des libertés (CNIL) propose un calculateur permettant d'estimer l'entropie pour un système d'authentification utilisant des mots de passe (voir bibliographie).

Gestion des mots de passe

L'utilisation de mots de passe en tant que facteur d'authentification reste très fréquente.

Il est important d'expliquer aux utilisateurs qu'en cas de compromission d'un mot de passe, l'attaquant va systématiquement essayer d'utiliser ce mot de passe sur les différents systèmes d'authentification auxquels il pourra accéder.

Être capable de mémoriser un grand nombre de mots de passe complexes peut devenir difficile pour les utilisateurs. Il peut être acceptable de stocker les mots de passe sur un support physique ou virtuel, à condition de garantir la confidentialité de ces mots de passe. L'outil numérique le plus adapté pour réaliser cette fonction est le coffre-fort numérique de mots de passe. Ce dernier permet de stocker des mots de passe dans une base de données chiffrée. Si l'accès au coffre-fort numérique est réalisé par mot de passe, il est fortement recommandé que ce mot de passe soit complexe, donc avec une entropie élevée (128 bits par exemple).

Additionnellement, les coffres-forts numériques de mots de passe proposent souvent des fonctionnalités complémentaires qui permettent une gestion automatisée des mots de passe : génération aléatoire de mots de passe complexes, remplissage automatique des identifiants sur les applications compatibles, enregistrement automatisé de nouveaux identifiants et mots de passe. Ces fonctionnalités permettent de faciliter l'usage du coffre-fort numérique de mots de passe, qui allie alors sécurité et praticité.

Pour les mots de passe qui ne peuvent pas être stockés dans le coffre-fort numérique et qui doivent donc être mémorisés (par exemple, le mot de passe pour déchiffrer la base de données du coffre-numérique), la CNIL propose un outil de génération de mots de passe solides et simples à retenir à partir d'une phrase (voir bibliographie).

Politique de sécurité d'authentification

Les politiques de sécurité d'authentification sont des directions et des choix techniques ou organisationnels définissant les modalités des processus d'authentification.

On y retrouve les mécanismes d'authentification acceptés, les complexités des facteurs d'authentification associés aux mécanismes d'authentification et les périodes de renouvellement des secrets.

Ces politiques doivent distinguer les profils (utilisateur, administrateur, etc.) qui sont concernés par l'authentification.

Elles permettent d'assurer que les processus d'authentification sont documentés. Il est recommandé de mettre ces politiques en œuvre techniquement dans les différents systèmes d'authentification liés aux ressources des systèmes d'information.

Application et règles de mise en œuvre

Les principes précédents se traduisent, dans la pratique, par un ensemble de règles opérationnelles visant à garantir la sécurité des secrets d'authentification et des canaux de communication associés :

- Dans le cas d'un compte nominatif, le ou les éléments secrets sont personnels et ne doivent pas être connus par d'autres personnes que l'utilisateur du compte. Si l'on considère deux personnes, prénommées Alice et Bob et si le secret (par exemple un mot de passe) d'Alice était connu par Bob, alors Bob pourrait se connecter à une ressource avec le compte d'Alice, se faire passer pour elle et réaliser des actions malveillantes sur la ressource en son nom.

- Dans le cas d'un compte partagé où un ou plusieurs mêmes secrets sont détenus par plusieurs utilisateurs, alors ces secrets ne doivent être connus que par ce groupe d'utilisateurs. Lorsqu'Alice entre dans le groupe ou quitte le groupe, alors le ou les secrets doivent être modifiés. Si les secrets ne sont pas modifiés, Alice pourrait continuer à se connecter à un compte en utilisant les secrets qu'elle connaît toujours. Même si Alice quitte l'entité (et que son compte est désactivé), il est préférable d'appliquer la même procédure.

