

2010

# Livre blanc sur l'authentification forte

## Fonctionnement de l'authentification « One Time Password » et son implémentation avec les solutions actuelles du marché

Dans le contexte actuel où le vol d'identité constitue une menace réelle et sérieuse pour les entreprises, il est vital que celles-ci puissent protéger leurs données numériques de façon satisfaisante pour éviter toute fuite d'information pouvant engendrer des coûts financiers élevés.

Ce document décrit les mesures de protection adéquates permettant de se protéger contre ce type de menace, typiquement par la mise en œuvre de solutions d'authentification forte – authentification à 2 facteurs (ce que je sais et ce que je possède).

Cet article illustrera ce type de contre-mesures à travers les solutions GEMALTO et permettra au lecteur d'appréhender les aspects technologiques mais également les aspects organisationnels et financiers.





## Sommaire

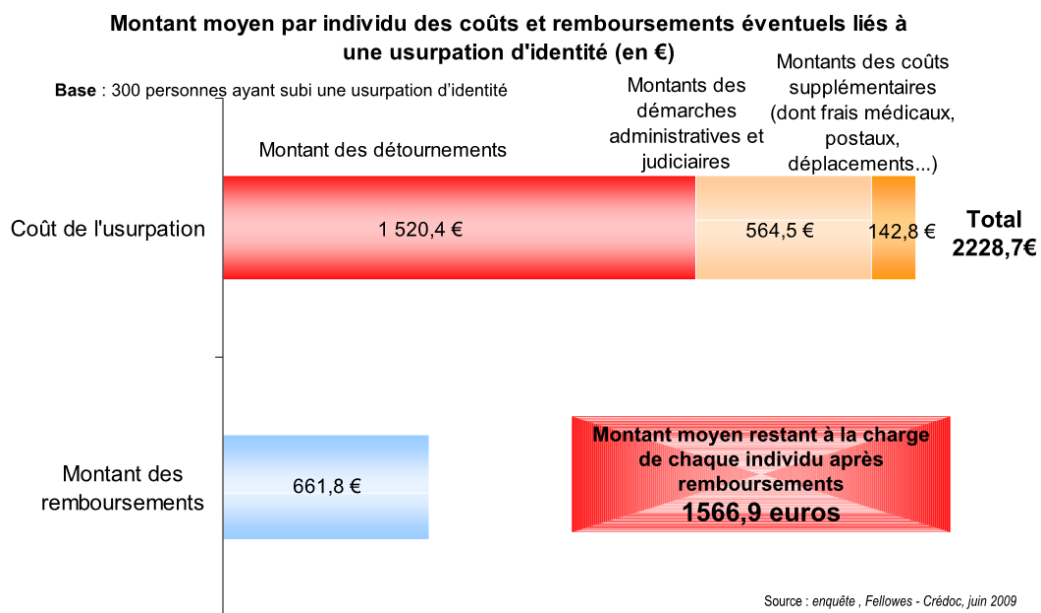
1) Introduction .....	3
2) Pourquoi l'OTP – One Time Password.....	4
a. Les besoins et les usages .....	4
b. Les limitations et freins à l'utilisation de l'OTP .....	5
3) Principe de fonctionnement de l'OTP .....	6
a. OTP ASYNCHRONE.....	6
b. OTP SYNCHRONE .....	7
4) ARCHITECTURE OTP .....	9
a. Architecture de la solution globale – Exemple : accès nomade.....	9
b. Environnement technique.....	9
5) Illustration d'une solution OTP – GEMALTO .....	11
a. Descriptif technique .....	11
b. Maquette.....	13
c. Pré requis techniques pour intégrer la solution OTP .....	15
d. Test réalisés .....	15
6) Aspects financiers.....	16
1) Avantages et inconvénients d'une solution OTP .....	17
a. Avantages .....	17
b. Inconvénients .....	17
2) Conclusion .....	18
3) Bibliographie .....	19
4) Référentiel normatif.....	19



# Livre Blanc - Authentification forte OTP

## 1) Introduction

Le vol d'identité constitue une menace de plus en plus répandue qui dans de nombreux cas, génère beaucoup de perte au niveau financier. Il est difficile pour les entreprises de se protéger contre ce type de fraudes. Par ailleurs dans le monde professionnel, le risque immatériel lié à la perte d'information est en général peu ou pas pris en compte par les gérants d'entreprise. Le constat est similaire au niveau des assurances professionnelles, car elles proposent souvent des dédommagements sur les pertes de bien informatiques matériels. Selon une étude réalisée en juin 2009 par le Credoc, il y a chaque année 210 000 victimes d'usurpation d'identité en France. Le coût moyen pour une victime d'un vol d'identité est d'environ 2229 euros soit 474 millions pour l'ensemble des victimes.



Sources : Credoc [1]

Les solutions d'authentification doivent être choisies en fonction du caractère stratégique et du risque liés aux ressources devant être protégées. Les technologies d'authentification des utilisateurs les plus populaires sont :

- Les systèmes de mots de passe, les dispositifs d'authentification par exemple des tokens USB, des tokens logiciels et des cartes à puce
- La biométrie, les signatures numériques (PKI<sup>1</sup>)

<sup>1</sup> PKI (Public Key Infrastructure) : Infrastructure à clés publiques  
[http://fr.wikipedia.org/wiki/Infrastructure\\_à\\_clés\\_publicques](http://fr.wikipedia.org/wiki/Infrastructure_à_clés_publicques)



## 2) Pourquoi l'OTP – One Time Password

Pour se protéger de l'usurpation d'identité, les entreprises ont recours à des techniques d'authentification à 2 facteurs - « ce que je sais et ce que je possède ». Parmi ces techniques existent les solutions d'authentification forte telles que le « One Time Password » – OTP, déjà existant dans les grandes organisations. Les PME peuvent désormais accéder à cette solution avec des produits financièrement accessibles et présentant une simplicité de mise en œuvre.

