# Nos Carnets de Secrets

L’URL d’accès est: <https://secrets-sportes-fr.appspot.com>

***Attention***: c’est **https** et non http, l’URL non sécurisée ne fonctionne pas.

L’application “offline” se charge automatiquement lors du premier appel à Internet et peut donc être ensuite utilisée sans connexion Internet. Normalement à chaque connexion sur Internet, si une nouvelle version existe elle est rechargée automatiquement.

Sur smart-phone, il suffit de créer un raccourci qui apparaîtra comme une application locale (mais ça n’en n’est pas une).

## Principes

##### Carnets

Chaque carnet de secrets est identifié par un nom “long” comportant,

* un ***préfixe***, par exemple daniel.sportes.fr
* suivi d’un ***nom*** (court), par exemple Banques.

##### Secrets d’un carnet

Chaque carnet contient plusieurs secrets, chacun identifié par un nom unique dans son carnet (exemple: ING dans le carnet Banques). Un secret a un texte (en général pas très long) **toujours crypté par une clé** que seuls le ou les propriétaires du carnet connaissent.

##### Clé d’un carnet

Un carnet a une **clé** indispensable pour crypter / décrypter le texte des secrets et en afficher et éditer le contenu. C’est une phrase ou un mot de 1 à 100 caractères comme par exemple “tom et jerry” qui n’est stockée nulle part en clair et doit être fournie à chaque ouverture du carnet sur un poste ou un mobile: en cas d’oubli le contenu du carnet est définitivement illisible.

Il faut être capable de vérifier qu’une clé fournie pour décrypter les secrets est bien celle qui a servi à les crypter. Il n’est pas question de stocker “en clair” cette clé pour d’évidentes raisons de confidentialité: on stocke le “**digest MD5**” de cette clé qui est un code calculé (par le procédé de calcul dit MD5) depuis celle-ci tel que deux clés différentes donnent toujours deux digests différents (en simplifiant) et tel qu’il est impossible de retrouver la clé depuis son digest.

##### Phrase d’aide

Une **phrase d’aide** facultative peut être enregistrée dans le carnet pour aider le ou les propriétaires à retrouver la clé, par exemple “chat et souris”.

**Le préfixe / nom, la clé et la phrase d’aide sont donnés à la création du carnet et ne peuvent plus être changés ultérieurement.** Toutefois le carnet peut être cloné en un autre ayant des nom, clé et phrase d’aide différents.

##### Carnet vivant ou archivé

Tant qu’un carnet est vivant les secrets peuvent y être ajoutés, modifiés, supprimés.

Un carnet vivant ne peut pas être supprimé.

Un carnet vivant peut être archivé: une fois dans cet état il ne peut plus être modifié, il ne peut plus qu’être lu ni rendu vivant à nouveau, mais après 10 jours au moins passé dans cet état il peut être supprimé (c’est une opération définitivement irréversible).

##### Exemplaires “nuage” et “locaux” d’un carnet

Un carnet peut être stocké en plusieurs exemplaires:

* un exemplaire (au plus) sur le “**nuage**” qui n’est pas obligatoire mais permet de retrouver ses secrets depuis n’importe quel appareil connecté à Internet, mobile ou poste de travail. Pour consulter ou mettre à jour cet exemplaire il faut être connecté à internet. Cet exemplaire s’auto-détruit au bout de quelques années après le dernier accès, ou sur volonté explicite de toute personne ayant la clé après au moins 10 jours passés en état archivé, ou sur demande d’urgence à l’administrateur;
* un exemplaire “**local**” sur chaque mobile ou session d’un poste de travail où il a été souhaité d’en stocker un. Le nom d’une session d’un PC ou d’un mobile (**PC-fixe-daniel**, **iphone-domi, inconnu** …) est fixé par son propriétaire (ou laissé à inconnu): il permet de savoir ***d’où*** a été éditée la dernière mise à jour d’un secret (ou d’où a été effectuée la dernière ouverture de l’exemplaire sur le nuage). Pour consulter ou mettre à jour les exemplaires locaux il n’est pas nécessaire d’être connecté à internet.

*Remarque*: il est possible sur n’importe quel appareil (le mobile d’un ami, un poste dans un cybercafé) de lire l’exemplaire sur le nuage sans laisser la moindre trace permanente sur cet appareil. Un exemplaire “local” n’est à déclarer que sur les appareils choisis par le propriétaire d’un carnet (ses appareils ou ceux de proches qui l’acceptent).

##### Sécurité sur le nuage

Un poste de travail est sécurisé par l’obligation d’ouvrir une session en fournissant un mot de passe.

