MINISTÈRE
DE L'INTÉRIEUR

Liberté
Égalité
Fraternité

CONCOURS EXTERNE ET INTERNE DE TECHNICIEN DE CLASSE NORMALE DES SYSTEMES D'INFORMATION ET DE COMMUNICATION

- SESSION 2021 -

Vendredi 9 avril 2021

Option «Solutions logicielles et systèmes d'information»

Traitement de questions et résolution de cas pratiques, à partir d'un dossier, portant sur l'une des deux options suivantes choisies par le candidat le jour de l'épreuve :

- infrastructures et réseaux,
- solutions logicielles et systèmes d'information.

Cette épreuve permet d'évaluer le niveau de connaissances du candidat, sa capacité à les ordonner pour proposer des solutions techniques pertinentes et à les argumenter.

Le dossier ne peut excéder 20 pages.

(Durée: 3 heures – Coefficient 2)

L'usage de la calculatrice est interdit

Le dossier documentaire comporte 20 pages. (hors page d'énoncé du sujet).

Il vous est rappelé que votre identité ne doit figurer que dans l'en-tête de la copie (ou des copies) mise(s) à votre disposition. Toute mention d'identité ou tout signe distinctif porté sur toute autre partie de la copie ou des copies que vous remettez en fin d'épreuve entraînera l'annulation de votre épreuve.

Si la rédaction de votre devoir impose de mentionner des noms de personnes ou de villes et si ces noms ne sont pas précisés dans le sujet à traiter, vous utiliserez des lettres pour désigner ces personnes ou ces villes (A …, B…, Y…, Z…).

IMPORTANT

1. LES COPIES SERONT RENDUES EN L'ÉTAT AU SERVICE ORGANISATEUR. A L'ISSUE DE L'ÉPREUVE, CELUI-CI PROCÉDERA À L'ANONYMISATION DE LA COPIE.
2. NE PAS UTILISER DE CORRECTEUR D'ORTHOGRAPHE SUR LES COPIES.
3. ECRIRE EN NOIR OU EN BLEU – PAS D'AUTRE COULEUR.
4. IL EST RAPPELÉ AUX CANDIDATS QU'AUCUN SIGNE DISTINCTIF NE DOIT APPARAÎTRE SUR LA COPIE.

QUESTIONS SLSI (10 points)

1) Que signifie UEFI ?

- Donner sa définition.
- Quel est son usage ?

2) Que signifie CMBD ?

- Donner sa définition.
- Que permet-elle de faire ?

3) Au niveau de la couche application, quel protocole permet d'expédier des courriels sur Internet ?

4) Citer les couches du modèle OSI.

5) A quoi sert le protocole SNMP ?

6) Qu'est-ce que l'open data ?

- Donner sa définition.
- Sur quel site institutionnel peut-on trouver ces données ?

7/ En sécurité des systèmes d'information, à quoi correspond l'acronyme DICT ?

8/ Dans un système d'infrastructure de gestion de clés asymétriques (IGC) :

- Avec quelle clé Pierre **signe-t-il** un fichier qu'il souhaite transmettre à Sophie ?
- Avec quelle clé Pierre **chiffre-t-il** un fichier confidentiel destiné à Sophie ?

9/ Qu'est une puce TPM ?

- Donner sa définition ?
- Citer au moins deux avantages de cette technologie.

10/ Qu'est-ce qu'un rançongiciel ?

ETUDES DE CAS SLSI

Cas 1: Mise en place d'une GED (5 points)

Dans le cadre de la mise en place du Secrétariat Général Commun Départemental (SGCD), service interministériel, le secrétaire général de la préfecture souhaite revoir l'organisation documentaire des services. Le contexte actuel laisse apparaître, entre autres, l'absence de traçabilité des courriers, des difficultés de conservation des documents et un volume d'archives en constante augmentation.
Dans cet objectif, votre chef de bureau vous demande de participer à la réflexion sur la mise en place d'une solution technique de gestion électronique de documents (GED) qui permettra le partage de documents et leur modification en ligne de manière optimisée.
Pour des raisons de confidentialité, l'accès aux différents documents devra être restreint aux seules personnes habilitées selon des droits attribués par les propriétaires des documents.

1) Définissez ce qu'est un système de GED et citez ses principaux composants.

2) Ce projet nécessite également de choisir le type d'infrastructure sur laquelle sera hébergée la solution.

- Citez les différents types d'hébergements que vous connaissez.

- Parmi ceux-ci, quelle solution préconisez-vous pour y installer la plateforme ? Pour quelles raisons ?

3) La note de cadrage de ce projet précise que les accès à la GED se feront au travers du portail Métiers du SGCD, que les personnels devront pouvoir se connecter de leur bureau et l'architecture mise en place devra également permettre le travail en nomadisme de façon sécurisée.

- Décrivez brièvement quelle serait, selon vous, une proposition d'implémentation pour cette infrastructure permettant les accès en mobilité et une authentification centralisée.

- Vous préciserez votre choix par un schéma simplifié d'architecture présentant les différents équipements ou environnements décrits.

4) Selon vous, quelles difficultés rencontrées au cours de ce projet ne permettraient pas de répondre aux critères du « triangle d'or » (coût, qualité, délai) ?

Cas 2 : Refonte d'un site web intranet (5 points)

Vous êtes technicien SIC affecté à la direction du numérique (DNUM) du ministère de l'Intérieur. Votre chef de section vous confie, dans le cadre d'un projet en cours, la refonte technique du site web intranet de la Direction générale des collectivités locales (DGCL). Le système de gestion de contenu (CMS) du site actuel n'est plus soutenu par l'éditeur et n'est plus conforme au cadre de cohérence technique (CCT) du ministère. Les utilisateurs se plaignent également de son ergonomie. Par ailleurs, la sécurité existante n'est pas satisfaisante au regard des données accessibles.

1) Afin d'être conforme au socle technique du ministère de l'Intérieur :

- Quel CMS proposez-vous pour remplacer celui qui est désormais obsolète ? Justifiez votre choix.
- Citez les principales fonctionnalités d'un CMS.

2) Dans le cadre du référentiel général d'amélioration de l'accessibilité (RGAA), veuillez recopier le texte en italique ci-dessous en y insérant les balises facilitant l'accès aux déficients visuels. **Les images sont identifiées en gras.**

Titre 1
Lorem ipsum dolor sit amet,.....

Titre 2
Aliquam pulvinar nulla varius nisl placerat.....

Titre 3
Donec est diam, lobortis at hendrerit in, vulputate eu mauris.....

Titre 4
Morbi sollicitudin ut sapien ac aliquam. Vivamus tempor urna non laoreet aliquet. Morbi sollicitudin sagittis libero porta auctor. Morbi viverra est nisl, vulputate faucibus augue suscipit sit amet. ***<img src="Minstère de l'interieur.png">****. Sed pellentesque condimentum pulvinar...*

Cette image n'est pas importante et l'image ne comporte pas de renseignement
<img src="accueil.png">

3) Afin de sécuriser ce site, il vous est demandé de mettre en place un flux HTTPS.

- Expliquez ce qu'est le protocole HTTPS et son fonctionnement.
- Comment faites-vous pour demander un certificat SSL ? Que vous faut-il générer pour l'obtenir ? A qui vous adressez-vous ?
- Que garantit d'un point de vue de la sécurité des systèmes d'information le protocole HTTPS ?

Dossier documentaire :

Alfresco Gestion électronique de documents

PRESENTATION DU SERVICE

DESCRIPTION :

L'offre de service proposée par la DSIC pour la gestion électronique de documents (GED) s'appuie sur le progiciel libre ALFRESCO COMMUNITY. Des développements spécifiques effectués pour le ministère de l'intérieur (MI) enrichissent cette solution pour constituer l'Offre Collaborative du Ministère de l'intérieur (OCMI).
OCMI intègre le partage et la diffusion (wiki, blog, forum, FAQ, calendrier), un espace documentaire permettant le traitement des documents ainsi que le stockage et le classement pour consultation.

PRESTATIONS :

- Accompagnement à la mise en place d'une solution de gestion collaborative
- Installation et paramétrage de l'instance de gestion collaborative
- Hébergement et exploitation des instances de gestion collaborative
- Maintien en condition opérationnelle
- Support technique
- Base de connaissances

UTILISATEURS POTENTIELS

Cette offre est destinée aux services en préfectures et sous-préfectures, aux directions départementales interministérielles et aux autres entités dépendantes, aux SGAMI et à l'administration centrale.

NB : les documents classifiés diffusion restreinte et au-delà sont éligibles s'ils sont chiffrés (sous ACID ou PRIM'X).

CHIFFRES CLES

FINANCEMENT :

Chaque service demandeur supporte les coûts de mise en œuvre, de maintien en condition opérationnelle et de formation/accompagnement spécifique.