### a. Les besoins et les usages

Dans un contexte où les entreprises s'ouvrent de plus en plus au monde extérieur, les besoins en sécurité deviennent de plus en plus importants. Afin d'éviter le vol d'identité des utilisateurs, les organisations ont recours à des solutions d'authentification forte tel que le « One Time Password ». L'usage du « One Time Password » pour les entreprises prend tout son intérêt dès lors que des ressources internes (applications, fichiers, etc.) doivent être partagées avec le monde extérieur.

Les exemples les plus flagrants s'articulent autour du nomadisme. Ainsi l'OTP conviendra parfaitement aux commerciaux en déplacement se connectant depuis un réseau non sécurisé (hot spot, cybercafé, etc.) ou aux personnes adeptes du télétravail.

L'OTP s'applique aussi aux entreprises faisant appel à des structures d'infogérance telles que les sociétés de télémaintenance. Ne pouvant impliquer une confiance absolue en la personne intervenant à distance, l'usage de l'OTP garantit qu'un intervenant ne pourra s'authentifier qu'une seule fois avec le mot de passe qui lui a été fourni. Le « turnover » étant particulièrement important dans les structures d'infogérance, l'OTP est un bon moyen pour les entreprises de garantir un accès unique et temporaire à leurs ressources et ceci de manière nominative.

En résumé, l'authentification forte prend tout son intérêt dans les contextes suivants :

- 1. Dans les environnements d'échange de donnée électronique, le besoin de valider l'identité des utilisateurs est essentiel. Pour capitaliser sur une stratégie efficace d'échange, l'entreprise doit quotidiennement exposer ses applications et ses données critiques auprès d'utilisateurs divers, à la fois internes et externes.*
- 2. Lorsque l'entreprise n'est pas capable d'authentifier ces utilisateurs de manière fiable, les ressources en ligne sont exposées aux risques de vol, aux menaces de sécurité et à d'autres activités malveillantes*
- 3. L'authentification des dispositifs présents sur le réseau est impérative pour la gestion des accès sécurisés aux ressources du réseau. Les certificats numériques offrent une méthode économique pour y parvenir.*
- 4. Sans un système d'authentification efficace, toutes les mesures de sécurité en place – firewall, VPN<sup>2</sup>, cryptographie, PKI et signatures numériques – sont également exposées au risque d'être compromises.*

---

<sup>2</sup> VPN (Virtual Private Network) : Réseau privé virtuel  
[http://fr.wikipedia.org/wiki/Réseau\\_privé\\_virtuel](http://fr.wikipedia.org/wiki/Réseau_privé_virtuel)



## b. Les limitations et freins à l'utilisation de l'OTP

Malgré les apports évidents en sécurité des solutions OTP pour la maîtrise des accès à l'information, le principal inconvénient est lié au coût financier. En effet, la majorité des solutions OTP nécessitent un support appelé « token ». Le coût global d'une solution OTP se décompose en un coût d'acquisition des tokens et d'un coût d'exploitation lié à la gestion du cycle de vie des tokens (renouvellement, perte, vol, resynchronisation).

A priori, l'aspect financier pénalise davantage les PME qui ne bénéficient peu ou pas d'une économie d'échelle. Néanmoins, nous verrons dans cet article que les éditeurs actuels de solutions OTP se concentrent sur le segment de marché des PME avec des coûts d'acquisition de plus en plus attractifs. Il reste cependant la gestion du cycle de vie des tokens. Si cette gestion n'est pas externalisée, elle représente un risque d'abandon ou de désintéressement par les PME. Par conséquent, une politique d'authentification forte pour l'ensemble du personnel d'une entreprise ne semble donc pas envisageable. Dans la même optique, l'OTP ne constitue pas non plus, une solution satisfaisante pour tous les usages informatiques courants. Par exemple, l'authentification forte des utilisateurs sur leur poste de travail dans l'entreprise ne semble pas pertinente, car les utilisateurs souhaitent une utilisation simple de leur outil informatique et seront donc réticents à l'emploi d'une solution OTP.



### 3) Principe de fonctionnement de l'OTP

#### a. OTP ASYNCHRONE

La première famille d'OTP est celle de l'**One Time Password Asynchrone**. Par asynchrone, on entend le fait que le serveur va commencer par envoyer à l'utilisateur un "challenge". L'utilisateur va le communiquer ce challenge à son générateur d'OTP (logiciel ou matériel). À partir de ce challenge, l'objet va calculer une réponse : l'OTP.

#### Les problèmes associés aux OTP asynchrones

- **Modification de la logique de l'application pour le challenge**

Le fait d'utiliser une authentification asynchrone entraîne le besoin de fournir à l'utilisateur le challenge, afin qu'il puisse calculer l'OTP correspondant. Ceci peut poser des problèmes pour certaines applications ou protocoles pour lesquels il n'est pas possible de demander un challenge.

Pour utiliser un OTP asynchrone comme moyen d'authentification, il est donc indispensable que :

- l'application soit modifiable pour afficher le challenge,
- le protocole de communication utilisé (si c'est le cas) soit capable de transporter le challenge au client,
- l'application puisse être modifiée pour vérifier l'OTP une fois celui-ci saisi par l'utilisateur.

Ces conditions ne permettent pas toujours d'utiliser une authentification asynchrone. Dans ces cas-là, des moyens d'authentification synchrones peuvent être envisagés.

