MINISTERE DU BUDGET
ET DU PORTEFEUILLE DE L'ETAT

DIRECTION GENERALE DES DOUANES

REPUBLIQUE DE COTE D'IVOIRE
Union - Discipline - Travail

NOTE D'INFORMATION N° 1166 /MBPE/DGD du 04 NOV. 2020

(DIFFUSION GENERALE)

Objet : Lancement de la phase pilote du projet d'authentification forte

Dans le cadre du projet de sécurisation du Système d'Informations des Douanes, une solution d'Authentification Forte a été mise en œuvre dans SYDAM.

J'ai l'honneur de communiquer à l'ensemble du service que la phase pilote du projet d'authentification forte débutera **le 16 novembre 2020** pour une période 3 mois.

Sont concernés par cette phase pilote, **les Chefs de Bureau** ci-après :

- Abidjan Port,
- Abidjan Scanner,
- Abidjan Aéroport,
- Bureau des Régimes Particuliers,
- Bureau Transit et Acquits,
- Bureau Abidjan Export,
- Bureau du Guichet Unique Automobile d'Abidjan.

Les Chefs de Bureau désignés pour la phase pilote sont priés de se rapprocher de la Direction des Systèmes d'Information pour les dispositions pratiques.

La généralisation de cette nouvelle procédure interviendra après l'évaluation de la phase pilote.

J'attache du prix au strict respect des dispositions de la présente qui prend effet à compter de sa date de signature et toute difficulté d'application me sera signalée d'urgence.

Le Directeur Général

DIRECTION GENERALE DES DOUANES
Le Directeur Général
COTE D'IVOIRE

Général DA Pierre A.
Officier de l'Ordre National

MINISTERE DU BUDGET ET DU
PORTEFEUILLE DE L'ETAT

Direction Générale des Douanes

DIRECTION DES SYSTEMES D'INFORMATION

REPUBLIQUE DE COTE D'IVOIRE
Union - Discipline - Travail

AUTHENTIFICATION FORTE

SYDAM WORLD

MEMO

Contexte :

Les actualités le prouvent trop souvent : la combinaison identifiant / mot de passe ne suffit plus à protéger correctement les accès aux applications aussi bien personnelles que professionnelles. En 2014 déjà, les vols de mots de passe ont coûté près de 3 millions d'euros à l'économie mondiale. C'est pourquoi de plus en plus d'entreprises et particuliers se tournent vers d'autres moyens pour sécuriser leurs données. Afin de contrer tout piratage, nous devons désormais choisir des mots de passe plus longs et plus complexes, un procédé qui s'avère de plus en plus pénible et fastidieux.

Mais alors que le mot de passe est le mode d'authentification (dit simple) utilisé par les douanes ivoiriennes au travers de leur application métier SYDAM World, peuvent-elles envisager un autre moyen d'accéder à ses comptes en toute sécurité ? Comment la formule « moins de mots de passe = plus de sécurité » peut-elle marcher ?

L'authentification forte, en opposition à sa version « faible ou dite simple » permet de répondre pleinement à ces enjeux.

L'authentification forte est, en sécurité des systèmes d'information, une procédure d'identification qui requiert la concaténation d'au moins deux facteurs d'authentification.

Dans SYDAM World, l'authentification forte, ou authentification à deux facteurs, devra donc combiner quelque chose que l'on sait (login, mot de passe) avec une autre chose qui peut être un code reçu par sms sur son téléphone portable, par mail ou encore un élément biométrique.

C'est dans ce cadre que le projet d'authentification forte dans SYDAM World a été initié.

Objectif : Sécuriser le Système d'Information.

Acteurs : DSI - Usagers Douaniers.

Action 1 : Implémentation du code de sécurité (OTP : One Time Password) dans SYDAM : JUILLET 2020 ;

Action 2 : Abonnement au service SMS PRO des opérateurs de téléphonie mobile MTN et MOOV pour le transfert du code de sécurité sur le mobile de l'utilisateur : JUILLET 2020 ;

Action 3 : Formation des utilisateurs le 28 AOÛT 2020 ;

Action 4 : Restriction de l'authentification forte à certains utilisateurs : OCTOBRE 2020 ;

Action 5 : Rédaction d'un projet de note d'information pour le démarrage du site pilote: OCTOBRE 2020.

Actions à venir :

- Signature de la note d'information pour le démarrage du site pilote ;
- Démarrage du site pilote.

