IRONKEY

Importé en
France par: HERMITAGE Solutions

Présentation de Ironkey

Alain Takahashi, Hermitage Solutions
www.hermitagesolutions.com

HI-SPEED USB

FIPS VALIDATED 140-2

WATERPROOF MIL-STD-810F

RoHS Compliant

Importé en
France par:

A propos de Hermitage Solutions:

Depuis 2002, importateur et distributeur de solutions pour la sécurité et les réseaux: PGP, Clearswift MIMEsweeper, phion, Astaro, Array Networks, Code Green Networks, OpenTrust …

A propos de Ironkey:

Société américaine à capitaux privés basée à Los Altos en Californie, fondée en 2005 avec des fonds de développement du DHS (= Oséo en France).

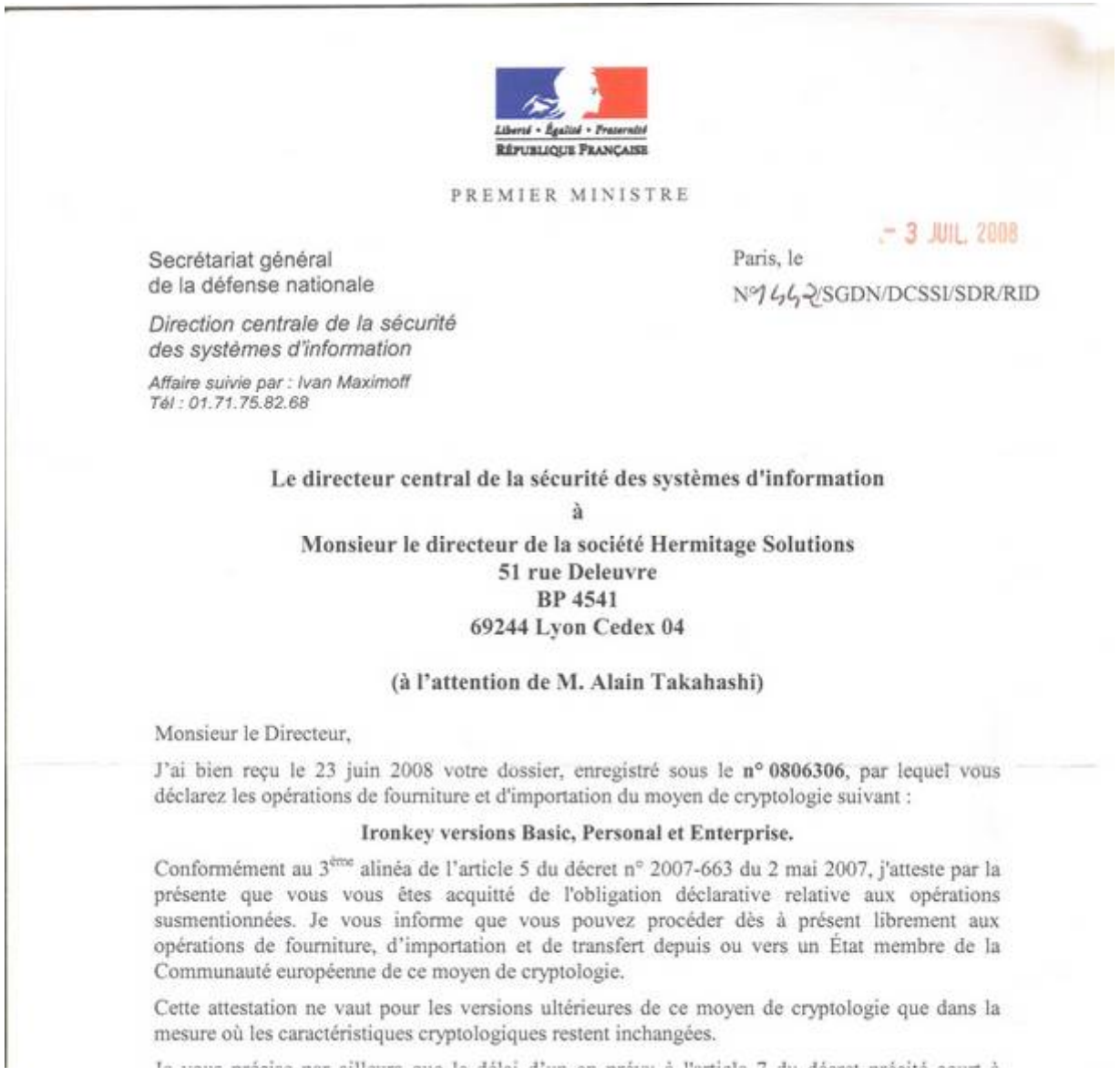
Président: Bill Evans (ancien Président de Intuit et de Paypal, membre du CA de RSA)

