HID® ActivID Push-based Authentication solution
Cible de sécurité CSPN

JUNE 2017
V1.1

hidglobal.com

TABLE OF CONTENTS

List of Tables

List of Figures

1. Glossaire

ActivID AS	ActivID Authentication Server
SSO	Single Sign-On
OTP	One Time Password (Mot de passe à usage unique).
MQ	Message Queue

2. Identification

2.1 Identification du document

Ce document décrit la cible de sécurité relative à l'appliance ActivID en vue de l'obtention d'une certification de sécurité de premier niveau des technologies de l'information (CSPN). Cette solution est constituée d'un serveur d'authentification et d'applications mobiles (Android et iOS).

2.2 Identification du produit

Editeur	HID Global
Site de l'éditeur	https://hidglobal.fr/
Nom commercial du produit	ActivID Authentication Appliance 8.0 et les applications mobiles (Android et iOS) HID Approve 2.0
Version évaluée	ActivID Appliance v8.0 – HID Approve v2.0
Catégorie de produit	Dispositif d'authentification (SSO)

3. Argumentaire du produit

3.1 Description générale du produit

Le système d'information d'une entreprise compte souvent un ensemble de services ayant chacun leur propre méthode d'authentification. L'appliance ActivID offre un ensemble de méthodes d'authentification communes pour tous les services d'une entreprise.

Les avantages de l'externalisation des fonctions d'administration sont les suivants :

- La délégation de l'authentification à un module conçu pour cette fonction. Cela permet une meilleure cohérence dans les méthodes d'authentification, une meilleure souplesse d'utilisation pour l'utilisateur final, et un meilleur suivit de ses actions sur les différentes applications.
- Les services métiers sont déchargés de cette fonctionnalité, et peuvent se concentrer sur les fonctions propres.

La solution ActivID et sa méthode d'authentification par notification PUSH se décompose en 4 parties :

- Un serveur principal d'authentification (Packagé sous forme d'appliance, contenant entre autre le logiciel ActivID Authentication Server), qui gère la base d'utilisateurs et vérifie leur authentification.
- Une application mobile (iOS ou Android) « HID Approve » permettant à l'utilisateur de valider une authentification, de valider une opération effectuée (un virement bancaire).et également de générer un mot de passe à utilisation unique.
- Un réseau de notification push : Apple Push Network et Google Cloud Messaging (supporté par les services cloud de Microsoft Azure).
- Une application cliente : il s'agit du service effectivement utilisé par l'utilisateur final (site de gestion bancaire par exemple).

Figure 1 : schéma organisationnel de l'architecture ActivID

3.2 Description de la manière d'utiliser le produit

La solution ActivID et sa fonction de validation PUSH, une fois installée, configurée et mis en route dans son environnement, est utilisée afin de valider les actions effectuées par un compte utilisateur sur les différents services à disposition.

Pour les besoins de l'évaluation, une application cliente de test est utilisée : il s'agit d'un service bancaire simplifié. Dans la suite du document, les appellations « le service » et « l'application cliente » réfèrent à cette application bancaire.

3.2.1 Workflow préalable d'enrôlement d'un smartphone pour l'authentification via notification PUSH :

- L'utilisateur souhaite valider des opérations via son mobile
- Il installe l'application « HID Approve »
- Il associe son téléphone à son compte ActivID AS (enrôlement du téléphone) :
  - L'utilisateur est identifié par le service (face-à-face, authentification par un autre moyen …)
  - Le service présente à l'utilisateur un QR code contenant diverses informations au format JSON.
  - L'utilisateur scanne le QR code avec l'application HID Approve
  - De façon transparente, l'application est initialisée et customisée (logo, fontes, couleur …)