- **Éviter de donner le challenge plusieurs fois.**

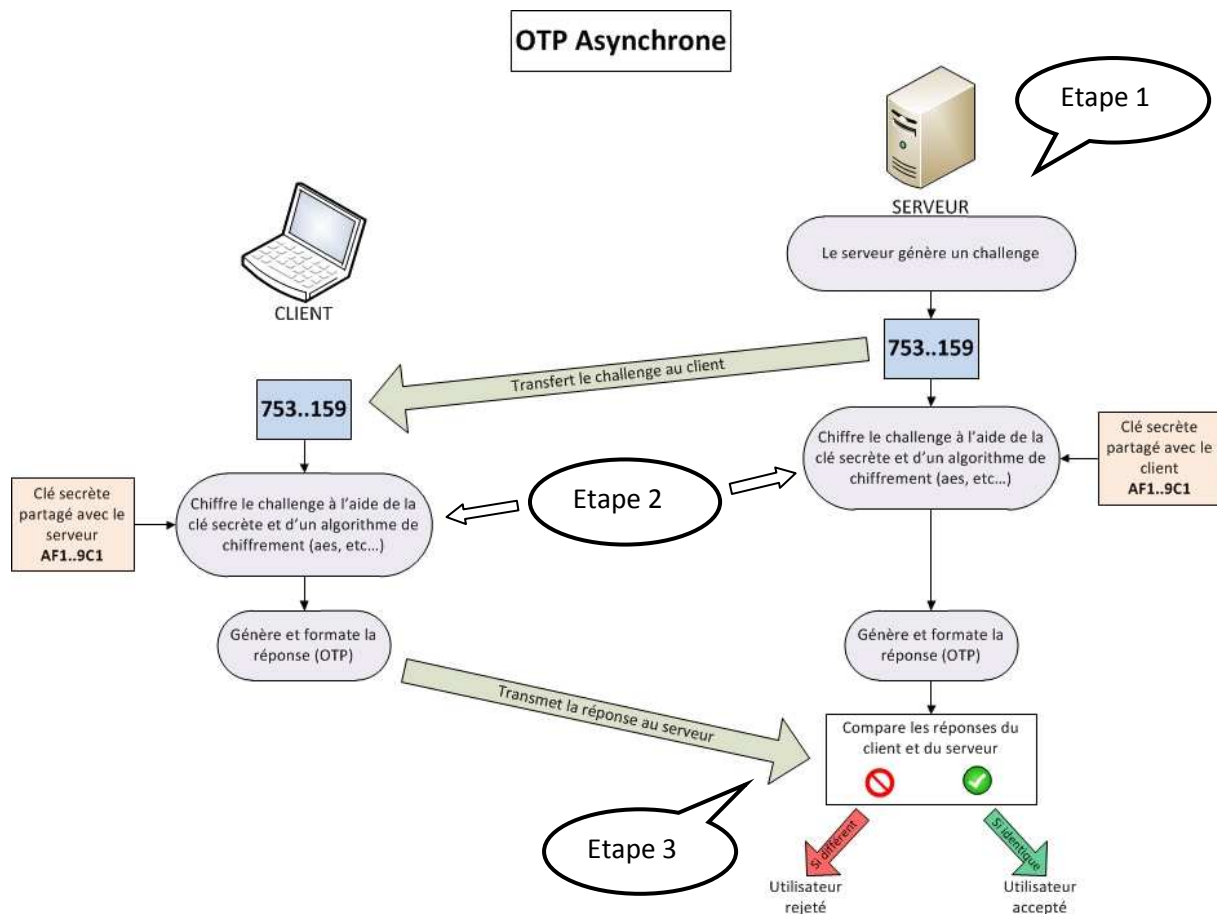
Pour les OTP asynchrones, le même challenge engendre toujours la même réponse. Si l'on suppose qu'un attaquant écoute tous les échanges pour essayer d'avoir accès au service à la place de l'utilisateur, on comprend alors que si le même challenge est utilisé deux fois de suite, l'attaquant va pouvoir la deuxième fois se faire passer pour l'utilisateur légitime. Une partie de la sécurité associée aux OTP asynchrones dépend donc de l'unicité du challenge. Ainsi, un challenge qui serait trop court (donc qui reviendrait trop souvent) fera que le même OTP sera souvent utilisé, ce qui donne plus de chances à l'attaquant.

Un challenge à un chiffre n'offre qu'une très faible protection alors qu'un à 8 chiffres est plus robuste sur cet aspect.

Source : Orange Business [2]



### Synoptique - OTP Asynchrone



## b. OTP SYNCHRONE

Les OTP synchrones, contrairement aux OTP asynchrones, ne nécessitent pas de challenge. Ainsi, il suffit de générer un OTP synchrone et de le fournir directement à l'application pour vérification.

L'OTP généré est toujours différent et peut être synchronisé selon différentes techniques :

- **basé sur le temps**

Chaque OTP généré est calculé à partir de l'heure courante. L'unité de temps pour calculer l'OTP doit être suffisamment longue pour minimiser les problèmes de synchronisation entre l'objet utilisé pour générer un OTP et le serveur (il est toujours difficile d'être synchronisé à la seconde près et il faut laisser le temps à l'utilisateur de rentrer l'OTP).

Ceci permet à cet OTP de n'être valide que durant une certaine période de temps (30 secondes ou 1 minute). Ainsi, s'il est réutilisé en dehors de cette période de temps, il est considéré comme invalide, ce qui évite que quelqu'un puisse rejouer le mot de passe plus tard.

- **ou basé sur un compteur**

Ce compteur, utilisé en entrée de l'algorithme cryptographique, est incrémenté chaque fois qu'un mot de passe est généré, ce qui aboutit à un OTP différent à chaque fois.