CEO: Dave Jevans (ancien VP de Tumbleweed et Valicert, président du consortium anti-phishing APWG www.antiphishing.org)

IRONKEY

Importé en France par: HERMITAGE Solutions

Importation conforme à la législation sur les moyens de cryptologie:



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général
de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Affaire suivie par : Ivan Maximoff
Tél : 01.71.75.82.68

Paris, le - 3 JUIL. 2008

N°1642/SGDN/DCSSI/SDR/RID

Le directeur central de la sécurité des systèmes d'information
à
Monsieur le directeur de la société Hermitage Solutions
51 rue Deleuvre
BP 4541
69244 Lyon Cedex 04

(à l'attention de M. Alain Takahashi)

Monsieur le Directeur,

J'ai bien reçu le 23 juin 2008 votre dossier, enregistré sous le **n° 0806306**, par lequel vous déclarez les opérations de fourniture et d'importation du moyen de cryptologie suivant :

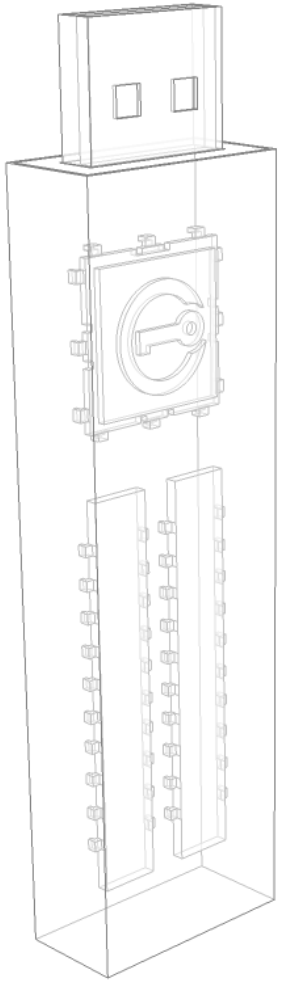
Ironkey versions Basic, Personal et Enterprise.

Conformément au 3ème alinéa de l'article 5 du décret n° 2007-663 du 2 mai 2007, j'atteste par la présente que vous vous êtes acquitté de l'obligation déclarative relative aux opérations susmentionnées. Je vous informe que vous pouvez procéder dès à présent librement aux opérations de fourniture, d'importation et de transfert depuis ou vers un État membre de la Communauté européenne de ce moyen de cryptologie.

Cette attestation ne vaut pour les versions ultérieures de ce moyen de cryptologie que dans la mesure où les caractéristiques cryptologiques restent inchangées.

IRONKEY

Importé en
France par: HERMITAGE Solutions



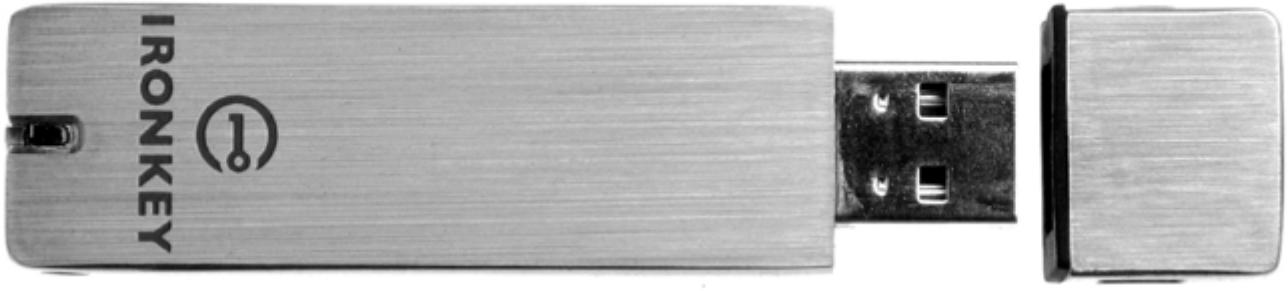
Ironkey est une gamme de clefs USB de stockage sécurisé (1, 2, 4, 8 Go.) de conception et de fabrication américaine, le seul du marché qui combine ces critères:

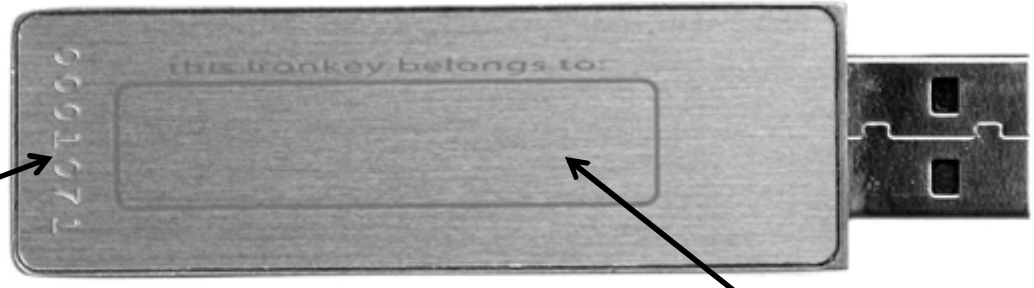
- Certifié FIPS 140-2 (niveau 3 sur certain critères)
- Certifié MIL-STD-810F (résistance aux éléments)
- Compatible PKCS#11, RSA et OATH
- En option: déployable et administrable à distance
- Ne nécessitant pas l'installation de logiciels ou pilotes
- Ne nécessitant pas de droits administrateur sur l'ordinateur
- Dont les données sécurisées sont accessibles sous Windows, Linux et Mac OS X
- Dont les données sécurisées peuvent être sauvegardées localement en restant chiffrées
- Disposant d'un mécanisme d'autodestruction électronique en cas d'effraction, qui peut même être déclenché à distance

IRONKEY

Importé en
France par: HERMITAGE Solutions

Vue extérieure





No. de série:

Espace de gravure

Vue intérieure: composants noyés
dans une résine époxy friable

IRONKEY

Importé en France par: HERMITAGE Solutions

Résumé du rapport de certification FIPS d'Ironkey (3 avril 2008):

The cryptographic module meets the overall requirements applicable to Level 2 security of FIPS 140-2.

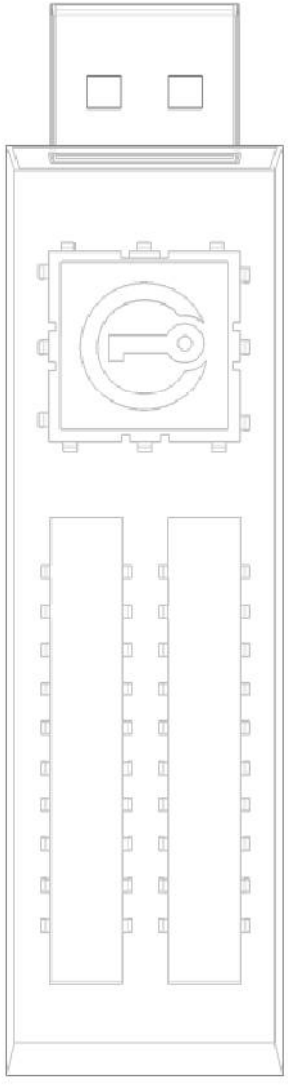
Table 1 - Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module Specification	3
Module Ports and Interfaces	3
Roles, Services and Authentication	3
Finite State Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	3
EMI/EMC	3
Self-Tests	2
Design Assurance	3
Mitigation of Other Attacks	N/A

