

# Analyse des applications en commerce électronique INF22307



Cours #12 – Sécurité des transactions électroniques et des sites web de commerce électronique

Martin Arsenault, ing., MBA, MGP

Novembre 2023

# Sécurité des transactions électroniques

Quelques éléments à considérer sur la sécurité des données...



# Qu'est-ce qu'une transaction électronique ?

- Selon L'OQLF :
  - Transaction sécurisée qui est effectuée, lors d'un achat ou d'un paiement en ligne, par l'intermédiaire du réseau Internet.
- De façon plus générale :
  - Une transaction électronique est l'autorisation donnée par le porteur d'une carte ou une méthode de paiement électronique d'effectuer un certain type d'opération au bénéfice d'un marchand, depuis le compte associé à sa carte bancaire et géré par son institution financière.
- Vise autant les sites web que les équipements de traitement bancaire électroniques.
- Vise autant le réseau Internet que les réseaux d'entreprises
- Implique une transmission de données sécurisés sur un réseau entre trois points :
  - Commerçant  $\longleftrightarrow$  vers sa banque      La banque du commerçant  $\longleftrightarrow$  la banque du client

# Transaction avec des cartes de crédit ?

- Si vous acceptez les paiements par carte de crédit, la **norme de sécurité de l'industrie des cartes de paiement** (Payment Card Industry - PCI) **doit être entièrement intégrée à votre site** de commerce électronique et dans vos pratiques internes.
- En d'autres mots, si vous faites des ventes à l'aide d'outils numériques, **vous devriez vous conformer** à la norme PCI.
- Ce n'est **pas un programme obligatoire** pour les commerçants, cependant, il peut assurer aux commerçant un rehaussement de leur sécurité en se conformant aux conditions de conformité.



# La norme PCI

- Visa, MasterCard, American Express, Discover et JCB ont formé un consortium appelé Conseil des normes de sécurité PCI (Payment Card Industry Security Standards Council). Le groupe continue à établir des normes de sécurité sur les données (PCI DSS) et s'attend à ce que tous les sites transactionnels respectent ces exigences.
- Ce standard a été créé afin d'augmenter le contrôle des informations du titulaire de la carte dans le but de réduire l'utilisation frauduleuse des instruments de paiement.
- Les normes de sécurité du Conseil comportent des lignes directrices et des processus visant à prévenir la violation des données et la fraude par carte de crédit.
- L'adhésion n'est malheureusement pas obligatoire mais les grands fournisseurs de service transactionnels y adhèrent.



[https://www.paypal.com/ca/business/security/pci-compliance?locale.x=fr\\_CA](https://www.paypal.com/ca/business/security/pci-compliance?locale.x=fr_CA)

[PCI Security Standards Council](#)

# Je n'adhère pas à la norme PCI ?

- Dans le pire des cas, votre **capacité d'accepter les paiements par cartes de crédit pourrait être suspendue ou révoquée**. Le non-respect de cette exigence du commerce électronique peut entraîner des **violations de données**, la **perte de confiance des clients** et même la **résiliation de l'entente qui vous permet d'accepter les paiements par cartes**.
- De plus, votre entreprise pourrait être **responsable envers les émetteurs de cartes de crédit** pour le remplacement de cartes et pour les dommages subis.



## POURQUOI LA SÉCURITÉ DES PAIEMENTS EST IMPORTANTE

- La sécurité des données des titulaires de cartes de paiement concerne tout le monde
- Une violation ou un vol des données des titulaires de cartes peut entraîner d'importantes pertes financières
- Lorsque les données relatives aux titulaires de cartes sont compromises, l'ensemble de l'écosystème de paiement peut être menacé
- Le respect des standards PCI améliore la sécurité des données des titulaires de cartes et contribue à réduire la fraude



# Statistique favorables envers la norme PCI

- Près de 80 % des violations ou des actes de piratage des données se produisent chez des marchands de petite ou de moyenne taille.
- La bonne nouvelle, c'est qu'aucune organisation qui adhère entièrement aux normes de sécurité PCI n'a jamais été victime d'effraction pour ce qui est des paiements ou des données sur les paiements.
- Même si la conformité a augmenté grandement de 2012 à 2016, quelque 80 % des organisations ne respectent toujours pas les normes.
- L'adhésion est cependant en baisse depuis en 2016.
- Pour obtenir l'accréditation PCI, votre entreprise de commerce électronique doit prouver qu'elle satisfait à de nombreuses exigences en matière de sécurité.

# Conditions de conformité à la norme PCI

- Bâtir et tenir à jour un réseau sécurisé
  - Mettre en place des pare-feux informatiques
- Protéger les données du titulaire de la carte
  - Protéger les données stockées du titulaire de la carte
  - Crypter la transmission des données du titulaire de la carte
- Maintenir un programme de gestion des vulnérabilités
  - Utiliser et mettre régulièrement à jour un logiciel antivirus
  - Développer et maintenir des systèmes et une utilisation sécurisée
  - Surveiller l'évolution des vulnérabilités



# Conditions de conformité à la norme PCI

- Mettre en place de solides mesures de contrôle d'accès
  - Restreindre l'accès des employés aux données des titulaires de cartes
  - Attribuer une ID unique à chaque personne qui a accès à l'ordinateur
  - Restreindre l'accès physique aux données des titulaires de cartes
- Surveiller les réseaux et faire régulièrement des tests
  - Suivre et surveiller tous les accès aux ressources du réseau et aux données des titulaires de cartes
  - Faire régulièrement des tests sur les systèmes et les procédures de sécurité
- Tenir à jour une politique sur la sécurité des informations
  - Maintenir une politique organisationnelle sur la sécurité des informations de même que les directives et les procédures s'y rattachant

# Tendances en matière d'adhésion

## PCI requirement

Requirement 1: Install and maintain a firewall configuration.

Requirement 2: Do not use vendor-supplied defaults.

Requirement 3: Protect stored cardholder data.

Requirement 4: Protect data in transit.

Requirement 5: Protect against malicious software.

Requirement 6: Develop and maintain secure systems.

Requirement 7: Restrict access.

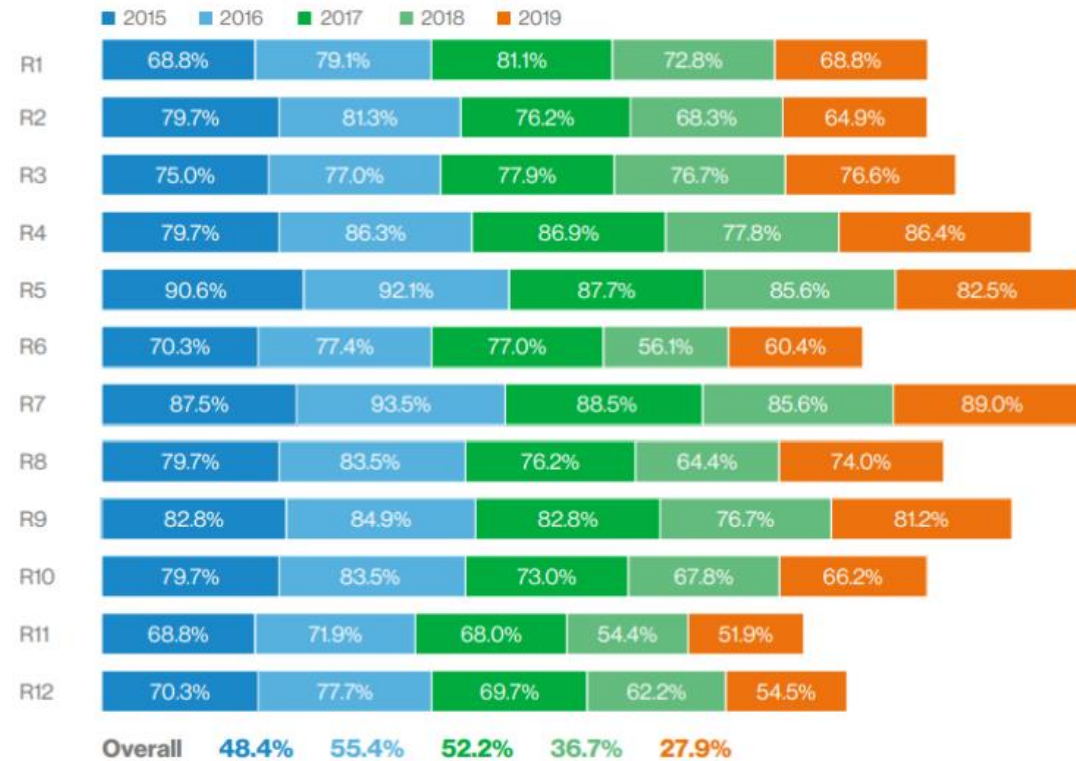
Requirement 8: Authenticate access.

Requirement 9: Control physical access.

Requirement 10: Track and monitor access.

Requirement 11: Test security systems and processes.