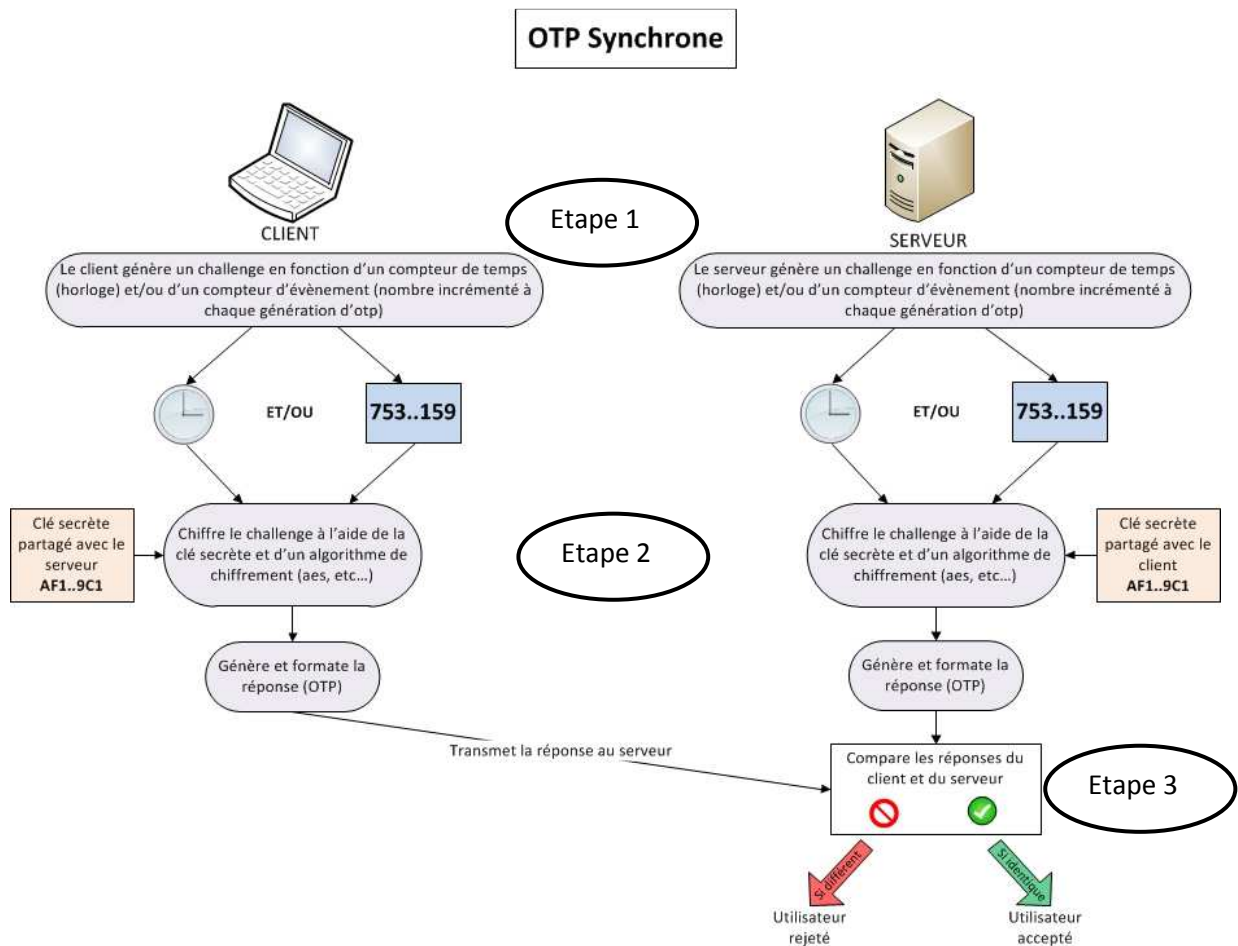


- **ou basé sur le temps et un compteur**

Mélange des deux techniques précédentes. Avec ces informations (et un secret bien sûr), l'OTP va être généré sans aucun challenge, ce qui le différencie des OTP asynchrones. Lorsque l'utilisateur souhaite accéder à un service, il suffit qu'il génère un OTP et qu'il l'utilise à la place de son mot de passe dans l'application. Aucun challenge n'est demandé donc, la logique de l'application n'a pas besoin d'être modifiée. Seule la partie de vérification du mot de passe a besoin d'être changée pour intégrer la vérification de l'OTP. De plus, comme il n'y a pas de challenge à saisir, les objets utilisés pour générer les OTP synchrones n'ont pas nécessairement besoin d'un clavier, ce qui peut les rendre plus simples à utiliser. Cependant, le fait d'avoir un clavier intégré permet de protéger la génération de l'OTP par un code PIN, ce qui renforce encore la sécurité.

Source : Orange Business [3]