COUT :

- Formation des gestionnaires et des utilisateurs finaux : pris en charge par le client (1 jour pour un gestionnaire, 2 heures pour un utilisateur)
- Création d'un site : nul (seule la validation de l'administrateur d'instance du service demandeur est nécessaire)
- Investissement : 13 k€ pour une instance (une instance est prévue pour 6 000 utilisateurs dont 500 concurrents)
- Fonctionnement : 1,3 k€ / an

DELAIS :

Prise en compte de la demande	Réalisation
8 jours ouvrés	15 jours pour un site, 3 mois pour une nouvelle instance (Si nécessaire, une AMOA peut être apportée dans le cadre de l'offre dédiée)

COMMENT COMMANDER

DEMARCHES :

La demande doit être validée par le Responsable du système d'information métier et de modernisation (RSIMM) de la direction métier concernée. Celui-ci la transmet, sous forme de note d'opportunité (téléchargeable directement sur l'intranet DSIC, dans le domaine d'activité concerné du catalogue de services), au responsable de portefeuille métier (RPM) en charge de la relation client à la DSIC.

CONTACTS :

Pour tout renseignement complémentaire, les RPM peuvent être contactés par e-mail à l'adresse suivante : catalogue-dsic@interieur.gouv.fr

Gestion de documents

Exploitez pleinement le potentiel de vos contenus

Lorsque les documents sont stockés à différents emplacements (sur papier, ordinateurs portables, clés USB, e-mails, réseaux et sites de partage de fichiers), la gestion du contenu s'apparente à un véritable chaos. Ces silos de contenu freinent considérablement la productivité et augmentent les risques liés à la sécurité.
Le logiciel de gestion de documents d'Alfresco vous permet de contrôler les contenus de l'entreprise sur la base d'une gouvernance de l'information transparente et d'une conformité GDPR garantie, avec à la clé des avantages immédiats et tangibles

Logiciel de gestion de documents : fonctionnalités

Tirez des données exploitables de vos contenus – de la numérisation de documents statiques permettant d'exploiter les informations pertinentes pour votre activité, à l'analyse basée sur l'IA et l'apprentissage automatique dans AWS pour extraire des renseignements précieux. Grâce à des options de déploiement flexibles (dans le cloud, sur site, hybride), gérez vos documents comme vous l'entendez.

Fonctionnalités puissantes de recherche

Avec Alfresco, vous trouvez rapidement le document recherché dans votre système de gestion parmi des milliers, voire des centaines de milliers de fichiers.

- Des fonctions de recherche puissantes, intégrant notamment des suggestions de recherche et des filtres simples, permettent de retrouver rapidement le contenu pertinent.
- Les smart folders (dossiers intelligents) facilitent le regroupement et l'accès aux fichiers en fonction de leur « nature » plutôt que de leur emplacement.
- L'accès au contenu sur les appareils mobiles et l'intégration aux applications de productivité permettent aux utilisateurs de travailler partout et à tout moment, avec les interfaces et appareils qui leur sont familiers.
- Alfresco Federation Services offre un moyen simple de rechercher et gérer du contenu dans plus de 60 applications métiers et systèmes de gestion de contenu parmi les plus courants (par exemple, Documentum, OpenText et IBM FileNet)

Intégration du contenu aux processus

Maximisez la valeur de vos contenus grâce à des fonctionnalités puissantes de gestion des documents et de workflow, et profitez de possibilités infinies d'optimiser et d'accélérer le flux des informations numériques. Les données sont transmises à la bonne personne, au bon moment – dans les applications et sur les appareils avec lesquels elle travaille habituellement.

- Des propriétés ou modèles de métadonnées enrichies peuvent être utilisés pour déplacer automatiquement les documents vers la prochaine étape du business process ou du système de gestion de cycle de vie.
- Les workflows intégrés simplifient la révision et l'approbation des documents ; les définitions de processus personnalisés rationalisent les activités documentaires.
- Les règles de dossiers déclenchent des actions automatiques pour les tâches répétitives et permettent de se concentrer sur des aspects plus cruciaux.

Sécurité des contenus sensibles

Des dispositifs de sécurité adaptés à l'entreprise et des fonctionnalités d'archivage électronique intégrées protègent le contenu sensible tout au long de son cycle de vie.

- Des permissions avec différents niveaux d'accès pour les bibliothèques de fichiers, dossiers et fichiers permettent de déterminer qui peut consulter, modifier et supprimer tel ou tel fichier
- Le contrôle de version, notamment la fonction permettant de rétablir une version précédente, simplifie le suivi et protège l'intégrité des fichiers.
- La fonction simple d'archivage électronique automatisé renforce la conformité aux politiques de gouvernance de l'information tout au long du cycle de vie des documents.
- Alfresco in the cloud assure la sécurité et la conformité des appareils de vos utilisateurs finaux toute en préservant la simplicité d'usage et d'accès dont ces derniers ont besoin.

Single Sign-On open-source avec CAS (Central Authentication Service)

Vincent Mathieu
Université de Nancy 2
vincent.mathieu@univ-nancy2.fr

Pascal Aubry
IFSIC - Université de Rennes 1
pascal.aubry@univ-rennes1.fr

Julien Marchal
Université de Nancy 2
julien.marchal@univ-nancy2.fr

Date : 12 Octobre 2003

Résumé

L'universalité du protocole HTTP a depuis longtemps séduit les développeurs ; les applications portées sur le web sont de plus en plus nombreuses.
La mise en place d'annuaires (LDAP par exemple) a épargné la tête des utilisateurs en ne leur faisant mémoriser qu'un seul mot de passe, mais leurs doigts sont encore durement sollicités car ils doivent s'authentifier chaque fois qu'il accèdent une application.
Plusieurs solutions de Single Sign-On (authentification unique et unifiée) sont d'ores et déjà disponibles dans le commerce. Cet article décrit une solution libre, simple, riche et sûre : CAS (Central Authentication Service), développée par l'Université de Yale, et adoptée par le projet ESUP-Portail.

Mots clefs

Single Sign-On, open-source, web, sécurité, authentification.

1 Pourquoi le Single Sign-On ?

Les services numériques accessibles par le *web* (*intranet*, courrier électronique, forums, agendas, applications spécifiques) à disposition des étudiants, enseignants, personnels administratifs se sont multipliés en quelques années. Ces services nécessitent très souvent une authentification.

L'utilisation de techniques de synchronisation entre domaines d'authentification hétérogènes, puis de serveurs LDAP a permis la mise en oeuvre d'un compte unique (*login* / mot de passe) pour chaque utilisateur, ce qui est un progrès. Se posent maintenant les problèmes suivants :

- **authentifications multiples** : il est nécessaire d'entrer son *login*/mot de passe lors de l'accès à chaque application.
- **sécurité** : le compte étant unique, le vol de celui-ci entraîne un risque très important. La sécurisation de l'authentification devient donc primordiale. Il est également fortement souhaitable que les applications n'aient pas connaissance du mot de passe.
- **différents mécanismes d'authentification** : certains utilisateurs disposent de certificats X509 [1][2], qui pourraient servir à l'authentification. En outre, il n'est pas exclu que l'utilisation de LDAP à cette fin ne soit pas remplacée à terme par autre chose, et que certaines politiques d'établissement exigent l'utilisation de bases de données additionnelles. Il semble donc intéressant de disposer d'un service d'abstraction par rapport au(x) mécanisme(s) d'authentification local(aux).
- **aspects multi-établissements** : le compte d'un utilisateur est unique à l'intérieur de l'établissement ; il serait souhaitable que l'accès à des ressources informatiques d'un autre établissement puisse se faire à l'aide du même compte.
- **autorisations** : il est nécessaire pour certaines applications de pouvoir disposer d'informations définissant les rôles des utilisateurs.

Les mécanismes de **SSO** (**S**ingle **S**ign-**O**n : authentification unique, et une seule fois) [3] tentent de répondre à ces problématiques, en utilisant tous des techniques assez semblables, à savoir :

- une **centralisation de l'authentification** sur un serveur qui est le seul à recueillir les mots de passe des utilisateurs, à travers un canal chiffré ;
- des **redirections HTTP** transparentes du navigateur client, depuis les applications vers le serveur d'authentification, puis du serveur vers les applications.
- le **passage d'informations entre le serveur d'authentification et les applications** à l'aide de *cookies* [4], et/ou de paramètres CGI de requêtes HTTP (GET ou POST).

Parmi les différentes solutions commerciales offertes aux administrateurs et développeurs émergent *Sun ONE Identity Server* [5] et *MicroSoft Passport* [6]. Cet article se propose de montrer qu'une solution libre permet d'implémenter un mécanisme de SSO puissant, sûr et souple pour les applications *web*.

