Cadre de référence et méthodologie

Introduction

Les sociétés modernes comme LaPoste sont aujourd'hui fortement dépendantes des technologies de l'information et des communications.
Dans un environnement ouvert, les interlocuteurs sont parfois inconnus et toujours dématérialisés. Les concepts et technologies de la confiance numérique et de la sécurité informatique vont se compléter pour permettre de réaliser un contrôle d'accès en environnement ouvert. Dans ces travaux, nous nous proposons d'étudier les concepts majeurs de cette problématique, puis de concevoir et enfin de développer un système fonctionnel d'authentification forte , basée sur OTP(One-Time Password)(mot de passe à usage unique) et déployer le SSL(https) avec certificat, pour un environnement ouvert et appliqué à l'Internet.

1.1 Contexte

Dans le contexte de sécurité actuel, le mot de passe est devenu en quelques années un élément incontournable de notre vie quotidienne. Nous les utilisons pour protéger nos appareils (ordinateurs, tablettes, smartphones, etc. . .), nos données, ou encore pour restreindre l'accès aux services que nous utilisons (comptes mail, applications bancaires, etc. . .). Mais le mot de passe est loin d'être un moyen d'authentification totalement fiable, et constitue de ce fait un risque pour les utilisateurs.

En effet, nous devons faire face à une multitude de comptes à créer, et donc à retenir. Il est alors très courant pour un utilisateur d'utiliser toujours le même mot de passe ou de choisir un mot de passe simple, facile à retenir et à saisir. Ensuite, il est relativement simple pour un malware de " capturer " un mot de passe. Les keyloggers par exemple, surveillent les touches du clavier et transmettent les mots de passe saisis à l'attaquant.

L'actualité, et notamment les nombreuses attaques massives visant à compromettre des mots de passe (1 milliard de comptes Yahoo piratés, 145 millions de comptes eBay ou encore 117 millions de comptes LinkedIn, et plus récemment le géant mondial du

VTC Uber avec plus 57 millions de victimes, dont au moins 600 000 chauffeurs nous le démontrent : Un simple mot de passe ne suffit plus à nous protéger.

Les réglementations se sont donc durcies afin de mieux protéger les utilisateurs. Par exemple la directive sur les services de paiement (DSP2) entrée en vigueur le 13 janvier 2018, impose aux établissement bancaires une authentification forte des clients lorsque ceux-ci accèdent à leur compte de paiement en ligne, initient une opération de paiement, ou exécutent une action susceptible de comporter un risque de fraude.

1.2 Problématique

en raison de la vulnérabilité des systèmes protégés par la seule utilisation de mots de passe. Concrètement, entre la négligence des utilisateurs et les techniques ultra sophistiquées des hackers, les mots de passe ne sont désormais plus suffisants pour assurer la sécurité des informations et des ressources des entreprises. Un utilisateur inconnu du fournisseur de service obtient un accès au travers de la confiance du fournisseur de service envers des organisations attestant d'informations sur l'utilisateur. Avec l'évolution de la technologie de l'information et de la communication, et principalement du « cloud computing », nous nous sommes posés la question de comment la confiance numérique entre organisations sera utilisée dans l'avenir pour permettre à des usagers d'accéder à des services en ligne offerts par des organisations desquelles ils sont inconnus ?

1.3 Proposition des solutions

L'authentification forte est une méthode permettant à un utilisateur de s'identifier/authentifier auprès d'un fournisseur de services en demandant une combinaison de deux méthodes d'authentification différentes parmi :

— Ce que l'on sait (exemple : un mot de passe)
— Ce que l'on possède (exemple : le téléphone qui reçoit un mot de passe)
— Ce que l'on est (exemple : une caractéristique biométrique)

Il existe également des mécanismes d'authentification émergents qui s'appuient sur :

— L'emplacement où vous êtes (exemple : géolocalisation)
— Les personnes que vous connaissez (exemple : réseaux sociaux)
— Ce que vous êtes en train de faire (exemple : analyse comportementale)

L'authentification forte permet donc de renforcer le niveau de sécurité lors de la connexion des utilisateurs à l'accès aux services.

Aujourd'hui, les mécanismes d'authentification forte les plus utilisés sont :

1. **Les OTP (One-Time Password) par SMS** :
   Ce mécanisme consiste à recevoir par SMS un mot de passe à usage unique (utilisable pour une durée déterminée) qui sera renseigné lors du processus d'authentification. Ce mécanisme est utilisé par de très nombreux établissements bancaires, notamment lors de la réalisation d'achats sur internet.