Un mobile est protégé par un code de verrouillage.

**Sur le nuage les “préfixes” des noms de carnet sont protégés par un code PIN:**

* l’enregistrement initial du code PIN associé à un préfixe est fait par l’administrateur du nuage à qui il faut donner le préfixe souhaité et le digest MD5 du code PIN choisi (donc l’administrateur ne peut pas connaître ce code);
* les carnets dont le nom commence par “/” peuvent être listés sans connaître le code PIN et lus à condition bien entendu d’en fournir la bonne clé: il est donc possible que certains carnets d’un préfixe donné soient rendus lisibles à des “invités” qui pourront les lire (en leur donnant la clé) mais pas les modifier (car ils n’ont pas le code PIN du préfixe);
* le code PIN d’un préfixe,est requis pour:
  + obtenir la liste de tous les carnets ayant ce préfixe et pas seulement ceux dont le nom commence par “/”;
  + modifier un carnet ayant ce préfixe (ajouter des secrets, les supprimer, en modifier le texte);
  + déclarer un carnet archivé;
  + supprimer un carnet.

##### Synthèse, contenu mémorisé d’un carnet:

Un carnet de secrets a donc les informations suivantes:

* une **entête** qui ne change pas au cours de la vie du carnet, de sa création à sa suppression:
  + son **préfixe** et son **nom**
  + le digest **MD5** de sa clé;
  + la **phrase** d’aide (facultative) qui aide à retrouver la clé (voire le code PIN);
* la date et heure de ***création*** et l’identifiant du **poste / mobile** (s’il est connu) d’où cette création à été faite;
* la date et heure de ***dernière mise à jour d’un secret*** et l’identifiant du **poste / mobile** (s’il est connu) d’où a été effectuée cette mise à jour. Pour un carnet archivé c’est la date de son archivage;
* une **liste de secrets**, chaque secret comportant:
  + son **nom** unique dans le carnet,
  + la **date et heure** de sa dernière mise à jour et l’identifiant du **poste / mobile** (s’il est connu) d’où a été effectuée cette mise à jour;
  + son **texte crypté** par la clé (donc illisible tant que la bonne clé n’est pas fournie). Lorsque ce texte est vide c’est que le secret correspondant a été “récemment” supprimé, information gardée pour garantir les synchronisations (voir plus loin). Toutefois au bout de deux ans ou lors de l’archivage le secret n’est plus considéré comme “récemment” supprimé et est physiquement effacé pour libérer de l’espace.

En conséquence même si le texte d’un carnet de secrets est intercepté sur le réseau ou extrait d’un serveur, d’un poste de travail ou d’un mobile par des personnes ne connaissant pas la clé, il est impossible d’en lire les secrets ou la clé (sauf à disposer des moyens d’un état riche et de beaucoup d’argent pour “casser” les codes).

## Actions sur les carnets

##### Ouverture d’un carnet local ou sur le nuage

La liste des carnets, vivants ou archivés, sur l’appareil ou sur le nuage, est proposée pour un préfixe donné afin de faciliter le choix. Sur le nuage il faut donner le (bon) code PIN pour avoir la liste complète sinon seuls ceux “accessibles en lecture aux invités” dont le nom commence par “/” sont listés. Il suffit de sélectionner celui souhaité et de donner sa clé:

* le carnet peut toujours être lu (la clé suffit);
* un carnet local peut toujours être édité (sauf s’il est archivé) et supprimé.
* sur le nuage le carnet ne peut être édité, archivé ou supprimé que si le code PIN est donné.

A un instant donné sur un mobile ou une session d’un PC un seul carnet peut être ouvert.

Pour ouvrir un carnet et accéder à ses secrets il faut fournir sa clé. Toutefois si cette clé est strictement égale à la phrase d’aide (ce qui ne protège pas grand chose), le carnet est ouvert sans demander la clé. Ceci permet d’accéder plus vite à des notes ou listes de courses n’ayant pas de caractère confidentiel en sautant la phase de frappe de la clé.

##### Création d’un nouveau carnet sur le nuage

Pour un préfixe donné il faut fournir le code PIN associé et la création d’un carnet sur le nuage peut être effectuée:

* ***soit en créant un carnet vide*** en spécifiant obligatoirement un nom inconnu sur le nuage et une clé, facultativement une phrase d’aide: il devient le carnet courant;
* ***soit par synchronisation depuis le carnet actuellement ouvert localement*** (s’il n’en existe pas un sur le nuage ayant déjà ce nom): la clé et la phrase d’aide du carnet créé sont inchangés et les secrets du carnet local sont recopiés sur celui qui vient d’être créé sur le nuage;
* ***soit en clonant le carnet sur le nuage actuellement ouvert*** en lui donnant un nouveau nom, une nouvelle clé et si souhaité une phrase d’aide. Les secrets du carnet sur le nuage actuellement ouvert sont recopiés sur celui qui vient d’être créé qui devient le carnet actuellement ouvert.