- Si le secret d'authentification d'une ressource ne peut pas être changé, alors il est nécessaire de mettre en place une ou plusieurs mesures de sécurité compensatoires permettant de savoir qui accède à la ressource en utilisant le secret fixe. Cette mesure peut être la même que celle permettant de compenser le risque d'utilisation de compte partagé. Alternativement, il est possible d'utiliser un journal d'accès virtuel (ex. : un fichier, une base de données) ou physique (un carnet) dans lequel les utilisateurs devront inscrire leurs accès (nom et date au minimum) à une ressource avec le secret.

- Il est recommandé que le choix des mesures compensatoires s'appuie sur l'analyse de risque.

- Il ne faut pas conserver les éléments secrets installés par défaut : mots de passe, certificats, clés de chiffrement, etc. Si la modification du secret est mal documentée ou difficile à réaliser, l'entité doit s'informer auprès de son fournisseur pour pouvoir l'effectuer. En particulier, elle doit s'assurer auprès du fournisseur qu'elle dispose de la liste complète des éléments secrets et que les procédures de modification d'éléments secrets sont documentées. De même, le fournisseur ou le fabricant ne doit pas pouvoir être le seul à avoir des droits permettant de modifier les secrets par défaut. Une fois le secret modifié par l'entité, le fournisseur ou le fabricant ne doit pas avoir de moyen de modifier ce secret sans l'accord de l'entité.

DROITS D'ACCÈS

Mesures ReCyF

Objectif de sécurité 10
Gestion des identités et des accès des utilisateurs aux systèmes d'information
- Droits d'accès : 10.C.1-EI/EE, 10.C.2-EI/EE, 10.C.3-EI/EE, 10.C.4-EI/EE

Pour accéder à une ressource, l'utilisateur doit s'identifier, puis s'authentifier, et enfin disposer d'une autorisation spécifique pour l'action qu'il souhaite réaliser. L'autorisation varie en fonction de l'utilisateur, il s'agit des droits d'accès de l'utilisateur.

Ces droits sont généralement donnés à des groupes ou des profils. Les droits doivent limiter les actions permises et les données visibles en fonction des besoins opérationnels de ces groupes ou profils. Par exemple, le profil « utilisateur » d'une application pourrait permettre d'utiliser l'application mais pas de l'administrer, contrairement au profil « administrateur ».

Lorsqu'un utilisateur possède un identifiant et est capable de fournir des facteurs d'authentification permettant de s'authentifier à une ressource à laquelle il n'a pas besoin d'accéder, alors l'accès doit lui être refusé, via la configuration des droits d'accès. Ce cas se présente, en particulier, lorsqu'un système d'authentification unique est mis en place. L'authentification unique, ou « *Single Sign-On* » en anglais, est un mécanisme qui permet à un utilisateur de s'authentifier une seule fois pour accéder à plusieurs applications ou ressources informatiques, sans avoir à ressaisir ses identifiants pour chacune d'elles. Ce mécanisme repose sur un système centralisé d'authentification, qui mutualise la gestion des accès aux différentes ressources en fonction des droits attribués à chaque utilisateur. Parmi les protocoles d'authentification unique couramment utilisés, il est possible de citer SAMLv2, *OpenID Connect*, Kerberos. Par exemple, si un système d'authentification unique gère à la fois l'authentification auprès d'une application de planification de projets et l'authentification auprès d'une application de gestion des salaires, alors un gestionnaire de projet aura une autorisation pour accéder à l'application de planification, mais n'aura pas d'autorisation pour accéder à l'application de gestion des salaires.

Cycle de vie des identités

Il est nécessaire que l'entité gère les moments clés du cycle de vie d'un compte :

- La création du compte avec le bon niveau de droits, en associant au compte un ou plusieurs profils (groupes) adaptés à ses besoins.

