PROTECTION DE DONNÉES L'INTEGRITÉ

Les types de contrôles de l'intégrité des données

Les algorithmes de hash

- Le hash est un outil qui garantit l'intégrité des données en prenant les données binaires (le message) pour en générer une représentation de longueur fixe appelée valeur de hash ou synthèse du message.
- Le hash est une fonction mathématique unidirectionnelle relativement simple à calculer, mais extrêmement difficile à inverser. On peut comparer une fonction unidirectionnelle à l'action de moudre des grains de café. Il est facile de moudre des grains de café, mais il est quasiment impossible de les reconstituer ensuite.
    - Une fonction de hash cryptographique possède les propriétés suivantes :
        - Il n'y a pas de limite de longueur pour le texte saisi.
        - La longueur du résultat est fixe.
        - La fonction de hash est unidirectionnelle et irréversible.
        - Deux valeurs d'entrée différentes produisent toujours des valeurs de hash différentes.

Les types de contrôles de l'intégrité des données

Les algorithmes de hash

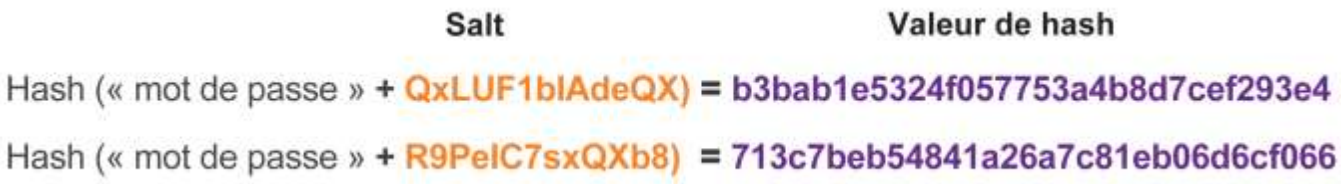
De nombreux algorithmes de hash modernes sont largement utilisés de nos jours. Les plus populaires sont MD5 et SHA.

- **Algorithme MD5 (Message Digest 5) :** algorithme de hash développé par Ron Rivest qui produit une valeur de hash de 128 bits.
- **Algorithme SHA (Secure Hash Algorithm) :** développé par le NIST (National Institute of Standards and Technology) des États-Unis, il peut être implémenté avec différentes forces :
- SHA-224 (224 bits)
- SHA-256 (256 bits)
- SHA-384 (384 bits)
- SHA-512 (512 bits)

Les types de contrôles d'intégrité des données

Le salage

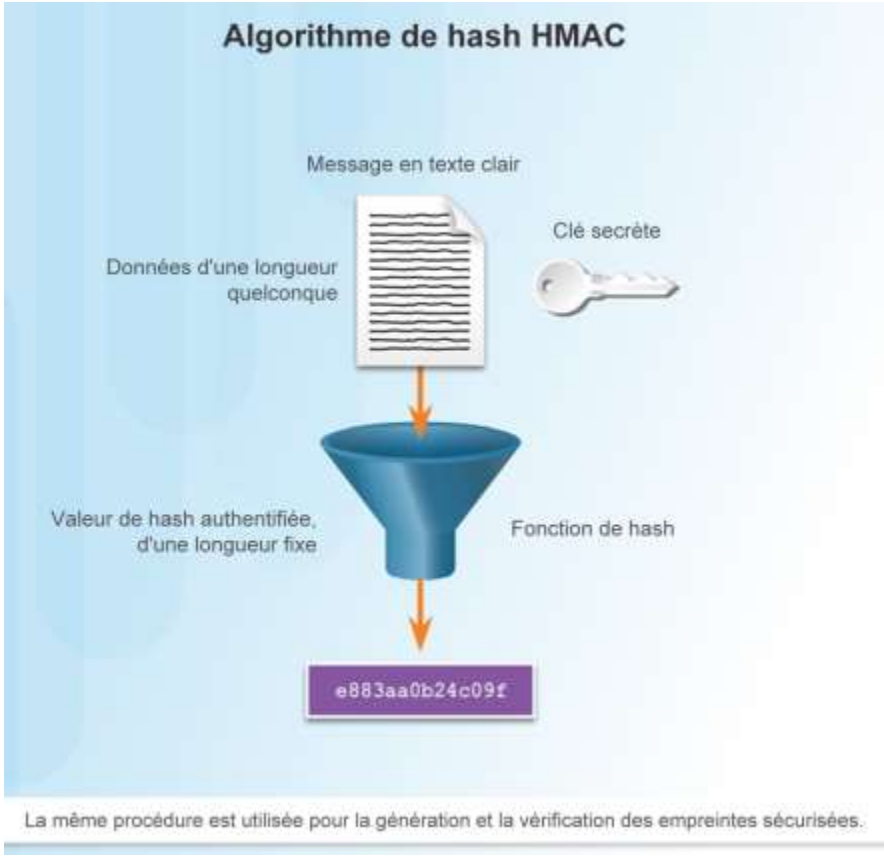
- Le salage permet de sécuriser davantage le hash. Si deux utilisateurs possèdent le même mot de passe, ils auront également les mêmes hashs de mot de passe. Une valeur de salage, qui correspond à une chaîne aléatoire de caractères, est une entrée supplémentaire du mot de passe avant le hash.
- Elle crée un résultat de hash différent pour les deux mots de passe, comme illustré sur la figure. Une base de données stocke le hash et la valeur de salage.