   La figure.1.1 résume toutes les étapes des OTP (One-Time Password) par SMS.

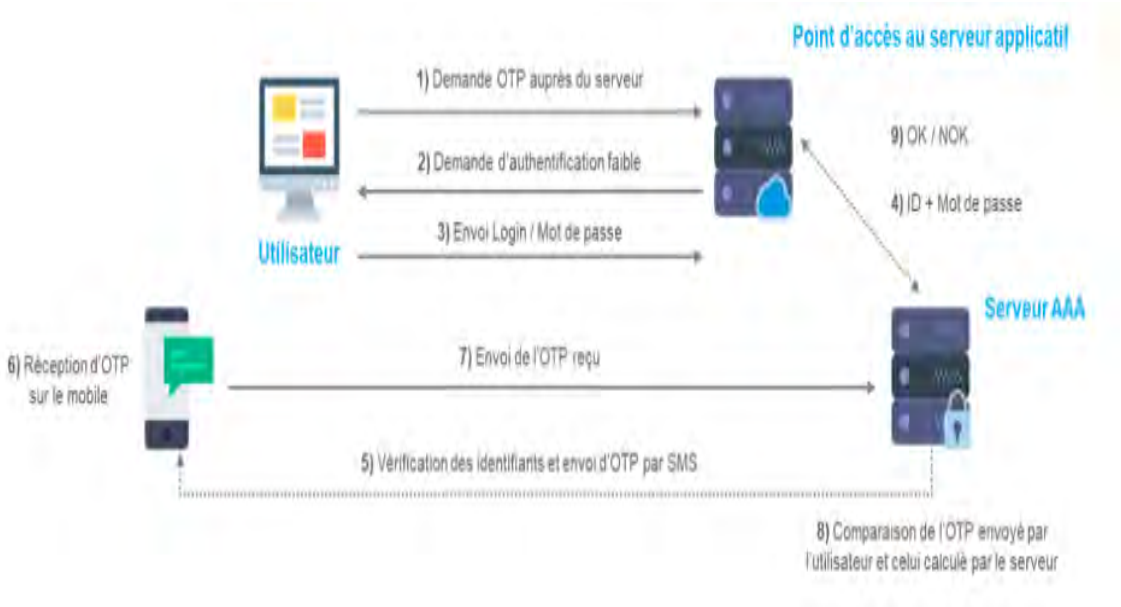

Figure.1.1.étapes des OTP (One-Time Password) par SMS source :[11]

2. **Les OTP (One-Time Password) par soft token** :
   Ce mécanisme consiste à générer un mot de passe unique via une application sur son smartphone. Il nécessite donc que l'utilisateur installe sur son smartphone l'application contenant le soft token (il peut s'agir directement de l'application de la banque en question).

   La figure.1.2 résume le processus des OTP (One-Time Password) par soft token.