- La modification des droits d'un compte qui change de rôle au sein de l'organisation en modifiant le profil associé au compte. Cela intervient dans le cas d'un changement de situation d'un utilisateur et cela permet de s'assurer que les utilisateurs ne conservent pas plus de droits que ceux dont ils en ont besoin dans le temps. Additionnellement, l'entité doit effectuer périodiquement une revue des droits d'accès des profils d'utilisateur. La revue de droits est réalisée de façon systématique, en considérant les besoins théoriques des utilisateurs et en les comparant à leurs accès dans la pratique. Il est donc nécessaire d'avoir une base des besoins associés aux droits d'accès « à jour » avec laquelle exécuter la vérification. Ceci nécessite généralement de s'appuyer sur les procédures RH de l'organisation, qui doivent être mises à jour en conséquence.

- La désactivation du compte lors du départ (temporaire ou définitif) d'un utilisateur. Si la personne quitte l'entité concernée, ses droits d'accès doivent être intégralement supprimés.

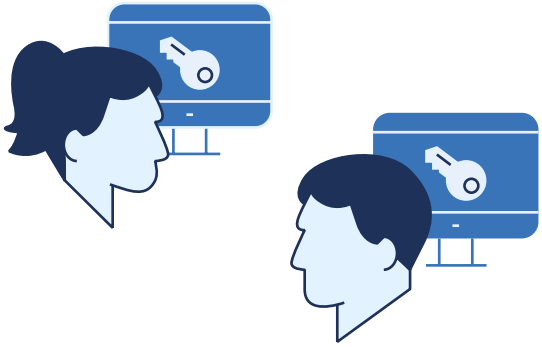
CAS PRATIQUES

Gestion centralisée ou locale des identités

La gestion des identités peut s'effectuer :

- De façon centralisée en utilisant des annuaires. Ces derniers sont des bases de données contenant l'ensemble des informations nécessaires à la gestion des identités : identifiants, informations personnelles, groupes d'appartenance, mots de passe (souvent hachés), politiques de sécurité d'authentification, droits d'accès. L'utilisation d'annuaires facilite grandement la gestion du cycle de vie des comptes.

- De façon décentralisée avec des comptes locaux sur chaque ressource. Les comptes locaux demandent un suivi plus important vis-à-vis de la revue des droits, mais sont parfois souhaitables ou nécessaires. En effet, certains appareils comme les automates industriels ne sont pas capables de fonctionner avec des annuaires, et des comptes locaux sont alors requis. Il peut être souhaitable de mettre en place des comptes locaux dits « brise-glace » sur les ressources critiques, utilisés uniquement en cas de dysfonctionnement des annuaires (si l'authentification passe obligatoirement par l'annuaire). Les comptes « brise-glace » étant souvent des comptes partagés et privilégiés, il est nécessaire de leur appliquer les recommandations concernant les comptes partagés explicitées précédemment et de mettre en place une authentification avec un niveau de sécurité élevé.



Annuaire ldap ou active directory (ad)

LDAP (*Lightweight Directory Access Protocol*) est un protocole standardisé permettant d'accéder et de gérer des services d'annuaire. AD (*Active Directory*) est une solution d'annuaire développée par Microsoft, qui utilise notamment le protocole LDAP pour ses échanges. Ces deux technologies sont parmi les plus répandues pour la gestion des identités et des accès.

Si la gestion des identités s'appuie sur un annuaire LDAP ou sur *Active Directory*, les mesures de sécurité suivantes peuvent être mises en place.

Au sein de l'annuaire :

- Placer les utilisateurs dans des groupes fonctionnels (rôles, métiers, projets) et attribuer les droits d'accès aux groupes plutôt qu'aux utilisateurs. Pour les AD, cette logique peut s'implémenter en utilisant la méthode AGDLP (*Account, Global, Domain Local, Permission*), qui consiste à mettre les utilisateurs dans les groupes globaux, et d'attribuer les permissions sur les groupes de domaine local, pour ensuite faire de l'inclusion de groupe.

- Assurer un échange sécurisé entre les applications métier et l'annuaire, en limitant les accès et en chiffrant les échanges (ex. : LDAPS).

- Appliquer la séparation logique entre les annuaires internes et les environnements externes (ex. : DMZ, services exposés).