Les types de contrôles d'intégrité des données

HMAC

- Les HMAC renforcent les algorithmes de hash en utilisant une clé secrète supplémentaire en entrée de la fonction hash.
- HMAC ne se contente pas d'assurer l'intégrité des données, il ajoute une étape d'authentification.
- HMAC utilise un algorithme spécifique qui combine une fonction de hash cryptographique et une clé secrète, comme illustré sur la figure.



Les signatures numériques

Les signatures et la loi

- Les signatures numériques fournissent la même fonctionnalité que les signatures manuscrites pour les documents électroniques.
- Une signature numérique est utilisée pour déterminer si un document a été modifié après avoir été signé par l'utilisateur.
- Une signature numérique est une méthode mathématique utilisée pour vérifier l'authenticité et l'intégrité d'un message, d'un document numérique ou d'un logiciel.
- Dans de nombreux pays, les signatures numériques ont la même valeur légale qu'un document signé manuellement.
- Les signatures numériques permettent également la répudiation.

Les signatures numériques

Fonctionnement de la technologie de signature numérique

La cryptographie asymétrique est à la base des signatures numériques. Un algorithme de clé publique comme RSA génère deux clés : une privée et l'autre publique. Ces clés sont associées mathématiquement.

Les certificats

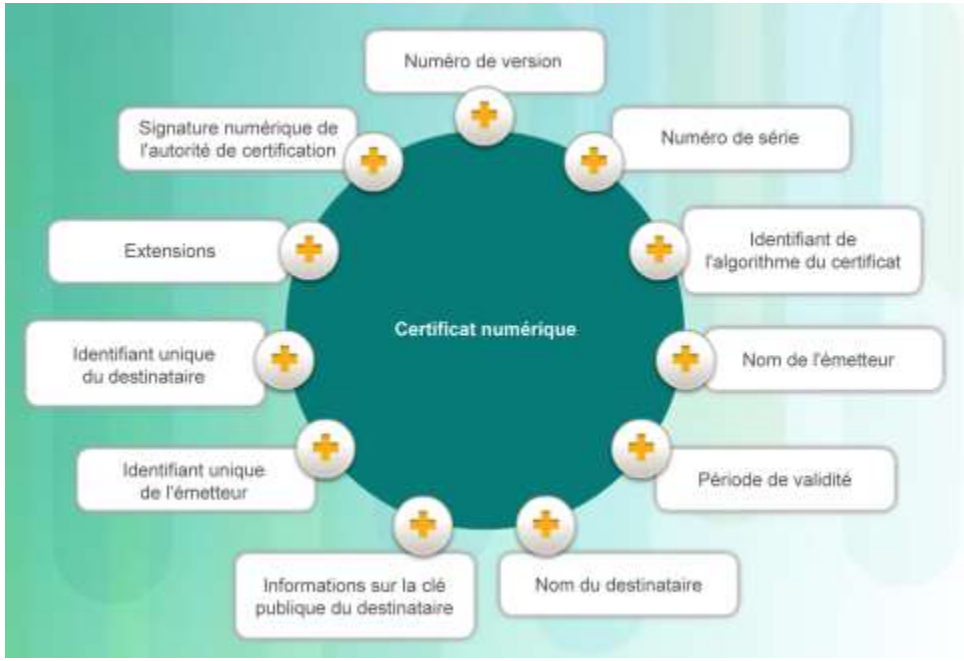
Les bases du certificat numérique

- Un certificat numérique est équivalent à un **passeport électronique.**
- Les certificats numériques permettent aux utilisateurs, aux hôtes et aux entreprises d'échanger des informations sur Internet de manière sécurisée.
- Un certificat numérique permet de vérifier que les utilisateurs qui envoient un message sont bien ceux qu'ils prétendent être.
- Les certificats numériques peuvent également assurer la confidentialité du destinataire en lui permettant de chiffrer sa réponse.