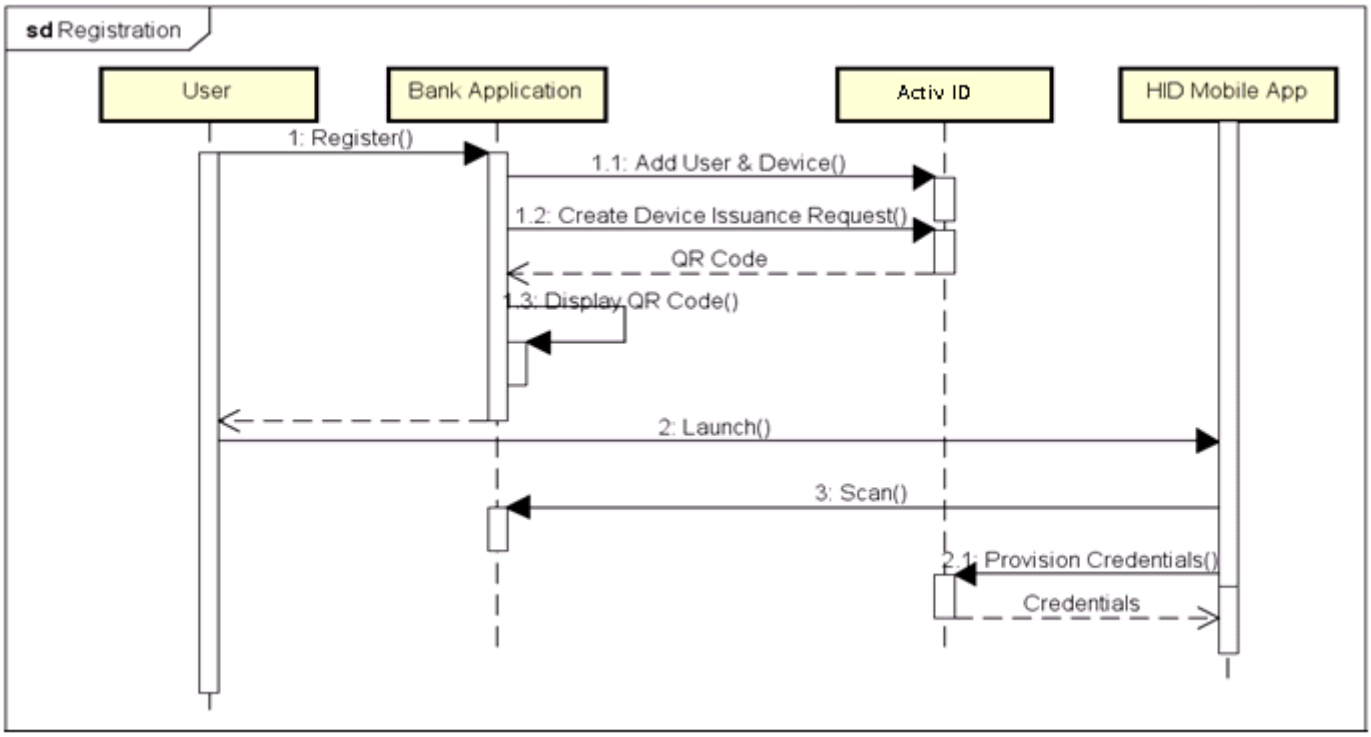

Figure 2 : Workflow de l'enrôlement du terminal mobile

3.2.2 Workflow nominal de l'authentification via notification PUSH :

- L'utilisateur initie une transaction (authentification, achat, virement bancaire …) sur un site web.
- Le site web demande la vérification de la transaction auprès d'ActivID AS.
- L'utilisateur reçoit une notification sur son appareil mobile, détaillant la transaction.
- Il approuve (ou refuse) la transaction
- ActivID AS reçoit le choix de l'utilisateur, et notifie le site web de la décision de l'utilisateur.
- Le site web prend en compte le choix effectué.