- Changer systématiquement les mots de passe par défaut avant mise en service et imposer des règles de complexité conformes aux guides ANSSI (ex. : longueur minimale, absence de mots du dictionnaire).

- Activer la traçabilité : journaliser les connexions, modifications de groupes, créations/suppressions de comptes.

- Vérifier la cohérence des droits entre systèmes connectés à l'annuaire (fédération d'identités, SSO, IAM).

- Restreindre les délégations et délégations d'administration dans l'AD pour éviter des propagations involontaires de privilèges.

- Privilégier l'utilisation de certificats (par exemple AD CS [*Active Directory Certificate Services*]) ou d'un système de fédération d'identité (par exemple AD FS [*Active Directory Federation Services*]) pour éviter la transmission de secrets sous leur forme brute.

- Utiliser des GPO (*Group Object Policy*) ou des PSO (*Password Settings Objects*) pour implémenter les politiques de mots de passe directement dans l'AD.

Au sein de l'entité :

- Définir des procédures d'urgence pour la création temporaire de comptes ou l'accès en cas d'incident majeur, avec approbation et trace.

- Mettre en place une revue annuelle des comptes et des groupes afin qu'ils n'aient pas plus de droits que nécessaire.

- Mettre en place une politique stricte de création et de suppression des comptes : validation par le manager, suivi du cycle de vie, désactivation automatique des comptes inactifs ou orphelins (hors d'une organisation ou d'un groupe).

- Documenter les règles de nommage et d'attribution des identifiants afin de garantir la cohérence et la traçabilité.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Certificats

Les certificats sont très utilisés pour l'authentification des services automatiques et des utilisateurs. Afin de sécuriser leur utilisation, les recommandations suivantes sont à considérer :

- **Structurer l'IGC/PKI dès le départ :** même pour un petit nombre de certificats, mettre en place une IGC/PKI structurée (même manuelle), avec une hiérarchie claire des autorités de certification (AC racines, AC intermédiaires) et des processus documentés.

- **Utiliser des outils dédiés dès que nécessaire :** au-delà d'une gestion manuelle simple (quelques dizaines de certificats), ou dès que la criticité des usages l'exige, déployer des outils de gestion d'IGC (ex. : EJBCA, Microsoft AD CS, *OpenXPKI*) pour automatiser et sécuriser les opérations.

- **Définir une hiérarchie d'autorités de certification adaptée :** organiser les AC en fonction des usages (interne, certificats machine, certificats réseau, tests, production) et des niveaux de confiance requis, en limitant le nombre d'AC intermédiaires pour simplifier la gestion et réduire les risques.

- **Protéger strictement la clé privée de l'AC racine :** stocker la clé privée de l'AC racine dans un ***HSM (Hardware Security Module)***. Si ce n'est pas possible, utiliser un support chiffré, déconnecté du réseau, et physiquement sécurisé (coffre, salle sécurisée). La clé ne doit jamais être accessible en clair ou stockée sur un système connecté.

- **Appliquer le principe de séparation des rôles :** isoler les rôles (administrateur de l'IGC, émetteur de certificats, auditeur) et mettre en place des règles de délégation strictes, avec des droits d'accès minimaux. La délégation consiste à attribuer des droits spécifiques à des personnes ou des services pour réaliser certaines tâches (ex. : émission de certificats, validation de demandes, audit), sans leur donner un accès complet à l'ensemble de l'infrastructure.

- **Documenter les politiques de certification (PC) et déclarations de pratiques de certification (DPC) :** rédiger et publier des PC et des DPC précisant les usages autorisés, les durées de validité maximales (ex. : 1 an pour les certificats utilisateur, 2 ans pour les certificats serveur), les algorithmes autorisés, et les procédures de révocation.

- **Gérer la durée de vie des certificats et automatiser leur renouvellement :** adapter les durées de vie des certificats en fonction des usages. Mettre en place les procédures nécessaires au renouvellement des certificats. Dans la mesure du possible, utiliser des protocoles comme ACME pour automatiser l'émission, le renouvellement et la révocation des certificats afin de réduire les erreurs humaines et assurer le renouvellement.