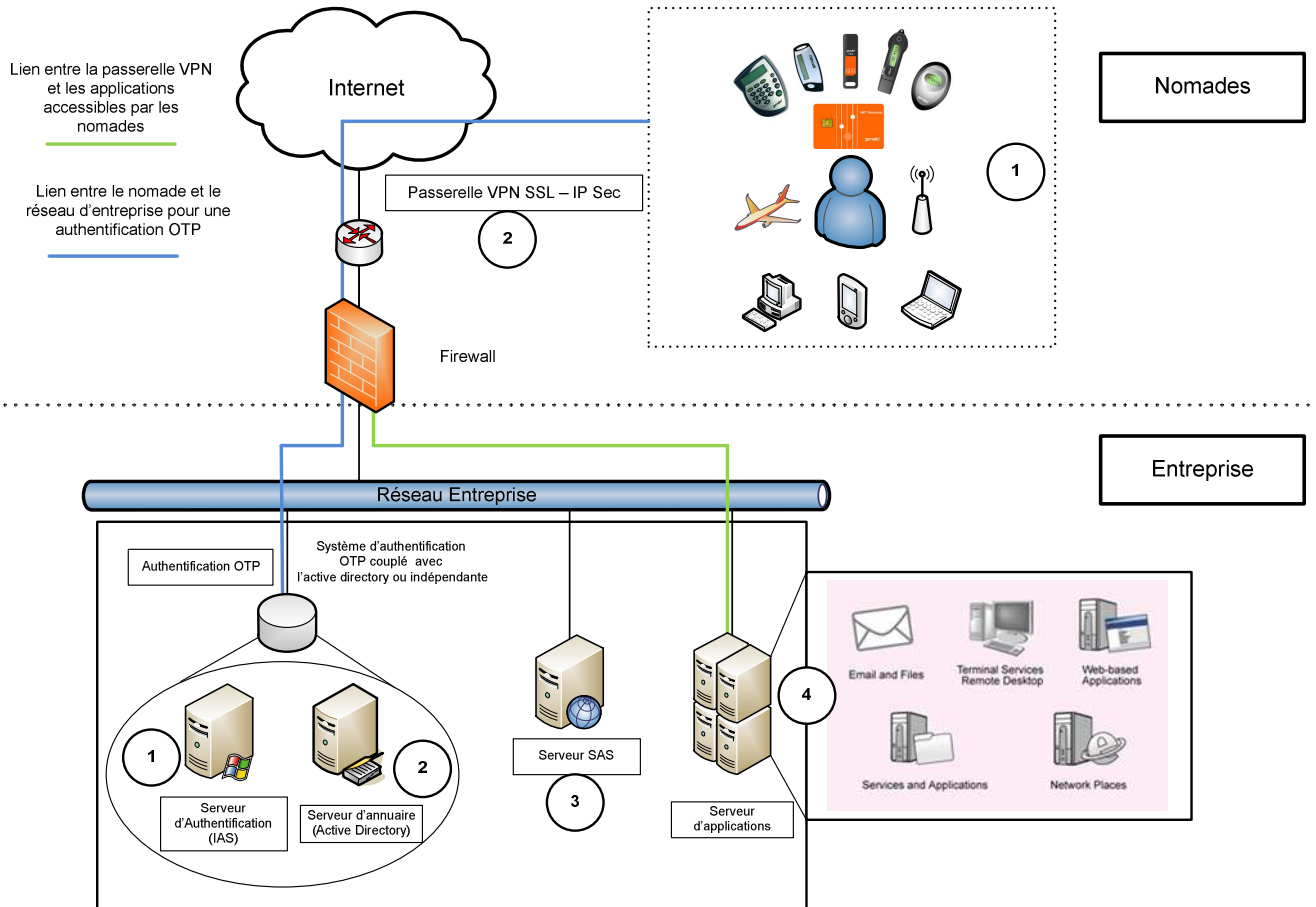
**Synoptique - OTP Synchron**





## 4) ARCHITECTURE OTP

### a. Architecture de la solution globale – Exemple : accès nomade



### b. Environnement technique

#### - Utilisateur Nomade : Token – Logiciel VPN

- o Token

Le token va permettre de générer le « One Time Password » en fonction d'un secret partagé avec le serveur d'authentification. Un token peut prendre la forme d'une clé USB, d'une carte à puce avec lecteur, d'un porte-clés avec écran d'affichage, d'un téléphone portable (SMS), ou encore sous forme d'un logiciel - si nécessaire.



- o Logiciel VPN SSL OU IPSEC

Le logiciel VPN permet une connexion sûre avec le réseau de l'entreprise. La technologie d'authentification par OTP peut être utilisée pour une connexion VPN (typiquement IPSEC ou SSL).

#### - Système d'information de l'entreprise : Service d'authentification – Annuaire Utilisateur – Service OTP – Applications tierces parties



- Service d'authentification (IAS Radius Microsoft)

Le serveur d'authentification est un tampon entre le client et le serveur OTP. Généralement, un agent OTP est installé sur le serveur d'authentification. Lorsque le serveur reçoit une connexion OTP, l'agent intercepte la requête contenant le mot de passe et la transmet au serveur OTP qui vérifie la validité de l'OTP.

Si l'OTP est valide, le serveur autorise l'accès. En l'occurrence, dans notre schéma, c'est Microsoft IAS qui joue le rôle de serveur Radius (service à installer sur le serveur).

- Annuaire utilisateur - Base de données utilisateur LDAP (Active Directory Microsoft)

Le serveur d'authentification repose sur une base de données pour vérifier l'existence des utilisateurs.

- Serveur OTP (GEMALTO SAS)

Le serveur OTP valide les OTP générés par les tokens utilisateurs grâce à une clé secrète partagée et un compteur qui s'incrémente à chaque génération d'OTP (ce compteur doit être synchronisé entre le token et le serveur OTP).

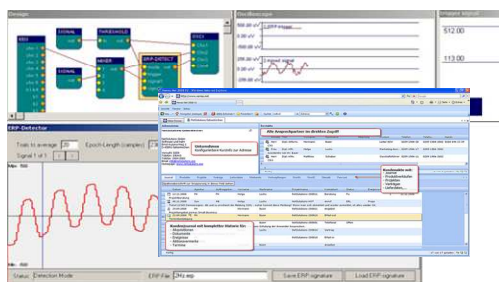
Dans son principe de fonctionnement, le serveur SAS reçoit l'OTP du client (généré par le token) par l'intermédiaire du serveur d'authentification. Le serveur calcule un OTP depuis la dernière valeur du compteur et le compare avec celui fournit par le client. Après comparaison des OTPs, le serveur OTP renvoi une réponse au serveur d'authentification. Dans notre cas, nous avons mis en place le serveur OTP de GEMALTO, le serveur SAS.

#### ◆ Dans le synoptique, ces 3 composantes sont installées sur le même serveur

- Applications - ressources accessibles par les nomades – en LAN déporté.

Typiquement, les ressources accessibles par les nomades sont :

- la messagerie
- les applications métiers (ERP, CRM,...)
- bureaux à distances
- application à maintenir (télémaintenance)





## 5) Illustration d'une solution OTP – GEMALTO

### a. Descriptif technique

La solution GEMALTO est composée d'un serveur d'authentification OTP (SAS pour Strong Authentication Server), d'une interface de service d'authentification et de différents tokens.

Le serveur SAS est composé d'une application Web et d'un moteur d'authentification.