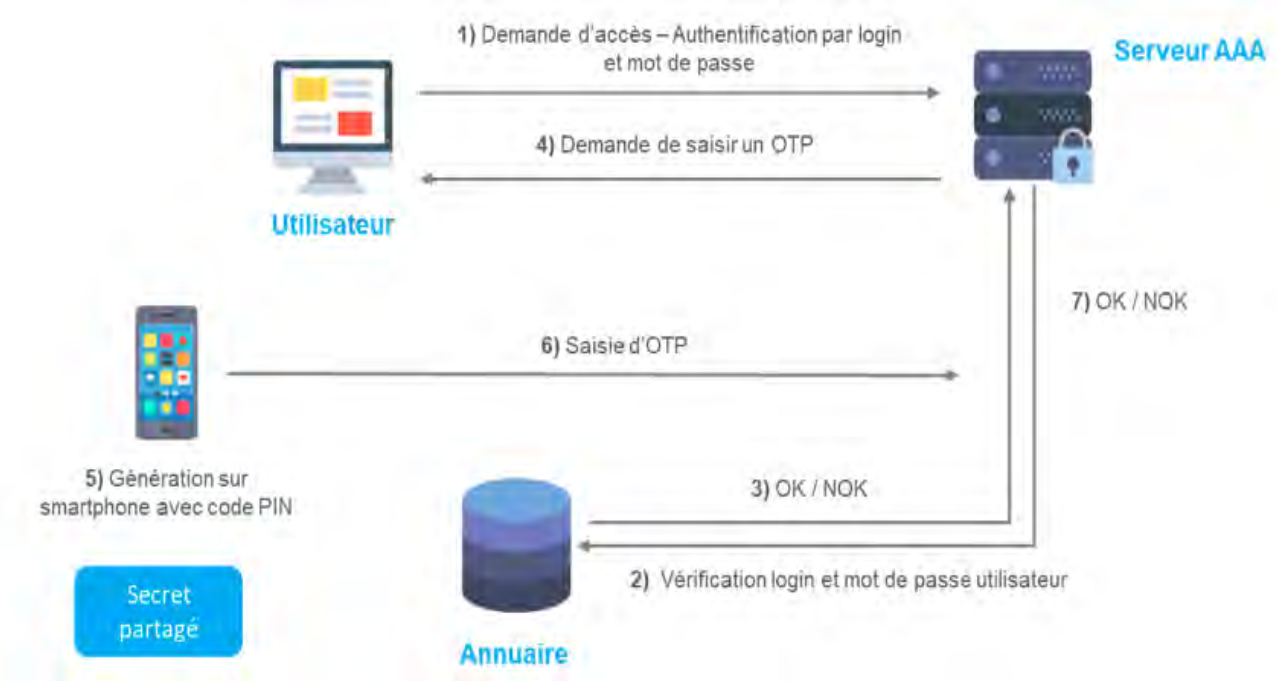

Figure.1.2.processus des OTP (One-Time Password) par soft token source :[11]

3. **Les OTP (One-Time Password) par hard token** :
   Ce mécanisme consiste à générer un mot de passe unique via un " token physique ". Le token RSA est un exemple célèbre de hard token. Le hard token génère un mot de passe aléatoire, valable pour une durée déterminée, qui est demandé lors de l'authentification de l'utilisateur.
   La figure.1.3 résume le processus des OTP (One-Time Password) par hard token.

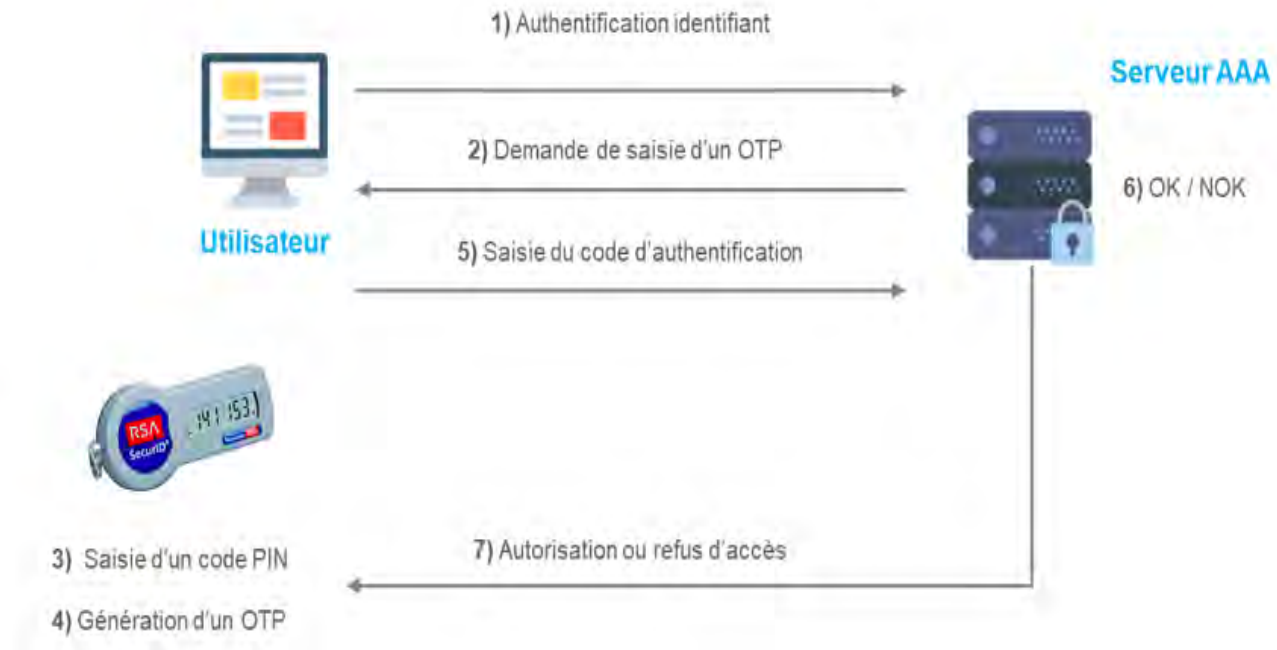

Figure.1.3.processus des OTP (One-Time Password) par hard token source :[11]

4. **La biométrie** :
   Considérée comme une des méthodes les plus prometteuses, la biométrie est de plus en plus utilisée dans le processus d'authentification forte. On distingue quatre cas d'utilisation de la biométrie :

   — La reconnaissance digitale
   — La reconnaissance vocale
   — La reconnaissance d'iris
   — La reconnaissance faciale

   La figure.1.4 résume les differentes etapes d'authentification forte par biométrie.