Les carnets ainsi créés sont toujours **vivants**, même par clonage ou synchronisation d’un carnet archivé.

##### Création d’un nouveau carnet local

Pour un préfixe donné, la création d’un carnet local peut être effectuée:

* ***soit en créant un carnet vide*** en spécifiant obligatoirement un nom inconnu localement, une clé et facultativement une phrase d’aide;
* ***soit par synchronisation depuis le carnet actuellement ouvert sur le nuage*** (s’il n’en existe pas un local ayant déjà ce nom): la clé et la phrase d’aide du carnet créé sont inchangés et les secrets du carnet sur le nuage sont recopiés sur celui qui vient d’être créé en local;
* ***soit en clonant le carnet local actuellement ouvert*** en lui donnant un nouveau nom: la clé et si souhaité la phrase d’aide peuvent être différents puis les secrets du carnet local actuellement ouvert sont recopiés sur celui qui vient d’être créé localement qui devient le carnet actuellement ouvert.

Les carnets ainsi créés sont toujours **vivants**, même par clonage ou synchronisation d’un carnet archivé.

##### Édition d’un secret du carnet ouvert

Sur le nuage il faut disposer du bon code PIN associé au préfixe du carnet.

Le carnet ne doit pas être archivé.

Il est possible d’ajouter un nouveau secret, d’éditer le texte du secret (le changer) et de supprimer un secret en lui donnant un texte vide.

##### Archivage d’un secret du carnet ouvert

Sur le nuage il faut disposer du bon code PIN associé au préfixe du carnet.

Le carnet ne peut plus être modifié.

##### Suppression du carnet ouvert

Sur le nuage il faut disposer du code PIN associé au préfixe du carnet.

Le carnet doit être archivé depuis plus de 10 jours. Sinon en cas d’urgence il faut demander à l’administrateur.

*Remarque*: supprimer un carnet local ne supprime pas le carnet nuage de même nom (et réciproquement).

##### Synchronisation entre un exemplaire local et celui du nuage

Un exemplaire local (respectivement sur le nuage) est ouvert: ses préfixe, nom, clé et statut vivant / archivé sont connus. Synchroniser cet exemplaire avec celui du nuage (respectivement local) nécessite a minima que ***les deux exemplaires aient les mêmes préfixe, nom et clé; le (bon) code PIN du préfixe sur le nuage est requis, sinon l’exemplaire sur le nuage ne recevra pas les mises à jours en provenance du local***:

* Chaque secret dont la mise à jour est la plus récente est reporté dans l’exemplaire dont la mise à jour est plus ancienne.
* Les secrets connus dans A et inconnu dans B sont ajoutés dans B;.
* Les secrets récemment supprimés (dont le texte est vide) dans A mais existants (non vide) dans B y sont supprimés sauf s’ils y ont été mis à jour postérieurement à la date de suppression dans A auquel cas ils sont recréés dans A.

La synchronisation s’effectue:

* dans les deux sens (mises à jour réciproques) si le code PIN du préfixe sur le nuage est donné et qu’ils sont vivants (non archivés);
* dans un seul sens (mise à jour de l’un mais pas de l’autre) si l’un des exemplaires est archivé ou pour celui du nuage si son (bon) code PIN n’a pas été donné;
* dans aucun sens si les deux sont en lecture seule (archivés ou sans code PIN correct).

Pour chaque secret il est tracé dans quel sens la synchronisation a été effectuée en affichant les dates de dernières modifications respectives.

*Remarque* : la synchronisation exige donc l’existence de l’exemplaire sur le nuage et ne peut s’opérer qu’en disposant d’une connexion Internet.

* En général l’exemplaire sur le nuage est créé en premier, les exemplaires locaux l’étant par synchronisation avec celui sur le nuage.
* Il est possible d’avoir plusieurs exemplaires locaux, puis de créer ensuite l’exemplaire sur le nuage par synchronisation.
* Il est aussi possible d’archiver puis de détruire l’exemplaire sur le nuage après avoir synchronisé les exemplaires locaux.