- *L'application Web traite les requêtes d'authentification et fournit un portail pour la gestion des équipements, des utilisateurs, des rôles, des politiques de sécurités, etc ...*  
*Le serveur SAS fournit un portail administrateur pour la gestion complète de la solution et un portail utilisateur afin de simplifier les tâches de l'administrateur.*

#### o Portail d'administration

The screenshot displays the Gemalto - Customer Care Portal administrative interface. The page header includes the Gemalto logo and the title 'Gemalto - Customer Care Portal'. Below the header, it indicates the user is logged in as 'Administrator' and provides links for 'About', 'Glossary', 'Home', and 'Logout'. The main content area is organized into a grid of management sections:

- CUSTOMER CARE PORTAL** (Left sidebar): Manage Users, Manage Devices, Manage Keys, Manage Policies, Manage Roles, Search Transactions, Batch Provisioning, System Administration.
- Manage Users**: Search Users, Migrate User, Remove Users.
- Manage OATH Devices**: Search OATH Devices, Create OATH Device, Live Provision OATH Devices, Live Re-provision OATH Devices, Activate Pin, Expire OATH Devices.
- Manage Time Based Devices**: Search Time Based Devices, Create Time Based Device, Expire Time Based Devices.
- Manage Keys**: View All Keys, Create Key.
- Manage Roles**: View All Roles, Create Role.
- Manage OATH Policies**: View All OATH Policies, Create OATH Policy.
- Manage Time Based Policies**: View All Time Based Policies, Create Time Based Policy.
- Manage Transactions**: Search Transactions.

Le portail d'administration fournit à l'administrateur plusieurs outils lui permettant :

- La gestion des utilisateurs (création, modification, suppression, ...)
- La gestion des tokens (enregistrement, synchronisation, affectation aux utilisateurs, blocage, création de tokens virtuels, ...)
- La gestion des politiques OATH (nombre de tentatives d'authentification, taille des OTP, ...)
- La gestion des rôles utilisateurs
- La gestion des logs
- ...



- Portail Utilisateur

**Le portail utilisateur** fournit aux utilisateurs plusieurs outils permettant (suivant le rôle) :

- De gérer les informations les concernant
  - De s'enregistrer et d'affecter un token
  - De resynchroniser un token
  - De demander un OTP par SMS (si la fonction est paramétrée sur le serveur)
  - De déclarer la perte d'un token
- *Le moteur d'authentification interagit avec la base de données utilisateur (Firebird ou LDAP), avec la liste des OTP et le module de calcul de cryptogramme.*

Le serveur SA s'installe de 2 manières différentes. Dans un premier cas, le serveur est dans un mode stand-alone (DB mode). Il utilise une base de données interne (Firebird) et ne nécessite pas de connexion à un serveur d'annuaire. Dans le second cas, l'installation est dite Mixed Mode. Dans ce mode, le serveur SA utilise les informations d'une base de donnée LDAP et maintient d'autres informations dans sa base de données interne (ce qui permet de ne pas étendre le schéma LDAP).



## Le serveur SAS est compatible avec Windows et Linux.

L'interface de service d'authentification est un logiciel qui s'occupe de transmettre les requêtes d'authentification vers le serveur SA. Ce composant est essentiel pour l'utilisation d'une authentification par OTP.

L'interface du service d'authentification interagit avec :

- Des requêtes http ou https
- Des requêtes XML<sup>3</sup> envoyées vers une api<sup>4</sup> Web
- Des requêtes Radius au travers d'un Agent pour :
  - o IAS ou NPS (Microsoft)
  - o Juniper Steel Belted Radius (Funk Software)
  - o Free RADIUS
  
- Des requêtes propriétaires au travers d'un Agent pour :
  - o Microsoft Outlook Web Access (OWA)
  - o Microsoft ISA
  - o Microsoft IAG
  - o Citrix Web Interface

Les tokens Gemalto sont divers et variés. Il est possible d'utiliser des clés USB, des porte-clés avec afficheur, des cartes à puces, etc. ...

## b. Maquette

Cette partie illustre une solution OTP à base de produit GEMALTO utilisée pour l'authentification des utilisateurs nomades se connectant à leur réseau d'entreprise par VPN.

Le socle technique de cette maquette se compose de différents produits parmi lesquels :

### Un serveur Windows 2003

- Un service d'annuaire (Active Directory)
- Un service d'authentification Radius (IAS)
- Un agent d'authentification installé sur le serveur radius (Agent IAS)
- Un serveur SA ( Strong Authentication Server) installé en mode mixte (Mixed Mode)

### Infrastructure réseau

- Un client radius (Appliance VPN SSL)
- Un client radius (Appliance VPN IPSEC)

---

<sup>3</sup> XML ( eXtensible Markup Language) : langage extensible de balisage

[http://fr.wikipedia.org/wiki/Extensible\\_Markup\\_Language](http://fr.wikipedia.org/wiki/Extensible_Markup_Language)

<sup>4</sup> API (Application Programming Interface) : Interface de programmation

[http://fr.wikipedia.org/wiki/Interface\\_de\\_programmation](http://fr.wikipedia.org/wiki/Interface_de_programmation)