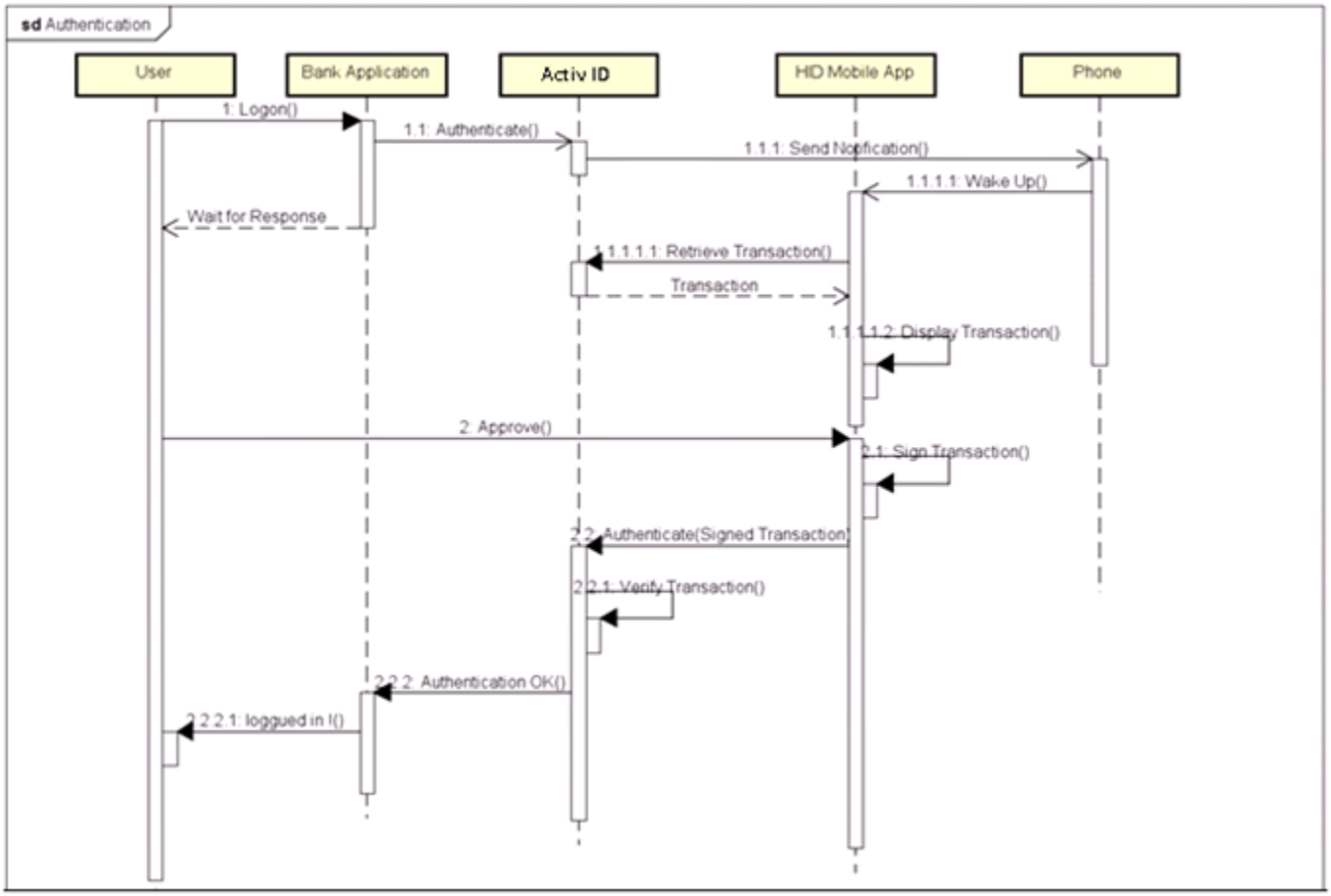

Figure 3 : Workflow d'une authentification via une notification PUSH

3.3 Environnement du produit

3.3.1 Environnement technique

3.3.1.1 ActivID Appliance

L'appliance évaluée possède les caractéristiques suivantes :

- Processeur Intel x86_64 (quad-cores)
- 8Gb de mémoire RAM
- Espace disque de 50Go

L'appliance est connectée à un HSM réseau Thales nShield Connect 6000+ – avec le driver/sdk Security World v12.300 x64

3.3.1.2 Terminaux mobiles

Les exigences relatives aux moyens matériels sont :

- les téléphones sont de type iPhone / Android
- sous Android, le terminal dispose d'un hardware avec TEE (Trusted Execution Environment) et supporte le système d'exploitation à la version minimum citée ci-dessous
- sous iPhone, le terminal dispose d'un hardware avec keyChain et supporte le système d'exploitation à la version minimum citée ci-dessous

Les exigences relatives aux versions de l'OS et des logiciels utilisés sont :

- iOS 10
- Android 6

3.3.2 Dépendances logicielles

3.3.2.1 Serveur ActivID AS

Les versions de l'OS et des middlewares intégrés sont :