Requirement 12: Security management

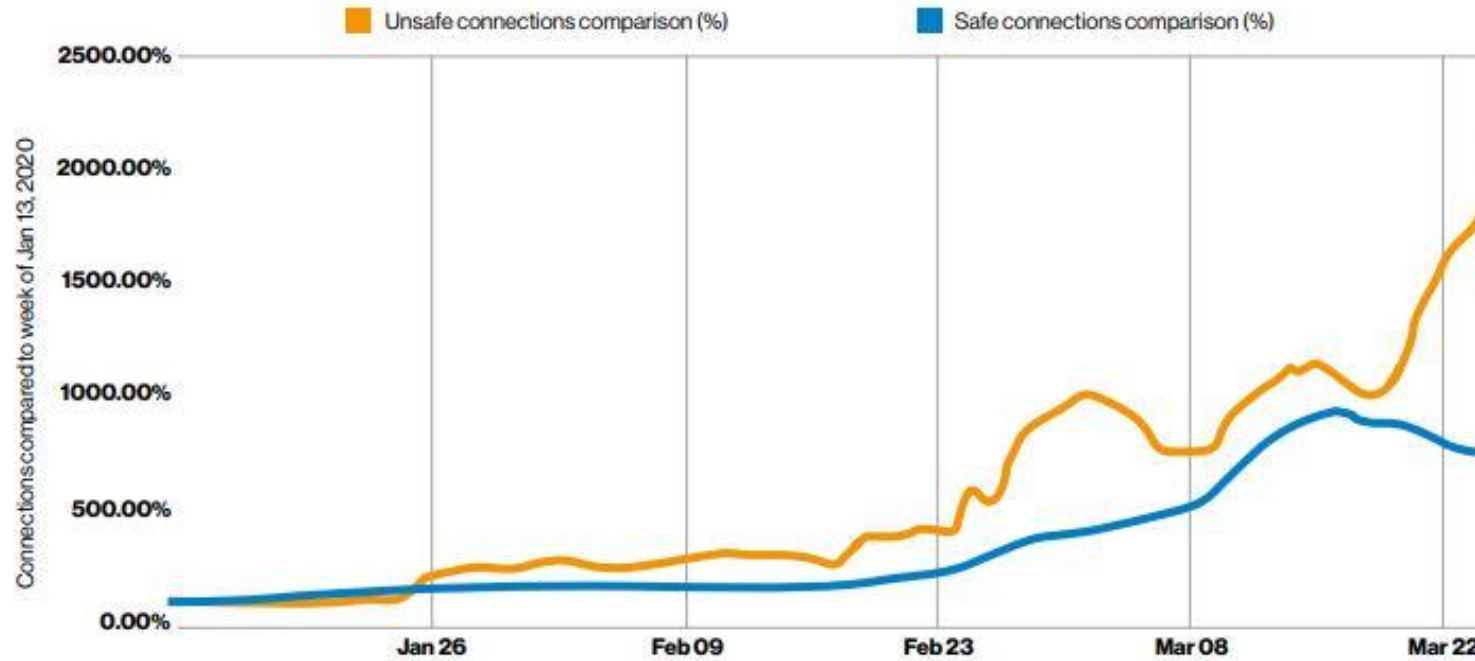


Full Compliance Rates from 2015-2019 for Each Main PCI Requirement. Source: Verizon 2020 Payment Security Report

Source : <https://www.thesslstore.com/blog/pci-compliance-numbers-drop-as-security-breaches-increase/>

# Depuis la COVID...

Safe vs unsafe connections to COVID-19-related domains



Baisse de  
l'adhésion à la  
conformité



Hausse des  
brèches de  
sécurité

# Utilisation de sites tiers – PCI Compliant

- Que se passerait-il, si les paiements sont faits par Paypal, par exemple, ou par shopify, ou par un service de traitement de paiement. Ai-je besoin de me conformer ?
  - Il y a un niveau de conformité aux normes PCI pour les utilisateurs tiers. Il est faux de croire que la conformité aux normes PCI est exigée uniquement des commerçants qui stockent des données de cartes de crédit. Même si le processus de paiement est entièrement sous-traité, vous devez tout de même vous conformer à certaines exigences PCI DSS, mais les exigences peuvent être moins strictes.

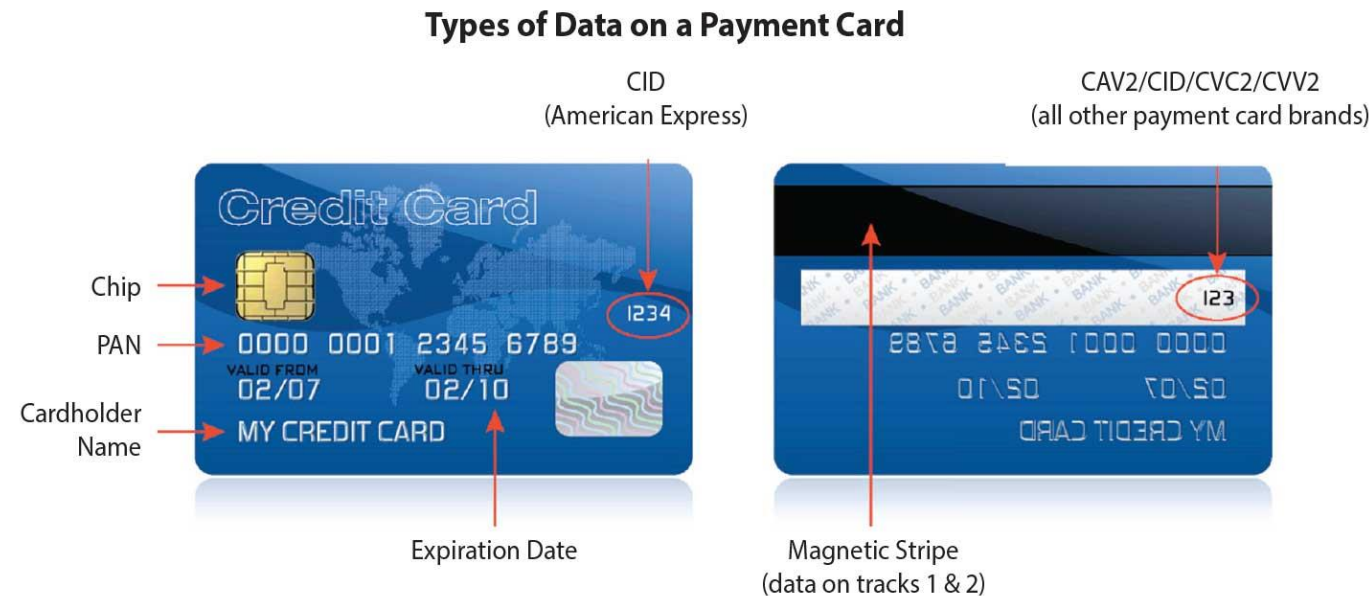
# Utilisation de sites tiers – PCI Compliant

- Bémol pour Paypal, selon leur site Internet :
  - Lorsque vos clients font leurs achats sur votre site, ils cliquent sur un bouton pour payer à partir de leur compte bancaire, de leur carte de crédit ou de leur compte PayPal. Dans tous les cas, ils paient sur une page sécurisée hébergée par PayPal. **Étant donné que PayPal stocke les informations relatives à la carte ou au compte bancaire de vos clients, vous n'avez pas à vous préoccuper de la protection des données des titulaires de carte stockées, du cryptage des données en transit ou de la restriction d'accès aux données des titulaires de carte.**

Nous maintenons en permanence et validons de façon régulière la sécurité de Paiements sur site marchand. Vous pouvez ainsi vous concentrer sur la recherche de nouveaux clients et sur l'excellence de votre service clientèle.

# Quelles sont les données sensibles ?

- Les pirates veulent vos données de titulaire de carte. En obtenant le numéro de compte principal (PAN) et les données d'authentification sensibles, un voleur peut usurper l'identité du titulaire de la carte et utiliser la carte pour réaliser des transactions.
- Tout ce qui se trouve au bout d'une flèche rouge est constitué de données sensibles du titulaire de carte. Tout ce qui se trouve à l'arrière et le CID ne doivent jamais être stockés. Vous devez avoir de bonnes raisons commerciales pour stocker quoi que ce soit d'autre, et ces données doivent être protégées.



# Où sont les données sensibles ?

- Vous sécurisez les données des titulaires de carte là où elles sont saisies, du point de vente jusqu'au moment où elles sont transférées dans le système de paiement.
- Où se font les vols d'information sur les cartes bancaire :
  - Lecteur de carte compromis
  - Papier stocké dans un classeur
  - Données dans une base de données de système de paiement
  - Caméra cachée saisissant des données d'authentification
  - Écoute d'un réseau sans fil ou câblé de votre commerce
  - Dans les files d'attente, dans le transport en commun, en plein public, etc.
- Où sont les données ?
  - Lecteurs de cartes
  - Systèmes de point de vente
  - Réseaux de magasins et routeurs d'accès sans fil
  - Stockage et transmission de données par carte de paiement
  - Données de carte de paiement stockées dans des enregistrements papiers
  - Applications de paiement en ligne et paniers d'achat



# Cartographier vos flux de données

- Avant de pouvoir protéger les données sensibles des cartes de crédit, vous devez savoir où elles se trouvent et comment elles s'y rendent. Vous souhaitez **créer une carte complète des systèmes, des connexions réseau et des applications qui interagissent avec les données de carte de crédit de votre entreprise**. Selon votre rôle, vous devrez probablement travailler avec vos équipes de sécurité et d'informatique pour ce faire :
  - **Identifiez tous les domaines de l'entreprise liés aux consommateurs qui impliquent des transactions de paiement.**
    - Par exemple, vous pouvez accepter des paiements via un panier en ligne, des terminaux de paiement en magasin ou des commandes passées par téléphone.
  - **Identifiez les différentes manières dont les données des titulaires de cartes sont traitées dans l'entreprise.** Il est important de savoir exactement **où les données sont stockées et qui y a accès.**
  - **Identifiez les systèmes internes ou les technologies sous-jacentes qui concernent les transactions de paiement.**
    - Cela inclut vos infrastructures de réseau, vos centres de données et vos environnements cloud.