## Espaces Locaux, postes / sessions / browsers

***Pour un téléphone mobile*** il n’y a par principe qu’un seul utilisateur: le propriétaire de l’appareil. ***Il n’y a qu’un seul “espace de stockage local”*** sur ces appareils qu’il est conseillé de nommer (par exemple iphone-Domi).

***Pour un poste de travail:***

* il peut y avoir plusieurs utilisateurs (plusieurs sessions sous *Windows* par exemple);
* il peut aussi y avoir plusieurs browsers: *Chrome, Firefox, Internet Explorer*;

Ceci définit potentiellement ***autant d’espaces de stockage locaux qu’il y a de couples utilisateur / browser***. Il est souhaitable de donner un nom à chacun des couples utilisés.

*Remarque*: pour un utilisateur Daniel par exemple sur un poste les espaces de stockage locaux *Chrome* et *Firefox* sont totalement étanches, l’un ignore tout de l’autre. De même sous *Chrome* l’espace de stockage local de l’utilisateur Daniel ignore tout de l’existence d’un éventuel espace de stockage local de l’utilisateur Dominique.

C’est vrai à plus forte raison entre des postes de travail différents.

Pour identifier d’où ont été effectuées les création, accès et mises à jour, il est proposé de donner un nom simple à chaque espace de stockage local (mais ce n’est pas obligatoire).

### Mémorisation locale des données d’identification

Afin d’éviter de frapper à chaque fois le nom du poste / session et le préfixe, il est possible de cocher la case demandant à mémoriser sur ce poste (pour cet utilisateur) ces identifiants : ainsi au prochain lancement ces codes s’affichent pré remplis à l’ouverture. C’est à éviter sur un poste public (cybercafé ou poste partagé).

De même le code PIN peut aussi être mémorisé localement sur le poste (en fait son MD5, pas le code lui-même) en cochant une case: ceci évite de le frapper. Toujours à éviter sur un poste public ou si une personne inconnue peut accéder à votre session.

## Administrateurs du nuage

Ils sont déclarés par le développeur de l’application et ont des possibilités restreintes:

* ***lister les préfixes existants*** (mais leurs codes PIN ne sont pas lisibles);
* ***déclarer un nouveau préfixe***: pour cela il faut leur donner le digest MD5 du code PIN choisi (et NON le code PIN lui-même) ce qui s’affiche dans la page à la saisie d’un code PIN;
* ***changer le code PIN d’un préfixe existant*** (en donnant le digest MD5 du nouveau code);
* ***lister les carnets existants d’un préfixe***, leurs dates de création, accès, modification et le statut archivé / vivant mais pas leurs secrets (qui d’ailleurs ne sont pas lisibles sans la clé);
* ***détruire brutalement un carnet existant*** sur demande urgente du propriétaire ou des autorités légales (identifiés comme tels).

Les administrateurs ne peuvent pas lire les codes PIN ou les clés, ni changer les clés, ni lire ni changer les secrets puisqu’il faut connaître les clés en clair pour cela et qu’elles ne sont notées que dans les mémoires des propriétaires.

A la limite les administrateurs peuvent “détruire” des carnets ou les rendre inaccessibles (ce qui peut être légalement requis).

## Informations techniques

Les sources de l’application sont hébergés par *Google Project Hosting* sous licence **GNU GPL v3** (open source): <https://code.google.com/p/secrets-sportes-fr/>

##### Browsers et OS supportés

Sur les postes et smart-phone l’application locale est de l’HTML 5 / CSS 3 / Javascript totalement standards W3C.

A priori l’application fonctionne donc sur tous les browsers récents: ***Chrome, Firefox, Safari (sur iphone aussi) et Internet Explorer (à partir de 8)***.

En mode offline déconnecté d’Internet, Internet Explorer, 9 compris, ne fonctionne pas.

Le plus rapide est Chrome (basé sur WebKit).

A priori il n’y a pas de dépendance vis à vis de l’OS car c’est une application Web HTML5 / CSS3 / Javascript (la vraie dépendance est vis à vis du browser).

* Windows (a priori depuis XP, Vista et 7 surement);
* MasOS: a priori oui mais pas testé;
* iphone et Android (à tester).

##### Support sur le nuage

C’est une une application Web (HTTPS) Google App Engine écrite en Java.

##### Confidentialité

Le texte crypté d’un secret pourrait être obtenu sur un poste local en étant un peu hacker et en sachant coder … mais il restera ensuite à disposer des moyens informatiques et financiers considérables pour casser un code AES à 256 bits. Obtenir ces textes cryptés demande donc un effort parfaitement inutile.