G-Tokenizer™

Solution de tokenisation «Vaultless»

Pour garantir la sécurité des transactions de paiement, les grands systèmes de paiement, American Express, Discover Financial Services, JCB, MasterCard et Visa, ont mis en place le standard de sécurité : Payment Card Industry Data Security Standard (PCI DSS) en 2004 qui a pour objectif de protéger les données porteurs.

- *Protection des données*
- *Sécurité renforcée*
- *Respect du standard PCI DSS*
- *Réduction du périmètre PCI DSS*
- *Diminution des coûts d'audit*

> Tokenisation

Aujourd'hui les acteurs traitant, stockant ou véhiculant des données porteurs, comme les commerces et les organismes de paiement, se voient dans l'obligation de respecter le standard PCI DSS.

La tokenisation est une des méthodes préconisées par PCI DSS pour la protection des données et la réduction du périmètre d'audit. Cette méthode est de plus en plus utilisée pour protéger les données et respecter la réglementation PCI DSS.

Le processus de tokenisation vise à remplacer les numéros de cartes bancaires *(«Primary Account Number» ou PAN)* par une valeur de substitution non sensible, appelée token. Ce token peut conserver toutes les caractéristiques essentielles du PAN tout en garantissant sa sécurité. L'utilisation de tokens permet ainsi de renforcer la sécurité et de répondre aux exigences sécuritaires de PCI DSS liées à la protection du PAN.

Galitt

> G-Tokenizer™

- *Solution «Vaultless» et «Stateless»*
- *Token réversible*
- *Impact minimal sur le SI*
- *Performances élevées*
- *Adaptabilité et évolutivité*
- *Diminution des coûts*
- *Respect des recommandations*

Galitt propose G-tokenizer™, une solution robuste de tokenisation «Vaultless», c'est-à-dire une solution sans stockage des PANs en base de données, qui permet de renforcer la sécurité et de réduire le périmètre de certification conformément aux exigences PCI DSS V3.0 et aux recommandations du «PCI DSS Tokenization Guidelines».

La solution G-tokenizer™ génère des tokens selon des formats variés tout en utilisant des clés cryptographiques différentes et cloisonnées entre elles. La solution est basée sur des mécanismes cryptographiques de type «Format Preserving Encryption» *(FPE)* qui permettent de retrouver le PAN en clair à partir d'un token par la fonction inverse de dé-tokenisation.

Galitt met à disposition un service d'accompagnement à l'intégration de la solution G-tokenizer™ pour minimiser l'impact sur les applications et les systèmes d'information de ses clients.

> Points forts

Impact minimal sur le Système d'Information
Production de tokens de format identique à celui des PANs

Performances élevées
Traitement de gros volumes sous forme de fichiers *(>25M de tokens par fichier)* et sous forme de demandes unitaires *(>6000 tokens/seconde)*

Facilité d'exploitation
Automatisation de la gestion de la solution

Adaptabilité et évolutivité
Evolution et adaptation en fonction des besoins des Systèmes d'Information