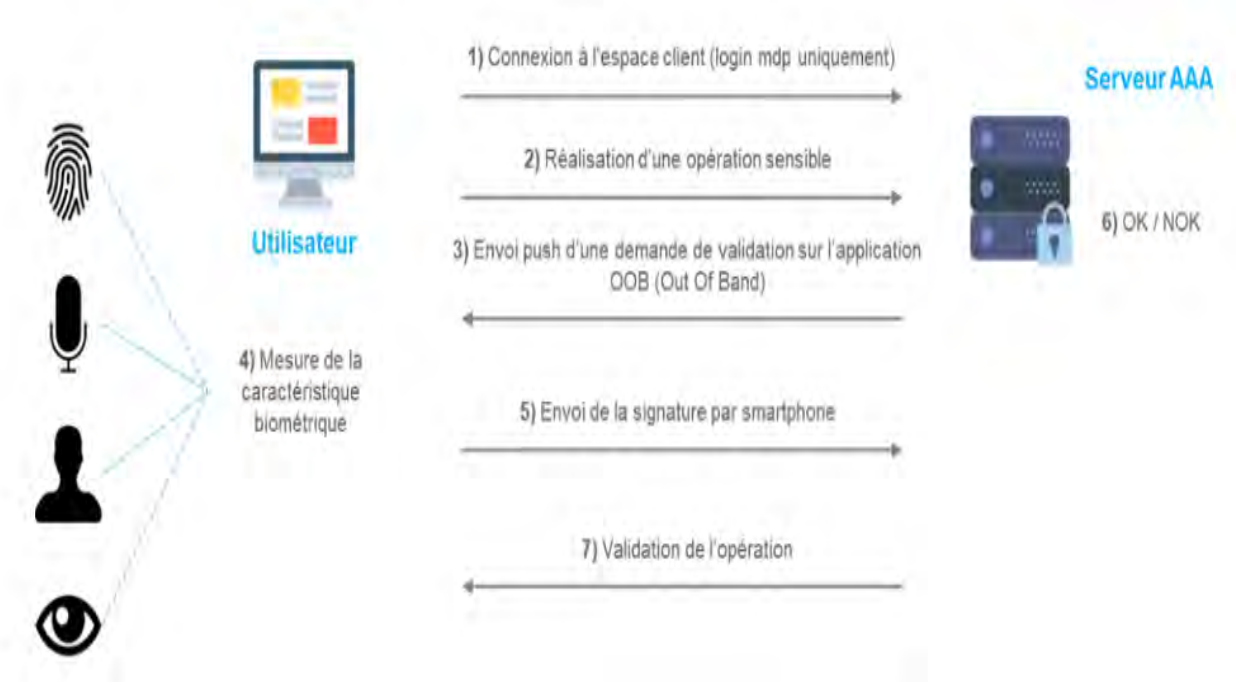

Figure.1.4.etapes d'authentification forte par biométrie source :[11]

5. **Les certificats numériques** :
   Un certificat numérique est l'équivalent virtuel d'une carte d'identité : il garantit que l'identité de l'utilisateur a été vérifiée et qu'il a l'autorisation d'accéder aux ressources concernées. L'authentification par certificats repose sur une technologie de chiffrement qui permet de chiffrer (ou signer) un message sans avoir à partager de " secret ". L'identifiant est un certificat public signé par une autorité de certification reconnue.

La figure.1.5 résume les differentes etapes d'authentification forte par certificats numériques.