- **Mettre en place des mécanismes de révocation fiables :** déployer au moins un mécanisme de révocation (CRL ou OCSP) et s'assurer qu'il est accessible et mis à jour régulièrement. Prévoir des alertes en cas de compromission ou d'expiration imminente.

- **Superviser et auditer régulièrement l'IGC/PKI :** vérifier périodiquement la validité des certificats, la configuration de l'IGC, l'absence d'algorithmes obsolètes (ex. : SHA-1, RSA < 2048 bits), et la conformité aux PC/DPC. Réaliser des audits internes ou externes au moins une fois par an.

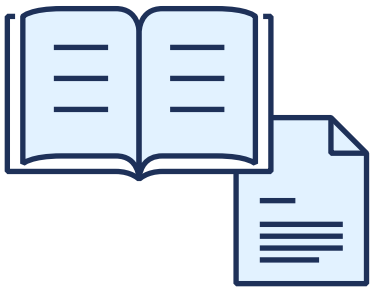
- **Restreindre les algorithmes cryptographiques :** n'autoriser que des algorithmes sécurisés et conformes aux recommandations ANSSI (ex. : RSA ≥ 2048 bits, ECC ≥ 256 bits, SHA-256 ou supérieur). Interdire les algorithmes obsolètes ou vulnérables.

- **Transférer et stocker les données sensibles de façon sécurisée :** lorsqu'une clé privée ou un élément secret associé à un certificat doit être transmis, il est impératif de privilégier un canal chiffré et authentifié pour le distribuer. Ne pas laisser de secret sur des supports qui n'ont pas d'usage de ce secret, mis à part pour des raisons de sauvegardes déconnectées.

- **Sensibiliser et former les acteurs :** former les administrateurs et utilisateurs aux bonnes pratiques de gestion des certificats, aux risques liés à une mauvaise utilisation, et aux procédures d'urgence (ex. : révocation en cas de compromission).

- **Préparer un plan de continuité et de reprise d'activité :** anticiper les pannes ou compromissions de l'IGC en mettant en place des sauvegardes sécurisées des clés et certificats, et des procédures de reprise d'activité testées régulièrement.

ANNEXES



Annexe 1: bibliographie

Documents ANSSI

- Référentiel Cyber France
Consulter le lien

- Guide d'hygiène informatique
Chapitre *« Identifier nommément chaque personne accédant au système et distinguer les rôles utilisateur »*
Consulter le lien

- Recommandations relatives à l'administration sécurisée des systèmes d'information
Chapitre *« Identification, authentification et droits d'administration »*
Consulter le lien

- Recommandations pour la protection des systèmes d'information essentiels
Consulter le lien

- Les moyens d'identification électronique et leur certification
Consulter le lien

- Recommandations relatives à l'authentification multifacteur et aux mots de passe
Consulter le lien

- Annexe B1 du Référentiel général de sécurité : Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement de mécanismes cryptographiques
Consulter le lien

- Guide de sélection d'algorithmes cryptographiques
Consulter le lien

- Automatisation de la gestion des certificats avec ACME
Consulter le lien

- Infrastructure de gestion de clés (IGC)
Consulter le lien

- Recommandations de déploiement du protocole 802.1X
Consulter le lien

- Recommandations pour l'administration sécurisée des SI reposant sur AD
Consulter le lien

Documents France en complément

- France Num – DGE – La Gestion des Identités et des Accès (IAM) : un enjeu clé pour la sécurité des entreprises
Consulter le lien

- CNIL – Authentification multifacteur : les recommandations de la CNIL pour mieux protéger les données
Consulter le lien

- CNIL – Sécurité : authentifier les utilisateurs
Consulter le lien

- CNIL – Mots de passe : recommandations pour maîtriser sa sécurité
Consulter le lien

