

**OSSIR**

**DIFENSO**  
JUST BE SAFE

---

*12 septembre 2017*

Protect your Data in the Cloud & respect the legal constraints...

# Notre conviction...



- \* Aujourd'hui, les solutions du marché protègent les services SaaS:
  - ❖ Le transport: Protection du « tuyau » (SSL/TLS-VPN);
  - ❖ Le stockage: Protection du « contenant » (coffre fort);
  - ❖ L'authentification: Garantir l'identité de l'utilisateur (login/mdp, forte 3 facteurs, certificat);
  - ❖ La traçabilité, généralement des accès;
  - ❖ L'analyse des comportements utilisateurs: détection des comportements anormaux ou interdits.
  
- ➔ **Toutes ces mesures de protection sont périphériques à ce qui reste la valeur de l'entreprise : la donnée elle-même.**

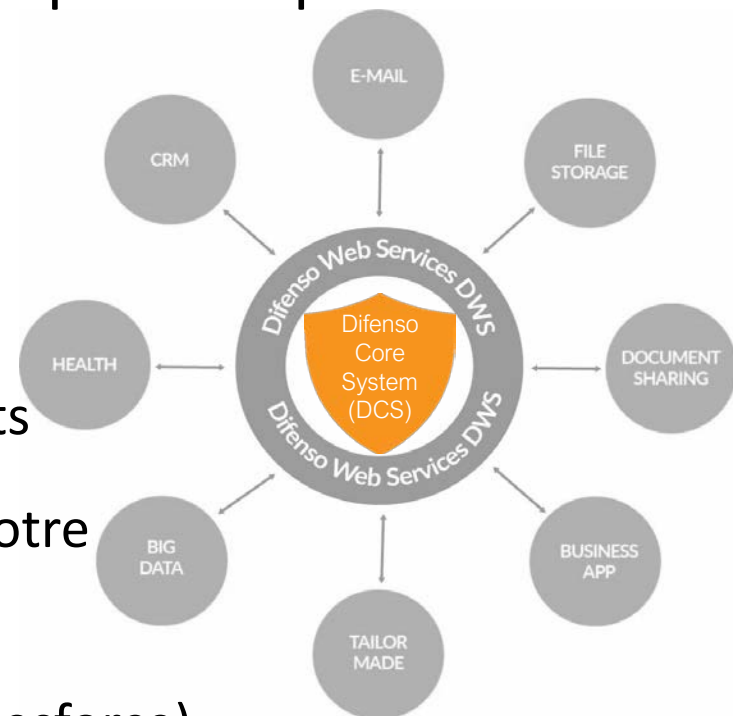
La protection et les mesures de sécurité doivent être apportées **directement sur la donnée**. Cette conviction est renforcée par le nouveau **Règlement Général sur la Protection des Données (RGPD)** qui impose d'ici le 25 mai 2018 notamment le « **droit à l'oubli** » (art.17) et la « **protection de la donnée dès la conception** » (art.25 et 47b)

# Une réponse, notre écosystème...



\* Difenso a développé un écosystème complet composé de:

- ❖ **Difenso Core system:** En charge de toutes les opérations cryptographiques
- ❖ **Difenso Web service:** Seule interface d'échange avec le **Core System**, il est en charge du traitement des appels au web service
- ❖ **Add-In/Plugin & Connecteurs:** Composants dédiés qui portent la protection Difenso au plus près de la donnée à protéger via notre Web Service (services de messageries, de partage de documents mais aussi des applications métier spécifiques de type Salesforce)



Grâce à l'écosystème Difenso, nous sommes en mesure de proposer un éventail complet de solutions : **Techniques** (basées sur le Difenso Web Service) et **Fonctionnelles/Métier** (Add-In/Plugin et Connecteurs)

# Notre Web Service de Chiffrement



- \* **Protège vos données par design et par défaut**
- \* **Fonctionne avec tout types d'applications et tout types de données**
- \* **Facile à intégrer** via des appels normalisés basés sur les technologies du marché
- \* Utilise (via le Difenso Core System) des **algorithmes de chiffrement et de signature considérés comme sûrs**
- \* Chaque clé unique générée aléatoirement en mémoire est dérivée d'une clé maîtresse protégée au sein d'un HSM certifié
- \* Réalise le **contrôle des autorisations** pour chaque donnée chiffrée individuellement
- \* Fournit **une interface d'administration de la protection** de vos données
- \* Fournit une **traçabilité opposable** de l'accès aux clés sur tout le cycle de vie de la donnée