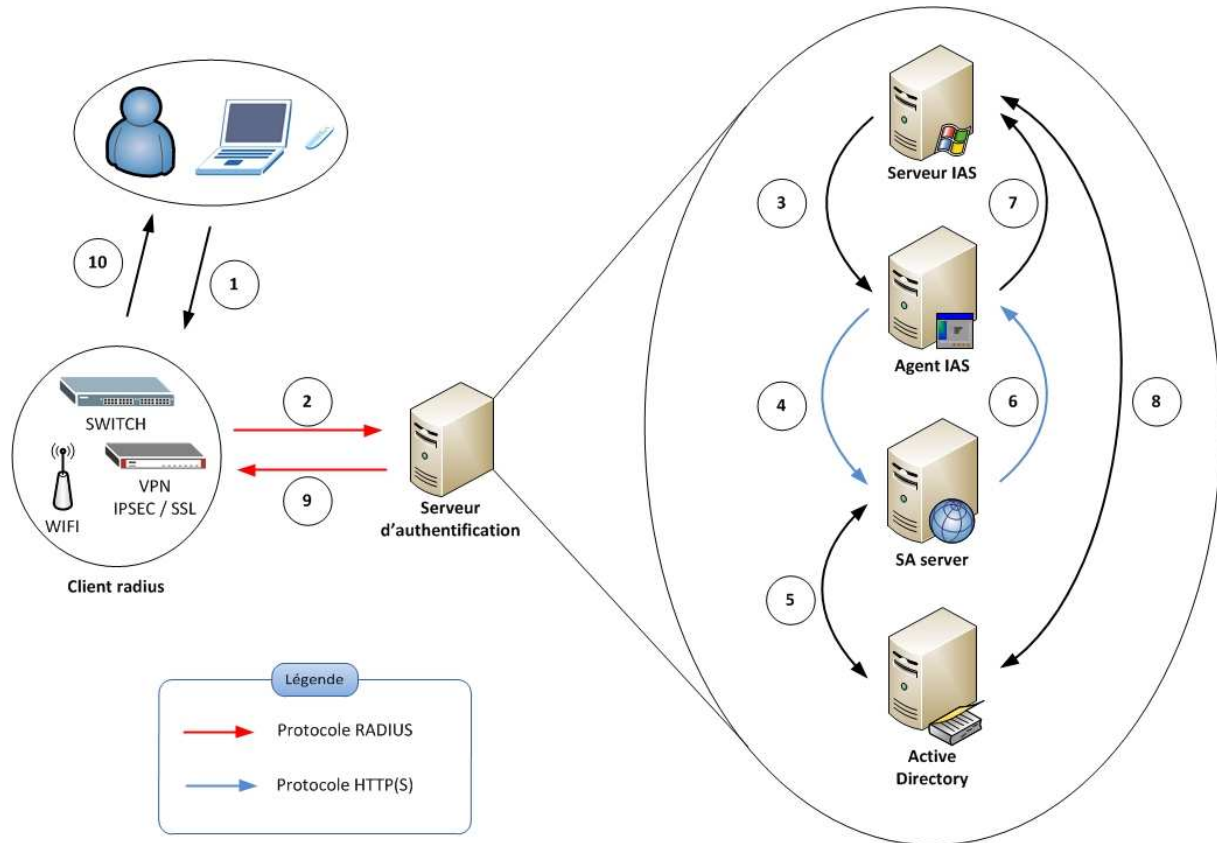
Client

- Un générateur d’OTP (Smart Enterprise Guardian)



Smart Enterprise Guardian

**Synoptique du fonctionnement entre les différents composants logiciels**



**Cinématique de l’authentification**

- 1) Le client se connecte au concentrateur VPN et fournit un mot de passe : **123456** **bonjour**  
**123456** est l’OTP généré par son token  
**bonjour** est le mot de passe de son compte utilisateur AD
- 2) Le serveur VPN envoie une requête d’authentification au serveur d’authentification (IAS)
- 3) Le serveur IAS délègue l’authentification à l’agent IAS
- 4) L’agent IAS envoie le mot de passe au serveur SA par le protocole http(s)
- 5) Le serveur SA vérifie le mot de passe en s’appuyant sur Active Directory
- 6) Le serveur SA renvoie une réponse à l’agent IAS par le protocole http(s)
- 7) L’agent IAS renvoie la réponse au serveur IAS
- 8) Le serveur IAS vérifie les informations utilisateurs en s’appuyant sur AD
- 9) Le serveur IAS renvoie la réponse d’authentification au client radius
- 10) Le client radius informe l’utilisateur de la réussite ou de l’échec de l’authentification



### c. Pré requis techniques pour intégrer la solution OTP

Dans notre exemple, l'entreprise dispose :

- D'un serveur d'annuaire : Dans cette maquette, le serveur d'annuaire est Active Directory. Il est hébergé sur une machine Windows 2003 Server. Ce serveur est paramétré avec un domaine : **otptest.local**. Un utilisateur a été créé pour tester l'authentification OTP : **greg**. Il fait partie du groupe d'utilisateur : **otp**
- D'un serveur radius : Le serveur radius utilisé est le composant **IAS** de Windows 2003 server.
- De clients radius : les appliances VPN utilisées font office de client Radius.

### d. Test réalisés

La configuration des serveurs VPN ne sera pas décrite dans cet article.

**Test N°1 – Accès Intranet:** l'utilisateur s'authentifie sur le portail utilisateur avec son OTP. L'administrateur a créé l'utilisateur et enregistré le token. Il a associé le token à l'utilisateur et activé celui-ci. L'utilisateur se connecte au portail utilisateur du serveur SA pour vérifier ses informations.

**Test N°2 – Accès distant VPN IPSEC :** l'utilisateur accède se connecte en VPN IPSEC avec un OTP. L'administrateur a déjà rempli les tâches administratives liées à l'utilisateur (création du compte, enregistrement, association et activation du token). L'administrateur a configuré son serveur radius et son client radius.

L'utilisateur utilise son application client VPN pour se connecter au système d'information de son entreprise. Il communique un mot de passe sous la forme **123456bonjour** où **123456** est l'**OTP** et **bonjour** le mot de passe **Active directory**.

**Test N°3 – Accès distant VPN SSL:** l'utilisateur accède se connecte en VPN SSL avec un OTP

L'administrateur a déjà rempli les tâches administratives lié à l'utilisateur (création du compte, enregistrement, association et activation du token). L'administrateur a configuré son serveur radius et son client radius. L'utilisateur utilise un navigateur internet et accède au portail d'authentification VPN de l'entreprise. . Il communique un mot de passe sous la forme **123456bonjour** où **123456** est l'**OTP** et **bonjour** le mot de passe **Active directory**.



## 6) Aspects financiers

L'estimation financière de la mise en place d'une solution OTP est basée sur une entreprise de 500 employés dont 50 utilisent une technologie par OTP. Les pré-requis technique (voir chapitre précédent) ne sont pas inclut dans cette estimation.