- Oracle Linux 7.3
- Serveur reverse proxy NGINX 1.12.0
- Serveur d'administration système Webmin 1.831
- Serveur applicatif Oracle Weblogic 12c (12.2.1.2) avec Oracle JDK 8u131
- Base de données Oracle DB Server 12.1.0.2 (stockage des données et audit)
- Oracle Grid Infrastructure 12.2.0.1.0
- Apache ActiveMQ 5.14.1
- OpenSSL 1.0.1e-60.el7_3.1 x86_64 (dernière version distribuée par RedHat/CentOS/Oracle)
- OpenSSH 6.6.1p1-35.el7_3 x86_64 (dernière version distribuée par RedHat/CentOS/Oracle)

Les dépendances logicielles de l'application sont les suivantes :

- Apache Commons CLI 1.1
- Apache Commons Codec 1.9
- Apache Commons Collections 3.2.2
- Apache Commons Collections 4.1
- Apache Commons Discovery 0.5
- Apache Commons FileUpload 1.3.1
- Apache Commons HTTP Client 3.1
- Apache Commons IO 2.4
- Apache Commons Lang 2.6

- Apache Commons Lang 3.4
- Apache Commons Logging 1.1
- Apache Commons Logging 1.1.1
- Apache Commons Net 3.0
- Apache Commons Pool 1.5.4
- Apache CXF 2.7.10
- Apache HttpComponents Client 4.4
- Apache HttpComponents Core 4.4
- Apache Log4j 1.2.17
- Apache Velocity 1.7
- Apache XML Security for Java 1.5.6
- Nimbus JOSE + JWT 4.35
- Nimbus Language Tags 1.4
- Nimbus OAuth 2.0 SDK with OpenID Connect extensions 5.25
- Jackson streaming JSON parser 2.7.7
- Google Guava 18.0
- IAIK PKCS11 Wrapper 1.2.17.ac.1
- Shibboleth Java helper classes 7.1.1
- Shibboleth Spring framework extension 5.1.1
- Oracle JDBC driver 12.1.0.1
- Bouncy Castle PKIX 1.56
- Bouncy Castle provider 1.56
- Cryptacular Extension Library for BouncyCastle 1.0
- Hamcrest 1.3
- Joda-Time 2.8
- JSON Smart 1.3.1
- MiGBase64 2.2
- OpenSAML-Java 3.1.1
- PrimeFaces 6.0
- Simple Logging Facade for Java 1.7.6
- Java SMPP API 0.3.7.ac.1
- Spring Framework 4.3.3
- Spring LDAP 2.1
- XADisk 1.2.2
- OWASP AntiSamy for Java 1.2
- OWASP CSRFGUARD 3.1.0.2
- OWASP ESAPI 2.1.0.1
- Java-CSV 2.1
- WSDL4J - Web Services Description Language for Java 1.5.1
- Sun Java EE SDK 6.0

3.3.2.2 Terminaux mobiles

HID Approve v2.0.x embarque les middlewares suivants :

- Sous la version iOS :
  - OpenSSL (1.0.2k)
- Sous Android :
  - Android Google Repository (v46)
  - Android Support Repository (v47)
  - Android SDK tool (25.3.0)
  - SLF4J API (1.7.6)
  - Logback (1.1.1.2)
  - BouncyCastle library (1.56 (jdk15on))
  - concurrency annotation (1.0.1)

- JSON Smart library (1.3.1)
- Nimbus JOSE JWT Sources (4.35)
- Nimbus OAuth 2.0 SDK with OpenID Connect extensions (5.25)
- Nimbus-LangTag (1.4.3)
- Commons language (3.5)
- Commons Collections (4.1)
- Java Regex (1.2_01)
- Dexguard (7.3.18)
- Jackson (2.7.7)

4. Définition du périmètre

4.1 Périmètre évalué

La cible de l'évaluation est constituée de 2 composants : le serveur ActivID AS, et le terminal mobile (Android ou iOS). Seul l'enrôlement du terminal mobile, et le mécanisme de validation par notifications PUSH sont évalués.