Référence	Date	Correctifs apportés
SW_OTP_SF_01	18/09/2019	Version provisoire du 18/09/2019
SW_OTP_SF_02	29/04/2020	Mise à jour du choix de la solution et détail de la non-répudiation

MISES A JOUR

OBJET

Ce document présente les spécifications fonctionnelles de la mise en œuvre de l'authentification forte dans le SYDAM World.

Ces spécifications fonctionnelles ont été définies sur la base des informations contenues dans le cahier des charges élaboré à cet effet.

NB. Les spécifications techniques feront l'objet du document référencé SW_OTP_ST

TABLE DES MATIERES

INTRODUCTION

Les actualités le prouvent trop souvent : la combinaison identifiant / mot de passe ne suffit plus à protéger correctement les accès aux applications aussi bien personnelles que professionnelles. En 2014 déjà, les vols de mots de passe ont coûté près de 3 millions d'euros à l'économie mondiale. C'est pourquoi de plus en plus d'entreprises et particuliers se tournent vers d'autres moyens pour sécuriser leurs données. Afin de contrer tout piratage, nous devons désormais choisir des mots de passe plus longs et plus complexes, un procédé qui s'avère de plus en plus pénible et fastidieux.

Mais alors que le mot de passe est le mode d'authentification (dit simple) utilisé par les douanes ivoiriennes au travers de leur application métier SYDAM World, peuvent-elles envisager un autre moyen d'accéder à ses comptes en toute sécurité ? Comment la formule « moins de mots de passe = plus de sécurité » peut-elle marcher ?
L'authentification forte, en opposition à sa version « faible ou dite simple » permet de répondre pleinement à ces enjeux.

L'authentification forte est, en sécurité des systèmes d'information, une procédure d'identification qui requiert la concaténation d'au moins deux facteurs d'authentification.
Dans SYDAM World, l'authentification forte, ou authentification à deux facteurs, devra donc combiner quelque chose que l'on sait (login, mot de passe) avec une autre chose qui peut être un code reçu par sms sur son téléphone portable ou encore un élément biométrique.

Le présent document décrit l'existant en matière d'authentification des usagers dans SYDAM World, en relève les limites et fait des propositions de solutions en vue de son optimisation.

I- DESCRIPTION DE L'EXISTANT

Le SYDAM World est basé à l'heure actuelle sur une authentification simple composée du login et du mot de passe pour chaque compte utilisateur.

L'utilisateur possède des identifiants de connexion basés sur la possession d'informations spécifiques, le plus souvent un nom ou un code PIN / mot de passe.
Un compte regroupe les notions suivantes :

- **Utilisateur** : Il représente une personne (physique ou morale) ayant la capacité de se connecter à la plate-forme, il possède donc à minima un login.

Les utilisateurs possèdent les principales caractéristiques suivantes :

- **Nom et prénoms** : Ils permettent d'identifier la personne.
- **Login** : Le login est l'identifiant unique d'un utilisateur, il est notamment utilisé pour identifier l'utilisateur lors de la phase de login.
- **Mot de passe** : Le mot de passe est utilisé lors de la phase de login, il est crypté et stocké en base de données.
- **Adresse e-mail (optionnel)** : L'adresse e-mail de l'utilisateur est utilisée lors d'un envoi de mail à un utilisateur ou à un groupe d'utilisateurs.
- **Habilitations** : Elles correspondent aux droits d'accès associés à un utilisateur.
- **Désactivation de compte** : Un compte ne peut êtes supprimé cependant on peut la désactiver.

Munis de ces informations, les utilisateurs peuvent alors accéder à tout ou partie de leurs documents électroniques et d'autres informations sensibles les concernant, ou faire des opérations cruciales dans l'application métier SYDAM World.

II- CRITIQUE DE L'EXISTANT

- La sécurité des comptes actuelle repose uniquement sur les mots de passe : la connexion à SYDAM World se fait en utilisant un login et un mot de passe, laquelle constitue la vulnérabilité principale des systèmes d'information.

  Le problème, bien sûr, c'est que toute personne qui se procurerait ces identifiants de connexion peut également accéder aux mêmes informations et avoir les mêmes privilèges. Quiconque s'empare donc du mot de passe d'un compte peut simplement y accéder et en extraire des informations à volonté. La sécurité des comptes repose alors uniquement sur la robustesse des mots de passe qui, comme chacun le sait, est en général insuffisante. Personne n'aime mémoriser des chaînes de caractères mêlant majuscules, minuscules, chiffres et caractères spéciaux. Les utilisateurs veulent quelque chose de simple et facile à retenir, mais qui se trouve, par la même occasion, facile à pirater. Les principaux risques liés au mot de passe sont donc sa divulgation et sa faiblesse.