Source: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2008.htm

IRONKEY

Importé en France par: HERMITAGE Solutions



Technologies de chiffrement:

- Authentification & signature: clef RSA 2048 bits préinstallée
- Contrôle d'intégrité (chiffrement du mot de passe): SHA2 256 bits
- Et l'aspect le plus original de Ironkey sur ces sujets: le chiffrement des données se fait avec une clef aléatoire AES 128 bits en mode CBC (« Chained Block Cypher »)

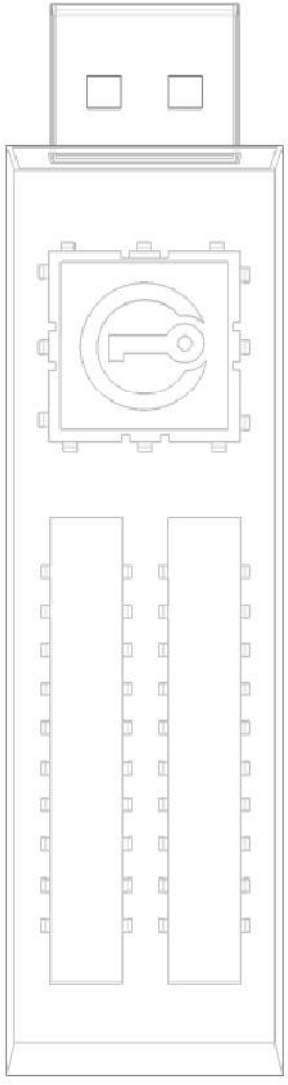
Il existe cinq modes opératoires de AES: Cipher Block Chaining (CBC), Electronic Code Book (ECB), Cipher Feedback (CFB), Output Feedback (OFB), et Counter (CTR).

La plupart des offres du marché utilisent le mode ECB, plus facile à mettre en oeuvre sur des solutions matérielles embarquées. Ironkey a choisi le mode CBC, plus complexe à mettre en oeuvre mais permettant d'affirmer que AES 128 bits CBC est plus sûr que AES 256 bits en mode ECB, mais le marketing des concurrents ne retient parfois que le nombre de bits …

(Sur les modes opératoires AES: http://csrc.nist.gov/publications/fips/fips81/fips81.htm)

IRONKEY

Importé en
France par: HERMITAGE Solutions



Mémoire vive:

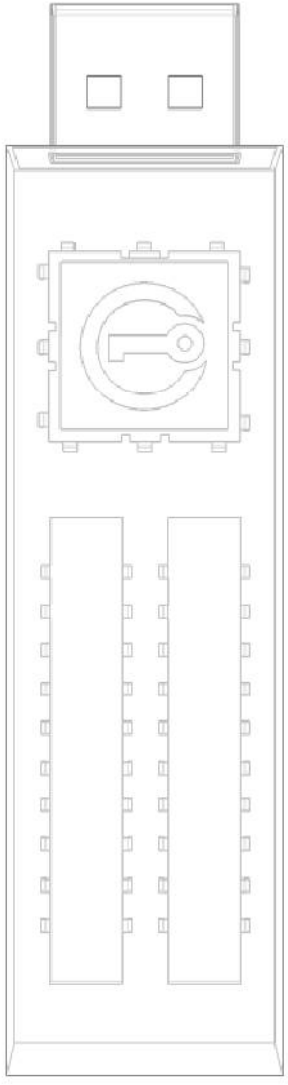
Ironkey utilise la mémoire flash « SLC » ou single-level cell

SLC (« single-level cell »): un bit stocké par cellule de transistor
- inconvénient: coûteux à fabriquer
- avantages: plus rapides (20-30 Mbit/sec, demande moins de courant électrique et plus résilient (env. 100.000 cycles d'écriture)

MLC (« multi-level cell »): plusieurs bits, 3 ou plus, stockés dans chaque cellule de transistor, les différents niveaux de charge électrique permettant de distinguer les bits entre eux.
- avantage: peu coûteux à fabriquer comparé à SLC
- inconvénients: vitesse de commutation beaucoup plus lent, consommation électrique élevée, et durée de vie plus court (env. 5-10.000 cycles d'écriture)

IRONKEY

Importé en
France par: HERMITAGE Solutions



Autodestruction:

Pour prévenir une attaque de type « force brute » ou « attaque du dictionnaire », à compter de 10 saisies de mots de passe incorrects (paramétrable pour la version Enterprise), la clef lance une procédure de destruction des clefs de chiffrement ainsi que des données.