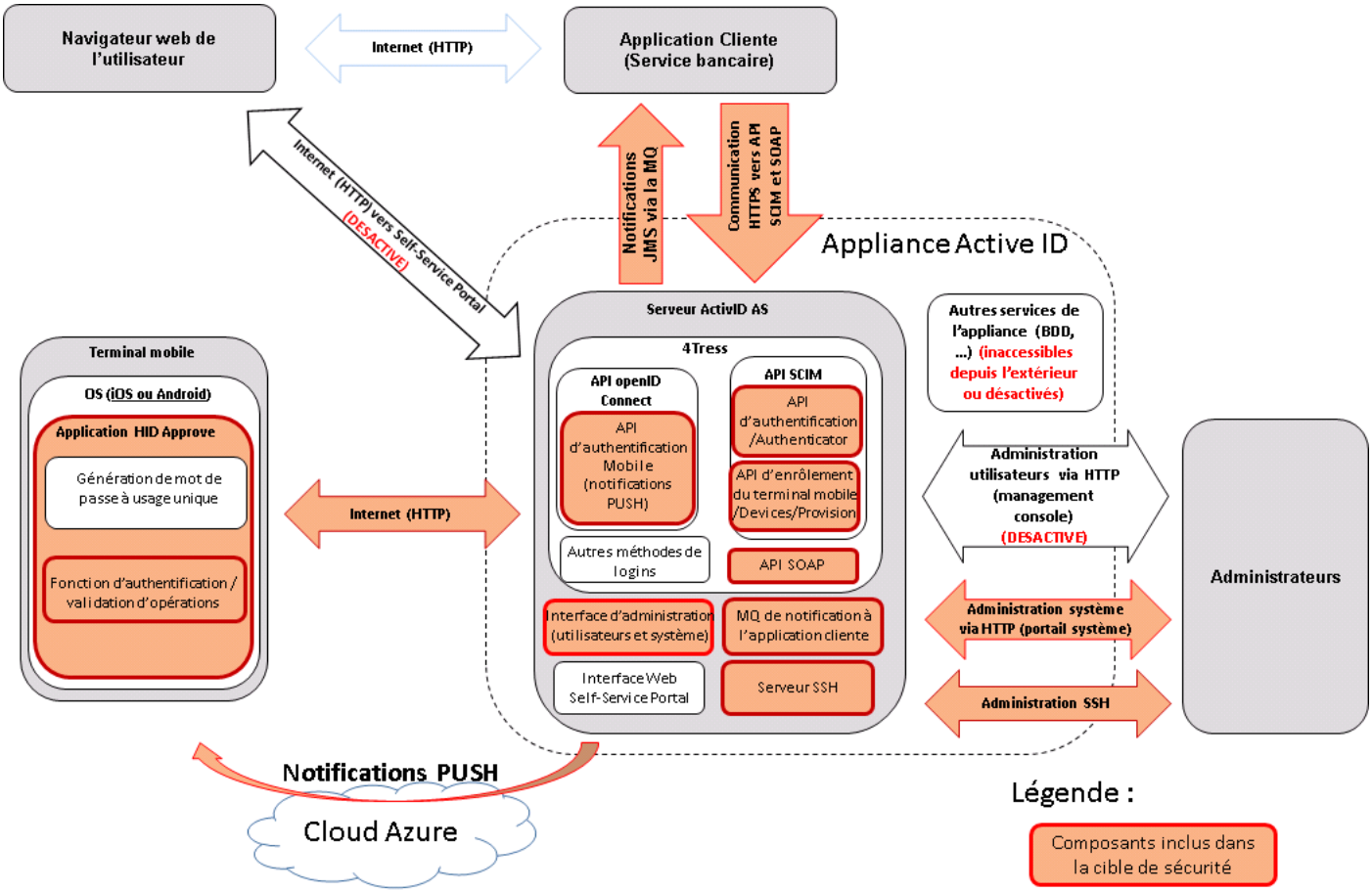

Figure 4 : schéma représentatif du périmètre évalué (en rouge)

Interfaces d'administrations :

L'appliance dispose de plusieurs interfaces d'administrations :

- Une interface d'administration système : https, port 1005. Elle permet de modifier la configuration de l'appliance, de contrôler les services lancés, modifier des paramètres réseaux, etc. …Cette interface est activée, accessible, et fait partie de la cible de l'évaluation.