2 Le choix de CAS

Développé par l'Université de Yale, CAS (*Central Authentication Service* [7]) met en oeuvre un serveur d'authentification accessible par W3, composé de servlets java, qui fonctionne sur tout moteur de *servlets* (*Tomcat* par exemple), et dont les points forts sont listés ci-dessous.

- La **sécurité** est assurée par les dispositifs suivants :
  - le mot de passe de l'utilisateur ne circule qu'entre le navigateur client et le serveur d'authentification, nécessairement à travers un canal crypté.
  - Les ré-authentifications suivantes sont faites de manière transparente à l'utilisateur, sous réserve de l'acceptation d'un *cookie* privé et protégé. Seul le serveur d'authentification peut lire et écrire ce *cookie*, qui ne contient qu'un identifiant de session.
  - L'application reçoit du serveur d'authentification un « ticket opaque » qui n'est pas porteur d'information personnelle. Ce ticket circule en clair via le navigateur (en paramètre CGI) ; il n'est pas rejouable, a une durée de vie courte, est n'est utilisable que par l'application qui l'a demandé. L'application va ensuite contacter directement (en http) le serveur CAS afin de faire valider (et expirer) ce ticket ; le serveur CAS va retourner à l'application l'identifiant de la personne, validé. L'application n'a ainsi jamais accès au mot de passe (schéma pourtant classique de pratiquement tous les mécanismes de SSO).
- Les mécanismes classiques imposent une communication entre le navigateur web et l'application, ce qui exclut les **configurations n-tiers**, où une application doit directement interroger un service nécessitant authentification (c'est le cas par exemple pour un portail accédant à un *web service*). CAS, dans sa version 2.0, résout ce problème en proposant un mécanisme de mandataires (*proxies*). Des tickets dédiés permettent à des applications tierces, n'ayant aucune communication avec le navigateur client, d'être assurées de l'authentification de l'utilisateur. Cette fonctionnalité est assurément le point fort de CAS.
- Le package proposé implémente tout le protocole de mise en oeuvre du SSO, à l'exception du module d'authentification locale qui est à la charge de l'administrateur du serveur d'authentification. Cela laisse la **liberté d'implémenter exactement l'authentification souhaitée** (LDAP, *Kerberos* [8], certificats X509, NIS, un panachage, ...).
- Des **librairies clientes** en *Java*, *Perl*, JSP, ASP, PL/SQL et PHP sont livrées. Cela permet une grande souplesse sur les serveurs d'applications. L'intégration dans des outils utilisés dans le monde universitaire est d'ores et déjà faite, comme celle d'*uPortal* [9].
- L'utilisation de *cookies* exclusivement privés dans CAS (passage de tickets entre serveur d'authentification et applications uniquement sous forme de paramètres de GET HTTP) permet à CAS d'être opérationnel sur des serveurs situés dans des **domaines DNS différents**.
- Un **module Apache** (*mod_cas*) permet d'utiliser CAS pour protéger l'accès à des documents *web* statiques, les librairies clientes ne pouvant être utilisées dans ce cas.
- Un **module PAM** [10] (*pam_cas*) permet de « CAS-ifier » des services non *web*, tels que FTP, IMAP, ...
- Enfin, CAS est en production dans plusieurs Universités américaines, avec des authentifications internes *Kerberos* ou LDAP, ce qui permet d'être confiant sur sa **fiabilité**[1].

Nous vous proposons de détailler dans cet article le fonctionnement d'une implémentation de SSO avec CAS, en nous attachant à présenter les avantages et inconvénients de cette solution.

3 Le mécanisme CAS

3.1 Architecture

3.1.1 Le serveur CAS

L'authentification est centralisée sur une machine unique, le serveur CAS. Ce serveur est le seul acteur du mécanisme CAS à avoir connaissance des mots de passe des utilisateurs. Son rôle est double
: - **authentifier** les utilisateurs ;
- **transmettre et certifier l'identité** de la personne authentifiée (aux clients CAS).

*3.1.2 Les navigateurs (*web*)*

Les navigateurs doivent satisfaire les contraintes suivantes pour bénéficier de tout le confort de CAS[2] :

[1] À l'Université d'Indiana, CAS contrôle environ 80 applications web destinées à une centaine de milliers d'utilisateurs ; Le serveur CAS y effectue une moyenne de 9000 authentifications par jour.

- disposer d'un moteur de **chiffrement** leur permettant d'utiliser le protocole HTTPS ;
- savoir effectuer des **redirections HTTP** (accéder à une page donnée dans une entête Location lors d'une réponse 30x à une première requête HTTP) et interpréter le langage ***JavaScript*** ;
- savoir stocker des ***cookies***, comme défini par [4]. En particulier, les *cookies* privés ne devront être retransmis qu'au serveur les ayant émis pour garantir la sécurité du mécanisme CAS.

Ces exigences sont satisfaites par tous les navigateurs classiquement utilisés, à savoir *MicroSoft Internet Explorer* (depuis 5.0), *Netscape Navigator* (depuis 4.7) et *Mozilla*.

3.1.3 Les clients CAS

Une application web muni d'une librairie cliente ou un serveur web utilisant le module *mod_cas* est alors appelé « client CAS ». Il ne délivre les ressources qu'après s'être assuré que le navigateur qui l'accède se soit authentifié auprès du serveur CAS.

Parmi les clients CAS, on trouve :
- des librairies correspondant aux langages communément employés en programmation web dynamique (*Perl*, *Java*, JSP, PHP, ASP) ;
- un module *Apache*, qui permet de protéger des documents statiques ;
- un module PAM, qui permet d'authentifier les utilisateurs au niveau système.

3.2 Fonctionnement de base

3.2.1 Authentification d'un utilisateur

Un utilisateur non déjà précédemment authentifié, ou dont l'authentification a expiré, et qui accède au serveur CAS se voit proposer un formulaire d'authentification, dans lequel il est invité à entrer son nom de connexion et son mot de passe :

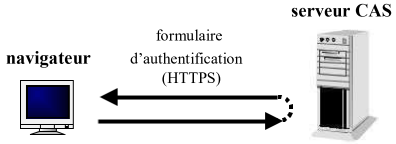


Figure 1 : *Premier accès d'un navigateur au serveur CAS (sans TGC)*

Si les informations sont correctes, le serveur renvoie au navigateur un *cookie* appelé TGC (*Ticket Granting Cookie*) :

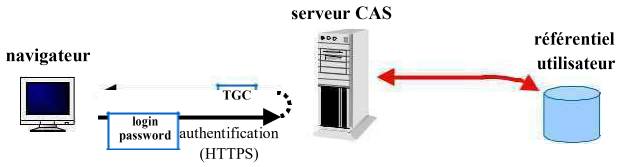


Figure 2 : *Authentification d'un navigateur auprès du serveur CAS*

Le *Ticket Granting Cookie* (TGC) est le passeport de l'utilisateur auprès du serveur CAS. Le TGC, à durée de vie limitée (typiquement quelques heures), est le moyen pour les navigateurs d'obtenir auprès du serveur CAS des tickets pour les clients CAS sans avoir à se ré-authentifier. C'est un *cookie* privé (n'est jamais transmis à d'autres serveurs que le serveur CAS) et protégé (toutes les requêtes des navigateurs vers le serveur CAS se font sous HTTPS). Comme tous les tickets utilisés dans le mécanisme CAS, il est opaque (ne contient aucune information sur l'utilisateur authentifié) : c'est un identifiant de session entre le navigateur et le serveur CAS.

[14] les tickets de type *granting* sont beaucoup plus rares que les PT et ST.

Qu’est-ce qu’un certificat SSL ?

Un certificat SSL (*Secure Sockets Layer)* est un certificat numérique que l’on associe à un nom de domaine ou une URL. Egalement nommé certificat TLS (Transport Layer Security), il permet d’établir avec certitude le lien entre le site internet et son propriétaire (entreprise, marchand ou individu). L’authentification du site Internet permet de sécuriser les échanges électroniques avec les utilisateurs qui s’y connectent via Internet.

Le Domain Name System est un service permettant de traduire un nom de domaine en informations, notamment en adresses IP du serveur hébergeant ce nom de domaine.

Un nom de domaine (DN) est l’identifiant d’un site internet (www.monsite.com par exemple).

Un sous-domaine est l’adresse internet d’une partie de votre site internet (par exemple mail.monsite.com)

Le certificat SSL permet d’instaurer la confiance :

- en authentifiant un site
- en chiffrant l’ensemble des informations (personnelles, bancaires, etc.) entre ce site et la personne qui s’y connecte. Il garantit ainsi la confidentialité des échanges.