Il n'y a aucune possibilité de récupération après autodestruction.

IRONKEY

Importé en France par: HERMITAGE Solutions

Ci-dessus: première cause de mortalité des clefs de stockage USB

Ironkey est conforme à la norme MIL-STD-810F (résistance à l'environnement):

- Températures de fonctionnement de – 40° à +85°*(« clef oubliée dans la boîte à gants»)*

- Résistance aux chocs de 16G *(« clef tombant sur le quai du métro »)*

- Imperméable *(«clef oubliée dans le pantalon qui part dans le lave-linge »)*

A noter: cette norme n'est pas exclusivement américaine, elle a été conçue en coopération avec le Canada et la France (Laboratoire de Recherches Balistiques et Aérodynamiques du Ministère de la Défense).

Source: http://www.dtc.army.mil/navigator/

WATERPROOF MIL-STD-810F

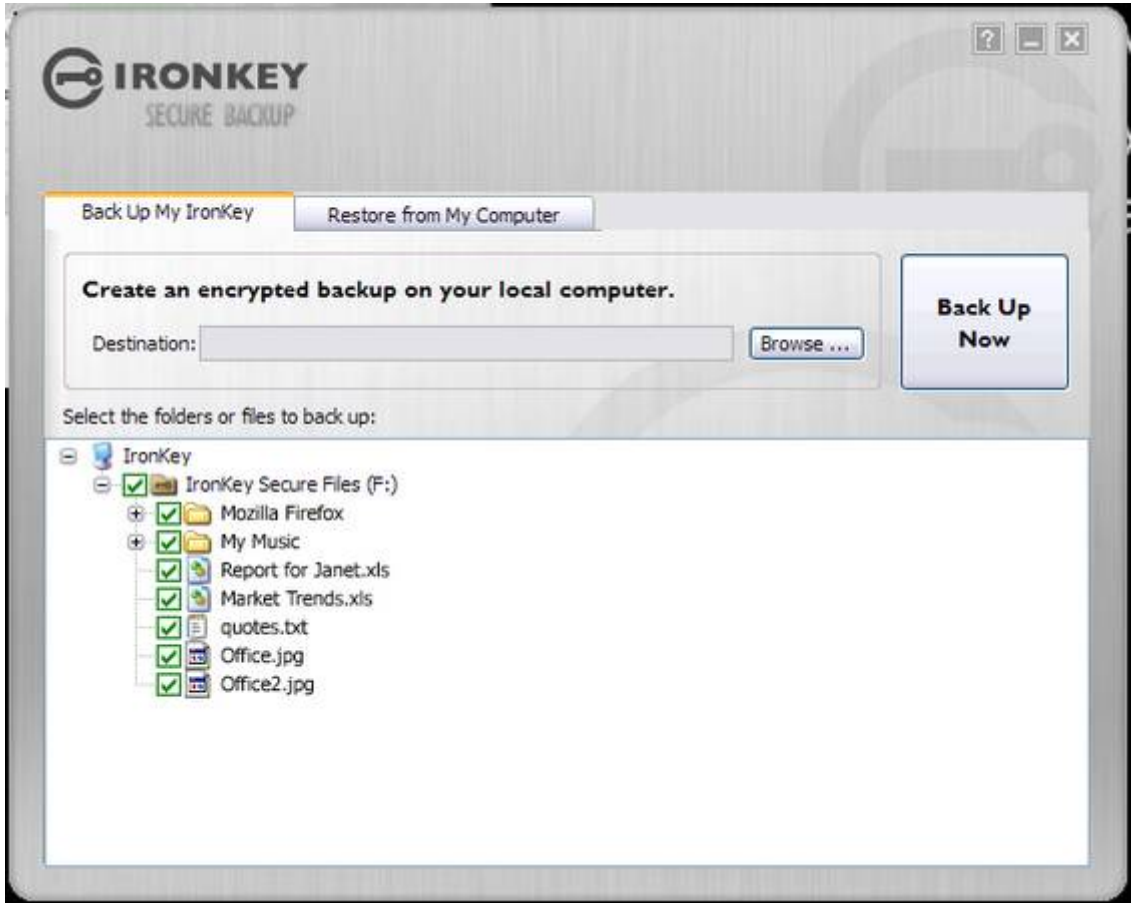
Importé en
France par:

Gestion de la clef au moyen d’un interface utilisateur

IRONKEY

Importé en
France par: HERMITAGE Solutions

Tous les modèles de clefs Ironkey proposent la sauvegarde locale chiffrée (et pas sur Internet). En cas de perte ou vol de la clef, en quelques clics on restaure ses données sur une nouvelle clef.



Importé en
France par:

Les mises à jour peuvent être téléchargées à distance de manière chiffrée

IRONKEY

Importé en
France par: HERMITAGE Solutions

Ironkey, c'est une clef et trois modèles:

Fonctions de stockage sécurisé et de sauvegarde local pour Windows (2000, XP, Vista), Mac OS X et Linux

BASIC + navigateur embarqué, navigation sécurisée, gestionnaire de mots de passe, services de gestion à distance de la clef, services PKCS#11 et OATH…

PERSONAL + gestion et déploiement à distance, multi-utilisateur, déploiement d'applications portables, configuration des politiques de sécurité…

NB: Sous Mac OS X et Linux, les fonctions avancées ne sont pas encore disponibles.

IRONKEY

Importé en
France par: HERMITAGE Solutions

La légende urbaine:

Plusieurs grandes sociétés nous ont rapportés qu'un courriel soi-disant émanant du Ministère de l'Intérieur recommanderait d'éviter d'utiliser Ironkey car il contiendrait un « cheval de troie ».

- Le Ministère de l'Intérieur, contacté à ce sujet, nous a assurés après enquête que rien de tel n'a été émis par aucun service au Ministère,
- Il est possible que quelqu'un ait confondu les fonctions contenues dans « my.ironkey.com » et les fonctions de mises à jour à distance, avec un cheval de troie, dans lequel cas on pourra aussi y cataloguer Windows Update et plusieurs autres services de mise à jour aussi.

IRONKEY

Importé en France par: HERMITAGE Solutions

IronKey Basic 1GB Secure Flash Drive	69,00 €
IronKey Basic 2GB Secure Flash Drive	96,00 €
IronKey Basic 4GB Secure Flash Drive	135,00 €
IronKey Basic 8GB Secure Flash Drive	265,00 €

IronKey Personal 1GB Secure Flash Drive	69,00 €
IronKey Personal 2GB Secure Flash Drive	96,00 €
IronKey Personal 4GB Secure Flash Drive	135,00 €
IronKey Personal 8GB Secure Flash Drive	265,00 €

IronKey Enterprise 1GB Secure Flash Drive	69,00 €
IronKey Enterprise 2GB Secure Flash Drive	96,00 €
IronKey Enterprise 4GB Secure Flash Drive	135,00 €
IronKey Enterprise 8GB Secure Flash Drive	265,00 €
+ obligatoire avec Ironkey Enterprise:	
I Year of Enterprise Managed Service:	21,00 €
2 Years of Enterprise Managed Service:	39,00 €
3 Years of Enterprise Managed Service:	53,00 €

IRONKEY

Importé en France par: HERMITAGE Solutions

Nous vous offrons une Ironkey Basic 1 Go.

Nous effectuons une enquête en ligne à propos du stockage sécurisé, les 15 premières personnes présentes à cette réunion à compléter l'enquête en ligne recevront une clef Ironkey Basic 1 Go.

www.hermitagesolutions.com/sondage Mot de passe: OSSIR

IRONKEY

Importé en France par: HERMITAGE Solutions

Questions ?

www.hermitagesolutions.com/sondage Mot de passe: OSSIR (majuscules)