- Une interface de management d'utilisateurs et du serveur Active ID AS lui-même, appelé la 'management console'. Celle-ci permet de créer des utilisateurs, modifier leurs droits, et modifier des paramètres liés au serveur Active ID. Pour l'évaluation, une fois le paramétrage effectué, cette interface est désactivée. Elle ne fait pas partie de l'évaluation.
- Une interface de management orientée vers l'utilisateur final, le 'Self-Service Portal', qui lui permet de gérer ses appareils et éventuellement d'en enrôler de nouveaux. Cette interface n'est pas nécessaire au fonctionnement de la solution, et est désactivée pour l'évaluation. Elle ne fait pas partie du périmètre et n'est pas accessible.
- Une interface SSH, pour accès au système à distance, qui fait partie de l'évaluation.

Font partie de l'évaluation :

- Pour les 2 applications mobiles HID Approve (iOS et Android)
  - La validation d'authentification
  - La validation d'opération (virement bancaire par exemple)
  - L'enrôlement du terminal
- Pour le serveur ActivID :
  - L'API d'authentification du mobile (OpenID)
  - L'API d'enrôlement du mobile (SCIM)
  - La Message Queue de notifications JMS entre le serveur ActivID et l'application cliente (service bancaire).
  - L'interface SOAP pour sur le serveur Active ID utilisée par l'application cliente.
  - Le serveur d'administration SSH
  - L'interface d'administration système.
- Canaux de communication :
  - Notifications PUSH : Seul le contenu des notifications est évalué. Le protocole de transport n'est pas contrôlé par le serveur ActiveID AS et n'est donc pas évalué.
  - Communication entre Terminal Mobile et Serveur ActivID
  - Message Queue entre Serveur ActivID et application cliente (service bancaire).
  - Communication SSH pour les administrateurs

Les fonctionnalités suivantes de la solution ne sont pas évaluées :

- Application HID Approve :
  - Génération de mot de passe à usage unique
  - Dispositifs anti clonage, anti-jailbreak, obfuscation, SSL certificate pinning et vérification de l'intégrité de l'application. L'obfuscation est réalisée avec Dexguard pour Android, et pour iOS, c'est avec Arxan Ensure IT.
  - Interface d'administration Self-Service Portal
  - Administration des utilisateurs du serveur ActivID AS (interface d'administration management console).
- Les différentes méthodes d'authentification sur le serveur qui ne sont pas utilisées par l'application mobile (mot de passe, question secrète, LDAP, SMS, OTP).
- La PKI (au sens création et gestion des certificats) n'est pas inclue dans la cible. Mais l'utilisation des certificats à des fins d'authentification fait partie de la cible.
- Sécurité des OS (Linux, Android et iOS)
- Sécurité et administration des services cloud (Microsoft Azure, Apple Push Network, Google Cloud Messaging)

- Services externes (PKI, LDAP, postes clients et périphériques).

4.2 Configuration évaluée

Le serveur ActivID est configuré pour utiliser HSM réseau Thales nShield Connect 6000 + avec le driver/sdk Security World v12.300 x64.

Une PKI externe est disponible et permet la génération de certificats (hors périmètre de l'évaluation).

L'application cliente utilisée est un service bancaire simplifié.

Les services Radius, SNMP, le Self-Service Portal et la Management Console du serveur Active ID AS sont désactivés et non accessibles.

L'interface d'administration système n'est pas accessible depuis internet.

4.3 Utilisateurs typiques

Cette section présente les différents intervenants possibles :

Administrateurs	Leur rôle est d'installer, de configurer et de maintenir le serveur ActivID AS. Ils disposent d'accès privilégiés au serveur (accès aux interfaces web d'administration, accès SSH).
Utilisateurs	Ils utilisent le système afin de s'authentifier.

4.4 Hypothèses sur l'environnement

H1 : Environnement physique sécurisé

Le serveur ActivID AS est installé dans un environnement d'exécution sécurisé. La machine sur laquelle il est installé est physiquement sécurisée (dans un local sécurisé).

H2 : Administrateurs de confiance

Les administrateurs sont considérés comme étant de confiances, non hostiles et formés à l'utilisation du produit.