Les visiteurs peuvent ainsi laisser en toute sécurité et confiance leur numéro de carte bancaire ainsi que des informations personnelles. Ce certificat SSL permet en outre de sécuriser les transactions en ligne ; les informations données par le client ne peuvent pas être interceptées, détournées ou déchiffrées par une autre personne.

Comment fonctionne un certificat SSL ?

Sur un plan technique, les identifications numériques ou certificats numériques permettent d’associer une clé publique à son véritable propriétaire. La clé publique du site permet l’échange d’une clé de session secrète ; celle-ci va chiffrer les informations transmises entre le client et ce site Internet. Elle permet également, via un module de contrôle d’intégrité inclus dans les fonctions de chiffrement, de vérifier que le message n’a pas été modifié au cours de son passage sur Internet.

L’Autorité de Certification, l’organisme qui délivre le certificat SSL, agit en quelque sorte comme une Préfecture ou une Mairie qui délivre des cartes d’identité ; Elle engage une série de vérifications selon des règles très strictes, afin d’établir avec certitude l’identité de l’entreprise et du serveur web ; l’Autorité de Certification émet alors le certificat SSL et le retourne à l’administrateur du site web certifié.

Votre certificat SSL, véritable passeport électronique de votre site web, contient les informations suivantes :

- L’url du site à certifier (ex: www.monsite.fr)
- Les coordonnées de votre entreprise
- Votre clé publique (qui permet le chiffrement des informations)
- Le nom de l’Autorité de Certification, qui émet ce passeport électronique
- La date d’expiration de ce certificat SSL
- La signature de l’Autorité de Certification

Pourquoi a-t-on besoin d'un certificat SSL ?

Les utilisateurs réalisent leurs transactions sur les sites qu'ils savent certifiés et sécurisés ; ils s'assurent ainsi que l'activité de l'entreprise est réelle et que les communications chiffrées, de manière à rester confidentielles.

Les certificats SSL permettent également de prouver l'identité du propriétaire du site web aux utilisateurs qui se connectent, et empêcher un site malveillant d'usurper l'identité de celui-ci et détourner ses clients ou visiteurs.

L'Autorité de certification s'engage sur une série de vérifications selon des règles très strictes, afin d'établir avec certitude l'identité d'une entreprise et de son serveur web. Le certificat SSL, une fois fabriqué, donnera aux clients les assurances suivantes :

- **La preuve de l'identité de l'entreprise** : un passeport électronique unique est délivré pour un site Internet, assurant aux clients l'authenticité du site, permettant le chiffrement et garantissant ainsi la confidentialité des communications.
- **Une forte sécurité** : reposant sur le modèle de chiffrement à « clé publique », dérivé des technologies militaires, les certificats SSL, procurent un très haut niveau de sécurité. La technologie de chiffrement SSL étant déjà implémentée sur un serveur, l'entreprise doit se procurer un certificat SSL.
- **Une utilisation simple** : Transparence pour les clients

Les certificats SSL, plusieurs choix possibles :

En fonction de la configuration de vos serveurs web et de vos sites internet il existe plusieurs types de certificats:

Il existe 3 types de certificats SSL :

- **DV** : "Domain validated" permet de sécuriser un site internet.
- **OV** : "Organisation validated" sécurise le site internet institutionnel de votre organisation.
- **EV** : "Extended validated" permet une sécurité renforcée de votre site par la présence d'une barre verte sur la ligne d'URL du browser
- **Certificat RGS*** : Ce certificat s'adresse aux organisations du secteur public. Il respecte la norme RGS et est reconnu par l'administration française.

Qui délivre des certificats SSL ?

Un tiers de confiance certifié peut émettre un certificat. Acteur du développement de la confiance dans le monde numérique, il intervient dans la protection de l'identité, des documents, des transactions et de la mémoire numérique. Il engage sa responsabilité juridique dans les opérations qu'il effectue pour le compte de son client.

Les organismes qui produisent les certificats SSL sont appelés des Autorités de Certification (AC ou CA en anglais pour Certification Authority).

2.7 Schéma d'architecture multi-services

En conclusion de ce chapitre consacré à l'architecture d'une passerelle Internet sécurisée, il est proposé sur la figure 2.22 un schéma d'architecture multi-services reprenant différents cas d'usage de la passerelle Internet sécurisée qui ne se veulent toutefois pas exhaustifs.
Voici quelques remarques sur les mutualisations et cloisonnements représentés (les numéros de cette liste sont reportés sur la figure 2.22).
Conformément à la recommandation R6 :
1. les pare-feux périmétriques (internes d'une part et externes d'autre part) sont dédiés par chaîne d'usage : flux entrants liés à l'hébergement, flux VPN entrants pour l'accès des collaborateurs au SI, flux sortants ;
2. pour les pare-feux externes, le choix d'un cloisonnement physique (*n* pare-feux physiques dédiés), logique (*n* pare-feux virtuels dédiés sur un socle de pare-feu physique) ou hybride doit être déterminé par l'analyse de risque ; au minimum les pare-feux des chaînes entrantes et sortantes sont physiquement distincts ;
3. la remarque 2 s'applique également pour les pare-feux internes ;
4. s'agissant des ressources (serveurs,...) de la zone de services relais, celles-ci sont dédiées par chaîne d'usage et le choix d'un cloisonnement physique (une ressource physique dédiée) ou logique (une machine virtuelle dédiée sur un socle physique mutualisé) doit être déterminé par l'analyse de risque ; au minimum les ressources des chaînes entrantes et sortantes sont physiquement distinctes ;
Par ailleurs :
5. les pare-feux internes et externes ne sont pas mutualisés conformément à la recommandation R13 ;
6. les flux VPN entrants pour l'accès des collaborateurs au SI ne font pas l'objet d'une analyse en amont du concentrateur VPN pour ne pas interrompre le flux IPsec (ou TLS) chiffré et authentifié, conformément au message d'avertissement page 13 ;
7. les flux de synchronisation d'annuaire sont à l'initiative de l'annuaire du SI de l'entité vers l'annuaire dédié de la passerelle Internet sécurisée conformément aux recommandations R7 et R10 ;
8. la passerelle Internet sécurisée est administrée depuis un système d'information d'administration sécurisé, conformément à la recommandation R16 (cf. section 3.1).

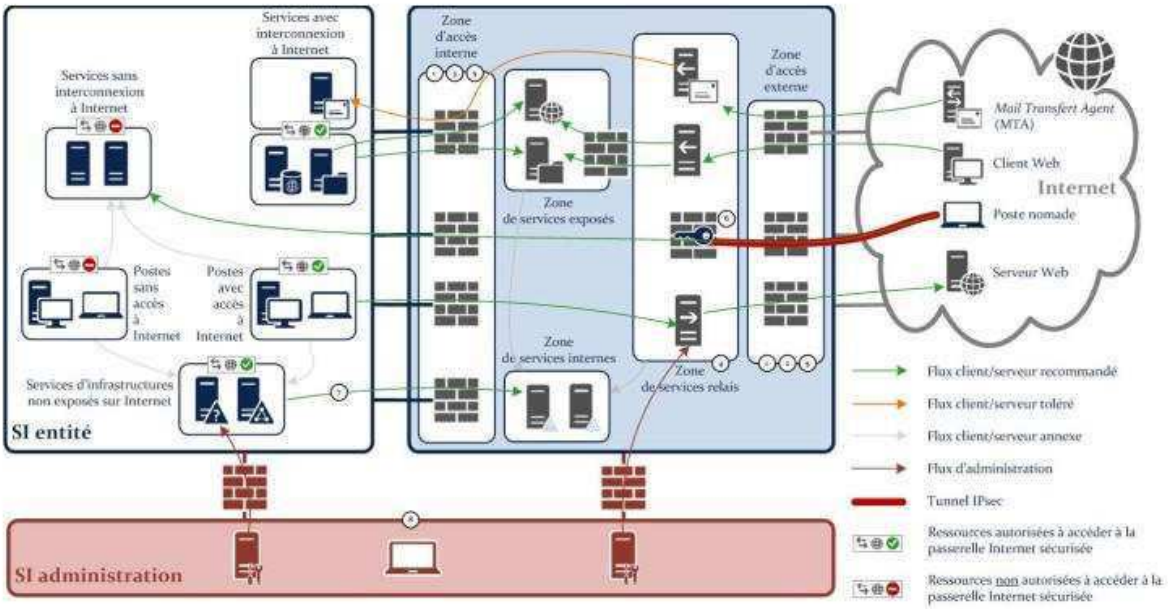


Figure 2.22 – Architecture multi-services de la passerelle Internet sécurisée

Extrait du cadre de cohérence technique (CCT)

Chapitre 9 : Gestion de contenu (ECM/GED) - [GC]