# Vérifier les contrôles de sécurité et les protocoles

- Une fois que vous avez **identifié tous les points de contact potentiels pour les données de carte de crédit** au sein de votre entreprise, collaborez avec les équipes informatiques et de sécurité pour vous assurer que les **configurations et protocoles de sécurité appropriés sont en place** (Conditions de conformité PCI). Ces protocoles sont conçus pour sécuriser la transmission de données (ex : **TLS et SSL**).
- Les conditions de conformité découlent des meilleures pratiques en matière de protection des données sensibles pour toutes les entreprises.

# Surveiller et maintenir

- Il est important de noter que la conformité PCI n'est pas un événement ponctuel. Il s'agit d'un processus continu visant à garantir la conformité de votre entreprise, même si les flux de données et les points de contact clients évoluent.
- Certaines marques de cartes de crédit peuvent vous obliger à soumettre des rapports trimestriels ou annuels, ou à effectuer une évaluation annuelle sur site pour valider la conformité continue, en particulier si vous traitez plus de 6 millions de transactions chaque année.
- Assurez-vous d'avoir une surveillance en continu des activités et des transactions sur votre réseau et vos infrastructures.
- La gestion de la conformité PCI tout au long de l'année (et d'une année à l'autre) nécessite souvent un soutien et une collaboration. Il peut être intéressant de créer une équipe dédiée pour maintenir correctement la conformité. Bien que chaque entreprise soit unique, un bon point de départ pour une «équipe PCI» comprendrait les représentants suivants...

# Surveiller et maintenir

- **Sécurité : le responsable de la sécurité**, le responsable de la sécurité de l'information et leurs équipes veillent à ce que l'organisation investisse toujours de manière appropriée dans les ressources et les politiques nécessaires en matière de sécurité et de confidentialité des données.
- **Technologie / Paiements : le directeur technique** et leurs équipes veillent à ce que les outils, les intégrations et l'infrastructure de base restent conformes au fur et à mesure de l'évolution des systèmes de l'entreprise.
- **Finances : le directeur financier** et son équipe veillent à ce que tous les flux de données de paiement soient comptabilisés en ce qui concerne les systèmes de paiement et les partenaires.
- **Juridique** : cette équipe peut vous aider à naviguer dans les nombreuses nuances juridiques de la conformité à la norme PCI DSS.

# Sécurité des sites web en commerce électronique



# Les sites web de commerce électronique sont la cible !

- Chaque propriétaire de site Web devrait craindre d'être piraté. Toutefois, les propriétaires de sites Web de commerce électronique devraient s'inquiéter plus que d'autres de la sécurité de leur site. Parce que ces sites sont beaucoup plus rentables et visés par les pirates que les sites ordinaires.

La question n'est pas : Est-ce que je vais me faire pirater ?  
Mais plutôt : Quand je vais me faire pirater ?

# Les sites web de commerce électronique sont la cible !

- Tout d'abord, les gens utilisent évidemment les sites de commerce électronique pour acheter des biens. Cela signifie que chaque client entre ses **informations personnelles** (données de carte de crédit, par exemple) dans le formulaire d'achat et qu'il s'agit d'une **bonne occasion pour les pirates de voler ces données et de les utiliser à leur avantage**.
- Deuxièmement, grâce au grand nombre d'utilisateurs qui interagissent avec ces sites Web, **ils sont devenus une base de choix pour le contenu malveillant, les redirections, les programmes malveillants, le spam et le phishing**. Et le plus gros problème est que les sites Web sont piratés en masse et que ce processus ne prend pas beaucoup de temps: en quelques minutes, les pirates peuvent disposer de centaines de sites.
- En tant que propriétaire de site de commerce électronique, vous devez comprendre que **vous êtes responsable non seulement de la sécurité de votre site Web, mais également de la sécurité de l'argent de vos clients et de leurs informations personnelles**. C'est pourquoi non seulement vous devriez, mais il est **absolument essentiel pour le propriétaire d'un site de commerce électronique de protéger son site Web contre les attaques d'un pirate informatique**.



# Conséquence du piratage

- La **principale préoccupation** de chaque entreprise est **sa réputation**. Les gens devraient vous faire **confiance**, sinon personne n'achètera quoi que ce soit sur votre site Web. Si les utilisateurs voient une **annonce ou une bannière suspecte** sur votre site Web (contenu réservé aux adultes, par exemple), cela éveillera **immédiatement les soupçons**. Si **l'antivirus** ou le navigateur des utilisateurs les **avertit d'un contenu malveillant** sur votre site Web, **ils quitteront** probablement votre site Web et ne reviendront pas.
- Un autre effet de l'attaque d'un pirate informatique devient une **liste noire**. Dès qu'un **moteur de recherche, un antivirus ou un tier rapport votre site Web comme compromis, il apparaît sur une liste noire**, vous allez perdre du trafic rapidement. Il va sans dire que **la suppression du site Web de toutes les listes noires prendra quelques jours**. Et pendant ce temps, votre site Web sera **invisible** pour les utilisateurs. Les listes noires influenceront considérablement votre revenu, alors pourquoi ne pas minimiser les risques à l'avance?



phishing.safebrowsingtest.com Search Google or type URL



### Phishing attack ahead

Attackers on **phishing.safebrowsingtest.com** are trying to steal your information (for example, passwords, messages, etc.).

[Details](#)



### MALICIOUS URL BLOCKED

avast! Network Shield has blocked a harmful site.  
Object: `http://dx8.52z.com/BDDown.exe`  
Infection: URL:Mal  
Process: `C:\Program Files\...iexplore.exe`

[More details... >>](#)

[Report the file as a false positive](#)

This website has been reported as unsafe  
We recommend that you do not continue to this website. It has been reported to Microsoft for containing threats that might reveal personal or financial information.  
[Go to my home page instead](#)



### This website has been reported as unsafe

We recommend that you do not continue to this website. This website has been reported to Microsoft for containing threats that might reveal personal or financial information.

- [Go to the antivirus home page instead](#)
- [Ignore this warning and open this site](#)

Security Warning!



### Chrome Security



### Chrome Security Warning!

Attackers currently on your browser might attempt to install dangerous programmes on your computer that steal or delete your information (for example, photos, passwords, messages and credit cards).

Install The Chrome Browser Security

[Back To Safety](#)



### Reported Attack Page!

This web page at **ekantipur.com** has been reported as an attack page and has been blocked based on your security preferences.

Attack pages try to install programs that steal private information, attack others, or damage your system.

Some attack pages intentionally try to trick you into giving away your information without the knowledge of the person you are talking to.

[Get more information](#)

### Firefox Critical ERROR

A serious try to get an access to your personal logins & bank information. We managed to block this suspicious connection. We will keep your accounts until some measures will be taken. We will protect your personal data.

and password. The site says:  
DESK: +1 (800) 308-2826 (Toll-Free)"

# Conséquence du piratage

- Sans compter tous les autres désagréments :
  - Poursuite civile
  - Pertes financières
  - Accusations
  - Faillite
  - Problème d'assurabilité
  - Etc.