# Les fonctions offertes par notre DWS



## Services de protection et d'accès:

- ❖ Chiffrement
- ❖ Déchiffrement
- ❖ Obtention d'une clé AES et d'un IV

## Services de gestion:

- ❖ Activation/Désactivation d'une clé
- ❖ Activation/Désactivation d'une autorisation
- ❖ Ajouter/Effacer une autorisation
- ❖ Listing des accès à une donnée
- ❖ Description des metadatas associées à une clé

Le DWS est un Webservice permettant la mise à disposition de fonctions de chiffrement/déchiffrement symétrique innovantes certifiées CSPN par l'ANSSI, faciles à mettre en œuvre et répondant aux exigences de protection des données sensibles par design dès leurs création et de droit à l'oubli par inactivation de la clé ayant servi à la chiffrer. Une traçabilité opposable est fournie sur tout le cycle de vie de la donnée par le DWS.

# Communication avec le DWS



L'application appelante doit posséder une bi-clé RSA pour pouvoir communiquer avec le Difenso Web Service (DWS)

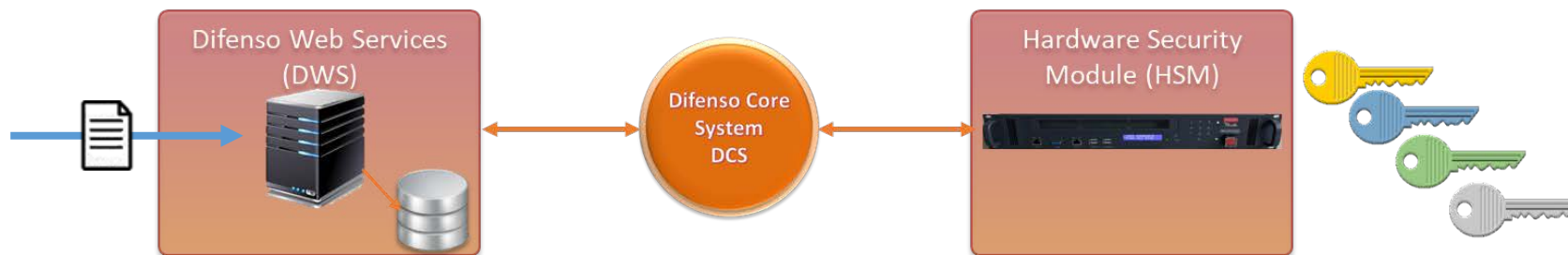
- \* Communication protégée par TLS 1.2
- \* Utilisation du protocole HTTP pour les communications
- \* Utilisation de Json Web Token et/ou Json Web Encryption pour les appels au DWS
  - ❖ **Signature RSA obligatoire de chaque Payload JSON (JWT)**
  - ❖ **Chiffrement RSA OAEP des JWT possible (JWE)**
- \* Les réponses du DWS sont aussi des JWT/JWE

# Protection des données par le DCS



- 1 Le DWS utilise la librairie certifiée DCS pour protéger les données
- 2 3 Génération d'une clé AES 256 par le HSM
- 4 Le DCS génère un IV et Chiffre des données (AES-CBC)
- 5 6 Signature des données chiffrées par le HSM
- 7 8 Signature des metadatas (liste d'autorisation, propriétaire) par le HSM
- 9 10 Signature de la trace de l'action par le HSM
- 11 Stockage des informations techniques