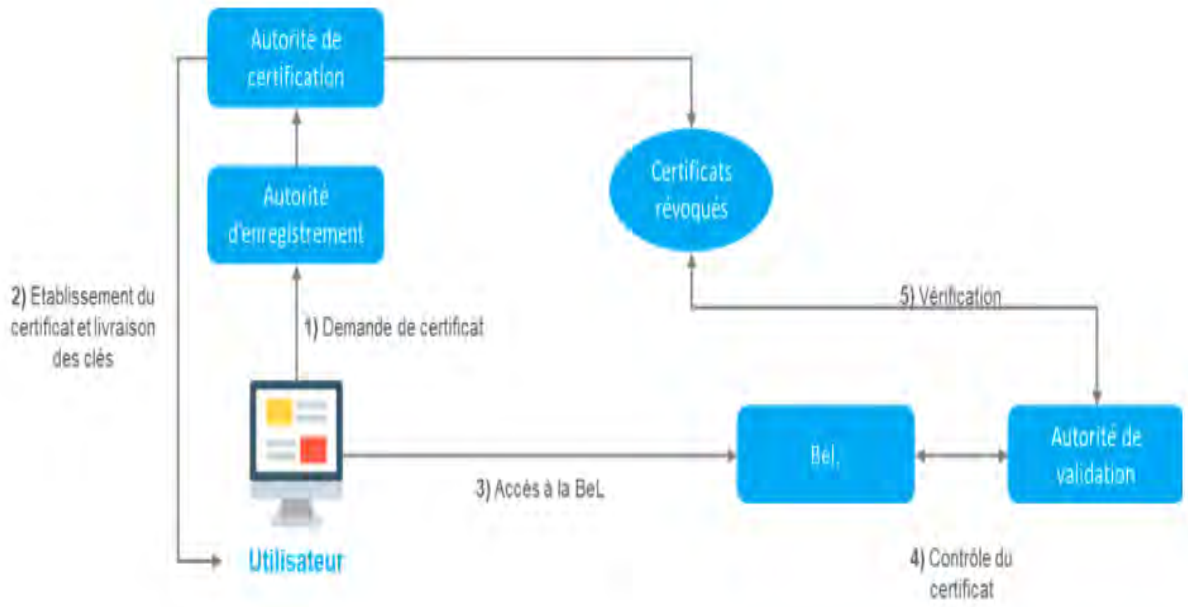

Figure.1.4.etapes d'authentification forte par certificats numériques source :[11]

Toutes ces solutions garantissent une sécurité et un contrôle des accès bien plus efficaces que l'utilisation seule de mots de passe.

1.4 Solution préconisée

Le choix de la solution d'authentification forte repose sur trois principaux critères :

— Le niveau de sécurité
— L'expérience utilisateur
— Le coût

Il est recommandé d'adopter une approche souple, en implémentant une méthode d'authentification basée sur le niveau de risque, et de choisir une solution qui permettra de s'adapter en cas de besoins. Cette approche offre généralement le meilleur compromis entre un niveau de sécurité élevé et une bonne expérience utilisateur. Compte tenu de la multitude de solutions d'authentification forte, il est également recommandé d'évaluer soigneusement chacune des solutions disponibles en se posant les questions suivantes :

— Quel est le niveau de sensibilité de mes données métier ?
— Mes utilisateurs doivent-ils accéder à de nombreuses applications protégées par un mot de passe ?
— Mes utilisateurs doivent-ils se connecter à distance ?

A l'inverse des autres solutions d'authentification forte , y compris la biométrie, Les certificats numériques ont des caracteristiques importantes :

— Processus d'intégration et de formation minimal
— Nombre réduit de demandes d'assistance technique
— Aucun équipement supplémentaire nécessaire
— Aucun jeton d'authentification à distribuer ou gérer
— Aucun plan de secours à mettre en place si oubli ou perte du jeton
— Les utilisateurs peuvent travailler sur plusieurs appareils sans interruptions
— Fonctionne avec très peu de ressources internes
— Identifiants faciles à émettre ou révoquer selon le renouvellement du personnel

En effet aucun équipement supplémentaire n'est nécessaire pour utiliser un certicat numérique. Le certicat est conservé sur l'ordinateur de l'utilisateur, il n'y a donc aucun risque d'oubli ou de perte du jeton d'authentification indispensable pour la création d'un mot de passe unique. Les certificats numériques peuvent être exportés sur d'autres appareils
Remarque : dans les situations à haut risque, la copie et l'installation des clés doivent être gérées avec prudence.

Voici donc quelques-unes des nombreuses raisons pour lesquelles on envisage de choisir comme type d'authentification forte OTP(One-Time Password)(mot de passe à usage unique) et déployer le SSL(https) avec certificat pour authentifier les utilisateurs internes , externes et les partenaires utilisants les differentes ressources de l'entreprise LaPoste.

Conclusion

Les mécanismes d'authentification forte sont nombreux. Cependant le choix du mécanismes d'authentification forte fait appel à plusieurs criteres comme : Le niveau de sécurité, L'expérience utilisateur et le coût. Ainsi il est necessaire d'étudier de plus prés toutes les notions fondamentales des mécanismes d'authentification forte.