Référence	Composant	Fournisseur	Version	Statut	Supp. LL	Commentaires
SG-1237	Alfresco	Communauté Alfresco	4.x	M	Oui	Suite d'outils pour le collaboratif via portail Web.
SG-1489	Alfresco	Communauté Alfresco	5.x	R	Oui	Suite d'outils pour le collaboratif via portail Web.
SG-1395	eZ Publish	ez.no	5.1	A	Oui	Version 5.1 réservée à la migration des sites existants. En raison d'une incertitude sur le maintien de la version communautaire, le produit est placé en observation (assujetti).
SG-1394	Joomla	Joomla.org	3.x	R		Création de sites Intranet institutionnels.Périmètre DNUM : offre de service limitée à l'hébergement.
SG-1238	Dokuwiki	dokuwiki.org		R		Wiki simple et ne nécessitant pas de base de donnée. Licence GNU GPL V2. Utilisation des plugins inclus dans le package distribué par le fournisseur
SG-1239	Mediawiki		Version SILL	A	Oui	Inscrit au SILL.
SG-1403	Drupal	Drupal.org	8.x	R		CMS autorisé sur le périmètre ST(SI)²

Extrait du RGAA permettant d'insérer les balises dans un texte HTML

TITRES – H1 - H2 – H3 – H4 – H5 - H6

Utiliser des titres et des sous-titres permet de structurer et découper un texte. Cela fournit à l'utilisateur un plan du document et lui permet de naviguer de titre en titre pour se déplacer plus rapidement dans le contenu de la page.

Le titrage des contenus est une étape importante dans la structuration des contenus qui répond à deux besoins : identifier rapidement un contenu recherché et, surtout, naviguer rapidement dans le contenu en se déplaçant de titre en titre.

Il y a 3 obligations pour le titrage des contenus :

- la page doit comporter au moins un titre <h1> ;
- la hiérarchie de titres doit être cohérente ;

Élément HTML (balise h) à 6 niveaux de hiérarchie (de h1 pour le titre le plus important à h6 pour le moins important).

La hiérarchie entre les titres doit être respectée dans une page web et les degrés de titre ne peuvent pas être sautés (un titre h3 ne peut pas venir directement après un titre h1, par exemple). Par contre, la hiérarchie ne doit pas obligatoirement débuter par un h1. Même si cet usage n'est pas encouragé, il est considéré comme conforme de débuter la hiérarchie des titres d'une page par un autre niveau que le niveau 1.

IMAGE

Les images véhiculent parfois une information non textuelle. Cette information, qui peut aider à comprendre le contenu auquel elle se rapporte, doit être accessible à tous.

Fournir une alternative est indispensable pour les utilisateurs qui ne perçoivent pas le contenu visuel. Un lecteur d'écran ou une loupe vocalisée vont pouvoir accéder à cette alternative et la restituer à l'utilisateur ou bien l'information sera affichée si l'utilisateur désactive les images.

ALTERNATIVE OBLIGATOIRE

Toutes les images doivent avoir un attribut alt. Cette obligation tient au fait qu'en l'absence de cet attribut, un lecteur d'écran restitue le chemin ou le nom du fichier source, ce qui n'a pas de sens pour l'utilisateur.

Les éléments concernés sont :

les images <img> ;
les champs de formulaire <input type="image">.

IMAGE DE DÉCORATION ALTERNATIVE RENSEIGNEE

Lorsqu'un lien est composé uniquement d'une image, c'est l'alternative de cette image qui constitue son intitulé.

Par exemple, pour les images <img>, c'est le contenu de l'attribut alt qui est l'intitulé du lien.

Dans ces cas, l'alternative de l'image indique à l'utilisateur la destination du lien.

```
<a href="#"><img src="home.png" alt="Accueil"/></a>
```

IMAGE DE DÉCORATION : ALTERNATIVE VIDE

Si l'image ne véhicule aucune information, l'image n'a pas vocation à être restituée. Son alternative doit alors être vide. De plus, elle ne doit pas posséder d'attribut title.

```
<img src="url.png" alt="" />
```

Un certificat SSL vous permet de sécuriser les échanges entre votre site web et les internautes par le biais d'une clé cryptographique. Il active le protocole HTTPS et fait apparaître le fameux cadenas de sécurité dans la barre d'adresse du navigateur – un gage de sécurité pour vos utilisateurs. Mais saviez-vous que l'obtention de ce précieux sésame passe par une étape préalable indispensable, appelée « demande de signature de certificat » ? Voici en quoi consiste la CSR certificat et comment l'utiliser pour mettre en place votre certificat SSL.

Qu'est-ce qu'une CSR certificat ?

Une demande de certificat SSL impose de suivre un certain nombre d'étapes. La première consiste à prendre contact avec une Autorité de Certification (AC) comme CertEurope et à sélectionner le type de certificat qui convient le mieux à vos besoins. La deuxième étape est autrement plus délicate : il s'agit de générer une demande de signature de certificat (ou CSR certificat pour *Certificate Signing Request*) et de l'adresser à l'AC dans le but d'obtenir un certificat numérique.

En substance, une CSR est donc un message adressé à une Autorité de Certification par un demandeur, dans le but d'obtenir un certificat d'identité numérique.

Comment s'utilise une CSR ?

La demande de signature de certificat est générée par le demandeur. Celui-ci doit créer une clé publique (qui sera incluse dans la CSR) et une clé privée (qu'il utilisera pour signer numériquement la demande et qu'il gardera secrète).

Quelles sont les informations contenues dans une CSR certificat ?

Ce sont les informations contenues dans la CSR certificat qui permettent à l'Autorité de Certification de délivrer un certificat en bonne et due forme. Sont demandés :

- Le nom du serveur (CN=);
- Le nom de l'entreprise qui génère la demande (O=) ;
- L'unité organisationnelle (OU=), sous la forme du numéro de SIREN précédé de « 0002 » ;
- La localité (L=) et la région (S=) où est situé le siège social de l'organisation ;
- Le pays (C=) sous la forme d'un code ISO à deux lettres ;
- L'adresse mail de l'intermédiaire au sein de l'entreprise (le plus souvent, c'est la personne en charge de la gestion des certificats).

Quelles sont les règles à respecter pour une CSR ?

La génération d'une demande de signature de certificat suppose de respecter quelques conventions, notamment :

- Créer une clé privée d'une longueur de 2048 bits (clé de type RSA 2018 Bits).
- S'assurer de la sécurité de la clé privée(en utilisant un outil de génération de clé suffisamment récent pour ne pas être vulnérable, et en définissant un mot de passe/une liste de contrôle pour en protéger l'accès).
- Utiliser un algorithme de signature en SHA256 (SHA 256withRSA) pour la CSR (en vertu des exigences du cahier des charges RGS).

Comment générer une demande de signature de certificat ?

La procédure de demande de signature de certificat comprend une partie technique et une partie administrative.

La procédure technique vient dans un premier temps. Elle consiste à générer la CSR certificat et la clé privée. L'utilisation de OpenSSL est recommandée, à la fois pour sa simplicité et pour ses performances. Nous allons prendre l'exemple d'une demande de signature de certificat adressée à CertEurope.

Pour générer la clé, vous devez :

- Accéder à la ligne de commande et entrer : *openssl genrsa -des3 -out key private/SERVEUR.key 2048* ;
- Choisir un mot de passe PEM (si vous ne souhaitez pas créer de mot de passe, il est toujours possible de supprimer la commande « -des3 », mais votre clé sera vulnérable) ;
- Générer automatiquement une clé privée RSA 2048 bits.

Votre clé est sauvegardée dans le fichier *key private/SERVEUR.key*.

Pour générer la demande de signature de certificat, il faut ensuite :

- Accéder au fichier de configuration adressé par l'Autorité de Certification (en fonction du type de certificat demandé : *openssl-OI-Cachet.cnf* pour un cachet serveur, *openssl-OI-SAN-authclient.cnf* pour un SSL Authentification Client, *openssl-OI-SAN.cnf* pour un SSL Authentification Serveur, *openssl-OI-SAN.cnf* pour un SSL Quovadis) en modifiant les valeurs par défaut par celles de votre organisation.
- Entrer la commande : *openssl req -new -out certeurope-seal-2048.csr -key certeurope-seal-2048.key -config* [*openssl-OI-Cachet.cnf*]. Entre crochets : le fichier de configuration de votre profil de certificat.
- Entrer votre mot de passe PEM si vous l'avez configuré.
- Vérifier que les informations sont correctes.
- Entrer la commande : *openssl req –in certeurope-seal-2048.csr – noout –text.*

Ce qui permet de générer votre CSR certificat. Celle-ci est créée dans le format PEM encodé en base64, PEM (*Privacy Enhanced Mail*) étant le format par défaut pour OpenSSL (il s'agit d'un fichier DER encodé en ASCII et entouré de balises de marquage).