Normes

- ISO – Gestion de l'identité : les principaux points à retenir
Consulter le lien

Outils

- CNIL – Générer un mot de passe solide
Consulter le lien

- CNIL – Calculateur de complexité de mots de passe
Consulter le lien

Annexe 2 : extrait du glossaire ReCyF

Mesures ReCyF	Définition
Annuaire	Ressource logicielle centralisant des informations relatives aux utilisateurs, et parfois aux autres ressources d'un système d'information et fournissant des mécanismes d'identification et d'authentification. *Par exemple : Microsoft Active Directory, OpenLDAP.*
Authentification multifacteur	Authentification mettant en œuvre plusieurs facteurs d'authentification appartenant à au moins deux des trois catégories suivantes : ▸ Facteur de connaissance (par exemple : un mot de passe) ; ▸ Facteur de possession (par exemple : une application mobile) ; ▸ Facteur inhérent (par exemple : l'empreinte digitale).
Cœur de confiance	Ensemble des ressources regroupant les annuaires, les ressources hébergeant ces annuaires ou permettant d'en prendre le contrôle.
Compte d'administration	Compte disposant de privilèges nécessaires aux actions d'administration. Il peut être partagé, individuel ou de service.
Facteur d'authentification	Élément utilisé pour réaliser l'authentification d'un utilisateur ou d'un processus automatique, sur la base d'une information mémorisée (facteur de connaissance), d'un élément physique stockant un secret (facteur de possession) ou d'une caractéristique liée à une personne (facteur inhérent).
Information sensible	Les données à caractère personnel « sensibles » au sens du 1 de l'article 9 du Règlement (UE) 2016/679, les données d'une sensibilité particulière au titre de l'article 31 de la loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique, les données protégées au titre de l'article L. 151-1 du code de commerce ainsi que les données protégées au titre de la protection du patrimoine scientifique et technologique de la nation.
Mécanisme d'authentification	Mécanisme permettant d'authentifier un utilisateur ou un processus automatique préalablement à l'accès aux ressources des systèmes d'information. Ce mécanisme s'appuie au minimum sur un facteur d'authentification et peut mettre en œuvre une authentification multifacteur.
Réseau	Ensemble de ressources interconnectées permettant de communiquer au sein d'un ou plusieurs systèmes d'information.
Sous-système	Ensemble de composants d'un système d'informations constitués pour assurer une fonctionnalité ou un ensemble homogène de fonctionnalités d'un système d'information ou encore pour isoler des ressources d'un système d'information ayant un même besoin de sécurité.
Système d'analyse	Système d'information exploitant les événements de sécurité à la recherche d'indicateurs de compromission et de techniques d'attaques, dans le but d'identifier des incidents de sécurité.
Système d'information	Ensemble des infrastructures et services logiciels informatiques relevant de la responsabilité de l'entité, permettant de collecter, traiter, transmettre et stocker sous forme numérique les données. Les ressources informatiques partagées ou mutualisées avec des tiers relevant du périmètre de responsabilité de l'entité, sont considérées comme faisant partie intégrante des systèmes d'information de l'entité, et sont à ce titre pleinement assujetties aux obligations de la directive NIS 2.
Système d'information d'infrastructure	Système d'information généraliste utile aux activités ou aux services de l'entité, ou nécessaire au fonctionnement de plusieurs systèmes d'information de l'entité. *Par exemple : annuaire, messagerie, téléphonie, service de résolution de nom de domaine.* Un système d'information d'infrastructure peut être un système d'information.
Systèmes d'information tiers	Système d'information ou ressource informatique partagée ou mutualisée avec l'entité qui n'est pas sous la responsabilité de l'entité. *Point d'attention : lorsque l'entité externalise tout ou partie de son système d'information, ce dernier reste sous sa responsabilité et n'est donc considéré comme un SI tiers au sens du présent référentiel.*
Utilisateurs	Personnels de l'entité et prestataires agissant pour le compte de l'entité qui accèdent aux systèmes d'information.