# Quoi faire pour minimiser les risques ?

- Assurez-vous d'avoir :
  - Antivirus à jour sur tous vos systèmes
  - Système de surveillance de vulnérabilité et de détection/protection d'intrusion
  - Journalisation active, SIEM, surveillance des performances et des activités en temps réels
- Éduquez les employés
  - Courriel malveillants et autres mauvaises pratiques – hack par social engineering
- Plateforme sécurisée
  - Ayez recours à un certificat SSL reconnu et offrez un site sécurisé
  - Un parefeu et les ports uniquement nécessaires qui sont ouverts
  - Attention aux hébergements partagés
- Données vulnérables doivent être stockés et sécurisés
- Vérifier les vulnérabilités
  - [SSL Labs](#) ou autres sites du genre
- Mise à jour en tout temps
  - Jusqu'au petit plug-in présent sur votre site

# Mettre à jour votre site Internet

- Pourquoi se mettre à jour ?
  - S'assurer de la sécurité
  - Suivre les évolutions techniques et légales
  - Se tenir à jour sur les habitudes de navigation
  - Optimiser le référencement
  - Intégrer de nouvelles fonctionnalités grâce à la dernière mise à jour du logiciel mis en place
  - Se démarquer de la concurrence
  - Améliorer le référencement et donc la visibilité
  - Rendre le site plus attrayant
  - Augmenter le taux de conversion de votre site Internet

# Qu'est-ce qu'un certificat de sécurité (web)

- Basé sur la technologie **SSL**, qui signifie **Secure Sockets Layer**, ou **TLS** pour **Transport Layer Security** est une technologie qui **permet de chiffrer la transmission de données sur Internet pour empêcher qu'elles ne soient interceptées et décodées**. Ceci est particulièrement important lorsque des **informations sensibles** telles que les numéros de cartes de crédit ou des mots de passe sont saisies sur votre site web, comme cela est souvent le cas pour les sites de commerce électronique ou les sections protégées par mot de passe.
- Les **sites sécurisés par un certificat SSL** affichent un cadenas de sécurité dans le navigateur web et peuvent afficher un sceau de sécurité. Si vous **vendez des articles en ligne**, si vous avez des **sections protégées par mot de passe** sur votre site web, ou si vous **hébergez des formulaires en ligne** demandant des informations personnelles, vous êtes **fortement encouragés à obtenir un certificat SSL**. Non seulement la **sécurité de votre site sera améliorée**, mais vous **augmenterez le niveau de confiance de vos visiteurs**, ce qui se traduit souvent par des taux de conversion et des ventes plus élevés.
- Depuis **janvier 2015**, **Google a commencé à donner priorité aux sites protégés par SSL dans ses résultats de recherche**. Un site sécurisé par SSL/TLS pourrait donc mieux s'afficher dans les résultats de recherche qu'un autre site similaire sans SSL/TLS.

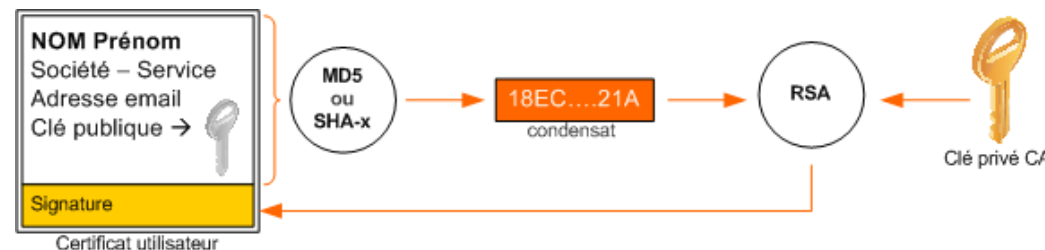
# Qu'est-ce qu'un certificat de sécurité (web)

- Un certificat est un **fichier de données qui lie une clé cryptographique aux informations d'une organisation ou d'un individu**. Installé sur un serveur, le **certificat active le protocole « https » (via le port 443) dans les navigateurs**, afin d'assurer une connexion sécurisée entre le serveur web et le navigateur.
- Généralement, le **SSL/TLS est utilisé pour sécuriser les transactions bancaires, le transfert de données et les informations de connexions**, telles que les noms d'utilisateur et les mots de passe. Le SSL/TLS est devenu la norme pour sécuriser l'utilisation de sites de réseaux sociaux. Les certificats SSL/TLS lient ensemble :
  - Un nom de domaine, un nom de serveur et un nom d'hôte.
  - L'identité de l'organisation (nom d'entreprise) et le lieu.
- **L'organisation doit installer le certificat SSL/TLS sur son serveur web** afin d'initialiser des sessions sécurisées avec les navigateurs.
- **L'organisation doit se soumettre à une vérification auprès de l'Autorité de Certification**, dont le degré va varier selon le type de certificat SSL pour lequel elle a effectué une demande.
- Une fois le certificat délivré et installé sur un site, les visiteurs pourront accéder à celui-ci à travers une connexion « https » qui indique au **serveur qu'il doit établir une connexion sécurisée** avec le navigateur.
- Lorsque la connexion sécurisée est établie, **l'ensemble du trafic entre le serveur et le navigateur sera sécurisé**. Les visiteurs d'un site web sont assurés que celui-ci est sécurisé grâce à différents indicateurs visuels de confiance.



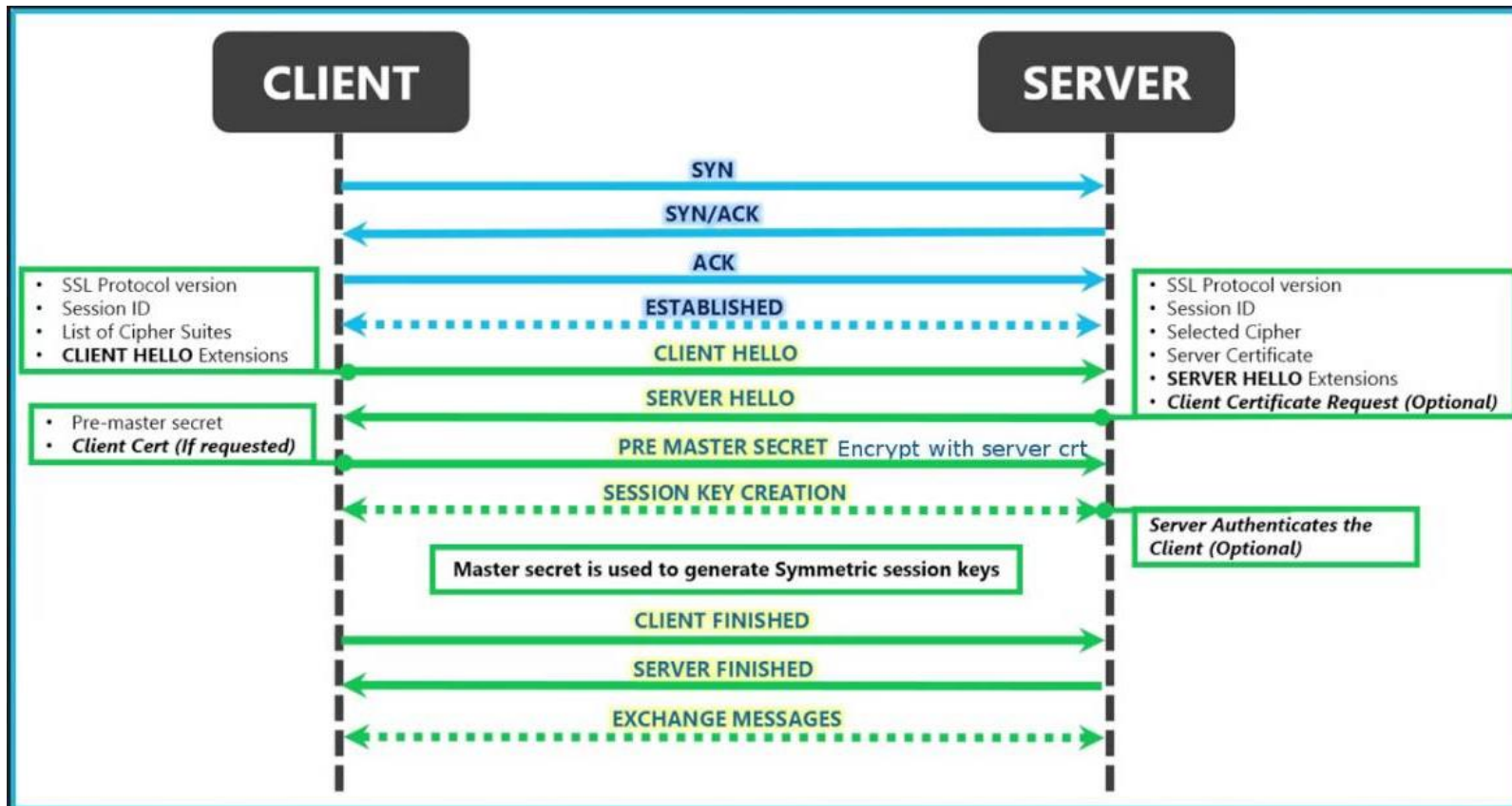
# Qu'est-ce qu'un certificat de sécurité

- Un certificat électronique est un ensemble de données bas sur un chiffrement asymétrique contenant :
  - une clé privé ;
  - des informations d'identification, par exemple : nom, localisation, adresse électronique ;
  - au moins une signature (construite à partir de la clé privée) ; de fait quand il n'y en a qu'une, l'entité signataire est la seule autorité permettant de prêter confiance (ou non) à l'exactitude des informations du certificat.



- Les certificats électroniques et leur cycle de vie doivent être gérés au sein des infrastructures pour assurer le bon fonctionnement des systèmes

# Échange de clé de chiffrement Client / Serveur web



## ClientHello :

1. Le client (le navigateur, par exemple) envoie un message ClientHello au serveur.
2. Ce message contient des informations telles que les versions de TLS prises en charge, les algorithmes de chiffrement préférés, et d'autres paramètres nécessaires pour établir une connexion sécurisée.

## ServerHello :

1. Le serveur répond avec un message ServerHello.
2. Il choisit la version de TLS la plus élevée prise en charge par les deux parties et sélectionne un ensemble commun d'algorithmes de chiffrement.

## Key Exchange :

1. Le serveur envoie son certificat au client. Ce certificat contient la clé publique du serveur.
2. Le client vérifie le certificat, et si tout est en ordre, il extrait la clé publique du certificat.