CMS – Définition & guide complet pour choisir votre CMS

Lorsque l'on lance son projet web, l'un des premiers choix auxquels on est confronté est la méthode de création de son site internet. Dans les faits, que l'on choisisse de travailler avec une agence web, un freelance, ou que l'on crée son site soit même, vous serez dans tous les cas amené à travailler avec un logiciel de création de site, plus communément appelé CMS (Content Management System). Il est donc primordial d'être familier avec ces outils incontournables.

Qu'est-ce qu'un Content Management System (CMS) ?

Définition d'un CMS

Un Content Management System, appelé plus couramment CMS, est un logiciel qui permet de créer, modifier et publier du contenu sur un site internet. La plupart des CMS propose aussi des outils collaboratifs, qui permettent à plusieurs personnes d'agir en même temps sur le site, en fonction de droits prédéfinis à l'avance par l'administrateur. Les CMS peuvent avoir d'autres noms, cependant beaucoup moins répandus, comme Web Content Management (WCM) ou encore Digital Experience Platform (DXP). Plus concrètement, un CMS permet de réaliser toutes les taches suivantes :

Rédaction de texte
Édition des méta-données (particulièrement utile pour le SEO)
Design du site
Hiérarchiser le contenu
Définir un URL logique
Importer du média (vidéo, image)
Programmer des dates de publication
Définir des rôles utilisateurs (rédacteur, administrateur, etc…)
Organiser automatiquement la publication du contenu (en fonction des dates de publication, du type de contenu, de la hiérarchie du site, etc…)
Historique des modifications apportées au site
Indexation de contenu
Recherche sur le site
Sauvegarde et récupération de contenu
Récolte d'information sur vos visiteurs

La plupart des CMS disponibles sur le marché propose aussi un système de plug-in. Les plug-in sont des petits logiciels que l'on peut rajouter au CMS pour acquérir de nouvelles fonctionnalités dont vous pourriez avoir besoin.

Pourquoi utiliser un CMS ?

Aujourd'hui, l'intégralité des entreprises présentes sur le web (ou presque) utilisent toutes un CMS pour gérer leurs sites web. C'est aussi le cas des blogueurs, ou des experts en marketing digital, qui passent par des CMS pour ne pas avoir à se concentrer sur la technique web, mais uniquement sur leur champ de compétence professionnel. Par exemple, il peut peu probable qu'un blogueur mode ou cuisine soit un expert du développement web mais, grâce aux CMS, ces derniers peuvent développer leur présence sur le web de manière ultra qualitative, sans avoir à éditer une seule ligne de code.

Si les avantages et objectifs d'un CMS vous semble encore flous, creusons un peu plus profond dans le web pour comprendre tout leur intérêt. Comment un site web est-il – concrètement – fabriqué ? Un site internet utilise principalement plusieurs langages pour fonctionner, dont les principaux sont :

HTML 5 : Le HTML est le langage universel d'architecture de site web. Il permet de créer différentes pages web dans un même site, de créer des liens hypertextes, de définir les différents types de contenu (titre de page, titre/paragraphe d'articles, balisage d'image, blocs de contenus, etc…).
CSS 3 : Le CSS est un langage complémentaire au HTML, et qui correspond à tout ce qui touche au style au design d'un site web (couleurs, taille et position des blocs HTML, animations basiques, etc…)
PHP : PHP est un langage de développement permettant de faire des sites internets dynamiques, et connectés à une base de données.
JavaScript : JS est un langage de programmation, principalement utilisé pour créer des interactions sur les sites internet.

Pour créer un site internet moderne et qualitatif de A à Z, il faudrait avoir des connaissances très poussées sur chacun de ces langages, et biens d'autres encore. Un CMS agit comme une interface entre l'utilisateur et ces différents langages, vous permettant ainsi de créer un site internet et du contenu, sans forcement avoir à mettre les mains dans le cambouis du code. De plus, un CMS adapté vous fera gagner beaucoup, beaucoup, de temps dans l'administration de votre site web.

Quels sont les différents types de CMS ?

CMS hébergés versus CMS gérés

Avant de plonger dans le coeur des CMS, la première des questions à se poser avant de se lancer est la suivante : préférez-vous acquérir votre propre CMS (CMS hébergé) ? Ou utiliser une solution pré-gérée (CMS gérés) ? Un CMS géré est une solution complète gérée par un fournisseur externe qui prend en charge tout l'aspect technique. C'est le cas des solutions les plus populaires comme WordPress, Shopify etc… Ces solutions CMS ont l'avantage de proposer un support actif et accessible, un développement continue et des mises à jours régulières qui permettent à la solution d'être au fait des meilleurs pratiques du web, aussi bien au niveau technique que sécuritaire. Cependant, ces solutions peuvent manquer d'adaptabilité et d'outils de personnalisation, notamment au niveau du design. En effet, ce dernier est inhérent au template que vous aurez sélectionné, et les templates sont souvent assez rigides. Par exemple, vous pouvez être sûr qu'un expert du e-commerce reconnaitra au premier coup d'œil un site qui tourne sous Shopify.

Les principaux CMS

WordPress
Shopify
Drupal
Joomla!

Présentation

WordPress, c'est le mastodonte des CMS. Avec environ 20 millions de sites internets propulsés par ses soins, WordPress est, de loin, la référence. Accessible et hautement personnalisable, il permet de faire à peu près tout sur le web. Shopify est la plateforme qui monte depuis plusieurs années maintenant. Ce spécialiste du e-Commerce propulse environ 600.000 sites à travers le web. Du design aux méthodes de paiement, Shopify est la plateforme idéale pour propulser rapidement votre commerce sur le web. Drupal est un CMS aux applications vastes. A la manière de WordPress, Drupal est un CMS open-source disponible gratuitement dans sa version native. Il a pour réputation d'être plus puissante que WordPress, mais plus difficile à utiliser pour un utilisateur non-avertit. Joomla est à Shopify ce que Drupal est à WordPress. Moins intuitif que la plateforme Canadienne, Joomla est cependant un outils extrêmement puissant entre les mains d'un développeur web aguerri. Bien que Joomla soit en perte de vitesse, il reste un CMS très utilisé par les professionnels du développement web.

Création du design

A ce stade, il est important de comprendre une chose concernant les CMS, et qui va vous faciliter la vie : La plupart des CMS séparent le design et le contenu. Si cette approche peut provoquer une certaine rigidité, elle représente un gain de temps formidable lorsque vous allez produire votre contenu. En effet, tout votre contenu va s'imbriquer automatiquement dans un design préalablement dessiné, un peu comme des poupées russes. De plus, la plupart des design des CMS sont « responsives », ce qui signifie qu'ils sont capables de s'adapter automatiquement à la taille de l'écran de l'utilisateur qui consulte votre site. L'écran d'un smartphone étant beaucoup moins large que celui d'un ordinateur, il apparait logique que le design doit s'adapter en fonction du « device utilisateur ». Le thème de votre CMS le fera pour vous, et vous proposera même – en fonction du CMS et du thème sélectionné – des outils de personnalisations de vos différents design mobiles et desktop.

Comme nous l'avons dit plus haut, le langage CSS est l'un des principaux acteurs du design. En réalité, les choses sont encore un peu plus complexes. Les langages HTML et CSS ont bien un intérêt important en terme de design, mais ils ont besoin d'un schéma précis pour s'imbriquer idéalement les uns dans les autres. C'est le rôle de la base de données inhérente à votre CMS que de vous offrir cette architecture de base, sorte de fondation avant que vous posiez les murs de votre site.

Comment s'exprime concrètement cette architecture ? Imaginons que, sur votre page d'accueil, vous souhaitiez afficher 3 articles, avec leurs titres respectifs, images mise en avant, et un court extrait de chacun. De plus, vous souhaitez que ne soit affichés sur votre page d'accueil que les articles les plus récents de la catégorie « bon plan ». Si vous deviez coder tout ça vous même en HTML, cela vous prendrait beaucoup de temps, et vous devriez réécrire votre code à chaque fois que vous écrivez un article. Avec un CMS, les choses ont beaucoup plus simples ! Il vous suffit simplement de lui expliquer une fois ce que vous souhaitez afficher sur votre page d'accueil, et le CMS calculera automatiquement quel article il doit « ranger » dans quelle case, en fonction des informations qu'il aura récolté dans sa base de donnée (date de publication de l'article, catégorie, etc…).
Ainsi, une fois votre CMS programmé, vous n'avez qu'à rédiger vos articles comme bon vous semble, et ces derniers atterriront automatiquement là ou ils sont censés être distribués à vos visiteurs.