Les certificats

Créer un certificat numérique

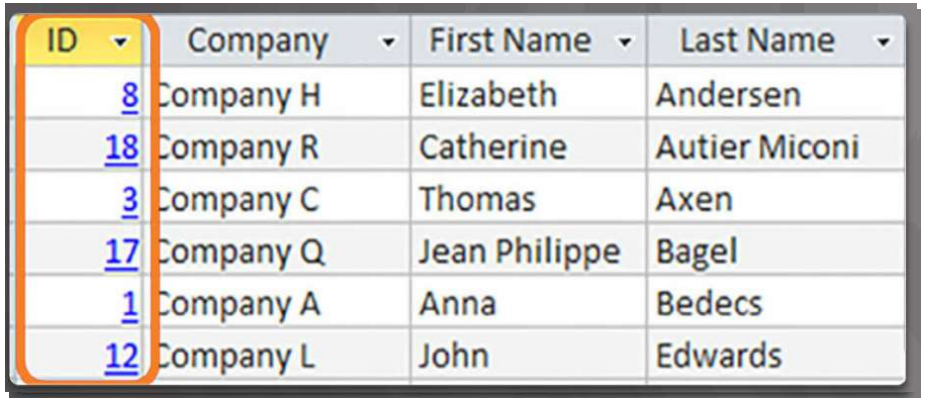
- Le certificat numérique doit suivre une structure standard pour qu'une entité puisse le lire et le comprendre, quel que soit l'émetteur.
- X.509 est la norme de création des certificats numériques et l'infrastructure de clé publique (PKI) utilisée pour gérer les certificats numériques.
- L'infrastructure à clé publique (PKI) correspond aux politiques, aux rôles et aux procédures nécessaires pour créer, gérer, distribuer, utiliser, stocker et révoquer des certificats numériques.



Protection de l'intégrité des bases de données

L'intégrité des bases de données

- Les bases de données permettent de stocker, de récupérer et d'analyser efficacement des données.
- À mesure que le volume des données collectées augmente et que les données deviennent plus sensibles, il est important que les professionnels de la cybersécurité protègent les bases de données toujours plus nombreuses.
- L'intégrité des données fait référence à l'exactitude, à la cohérence et à la fiabilité des données stockées dans une base de données.



ID	Company	First Name	Last Name
8	Company H	Elizabeth	Andersen
18	Company R	Catherine	Autier Miconi
3	Company C	Thomas	Axen
17	Company Q	Jean Philippe	Bagel
1	Company A	Anna	Bedecs
12	Company L	John	Edwards

Protection de l'intégrité des bases de données

L'intégrité des bases de données (suite)

Il existe quatre règles ou contraintes pour la protection de l'intégrité des bases de données :

- **Intégrité de l'entité** : toutes les lignes doivent avoir un identifiant unique appelé clé principale.
- **Intégrité du domaine** : toutes les données stockées dans une colonne doivent suivre un format et une définition identiques.
- **Intégrité référentielle** : les relations entre les tables doivent rester cohérentes. Par conséquent, un utilisateur ne peut pas supprimer un enregistrement associé à un autre.
- **Intégrité définie par l'utilisateur** : ensemble de règles définies par un utilisateur n'appartenant pas à l'une des autres catégories. Par exemple, un client passe une nouvelle commande. L'utilisateur vérifie d'abord s'il s'agit d'un nouveau client. Si c'est le cas, il l'ajoute dans la table des clients.

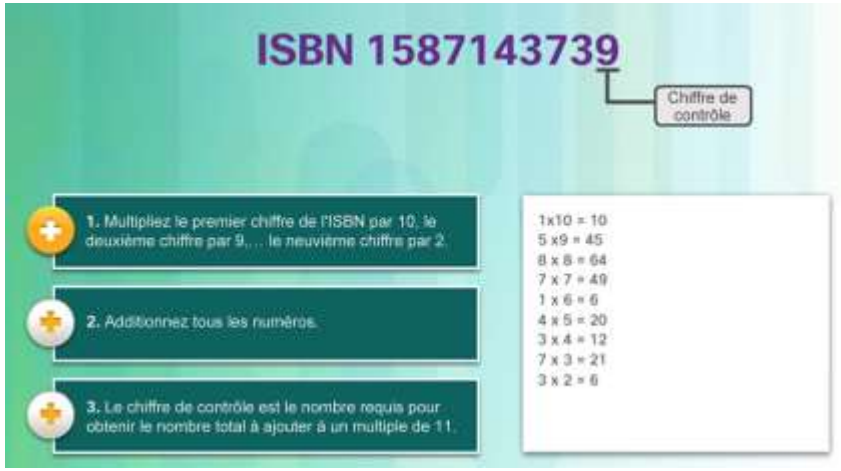
ID	Company	First Name	Last Name
8	Company H	Elizabeth	Andersen
18	Company R	Catherine	Autier Miconi
3	Company C	Thomas	Axen
17	Company Q	Jean Philippe	Bagel
1	Company A	Anna	Bedecs
12	Company L	John	Edwards