## ClientKeyExchange :

1. Le client génère une clé de pré-maître secret, l'encrypte avec la clé publique du serveur, puis envoie la clé de pré-maître secret encryptée au serveur.

## ServerKeyExchange (parfois omis) :

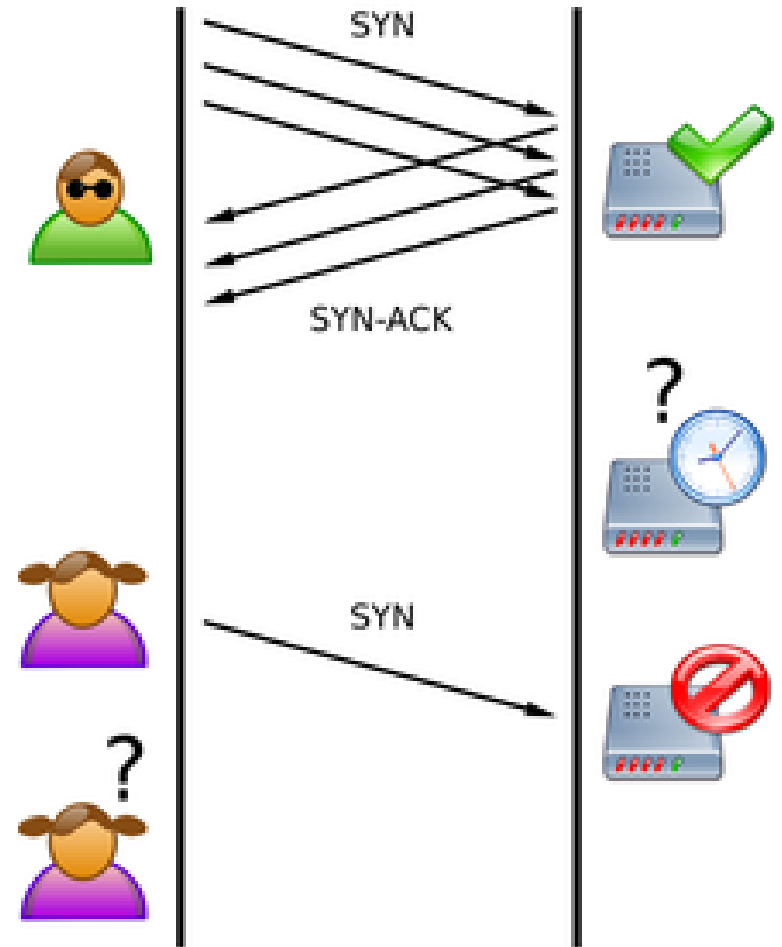
1. Dans certains cas, le serveur peut envoyer un message ServerKeyExchange pour fournir des informations supplémentaires nécessaires à l'échange de clés. Cependant, cela n'est pas toujours nécessaire, surtout si le serveur utilise un certificat signé par une autorité de certification reconnue.

## Finished :

1. Le client envoie un message Finished pour signaler qu'il a terminé l'échange de clés.
2. Le serveur fait de même.

# Pour ceux qui ont besoin du rappel de l'échange SYN-ACK

- L'échange SYN-ACK est une partie du processus de connexion TCP (Transmission Control Protocol) qui se produit lorsqu'un client souhaite établir une connexion avec un serveur, par exemple, lors de la connexion à un site web. Voici comment fonctionne cet échange :
- SYN (Synchronize) :
  - Le processus débute lorsque le client envoie un segment TCP avec le drapeau SYN activé (SYN=1) au serveur. Ce segment contient également un numéro de séquence initial choisi par le client.
- SYN-ACK (Synchronize-Acknowledge) :
  - Le serveur, s'il est prêt à accepter la connexion, répond avec un segment TCP contenant les drapeaux SYN et ACK activés (SYN=1, ACK=1). En plus, le serveur choisit son propre numéro de séquence initial et inclut également le numéro de séquence du client incrémenté de 1.
- ACK (Acknowledge) :
  - Enfin, le client répond avec un segment TCP contenant le drapeau ACK activé (ACK=1). Ce segment confirme la réception du message SYN-ACK du serveur. Le numéro de séquence dans ce segment est également incrémenté de 1 par rapport au numéro de séquence du serveur.



# Quand utiliser un certificat ?

- Pour sécuriser les transactions bancaires en ligne.
- Pour sécuriser les connexions et tout échange d'information confidentielle .
- Pour sécuriser les applications et les messageries web, telles que Outlook Web Access, Exchange et Office Communications Server.
- Pour sécuriser les flux de production et les applications de virtualisation tels que Citrix Delivery Platforms et les plates-formes sur le Cloud.
- Pour sécuriser les connexions entre un client de messagerie, tel que Microsoft Outlook et un serveur mail, tel que Microsoft Exchange.
- Pour sécuriser le transfert de fichiers au travers de services FTP, dans les cas de mise à jour de sites Internet par exemple.
- Pour sécuriser les connexions aux panneaux de contrôle et les activités d'hébergement, telles que Plesk, cPanel, et bien d'autres encore.
- Pour sécuriser les trafics intranet.
- Pour sécuriser les connexions aux réseaux et aux trafics de réseaux utilisant les VPN, RDP, et des applications telles que Citrix Access Gateway.

# Ce que ces applications ont en commun ?

- Les données transmises sur Internet ou sur un réseau doivent rester confidentielles. En d'autres termes, les individus ne veulent pas que leur numéro de carte bancaire, leurs informations de connexion, leurs mots de passe ou tout autre information personnelle soient exposés sur le Web.
- Les données indiquées lors de la transaction (montant, destinataire, etc.) doivent rester inchangées.
- Les organisations doivent s'authentifier auprès de leur clientèle et leurs utilisateurs extranet, et leur garantir leur identité.
- Les organisations doivent se conformer aux réglementations régionales, nationales ou internationales sur la confidentialité, la disponibilité et l'intégrité des données.

# Types de certificat

- **Certificat SSL de base**

- Limité souvent à la validation du droit de propriété du domaine (Domain Validation) ou de l'organisation (Organisation Validation).
- Certificat abordable, qui offre un cryptage SHA256 pour un seul domaine. C'est le certificat le plus populaire et il est recommandé pour les sites qui génèrent un faible chiffre d'affaires annuellement.

- **Wildcard SSL**

- Il fournit le même cryptage sur un nombre illimité de sous-domaines. C'est une bonne solution pour les sites multilingues / multi-sujet ou tout autre site utilisant plusieurs sous-domaines.

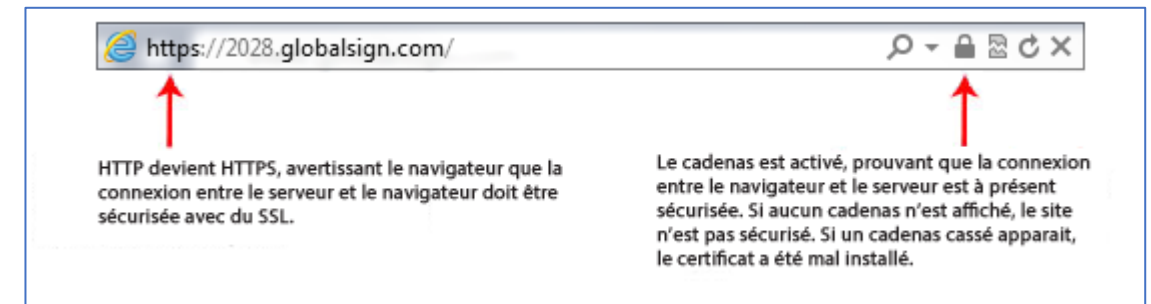
- **Certificat SSL de validation étendue (EV)**

- Validation complète de l'existence juridique et physique de l'organisation.
- Vérification de l'exclusivité de l'utilisation du domaine.
- C'est le certificat le plus avancé donnant ainsi à vos visiteurs un niveau supplémentaire d'assurance. Le certificat EV comprend également un sceau dynamique, qui affiche le nom et l'adresse de votre entreprise, ainsi que la période de validité du certificat. Si la confiance des clients est cruciale pour votre site, les certificats EV vous sont recommandés.

# Standard ou à validation étendue

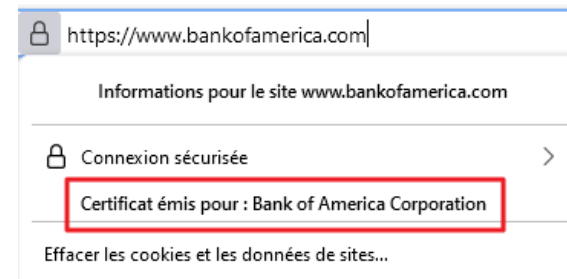


Certificat à validation étendue (EV)



Certificat SSL Standard

Plus maintenant!!





# DV, OV ou EV

## DOMAIN VALIDATED

Domain Validated (DV) certificates are the least-identity-validated SSL certificates and can be obtained quickly and easily—even by a malicious bot. These certificates are low-cost certificates that only require validation that a company or person can demonstrate control over a web domain for which they want to secure a certificate.