- Inexistence d'accord de non-répudiation : les mots de passe présentent de nombreuses limites. En premier lieu, ils ne fournissent pas une preuve d'identité suffisante.

  Aussi, l'absence d'accord de non-répudiation dans la gestion des comptes utilisateurs donne la possibilité à toute personne dont les paramètres de connexion sont engagés dans une transaction sur SYDAM World, de nier être l'auteur desdites opérations.

Vu ces faiblesses, la DSI a entrepris des actions à cours termes dont :

- La complexification des mots de passe par l'augmentation du nombre de caractères et l'exigence de caractères spéciaux ;
- L'activation de la demande de changement automatique du mot de passe chaque 03 mois (actions déjà réalisée) ;
- La sensibilisation des usagers à l'éthique et à la déontologie relatives à la confidentialité des mots de passe ;

Pour pallier ces limites de manière durable, l'intégration de l'authentification forte pour l'accès à SYDAM World se présente comme une solution idéale et respectant des normes en thème de sécurisation de la plateforme métier.

III- SOLUTION PROPOSEE

En effet, l'authentification forte prétend remédier aux problèmes de fraude et de vol d'identité de façon générale, en ajoutant un ou plusieurs facteurs de natures différentes, annihilant ainsi tous les défauts du mot de passe, et empêchant ainsi l'attaquant d'avoir un accès permanent aux informations de l'utilisateur. Les autres facteurs seraient bien plus compliqués à contourner ou dérober pour un attaquant, ce qui permet de rassurer les utilisateurs en leur garantissant un gain de sécurité considérable.

Par ailleurs, la protection renforcée qu'offre l'authentification forte permet aux entreprises d'utiliser des options de connexion plus avancées comme l'authentification unique (SSO). La méthode SSO valide l'identité de l'utilisateur par authentification multi facteur lorsqu'il se connecte. Une fois authentifié, l'utilisateur est connecté à son logiciel SSO. Il peut par la suite accéder aux applications prises en charge par ce logiciel, sans avoir à se connecter à chacune séparément.

Conscients que l'authentification multi facteur n'est pas une solution invulnérable et que son rôle est d'ajouter une ou des contraintes supplémentaires, qui sont plus fortes pour les attaquants potentiels, quelle solution technique proche de notre environnement système adopter pour protéger les données de notre application métier et à coût raisonnable ?

Dans le cadre de notre étude, nous avons retenu la technologie de l'authentification multi facteur « Code OTP transmis à la demande » qui a pris de l'ampleur ces dernières années, et suscité l'intérêt des grandes firmes tels que : Microsoft, Google, Amazone etc.
En effet notre environnement métier « SoClass » contient déjà une solution OTP (One time password) qui permet d'utiliser un code de sécurité en plus du login et du mot de passe SydamWorld de l'utilisateur.

- Dans la fenêtre d'authentification de SydamWorld, nous aurons un nouveau champ (code de sécurité) qui sera désactivé par défaut. Quand l'utilisateur saisie son login et mot de passe SydamWorld, le système enverra les informations encodées « token » et le numéro de téléphone de l'utilisateur soit à :
  - un service d'envoi de sms d'un opérateur télécom ou à
  - un équipement de SMSGateway qui est un type de passerelle SMS ou une passerelle MMS permettant à un ordinateur d'envoyer ou de recevoir des transmissions du service de messages courts (SMS) ou du service de messagerie multimédia (MMS) vers ou depuis un réseau de télécommunications.
- Dans les secondes qui suivent (la durée est fonction du choix de l'équipement ou de l'opérateur télécom), l'usager reçoit un code de sécurité valide su son téléphone mobile.
- Pendant ce temps, le champs code de sécurité sera activé tandis que les champs login et mot de passe seront désactivés. L'usager renseigne le nouveau champ activé de la fenêtre d'authentification avec le code de sécurité reçu dont la durée de validité est d'une minute. Si le code renseigné est identique au « token » généré par SydamWorld, alors il accède à la plateforme.
- En cas de tentative infructueuse, l'usager sera invité à reprendre le processus de connexion.