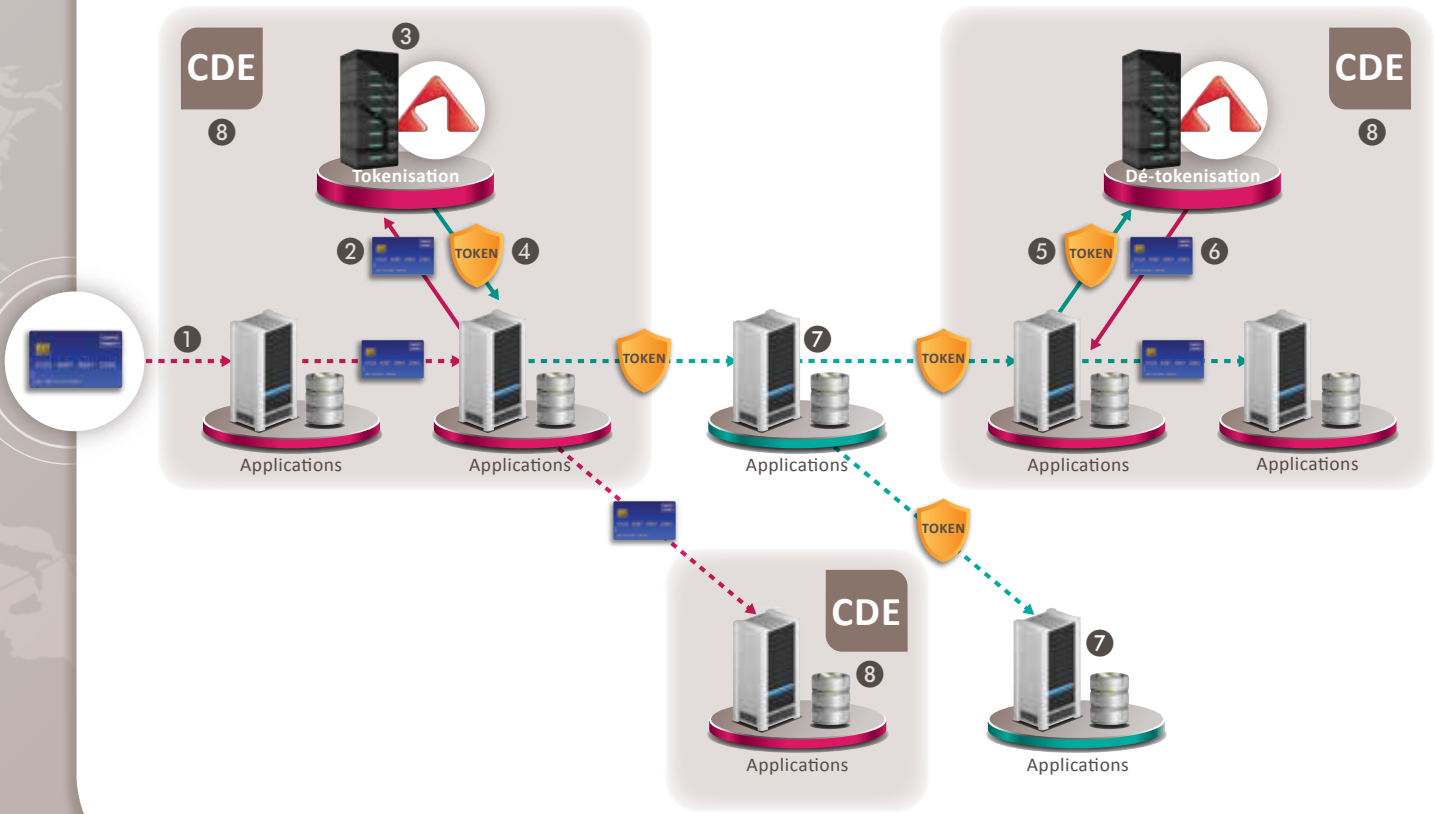
Diminution des coûts d'audit
Réduction au maximum du périmètre PCI DSS en diminuant le nombre d'applications à auditer

Respect des recommandations
Conformité aux recommandations du «PCI DSS Tokenization Guidelines» et du «Visa Best Practices for Tokenization»

Services autour de la tokenisation
Compétences métier, techniques cryptographiques et de sécurité

> Fonctionnement

1. Réception des données sensibles par le SI
2. Demande par le SI, intégrant un mécanisme d'authentification forte, d'un token à la solution G-Tokenizer™
3. Remplacement du PAN par un token.
4. Renvoi du token à l'application demandeuse
5. Inversement, demande par le SI, intégrant un mécanisme d'authentification forte, d'un PAN à la solution G-Tokenizer™
6. Dé-tokenisation et renvoi du PAN à l'application demandeuse
7. Sortie des applications du périmètre PCI DSS
8. Réduction du «Card Data Environment» *(CDE)*



Galitt

> Fonctionnalités

- *Gestion automatique des clés cryptographiques*
- *Haut niveau de sécurité (HSM)*
- *Tokens paramétrables*
- *Tokens multi-usages et multi-sites*
- *Trans-tokenisation*

Gestion automatique des clés cryptographiques
Génération, distribution, renouvellement, activation / désactivation, archivage et suppression des clés de tokenisation

Haute disponibilité
Clusters de serveurs et de HSM répartis sur plusieurs sites

Haut niveau de sécurisation des données
Utilisation de mécanismes cryptographiques implantés dans des enceintes cryptographiques HSM IBM 4765 certifiées FIPS 140-2 niveau 4

Tokens paramétrables
Multiples formats de tokens disponibles *(choix de la partie tronquée du PAN)*

Tokens multi-usages et multi-sites
Gestion sur plusieurs points d'entrée avec attribution du même token pour un PAN donné

Trans-tokenisation
Echange des PANs avec des partenaires de façon sécurisée

> A propos de Galitt

Galitt est un acteur majeur sur les projets PCI et possède toutes les compétences et experts à même d'accompagner ses clients sur les projets d'assistance pour la certification PCI.

Galitt est une «QSA Company» qui dispose de consultants accrédités QSA par PCI SSC.

17 route de la Reine - 92100 Boulogne - France
Tél. : +33 1 77 70 28 00 - Fax : +33 1 77 70 28 23
contact@galitt.com
www.galitt.com

Galitt