### Coût d'investissement

	Coût à l'unité	Coût pour 50 personnes
<b>Achats des tokens incluant les licences</b>	95 €	4.750 €
<b>Installation du serveur (SA + configuration RADIUS) et formation au produit GEMALTO</b>	1.100 €	1.100 €
<b>Procédure d'enregistrement des utilisateurs pour l'OTP</b>	10 min / utilisateur	Une journée
	<b>TOTAL INVEST.</b>	<b>5.850 €</b>

### Coût d'exploitation

	Coût mensuelle	Coût annuel
<b>Coût de gestion du cycle de vie du token<sup>5</sup></b>	160€	1.920 €
<b>Coût lié à la perte/vol d'un token<sup>6</sup></b>	39,6 €/an	475 €
	<b>TOTAL EXPLOIT.</b>	<b>2.395 €</b>

<sup>5</sup> Monopolise 10% du temps de travail d'un technicien par mois. Pour un technicien rémunéré à 1.600 € Net, le coût d'exploitation reviendrai à 160 €/mois donc 1320 € : an.

<sup>6</sup> Rachat d'un token – taux de perte – 10% sur un investissement de 4.750 € soit 475 € par an.



## 1) Avantages et inconvénients d'une solution OTP

### a. Avantages

- **Gain en sécurité avec une solution OTP – atteinte des objectifs de sécurité :** Les solutions OTP font parties des solutions d'authentification forte (authentification à 2 facteurs). L'utilisateur possède un objet (token) et un savoir (mémoire de son mot de passe) qui lui permettront de créer un mot de passe à usage unique. La force de l'OTP est d'être valable qu'une seule fois. A ce titre, si un « pirate » venait à découvrir un OTP, il ne pourrait pas l'utiliser. Le rejeu est impossible. A ce titre, les solutions OTP améliorent considérablement le niveau de sécurité pour toutes les entreprises qui nécessitent d'ouvrir leur réseau au monde extérieur.
- **Intégration de la solution OTP dans l'existant de l'entreprise :** la solution GEMALTO s'intègre parfaitement dans une infrastructure existante en respectant les protocoles normes et standards en vigueur dans la majorité des entreprises. Ainsi les entreprises ne sont pas captives et n'ont pas besoin d'acquérir de composants supplémentaire pour intégrer cette solution.
- **Simplicité d'administration de la solution GEMALTO :** les environnements mis à disposition par la solution GEMALTO à destination de l'administrateur et de l'utilisateur, via les portails ad hoc, sont simple d'utilisation et intuitifs.
- **Responsabilisation de l'utilisateur :** l'utilisateur est au cœur de la solution via le portail utilisateur. Il est acteur de la gestion du cycle de vie de son propre token dès le processus d'enrôlement jusqu'à la révocation du token.

### b. Inconvénients

- **Délai d'obtention des supports tokens et des licences :** la logistique des Tokens au de est un aspect à prendre en compte en amont du projet, car le délai de livraison des tokens de la part de GEMALTO et l'obtention des numéros de licence est hasardeux et peut prendre jusqu'à 3 ou 4 semaines.
- **Gestion du cycle de vie des tokens :** il est nécessaire de mettre en place une organisation de gestion des tokens et de définir des règles précises d'utilisation des tokens.
- **Mode d'authentification :** une fois les composants logiciels de la solution Gemalto installés (Service SAS et Agent SA), toute authentification Radius sera automatiquement traitée par le service SAS. Dans le cas d'une architecture d'authentification par Radius déjà existante, l'utilisation de tokens devient indispensable à moins de définir plusieurs politiques d'authentification RADIUS dans le service IAS.



## 2) Conclusion

Jusqu'à présent, les solutions d'authentification OTP étaient réservées uniquement aux grandes entreprises. Désormais, ces solutions se démocratisent auprès des PME et TPE grâce à l'apparition de solutions simples et rapides à mettre en place sur des infrastructures existantes et financièrement accessibles.

La solution GEMALTO illustre cette tendance actuelle. La présente solution est un bon compromis entre exigences de sécurité et contraintes financières afin d'être intégrée dans des PME et TPE souhaitant se protéger contre des menaces d'usurpation d'identités.

Pour plus d'information à ce sujet, veuillez nous contacter à l'adresse mail suivante : [info@pronetis.fr](mailto:info@pronetis.fr)



### 3) Bibliographie

[1] Credoc : [http://www.credoc.fr/pdf/Sou/synthese%20Presentation%20fellowes%20-%20CREDOC%202009%20\[Lecture%20seule\].pdf](http://www.credoc.fr/pdf/Sou/synthese%20Presentation%20fellowes%20-%20CREDOC%202009%20[Lecture%20seule].pdf)

[2] Orange Business: [http://www.orange-business.com/fr/lna/events/club\\_assurance/deja\\_demain/att00005019/cahier\\_tech\\_One\\_Tlme.pdf](http://www.orange-business.com/fr/lna/events/club_assurance/deja_demain/att00005019/cahier_tech_One_Tlme.pdf)

[3] Orange Business: [http://www.orange-business.com/fr/lna/events/club\\_assurance/deja\\_demain/att00005019/cahier\\_tech\\_One\\_Tlme.pdf](http://www.orange-business.com/fr/lna/events/club_assurance/deja_demain/att00005019/cahier_tech_One_Tlme.pdf)

### 4) Référentiel normatif

[OTP Extended Responses \(RFC 2243\)](#) (Novembre 1997)

[A One-Time Password System \(RFC 2289\)](#) (Février 1998)

[The One-Time-Password SASL Mechanism \(RFC 2444\)](#) (Octobre 1998)

[RADIUS Authentication \(RFC 2865\)](#) (Juin 2000)

[RADIUS Accounting \(RFC 2866\)](#) (Juin 2000)