To obtain a DV certificate, a website owner only verifies domain ownership via an email to the [WHOIS record](#). When you look beyond the lock of a DV certificate you will not see any organization details. DV certificates are the minimum viable product for encrypting websites.

Types of websites that use DV certificates:

- Blogs
- Personal websites
- Any website that doesn't conduct transactions or gather personal information

WHOIS : <https://whois.arin.net/ui/>

## ORGANIZATION VALIDATED

Organization Validated (OV) certificates are authenticated with nine validation checks and are considered a mid-level business certificate. With OV certificates, CAs authenticate domain ownership similar to DV certificates. But when you look beyond the lock of an OV certificate you will find more details about the company that owns the website.

What distinguishes OV from DV is the steps taken by CAs to authenticate that the business organization (ie. Inc., Corp, LLC, Ltd, Pty Ltd, etc.) affiliated with the certificate is valid and remains in good standing.

Best used on these websites and pages:

- Log-in screens
- Business sites

## EXTENDED VALIDATION (EV)

Extended Validation (EV) certificates provide the highest level of brand identity security and are authenticated with 16 validation checks. When you look beyond the lock of an EV certificate you will immediately find details about the company or parent company that owns the website.

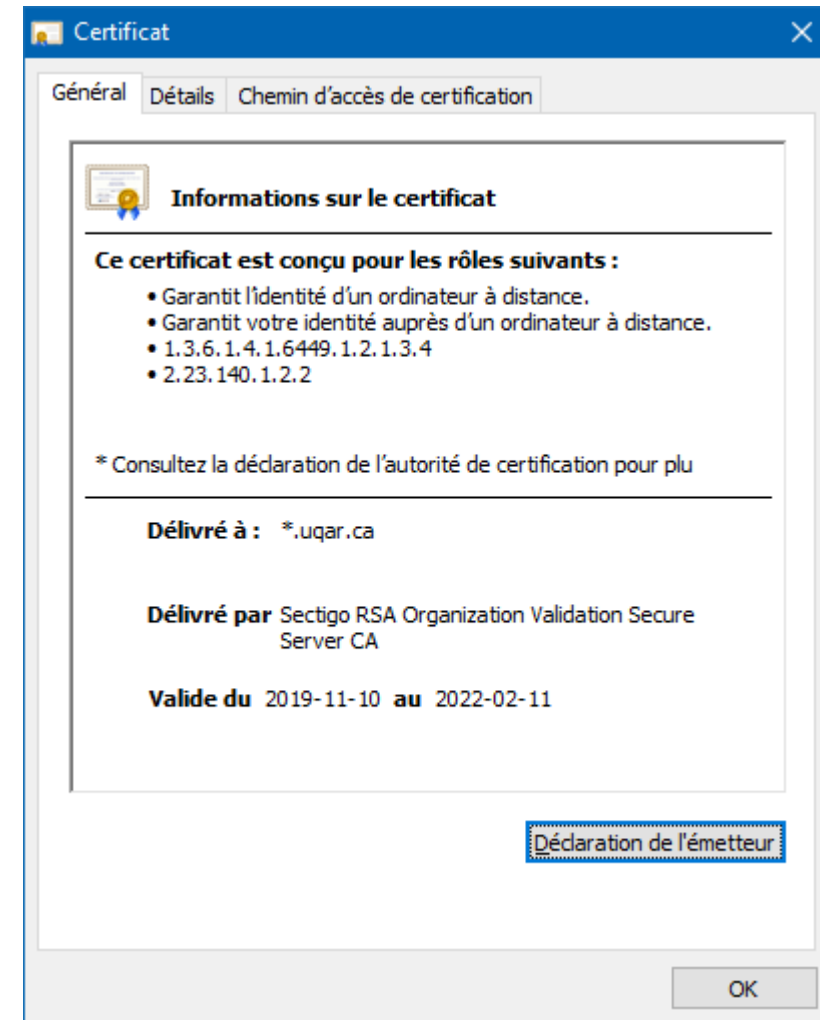
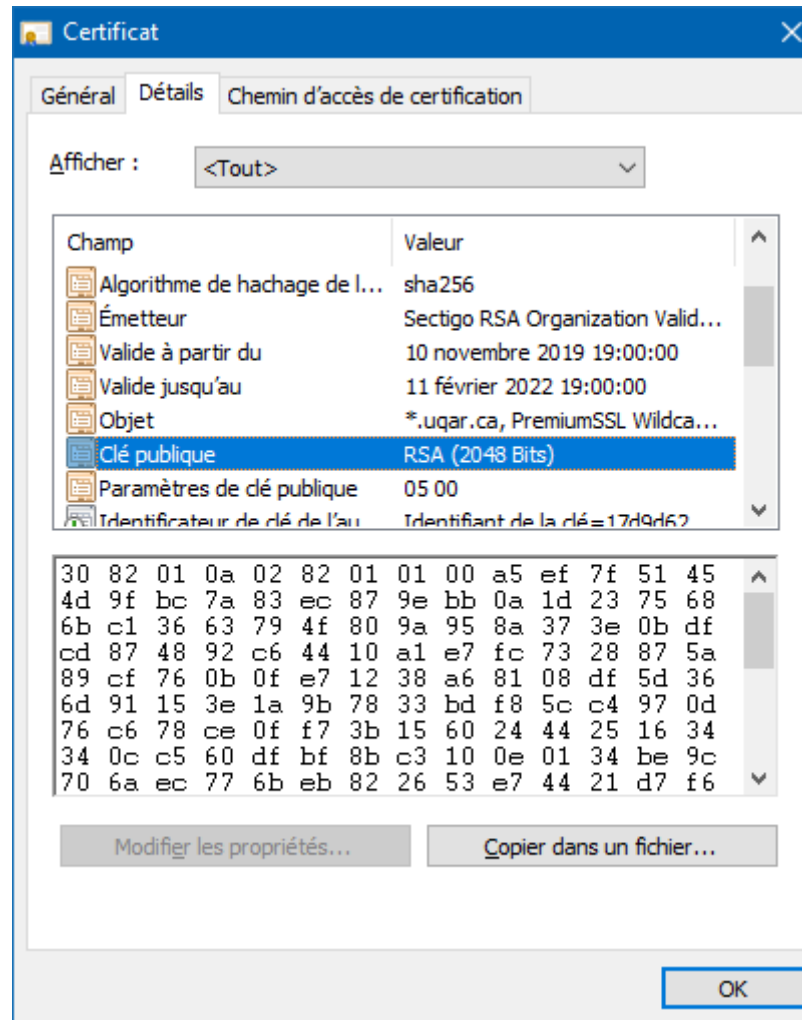
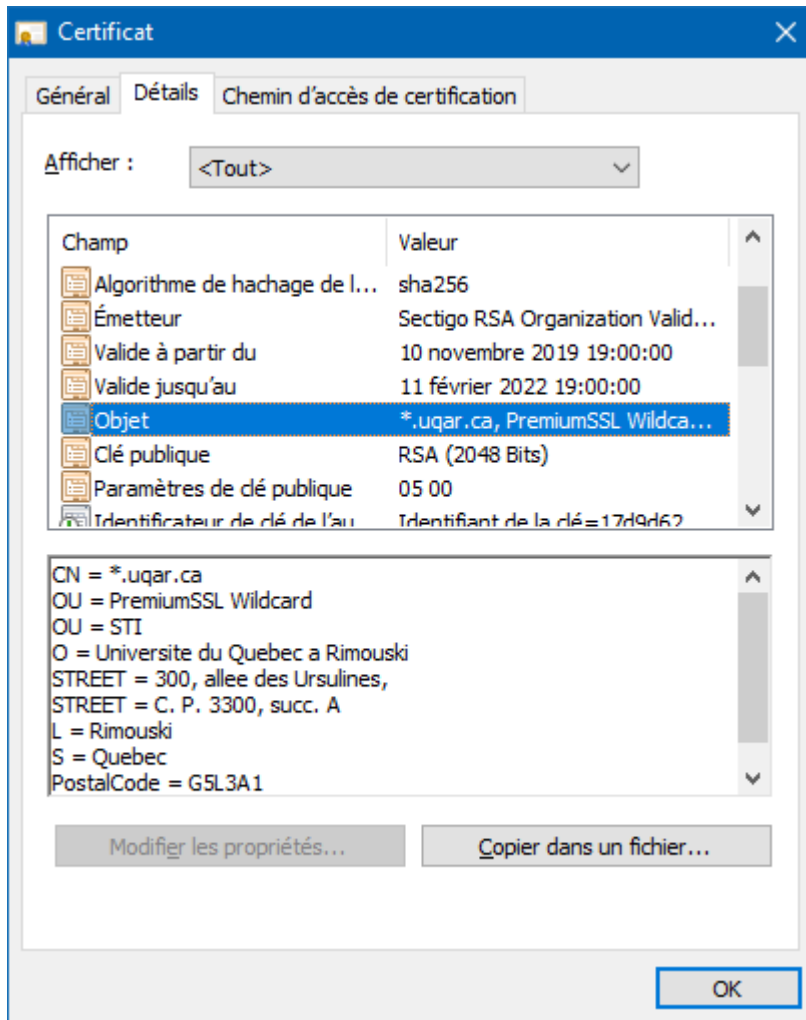
In addition to all of the authentication steps CAs take for DV and OV certificates, EV certificates require vetting of the business organization's operational existence, physical address and a telephone call to verify the employment status of the requestor.