Au delà de ces considérations techniques, le CMS vous proposera également de générer un menu, un header, un footer, et d'autres éléments design que vous pourrez afficher – ou non – sur vos différentes pages. Pour faire simple, le design de votre site, propulsé par un template que vous aurez choisi, vous permet de donner des directives à votre CMS pour qu'il puisse distribuer le contenu de manière autonome, selon vos souhaits. De manière générale, on vous conseille de bien réfléchir à l'architecture de votre site avant de le rendre « live ». Une bonne architecture est une architecture lisible, efficace, et facilement modulable par vos équipes.

Rédaction et gestion éditoriale

Si le contenu est le roi du marketing en 2018, le timing devrait être considéré comme sa légitime reine. L'association de ces deux éléments est assurément un vecteur de succès sur le web, à condition que ces deux facteurs soient parfaitement maitrisés. Cette activité peut être résumée en deux mots : le management de contenu.

A ce titre, les CMS sont d'excellents outils mis à votre disposition. Non seulement ils disposent, pour la plupart, d'outils vous permettant de rédiger facilement vos contenus (textes, insertion de vidéos, etc…) mais, et c'est là leur force, vous permettent aussi de déterminer à l'avance de la date de publication dudit contenu. Avec un CMS, il devient facile de produire du contenu et le partager en temps voulu, sans nécessairement être devant son ordinateur jour et nuit. De fait, il devient beaucoup plus simple de mettre en place une stratégie éditoriale efficace dans le temps. Prenons un exemple simple : vous avez passé la matinée à rédiger du contenu promulguant votre nouveau projet, mais le lancement officiel de ce projet doit intervenir le soir même à 22h. Grace à votre CMS, vous n'aurez pas besoin de faire des heures supplémentaires. Vous n'aurez qu'à préparer entièrement votre contenu, et programmer sa publication à 22h. Ainsi, votre CMS – qui est hébergé sur un serveur actif 24h/24 – attendra sagement 22h avant de rendre « live » votre contenu.

Suivant la même idée, vous pourriez aussi vouloir qu'un contenu soit automatiquement supprimé à une date précise. C'est, par exemple, souvent le cas dans les promotions e-Commerce. La encore, votre CMS peut le faire pour vous. Admettons que vous ayez fabriqué une bannière promotionnelle dont la campagne durera deux semaines. Vous propulsez votre bannière sur votre site, et demandez à votre CMS de la retirer, ou de la remplacer, au bout de deux semaines. Rien de plus simple.

Si vous créez du contenu, vous risquez certainement d'avoir de temps à autres quelques coquilles. Une erreur d'orthographe est vite arrivée, tout comme une suppression intempestive, ou l'utilisation d'une image/vidéo qui ne devrait pas se retrouver sur votre site. La encore, un bon CMS vous proposera des solutions automatiques d'archivage et révision du contenu. Ainsi, vous pourrez facilement modifier n'importe quel contenu, et le mettre à jour instantanément sur votre site. De manière globale, la gestion des révisions de contenu devrait être l'une des priorités lors de choisir votre CMS, puisqu'une mauvaise gestion/révision du contenu peut rapidement devenir chronophage, et prise de tête

Le CMS et ses « user roles »

A la manière d'une entreprise physique traditionnelle, vous pourriez être amené à déléguer certaines responsabilités sur votre site web. Les développeurs de CMS ont évidemment pensé à ça, et vous permette de définir une hiérarchie et un niveau de responsabilité spécifique à chacun de vos collaborateurs, c'est le principe des « user roles ». Les users roles vous permettent de définir, pour chaque personne ayant accès au site, les éléments auxquels ce collaborateur a accès, ou pas.

Prenons l'exemple d'un site média. Vous employez des journalistes qui distribuent de l'information sur votre site. Ces derniers doivent avoir accès à la section « blog » de votre site, et doivent avoir le pouvoir de rédiger/modifier leurs articles, et seulement les leurs : c'est très facile à programmer sur un CMS. Ensuite, admettons que vous disposez d'un rédacteur en chef, ou d'un chef éditorial. Ce dernier pourra avoir accès à l'ensemble des articles rédigés sur le site, pourra les modifier s'il le souhaite, et pourra également décider de dates de publication (ce que ne pourra peut-être pas faire un journaliste). La encore, c'est très facile à programmer via un CMS. Enfin, vous disposerez surement dans votre équipe de développeurs web qui s'occuperont de toute l'architecture du site. Ces derniers devraient avoir accès à toute la dimension technique du CMS de votre, mais n'auront pas accès aux articles des journalistes, et ne pourront pas non plus décider des dates de publication, puisque tout ce pan n'est pas de leur ressort. Ce système hiérarchique pourrait être conçu très simplement sur un CMS, permettant ainsi à l'ensemble de vos collaborateurs de travailler en même temps sur le site, sans sortir de leurs zones de compétences.

Dans la plupart des CMS, les rôles classiques sont les suivant, et ils sont modifiables à souhait en fonction de vos besoins :

Administrateur
Éditeur
Auteur
Contributeur

Lisibilité & SEO

Pour être efficace, un site internet doit avant tout être consulté par des visiteurs. Si vous n'optimisez pas l'architecture de votre site et son SEO (Search Engine Optimisation, ou optimisation du trafic organique en français), vos contenus risques de tomber dans les limbes du web. La encore, les CMS peuvent vous être d'une aide redoutable. Le SEO est un vaste sujet en soi, mais les CMS – aidés par certains plug-in – peuvent vous permettre d'optimiser rapidement et facilement les liens et méta-données de vos pages web, afin que ces dernières correspondent aux exigences et algorithmes des moteurs de recherche.

Si l'on prend l'exemple de WordPress : Lorsque vous rédigez un article, le CMS pré-fabrique un URL logique en fonction du titre de votre article, mais vous pouvez tout à fait le renommer à votre bon vouloir pour, par exemple, y intégrer des mots clefs susceptibles d'être souvent recherchés dans Google.

Au delà du titre d'une page, les moteurs de recherches se basent également sur votre contenu et la structure de ce dernier, notamment via les balises HTML. Éditer ces balises demandent d'avoir certaines connaissances en HTML, mais à l'aide d'un bon CMS, vous pourrez organiser votre contenu de manière logique, et optimiser ainsi son référencement sans même vous en apercevoir.

Conclusion

Un bon CMS est incontournable lorsqu'on développe un projet sur le web. Si le développement web repose sur plusieurs langages décrits ci-dessus, les ressources web disponibles aujourd'hui sont devenus si colossales qu'il est devenu indispensable de s'appuyer sur un CMS pour développer son projet. Il existe certaines solutions pré-existence qui font déjà un travail très qualitatif, mais vous pouvez aussi, si vous le souhaiter, faire développer votre propre CMS par une agence spécialisée. Enfin, le web est un univers en constante évolution, dont l'une des plus intéressantes sont les PWA (Progressive Web Apps). Ces dernières peuvent être considérées comme des applications en ligne, très puissante, accessibles, et qui ne nécessitent pas d'être téléchargées par l'utilisateur, comme l'outil graphique canva.com par exemple. Développer un projet en PWA coute cher, mais peut vous permettre d'aller encore plus loin dans l'interactivité avec vos clients sur le web.

Comment passer votre site web en HTTPS ?

Le HTTPS est un protocole permettant de sécuriser les échanges de données entre un serveur et un client, et de valider l'identité d'un site visité. Cette double sécurisation est essentielle : elle garantit la confidentialité des données et rassure les internautes qui se connectent à votre site web, tout en répondant aux exigences de Google. Vous n'avez pas encore affiché le HTTPS (et le petit cadenas vert qui l'accompagne) dans votre barre d'adresse ? Vous devez commencer par obtenir un certificat HTTPS auprès d'une Autorité de Certification avant de l'activer sur votre site. Voici la marche à suivre en 5 étapes.

1/ Choisissez le certificat HTTPS adapté à vos besoins

Première chose à faire : choisir un certificat HTTPS (ou certificat SSL) adapté aux besoins de votre entreprise en matière de sécurité. C'est ce certificat électronique qui permet le chiffrement des données échangées entre un serveur et un client. Il est donc indispensable d'en obtenir un pour activer le protocole HTTPS sur votre site. Celui-ci s'obtient auprès d'une Autorité de Certification. Mais avant toute chose, il faut sélectionner le bon niveau de sécurisation parmi les certificats suivants :

- À validation de domaine (certificat HTTPS rudimentaire qui chiffre les données sans vérifier l'identité du propriétaire du site).
- À validation d'organisation (certificat SSL plus poussé qui nécessite l'authentification du propriétaire du site).
- À validation étendue (certificat HTTPS offrant une sécurité optimale, particulièrement adapté aux sites qui collectent des données confidentielles et/ou des informations bancaires).

Il n'est pas forcément nécessaire d'acheter un certificat SSL trop pointu (à validation étendue) si votre domaine d'activité et le type de données collectées ne le justifient pas.