# Accès aux données chiffrées par le DCS



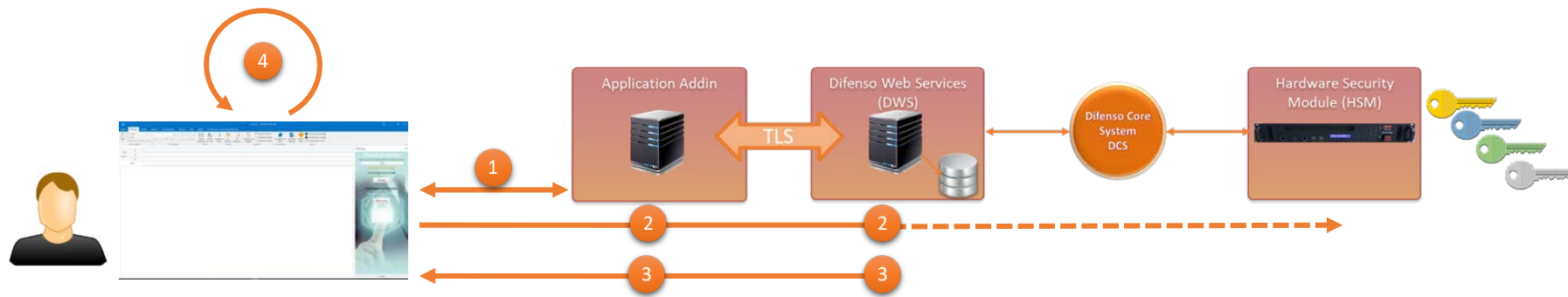
- 1 Le DWS utilise la librairie certifiée DCS pour accéder aux données chiffrées
- 2 Vérification de la signature des données chiffrées par le HSM
- 3 Récupération des metadatas
- 4 Vérification de la signature des metadatas par le HSM
- 5 Génération de la clé AES 256 par le HSM
- 6 Le DCS déchiffre des données (AES-CBC)
- 7 Signature de la trace de l'action par le HSM





- \* L'application peut ajouter des metadatas supplémentaires:
  - ❖ Début/Fin de validité de la donnée chiffrée
  - ❖ Durée de vie de la clé
  - ❖ Activation/Désactivation d'une ou plusieurs clés
  - ❖ Activation/Désactivation d'une autorisation
  - ❖ Règles de sécurité spécifiques .../...
  
- \* L'ensemble de ces metadatas sont vérifiées pendant la phase de déchiffrement

# Cas d'utilisation : l'Add-In Outlook



- 1 L'application Add-In s'occupe de l'authentification de l'utilisateur et de la communication avec le DWS
- 2 L'Add-In fait une demande de génération de clé en précisant les autorisations
- 3 L'Add-In reçoit la clé de chiffrement AES 256 (protégée par une clé de session), un vecteur d'initialisation et de la clé AES 256 chiffrée par le DCS
- 4 L'Add-In chiffre le message avec la clé AES
- 5 L'Add-In envoie le message/fichier chiffré avec la clé AES chiffrée par le DCS

# Difenso for Outlook



Difenso complement for outlook

**Encryption Body and/or attachment**

**Decryption Body and/or attachment**

**Management Key**

Déchiffrement des données

- Déchiffrier le message
- Déchiffrement des fichiers
- Clé d'accès à la liste
- Liste d'autorisation
- Activé la clé
- Désactiver la clé

# DWS: Web Service “On Demand” de protection de données

## Synthèse



### \* Principales caractéristiques

- ❖ Protection robuste des données
- ❖ Facile à implémenter
- ❖ Temps de latence négligeable
- ❖ Les données ne sont ni vues, ni stockées par Difenso
- ❖ Chaque donnée est chiffrée avec une clé unique et aléatoire
- ❖ Infrastructures disponibles en mode SaaS ou « On-Premise »
- ❖ Difenso Core System (DCS) certifié par l'ANSSI

### \* Administration des clés

- ❖ Traçabilité de tous les accès aux clés de chiffrement/déchiffrement
- ❖ Délégation totale de la gestion des clés
- ❖ Contrôle robuste des autorisations
- ❖ Gestion du droit d'en connaître dynamique
- ❖ Activation/désactivation des clés
- ❖ Intégration SOC en mode « On Premise »

Le **Difenso Core Système** cryptographique (DCS) appelé par le DWS utilise les algorithmes les plus robustes du marché et est **certifié CSPN par l'ANSSI** (Agence Nationale de la Sécurité des Systèmes d'Information)

# Difenso for Gmail



The screenshot shows the Gmail web interface. At the top, the browser address bar displays 'Sécurisé | https://mail.google.com/mail/u/1/#inbox'. Below the search bar, the Gmail navigation menu includes 'Principale' and 'Réseaux sociaux'. A 'NOUVEAU MESSAGE' button is visible. The email composition area is active, showing a 'Confidential' status bar and a 'Send Encrypt' button highlighted with a red box. The email body contains the text 'Encryption test body'.