Best used on these websites and pages:

- Global banks and financial services
- Fortune 500 companies
- Global 2000 companies
- E-commerce
- Enterprises






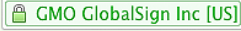



The DigiCert Validation team rejects approximately 3,750 EV certificates every year in some part due to fraudulent requests.









# Certificat pour UQAR.CA



# Les certificats SSL

- Le prix peut sembler élevé, mais il est préférable de commencer son site avec un certificat sécurisé plutôt que de le modifier par la suite. De plus, des options gratuites sont offertes. Dans le doute, il s'agit d'une bonne option.
- Un certificat SSL gratuit par rapport à un payant est une question de confiance et cela dépend du profil des visiteurs. Si c'est pour la gestion d'un site Web personnel ou un site Web de petite ou moyenne entreprise qui ne comporte pas de commerce électronique, vous pouvez faire confiance à un certificat gratuit.
- Une banque ou un important site de commerce électronique devrait utiliser un certificat Extended Validation.
- Il est toujours possible que votre site Web recueille des renseignements personnels, que ce soit une adresse de courriel ou des comptes de médias sociaux.
- Un certificat SSL concerne autant la confiance que la sécurité. Si un utilisateur voit dans son navigateur que votre site n'est pas « sécurisé », il y aura des incidences sur les consultations de pages et le trafic.
- Le chiffrement SSL devient rapidement la norme anticipée, et les modifications apportées par Google dans le navigateur Chrome illustrent cette situation. Le passage à un site Web sécurisé vous offre une position favorable pour l'avenir, lorsque le chiffrement pourrait être exigé par les navigateurs Web ou d'autres modifications technologiques.

	DomainSSL	OrganizationSSL	ExtendedSSL
Niveau de confiance			
Le navigateur montre	Cadenas 	Cadenas 	Barre d'adresse verte 
Sceau de site sécurisé cliquable			
Information affichée dans le certificat	Nom de domaine vérifié	Nom de domaine vérifié Nom de l'entreprise	Nom de domaine vérifié Nom de l'entreprise Adresse de l'entreprise
Vitesse d'émission	5 minutes ou moins	1 - 2 jours ouvrés	3 - 4 jours ouvrés
Conditions de vérification	Droit d'utiliser le domaine	Droit d'utiliser le domaine et vérification complète de l'entreprise	Droit d'utiliser le domaine et vérification étendue de l'entreprise, y compris confirmation de son existence légale, physique et opérationnelle
Période de validité	1 - 2 ans	1 - 2 ans	1 - 2 ans
Garantie	10 000 \$	1,25 million \$	1,5 million \$

Options			
Wildcard	 Sous-domaines illimités	 Sous-domaines illimités	—
Option multi-domaine (SANs)	 Jusqu'à 100 sous-domaines	 Jusqu'à 100 sous-domaines, domaines de 1er niveau ou adresses IP publiques	 Jusqu'à 100 sous-domaines ou domaines de 1er niveau
Prix	Changer la devise (\$ USD) ▼		
1 an	\$249	\$349	\$599
2 ans	\$448	\$628	\$939
Réductions	 Réductions pluriannuelles	 Réductions pluriannuelles et sur volume	 Réductions pluriannuelles et sur volume

# Les certificats SSL

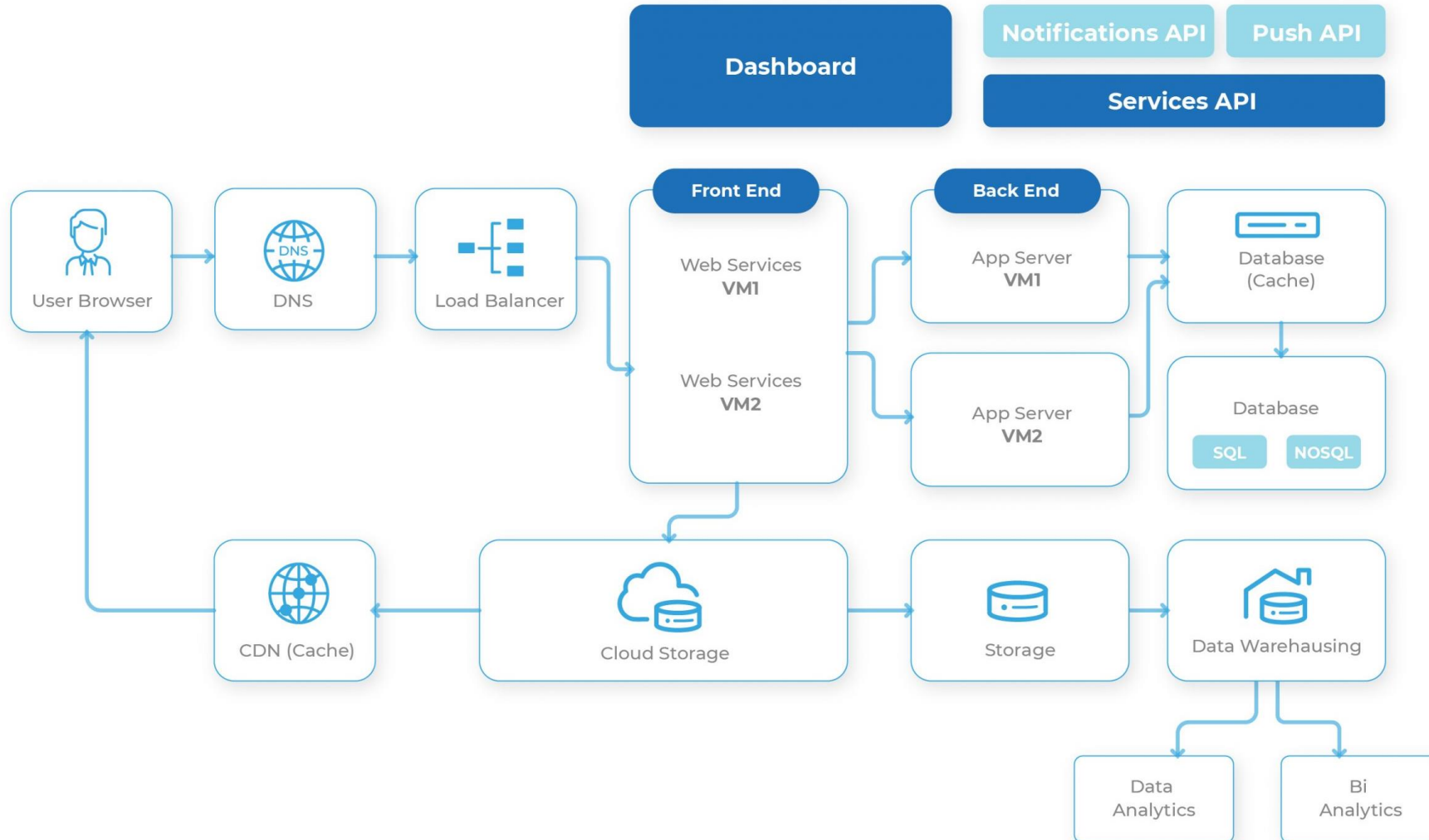
- Les certificats SSL expirent après une période spécifique et devraient être suivis et renouvelés au besoin. La période de renouvellement peut être de quelques jours ou jusqu'à deux ans. Cette limite de deux ans est une nouvelle règle; les certificats émis avant le 1er mars 2018 pourraient avoir des périodes de validité plus longues.
- Certaines intégrations plus avancées comme LetsEncrypt demandent un renouvellement tous les 30-90 jours, mais comprennent la possibilité de renouveler ces certificats automatiquement.
- Les certificats SSL doivent être émis depuis le certificat racine d'une Autorité de Certification de confiance avec une clé publique de 2048 bits. Pour que le certificat SSL soit considéré fiable, le certificat racine doit être présent sur la machine de l'utilisateur final. Si le certificat n'est pas reconnu, le navigateur affichera des messages d'alerte indiquant qu'il ne faut pas lui faire confiance. Sur les sites de e-commerce, de tels messages d'alerte inquiètent les visiteurs. La réputation des organisations et leur base de clients potentiels en sont directement affectées.