Protection de l'intégrité des bases de données

Validation de la base de données

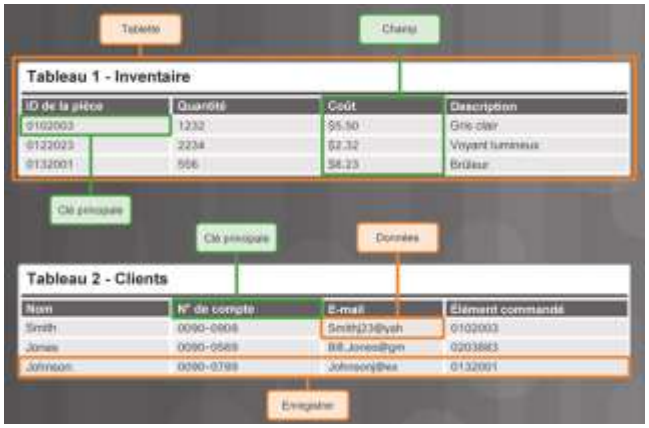
Une règle de validation vérifie que les données respectent les paramètres définis par le concepteur de la base de données. Une règle de validation permet de s'assurer de l'exhaustivité, de l'exactitude et de la cohérence des données. Voici quelques critères utilisés dans une règle de validation :

- La taille : vérifie le nombre de caractères dans un élément de données
- Le format : vérifie que les données respectent un format spécifié
- La cohérence : s'assure de la cohérence des codes contenus dans les éléments de données
- La plage : vérifie que les données sont comprises entre une valeur minimale et une valeur maximale
- Chiffre de contrôle : fait un calcul supplémentaire qui génère un chiffre de contrôle pour la détection des erreurs.



Protection de l'intégrité des bases de données

Les exigences en matière d'intégrité des bases de données



- Il est fondamental de bien classer les données dans la base de données pour préserver leur fiabilité et leur utilité.
- Une base de données se compose de tables, d'enregistrements, de champs et de données.
- Pour préserver l'intégrité du système de classement de la base de données, les utilisateurs doivent respecter certaines règles.
- L'intégrité de l'entité est une règle d'intégrité qui stipule que chaque table doit posséder une clé principale et que la ou les colonnes qui correspondent à la clé principale doivent être uniques et non nulles.
- Dans une base de données, « nul » désigne des valeurs manquantes ou inconnues. L'intégrité de l'entité permet d'organiser les données de manière appropriée pour cet enregistrement.

Protection de l'intégrité des bases de données

Les exigences en matière d'intégrité des bases de données (suite)

- L'intégrité référentielle, qui repose sur les clés étrangères, est un autre contrôle d'intégrité important. Une clé étrangère dans une table fait référence à une clé principale dans une autre table. La clé principale identifie de manière unique des entités (lignes) dans la table. L'intégrité référentielle préserve l'intégrité des clés étrangères.

Protection de l'intégrité des bases de données

Les exigences en matière d'intégrité des bases de données (suite)

N° S.S. 243-27-3361	• Doit être composé de neuf nombres entiers • Format xxx - xx - xxxx • Saisi ou modifié par le client uniquement • Doit être validé
Numéro de carte de crédit 4539 4769 0728 4479	• Doit être composé de seize nombres entiers • Format xxxx - xxxx - xxxx - xxxx • Saisi ou modifié par le client uniquement • Doit être validé
Adresse e-mail tortor@odio.com	• Ne doit pas être composée de plus de 128 caractères • Format xxxx@xxxx.xxx • Saisi ou modifié par le client uniquement • Validée par un e-mail de réponse

- L'intégrité du domaine garantit que tous les éléments de données d'une colonne respectent un jeu défini de valeurs valides. Chaque colonne d'une table est composée d'un jeu défini de valeurs, comme des numéros de carte de crédit, des numéros de sécurité sociale ou des adresses e-mail. Si vous limitez la valeur attribuée à une instance de cette colonne (un attribut), vous protégez l'intégrité du domaine. La protection de l'intégrité du domaine peut être aussi simple que de choisir le type, la longueur ou le format appropriés des données d'une colonne.