IV- ELABORATION D'UN ACCORD DE NON-REPUDIATION

4.1 Définition de la non-répudiation

La non-répudiation est le service de sécurité qui propose des solutions aux problèmes posés par les risques de répudiation. Il vient en complément des services tels que :

- L'intégrité des données ou authentification de données ;
- L'authentification des entités ou vérification de l'identité des parties en communication ;
- Les signatures digitales ;
- La confidentialité qui fournit des mesures de protection contre une révélation non-autorisée d'informations ;
- Le contrôle d'accès qui offre des outils permettant d'empêcher l'usage non autorisé de ressources.

En effet, Il est important que les parties impliquées dans une communication au travers d'un réseau ne puissent déclarer à tort avoir été étrangères à tout ou partie de la communication. Pour empêcher de tels comportements, des méthodes particulières de sécurité peuvent être mises sur pied, regroupées au sein du « service de non-répudiation » et définies dans un accord de non-répudiation.
Le but essentiel du service de non-répudiation est donc d'assurer une protection vis à vis d'une autre partie impliquée dans la communication (ou d'une panne du médium de communication qui les relie), plutôt que d'un attaquant extérieur.
Les preuves fournies par les mécanismes de non-répudiation permettront de convaincre une tierce partie de confiance (entité ayant les prérogatives d'une autorité et présentée comme un arbitre) de la réalité d'événements passés.
Cet arbitre statuera dans le cadre d'une dispute, évaluant la validité des preuves de non-répudiation présentées par les parties en dispute (ayant ainsi un comportement passif par rapport à la communication).

Dans notre cas, cette tierce entité de confiance pourrait être l'Inspection Générale des Douanes (IGD)

4.2 L'accord de non-répudiation

La procédure de gestion des habilitations pourrait servir de base de travail à la Direction en charge de la Réglementation et du Contentieux (DRC) pour l'élaboration d'un accord de non-répudiation intégrant l'entité tiers de confiance. Cet accord de non-répudiation qui sera signé par le requérant, sera rajouté à la liste des documents exigibles pour la demande de création de compte SYDAM.

Procédure existante gestion des habilitations :

1. La DSI reçoit une demande de création ou de mise à jour de login

Pour la création, les documents suivants sont à fournir :
- Fiche d'identification dument remplie et signée ;
- Une copie de la décision d'affectation du requérant ou le compte rendu de prise de service du requérant ;
- La copie de l'agrément pour les usagers non douaniers (Déclarants, Consignataires ...) ;
- Une copie de la pièce d'identité.

Pour la mise à jour, les documents suivants sont à fournir
- Une copie de la décision d'affectation du requérant ou le compte rendu de prise de service du requérant ;
- Une copie de la pièce d'identité ;
- Un courrier du supérieur hiérarchique.

2. Le DSI transmet la demande au bureau BAGMP par voie hiérarchique pour analyse et traitement

3. Le BAGMP procède à une analyse documentaire

4. Si la demande n'est pas recevable, le BAGMP saisit l'usager par téléphone ou par mail pour lui signifier l'irrégularité afin que celui-ci puisse reformuler sa demande.
   En cas de recevabilité, le BAGMP traite la demande conformément au profil de l'usager.

5. Le BAGMP communique le login et le mot de passe standard soit par courrier, mail ou par téléphone à l'usager.

Le système oblige l'usager à créer un nouveau mot de passe parce que le standard devient caduc dès la première connexion.

V- DICTIONNAIRE DE DONNEES

CODE	LIBELLE
SECUTYCODE	Code d'authentification OTP
USEROLDPASSWORDS	Ancien mot de passe
FORCEPASSCHANGE	Forcer le changement de mot de passe
USERPASSDATE	Date du mot de passe
CUSTOMERACCOUNTID	
ADDRESS	Adresse
CITY	Ville
ZIP	Code zip
COUNTRYCODE	Code pays
COUNTRYNAME	Pays
PHONE	Téléphone
CELLPHONE	Mobile
FAX	Fax
EMAIL	Email
LANGUAGE	Langue
NUMERICALTYPE	Type langue

JOB	Fonction
FULLNAME	Nom fonction
PHOTO	Photo
SIGNATURE	Signature
VOICE	Voix
FINGERPRINT	Emprunt digitale
EYEIRIS	Iris
CUSTOMERACCOUNTNAME	type de compte
CERTIFICATE	Certificat

LIENS

https://2013.jres.org/archives/34/paper34_article.pdf

https://weave.eu/cybersecurite-sommes-moyens-dauthentification/

https://www.biometrie-online.net/images/stories/dossiers/securite/RSA_01.pdf