*Email encryption*

*Difenso Plug-in for Gmail*

The screenshot shows the Gmail interface for an incoming email. The email is marked as 'Confidential'. The sender is 'testa test' and the recipient is 'À Jérôme'. A 'Decrypt body' button is highlighted with a red box. Below the button, a message states: '\*This message has been protected. You can read it by acc... \$AAAAJAMxLjA37h1oTVdQGa/Qb+zJJIBhATKLMUTuXG'.

*Email decryption*

# Difenso for File sharing solutions



The screenshot shows the Difenso web interface. At the top, there is a navigation bar with the Difenso logo and a search bar labeled "Search in All Drive". Below this, a row of icons represents various cloud storage providers: OneDrive, Shared, SharePoint, Box, Dropbox, Shared, GoogleDrive, and Shared. A red box highlights these icons with the text "Single point of access to all your drives".

Below the navigation bar, there is a "Local Search" bar and a "Search" button. A red box highlights this search function with the text "Search function".

In the main content area, there is a navigation bar with icons for home, folders, files, and a shield icon labeled "Encrypt files". A red box highlights the shield icon.

Below the navigation bar, there is a table of files. The table has columns for "Nom", "Date", "Taille", "Type", and "Action". The file "GoogleEarthSetup.exe.encrypt" is highlighted with a red box and labeled "1 click decrypt files".

The "Action" column for each file contains icons for delete, refresh, and a key icon. A red box highlights the key icon with the text "Key Activation/deactivation".

1 click  
decrypt  
files

Key  
Activation/deactivation

# Difenso for SharePoint



The screenshot shows the SharePoint interface for 'Secure Difenso'. The top navigation bar includes 'Office 365' and 'SharePoint'. Below it, the 'Accueil' (Home) section features a blue 'SD' logo and the text 'Secure Difenso'. To the right, the text 'File encryption' is displayed. A red box highlights the 'Transfert chiffré' (encrypted transfer) icon in the top right corner of the document list area. The main content area shows a list of documents under the 'Documents' heading, including files like '[Chiffré] DIFENSO\_ANSSI Certification strategy v1.0.pptx.encrypt'.

The screenshot shows the same SharePoint interface, but with a context menu open over a document. The menu options include 'Partager', 'Obtenir un lien', 'Télécharger', 'Supprimer', 'Épingler en haut', 'Déplacer', 'Copier dans', 'Renommer', 'Historique des versions', 'M'avertir', 'Plus', and 'Déchiffrer'. The 'Déchiffrer' option is highlighted with a red box. The text 'File decryption' is written to the right of the menu. The document list in the background shows files like '[Chiffré] DIFENSO\_ANSSI Certification' and '[Chiffré] DWS\_DevGuide-v1.0.pdf.encrypt'.

# Difenso for Office 365

# Difenso for Word Online & Word desktop



Office 365 OneDrive

PARCOURIR FICHIERS BIBLIOTHÈQUE

rechercher dans OneDrive

Documents

Récents

Partagés avec moi

OneDrive @ Infinite Square

## Documents

**Nouveau** Télécharger

Create new document

Word Online

Document17.docx

Word Online

Document17 - Enregistré

Difenso

Log out office 365

### Secure your word document

Encrypt all Documents Encrypt selected

Decrypt all Documents Decrypt selected

Add recipients that could decrypt your document

Recipient email Add

Document - Word

Encrypted data



# Difenso Web Service : “On Demand” protection data web service Administration platform for data protection



**DIFENSO** OUR SOLUTIONS - SERVICES -

HOME ADMIN CENTER KEYS MANAGEMENT razniewski

Name: jerome.razniewski@difenso.com  Owner  Recipient

Begin: jj/mm/aaaa  All the keys

End: jj/mm/aaaa  Active  Disable Document Name: Concerned application:

KeyId	Status	Name	Application	Creation Date	Tag	Expiration Date	Action
<input type="checkbox"/> n3JI EgmMPPiPrc631JJHJ		jerome.razniewski@difenso.com		Nov 14, 2016 11:10		Nov 14, 2017	
<input type="checkbox"/> Ve5SzBsVPCiEuwzIBTurm		jerome.razniewski@difenso.com ON		Nov 14, 2016 11:26		Nov 14, 2017	
<input type="checkbox"/> d5OmdU0Az+VLVc1ATzA4		jerome.razniewski@difenso.com ON		Nov 14, 2016 12:30		Nov 14, 2017	
<input type="checkbox"/> Hw0c9UMoueb7YA2rgBK4		jerome.razniewski@difenso.com ON		Nov 14, 2016 12:30	Nov 14, 2016 12:30	Nov 14, 2017	
<input type="checkbox"/> tB9r7K07RbahVmluhHlSqz		jerome.razniewski@difenso.com ON		Nov 14, 2016 02:48		Nov 14, 2017	
<input type="checkbox"/> KcK4dyzZCbHYaF3M2ER		jerome.razniewski@difenso.com ON		Nov 14, 2016 06:07		Nov 14, 2017	
<input type="checkbox"/> idQLPhLLS3Bxe9JOXgSC		jerome.razniewski@difenso.com ON		Nov 14, 2016 08:16		Nov 14, 2017	
<input type="checkbox"/> T4jg+iv69/4gLOtrFXDAV8		jerome.razniewski@difenso.com ON		Nov 16, 2016 10:59		Nov 16, 2017	
<input type="checkbox"/> i1CVoNfJmqqYL3LRGmi		jerome.razniewski@difenso.com ON		Nov 16, 2016 11:37		Nov 16, 2017	
<input type="checkbox"/> NYg0TTX0BjWT6cs+Cy8		jeromeraz@gmail.com FAILURE.26		Nov 16, 2016 11:05		Nov 16, 2017	
<input type="checkbox"/> peHhpOh85qzH8o+QNoX		jerome.razniewski@difenso.com ON		Nov 16, 2016 11:41		Nov 16, 2017	

# Annexe

## Trace opposable



- \* 2017-03-02 18:05:09 [application-akka.actor.default-dispatcher-7] INFO SECURITY - {
  - ❖ "Version": "1.0",
  - ❖ "Global-ID": "2",
  - ❖ "DCS-ID": "2",
  - ❖ "Id-Mi": "ac1cQp0Plx9WxR9EHo2vIkPhLk5FzoHMP8Z77apQXPY=",
  - ❖ "Date": "2017-03-02T17:05:09.465Z",
  - ❖ "User": "denis.diguet@difenso.com",
  - ❖ "IP": "164.177.56.113",
  - ❖ "Action": "ACCESS DENIED",
  - ❖ "Signature": "2YhX1MziDla+/K50Sus+VjanuoqsWjwN0CmUF6ulMgg="}
- \* 2017-03-02 18:05:56 [application-akka.actor.default-dispatcher-8] INFO SECURITY - {"Version": "1.0", "Global-ID": "3", "DCS-ID": "3", "Id-Mi": "ZkbDrPLxTcHiX7qrz+Yu0NRkibUCqZyHF7FNWLlcyCs=", "Date": "2017-03-02T17:05:56.330Z", "User": "denis.diguet@difenso.com", "IP": "164.177.56.113", "Action": "ACCESS GRANTED", "Signature": "MxSUf2r7HfKEkrsHZw+hHDwkUGPcaEL4kHk3fHei+g="}
- \* 2017-03-02 18:06:51 [application-akka.actor.default-dispatcher-13] INFO SECURITY - {"Version": "1.0", "Global-ID": "4", "DCS-ID": "4", "Id-Mi": "sO8/Cl4GbBtlxjte3JL+jl+67gA7lqsZ8FULAl8nWxQ=", "Date": "2017-03-02T17:06:51.161Z", "User": "denis.diguet@difenso.com", "IP": "10.200.1.10", "Action": "ACCESS GRANTED", "Signature": "UMloG3j3GBCfH3sSk8txHsnaMXiSHgbZz4qV5Qj6OGw="}
- \* 2017-03-02 18:09:17 [application-akka.actor.default-dispatcher-16] INFO SECURITY - {"Version": "1.0", "Global-ID": "5", "DCS-ID": "5", "Id-Mi": "907mXOi19jX+/8s3fqWqBHtmUQEcaMDVZWWDa2YcoaQ=", "Date": "2017-03-02T17:09:17.186Z", "User": "jerome.razniewski@difenso.com", "IP": "164.177.56.113", "Action": "ACCESS GRANTED", "Signature": "/BV7ymOf/04drZHegxE+LfMtJpFqd/avsgNb2ERzvZ4="}



DIFENSO

[www.difenso.com](http://www.difenso.com)