H3 : Navigateurs à jour et fonctionnels

Les navigateurs internet des utilisateurs et administrateurs sont supposés fournir un minimum de fonctionnalités comme les cookies, certificats, le JavaScript, doit supporter la communication SSL (TLSv1.2) et une des suites de chiffrement suivantes :

- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-SHA384
- ECDHE-RSA-AES128-SHA256

Les navigateurs récents et couramment utilisés comme Microsoft Edge, Internet Explorer 11, Firefox, Safari et Google Chrome sont tous compatibles

H4 : Postes utilisateurs et administrateurs sécurisés

Les postes de travail des utilisateurs et administrateurs sont supposés être en accord avec la politique de sécurité de l'entreprise (mise à jour de sécurité, antivirus, …).

H5 : Services externes correctement configurés et utilisés

Les services externes utilisés (PKI, serveur DNS, …) doivent être correctement configurés et administrés, à jours des correctifs de sécurité. Les postes utilisateurs hébergent un OS à jour des correctifs de sécurité, correctement administrés et équipés d'un antivirus à jour.

H6 : Terminaux mobiles sûrs

Les terminaux mobiles utilisés sont considérés comme sûrs : aucune application malveillante n'est installée, à jour des correctifs de sécurités. Ils fonctionnent sous Android ou sous iOS. Ces terminaux ne sont pas 'rootés' ou 'jailbreakés', correctement configurés et administrés en accord avec la politique de sécurité de l'entreprise. Leur communication avec internet peut se faire en wifi (IEEE 802.11), ou via la connexion mobile du téléphone (2, 3, 4G). L'authentification de l'utilisateur sur son téléphone est considérée comme sûre.

H7 : Vol de terminal mobile détecté immédiatement

Le vol ou la perte d'un terminal est supposée être détectée immédiatement. Des protections appropriées sont supposées être mises en place afin de garantir l'absence de fuite d'informations dans ces cas. En particulier, l'application HID Approve ne peut pas être clonée sur un terminal malveillant.

H8 : Délivrance au bon utilisateur

On considère qu'un QR Code d'enrôlement de terminal n'est accessible que par l'utilisateur à qui il est destiné. En particulier, s'il est imprimé, il est transmis au bon utilisateur. L'obtention frauduleuse d'un QR code valide n'est pas considérée comme un vecteur d'attaque.

5. Biens sensibles à protéger

5.1 Biens de l'environnement

Certaines données concernant l'environnement du produit sont sensibles et doivent être protégées :

- **Les données utilisateur personnelles**, telles que l'identité, les attributs des utilisateurs, doivent rester confidentielles, intègres et correspondre à la réalité (authenticité).

5.2 Biens sensibles inclues dans la cible

Les biens que doit pouvoir protéger l'appliance ActivID sont de plusieurs types :

- **Configuration des équipements et services contenant des secrets**. Certaines informations de configurations sont publiques (URL de la page de connexion par exemple), mais la configuration du serveur peut contenir des informations secrètes (chaines de connexion à une base de données, mots de passe d'un service tiers, …).
- **Les mots de passes et informations de connexion** des utilisateurs ne doivent pas être divulgués.
- **Les informations concernant les sessions ouvertes** pour un utilisateur ne doivent en aucun cas être utilisées par un tiers, qui pourrait alors procéder à une usurpation d'identité. Les cookies et jetons de sessions ne doivent pas pouvoir être volés et/ou réutilisés, et doivent rester confidentiels et intègres.
- **Les secrets cryptographiques** utilisés pour les communications et l'élaboration des jetons de sessions sont protégés afin de conserver la confidentialité et l'intégrité.
- **Validation des opérations par l'utilisateur** auprès de l'application tierce, via le message queue et les notifications JMS.
- **Nature et description des opérations effectuées :** l'application cliente utilisée peut manipuler des données sensibles. La nature des opérations à valider et leur description peut contenir des informations sensibles (montant de virement bancaires par exemple).
- **Logs du serveur ActivID AS :** les logs du serveur ActivID AS contiennent des informations sensibles (opérations effectuées, connections des utilisateurs).

5.3 Caractéristiques de sécurité des biens

Bien sensible	Confidentialité	Intégrité	Authenticité	Disponibilité
Données utilisateur	X	X		
Secrets de configuration	X	X		
Mot de passes	X	X		
Informations sur les sessions ouvertes	X	X	X	
Secrets cryptographiques	X	X		
Validation des opérations	X	X	X	X
Nature et description des opérations	X	X	X	
Logs du serveur ActivID AS	X	X		

Tableau 1 : caractéristiques de sécurité des biens à protéger

6. Menaces sur le système

6.1 Vecteurs d'attaque

Application HID Approve détournée : un attaquant peut tenter d'usurper l'application HID Approve, afin d'accéder au système.