# Let's Encrypt – Certificat Gratuit!

- Let's Encrypt est une autorité de certification (AC ou CA pour Certificate Authority en anglais) gratuite, automatisée et ouverte, exploitée pour le bénéfice du public. C'est un service fourni par Internet Security Research Group (ISRG).
- Ils donnent aux gens les certificats numériques dont ils ont besoin pour activer HTTPS (SSL/TLS) pour les sites Web, gratuitement, de la manière la plus intuitive possible. L'objectif est de créer un Web plus sûr et respectueux de la vie privée.
- Les principes clés de Let's Encrypt sont les suivants :
  - **Gratuit** : Toute personne possédant un nom de domaine peut utiliser Let's Encrypt pour obtenir un certificat reconnu, à coût nul.
  - **Automatique** : Un logiciel s'exécutant sur un serveur Web peut interagir avec Let's Encrypt pour obtenir sans difficulté un certificat, le configurer de manière sécurisée pour l'utilisation et prendre automatiquement en charge le renouvellement.
  - **Sécurisé** : Let's Encrypt servira de plate-forme pour faire progresser les meilleures pratiques de sécurité TLS, tant du côté de l'autorité de certification que pour aider les responsables de site Web à sécuriser correctement leurs serveurs.
  - **Transparent** : Tous les certificats délivrés ou révoqués seront enregistrés publiquement et disponibles pour inspection par quiconque.
  - **Ouvert** : Le protocole d'émission et de renouvellement automatique sera publié en tant que norme ouverte que d'autres peuvent adopter.
  - **Coopératif** : Tout comme les protocoles Internet sous-jacents eux-mêmes, Let's Encrypt est un effort conjoint au profit de la communauté, au-delà du contrôle d'un organisme en particulier.

<https://letsencrypt.org/fr/how-it-works/>

# Architecture d'un site de commerce électronique





# Un site de commerce électronique

- Dans le commerce, l'expérience des utilisateurs des services fournis est ce qui fait le profit. Le commerce en ligne consiste à mieux servir, servir facilement et gagner la confiance nécessaire pour fidéliser les clients. Pour garder votre longueur d'avance sur les autres, les propriétaires d'entreprise en ligne adoptent les dernières technologies pour apparaître sous leur meilleur jour devant les clients.
- Étant donné que les clients du commerce électronique ne voient que le site Web ou les applications mobiles qu'ils utilisent pour prendre leur décision d'achat, le combat est là. Tout le monde veut rendre son site Web ou son application mobile lucratif, facile à naviguer et opérationnel en quelques secondes lorsque les clients le souhaitent.
- Puisqu'il est temps de passer au mobile, les sites Web doivent être de plus en plus fonctionnels et « responsive ». Par conséquent, le développement Web de commerce électronique revêt une importance particulière pour les entreprises développant le logiciel de commerce électronique et les propriétaires du commerce en ligne.

# Un site de commerce électronique

- Les achats en ligne représentent une part importante des ventes au détail de nos jours et la mise en ligne des produits à la disposition du monde entier est l'un des moyens les plus rapides de bâtir une entreprise, une marque et des revenus.
- Il existe une multitude de plates-formes disponibles pour répondre à vos besoins spécifiques aussi bien du côté client que du côté serveur.
- Par conséquent, le développement Web de commerce électronique a deux visages: l'un est l'interface client (Front End) et l'autre est l'arrière boutique (Back end).
- Dans tout processus de développement de site Web de commerce électronique, les entreprises de conception de sites Web de commerce électronique suivent un certain standard en termes de technologies afin de mettre en valeur leurs listes de fonctionnalités qui fonctionnent parfaitement chez l'utilisateur.

# Front-End

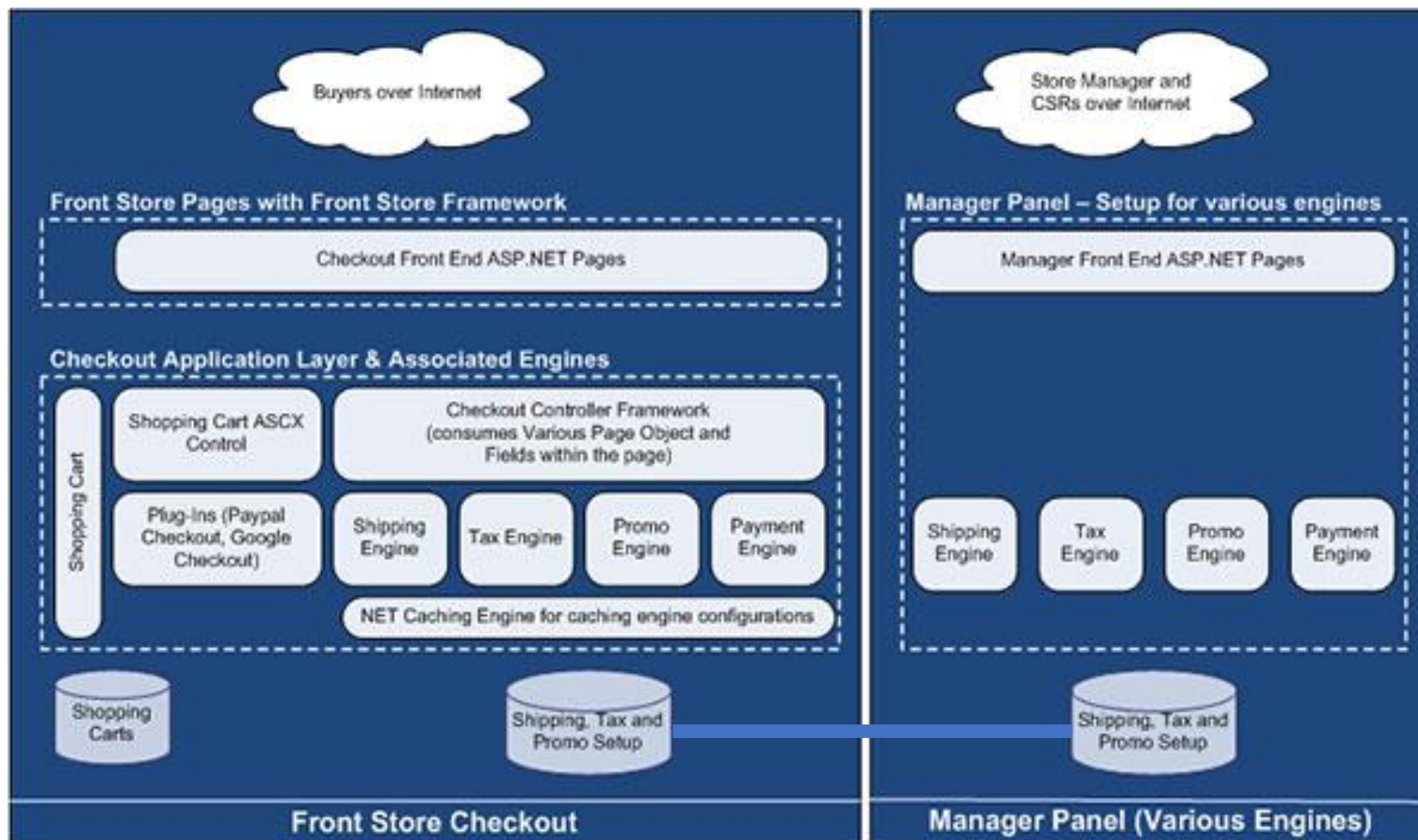
- Le terme « frontend » désigne les éléments d'un site que l'on voit à l'écran et avec lesquels on peut interagir depuis un navigateur. En effet, tout ce qu'on voit sur un site internet par exemple, est une combinaison de HTML, CSS et JavaScript. Ces langages de programmation utilisés par le développeur Front End sont interprétés par le navigateur de votre ordinateur pour afficher un résultat « visuel ». Il s'agit notamment de polices, de menus déroulants, de boutons, de transitions, de curseurs, de formulaires de contact, etc.
- Le Frontend se compose généralement :
  - D'un design créé par un designer
    - Ils peuvent provenir de maquettes graphiques via des outils de création comme Photoshop ou Fireworks
    - Ou d'un designer graphique
  - De code HTML, CSS, JavaScript et jQuery mis en place par un développeur Frontend.

**Le Front-End nécessite .... Un Back-end**

# Back-End

- Le « backend » est un peu comme la partie immergée d'un iceberg. On ne la voit pas en tant que simple Internaute mais elle représente une très grande partie d'un projet web.
- Le Backend se compose généralement de trois éléments :
  - Un serveur (hébergement web)
  - Une application (site web, administration)
  - Une base de données (sorte de feuille de calcul pour organiser les données)
- Prenons un exemple pour comprendre le fonctionnement du Back End : Imaginons que vous deviez réserver un vol en ligne pour vos futures vacances. Vous vous rendez sur le site de la compagnie aérienne et recherchez le vol qui vous convient. Une fois le vol sélectionné, vous renseignez vos informations personnelles et validez votre réservation. Vos informations sont alors enregistrées dans une base de données stockée sur un serveur.
- Toutes ces informations restent sur le serveur, alors quand vient l'heure des vacances (2 mois plus tard) vous vous connectez à l'espace client (application) pour imprimer vos billets d'avion et toutes les informations que vous aviez renseignées lors de votre réservation sont disponibles sur votre compte.
- La personne qui administre toute cette technologie est le développeur back end. Les technologies Backend se composent généralement de langages comme PHP, Ruby, Python, etc. Pour les rendre encore plus faciles à utiliser, ils sont généralement améliorés par des Framework comme Ruby on Rails, Cake PHP, Symfony et Code Igniter qui rendent le développement plus rapide et plus sécurisé.
- De plus en plus de développeurs disposent à la fois de compétences en backend et en frontend. On les appelle développeurs Full Stack.

# Exemple d'un E-Commerce Back/Front End



# E-Commerce avec un PGI