2/ Générez une demande de certificat

Une fois votre certificat HTTPS choisi, vous devez le demander auprès d'une Autorité de Certification (AC), un organisme chargé de délivrer des certificats et d'opérer les vérifications nécessaires (comme CertEurope). L'obtention de ce sésame passe par une étape préalable : une demande de signature de certificat (ou CSR certificat). Générer cette demande permet de soumettre votre besoin de certificat SSL à l'Autorité de Certification choisie, de manière à ce qu'elle enclenche les indispensables procédures de vérification exigées par le niveau de sécurité souhaité.

Une fois la demande validée par l'AC, celle-ci émet un certificat HTTPS que vous devez récupérer et installer sur vos serveurs, puis lier à votre site web. La procédure d'installation et d'activation du certificat SSL dépend du serveur et du langage utilisé. Si vous achetez votre certificat électronique auprès d'une Autorité de Certification, celle-ci peut vous proposer de prendre en charge cette étape.

Un conseil : avant de passer à l'étape suivante, effectuez une sauvegarde complète (back up) de votre site web. Cela vous permettra de revenir en arrière en cas de problème lors de l'activation du HTTPS.

3/ Redirigez les pages de votre site web

Vous avez obtenu votre certificat HTTPS et activé le protocole sur votre serveur. Mais ce n'est pas terminé ! Car le fait de passer du HTTP au HTTPS s'apparente à une migration de site à part entière, puisque votre nom de domaine change. Aux yeux des moteurs de recherche, votre site en HTTPS est donc différent de votre site en HTTP, ce qui suppose de rediriger toutes vos pages vers le HTTPS pour contourner les risques liés aux contenus dupliqués.

(Différentes méthodes existent pour basculer vos pages en HTTPS, depuis la modification manuelle de chaque URL à la création de redirections permanentes depuis le fichier .htaccess à la racine de votre site, en passant par l'utilisation de plugins dédiés – sur un CMS comme WordPress, par exemple.)

4/ Mettez à jour les différents éléments de votre site

Plusieurs éléments de votre site web doivent être mis à jour une fois votre certificat HTTPS activé, dans la mesure où certains fichiers peuvent continuer d'être chargés en HTTP, ce qui suppose de modifier les URL correspondantes. Cela concerne les liens internes (si vous utilisez des URL absolues) ainsi que les images.

Tous ces changements ne sont pas automatiquement pris en compte par Google : à ses yeux, votre site en HTTPS est un nouveau site. Quand tout est prêt, vous devez donc prévenir le moteur de recherche (via la Google Search Console) afin qu'il procède à une nouvelle indexation de vos URL. Plus vite vous indiquerez à Google le basculement de votre site, moins vous serez affecté par les conséquences de ce changement sur le positionnement SEO de vos pages.

5/Testez votre site en HTTPS

Vous n'avez plus qu'à vous assurer que vos démarches ont abouti en testant votre nouvelle configuration. Explorez votre site page après page pour vérifier que le certificat HTTPS a bien été activé partout et que le cadenas vert apparaît chaque fois. Contrôlez aussi les redirections : est-ce qu'elles fonctionnent bien ? Des outils (comme celui-ci) vous permettent d'auditer votre site pour vous assurer de la qualité du certificat SSL installé.

FUTURA SCIENCES

la rédaction de Futura

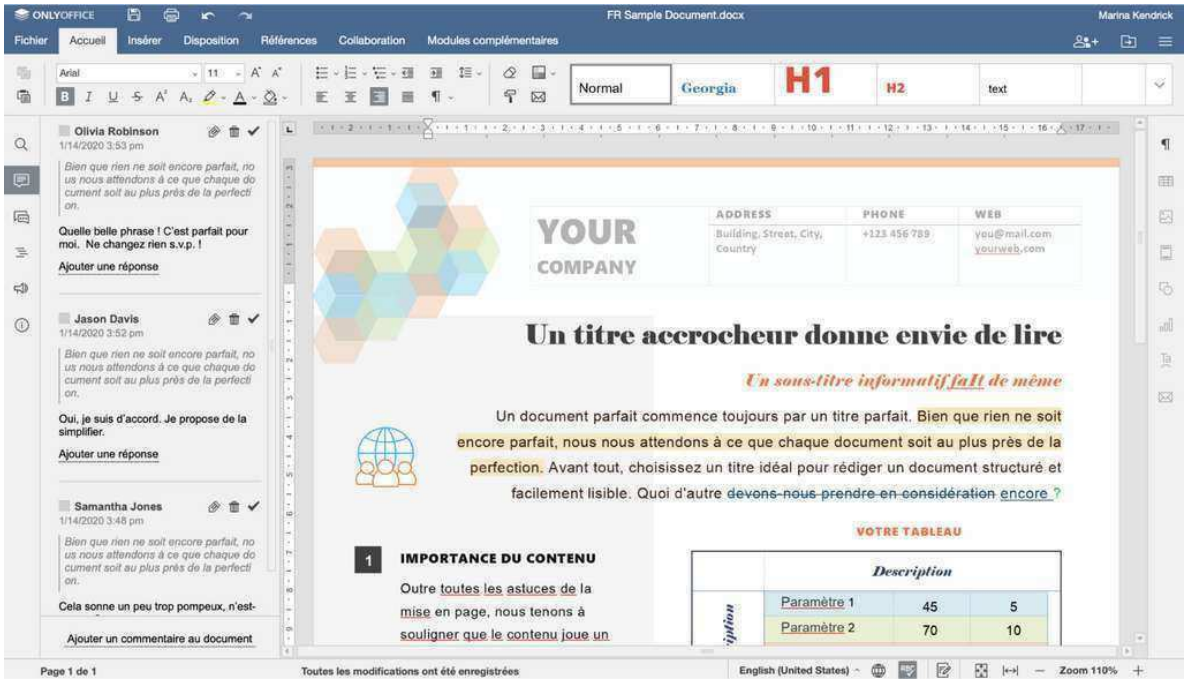
OnlyOffice Docs: notre avis sur cette suite bureautique Web autohébergée

Avec la version 6.1 sortie récemment, ONLYOFFICE Docs gagne en popularité et se pose en véritable alternative à Google Docs et Microsoft Office Online. Installez la suite bureautique européenne sur votre propre serveur pour éditer vos documents et collaborer avec vos collègues via l'éditeur gratuit ou directement dans votre navigateur.

ONLYOFFICE Docs est une suite bureautique en ligne à installer sur son propre serveur © ONLYOFFICE

Les suites bureautiques en ligne ont changé la manière dont on accède à nos documents. Fini les clés USB pour transporter ses documents, fini également de devoir installer un logiciel sur chaque appareil pour les consulter. En créant un serveur ONLYOFFICE Docs, vous pourrez utiliser son éditeur Web sur n'importe quel appareil pour créer et éditer vos documents. Contrairement à d'autres suites Web comme Microsoft Office Online ou Google Docs, toute l'interface Web et le stockage des documents s'effectue sur vos propres serveurs. Vous gardez donc entièrement la main sur vos données.

Cette suite bureautique 100% européenne comprend un logiciel de traitement de texte, un tableur et un logiciel de présentation. L'éditeur utilise l'élément Canvas du HTML5 et prend en charge les documents OOXML (.docx, .xlsx, .pptx), ainsi que les formats Microsoft Office plus anciens et le format ouvert OpenDocument (.odt, .ods., .odp). ONLYOFFICE Docs propose également de nombreux modules complémentaires, comme Google Traduction, YouTube, un module OCR ou même la messagerie Telegram pour discuter avec ses collaborateurs directement dans l'éditeur.



ONLYOFFICE Docs intègre un éditeur de documents compatible avec les formats Word et OpenOffice © ONLYOFFICE

Un version libre compatible avec ownCloud et NextCloud

Le site d'ONLYOFFICE propose différents connecteurs afin de l'intégrer avec de nombreuses plateformes professionnelles comme NextCloud, ownCloud, Alfresco, Confluence, HumHub, Liferay, SharePoint, Plone, ou encore Nuxeo. Pour le travail collaboratif en temps réel, l'éditeur intègre deux modes de coédition, des fonctions de partage, ainsi que différents outils pour échanger avec ses collaborateurs et suivre leurs modifications. De plus, ONLYOFFICE Docs permet de créer des salles privées pour la collaboration avec une protection par l'algorithme de chiffrement AES-256.

ONLYOFFICE Docs est proposé sous trois formules, à installer sur un ordinateur équipé de Windows Server ou une des nombreuses distributions Linux. L'édition Community est gratuite pour une utilisation personnelle, distribuée sous licence libre GNU AGPL v.3. Cette version accepte jusqu'à 20 utilisateurs simultanément et propose quasiment toutes les fonctions des autres éditions, excepté l'éditeur Web mobile, la comparaison de documents et l'affichage tableau.