Service ActivID AS détourné : un attaquant peut tenter de se faire passer pour le serveur ActivID AS, afin de :

- Faire valider des actions frauduleuses par l'utilisateur (canal des notifications Apple/Google)
- Contourner la validation de l'utilisateur final sur le service client (canal http service client <=> ActivID AS)

Conformément à l'hypothèse H2 : les administrateurs sont supposés de confiance, et ne sont donc pas une menace pour le système.

6.2 Identification des menaces

M1 : Dénis de service applicatif sur l'enrôlement et la validation d'opérations

L'attaquant parvient à empêcher aux utilisateurs de se servir du système. Par exemple, il peut faire en sorte que toutes les opérations soient systématiquement refusées, ou parvenir à révoquer tous les terminaux mobiles utilisés. Les dénis de service survenant en surchargeant les capacités du serveur (envoie massif de données sur le réseau, surcharge d'utilisation du CPU ou de la RAM) ne sont pas considérés durant l'évaluation.

M2 : Vol d'information de connexion

Un attaquant réussi à obtenir le mot de passe ou le jeton de session d'un utilisateur légitime, lui permettant d'usurper son identité aux yeux du système.

M3 : Divulgation de données personnelles d'utilisateurs

Le système manipule des données concernant ses utilisateurs, qui peuvent être amenées à être divulguées à des personnes non autorisées.

M4 : Divulgation des opérations d'un utilisateur

Le système transmet les opérations effectuées par un utilisateur, qui présentent un intérêt et peuvent être amenée à être divulguées.

M5 : Bypass de l'authentification
L'attaquant obtient un accès au système sans s'être authentifié.

M6 : Bypass de la vérification d'opération
L'attaquant parvient à exécuter une opération nécessitant une approbation par le terminal mobile sans avoir à obtenir cette approbation.

M7 : Divulgation de la configuration
L'attaquant obtient illégalement une partie de la configuration du système. La lecture d'un paramètre excédant les droits utilisateur est également incluse sous cette menace.

M8 : Modification de la configuration
L'attaquant parvient à modifier une partie de la configuration. La modification d'un paramètre excédant les droits utilisateurs est également incluse sous cette menace.

7. Fonctions de sécurité du produit

7.1 Liste des fonctions de sécurité

Les principales fonctions de sécurité que le produit fournit sont :

FS1 : Communications sécurisées

Les utilisateurs accédant au système sont authentifiés afin de s'assurer de leur identité. Plusieurs méthodes d'authentification sont disponibles sur le serveur ActivID AS (login et mot de passe, certificat, …).

L'authentification du serveur ActivID AS auprès de l'application cliente et de l'application mobile HID Approve fait partie de la cible, ainsi que l'authentification de l'application cliente auprès du serveur Active ID (certificat client pour les notifications JMS).

Le terminal mobile doit être associé au compte de l'utilisateur avant de pouvoir être utilisé pour valider des opérations. Durant cette association, des clefs de chiffrements sont générées et utilisées pour chiffrer les échanges futurs. Cette association s'initie :

- Soit en enregistrant manuellement sur l'application HID Approve :
  - L'URL du service ActivID AS ;
  - L'identifiant de l'utilisateur final ;
  - Un code d'invitation à usage unique.
- Soit, plus simplement, en scannant avec le téléphone mobile un QR Code contenant ces informations au format JSON.

Ensuite, de manière transparente à l'utilisateur :

- L'application HID Approve s'authentifie auprès du serveur ActivID AS en utilisant les informations du QR Code (mot de passe à usage unique et url)
- Le serveur ActivID AS valide le mot de passe, ce qui permet d'établir une connexion sécurisée
- Le serveur ActivID AS récupère la demande d'association créée durant l'enregistrement de l'utilisateur.
- Le terminal mobile contacte le serveur pour obtenir les opérations en cours et définir une clé de chiffrement de session (utilise ECC-DH).
- Le terminal crée les clés publiques / privée / symétriques pour la validation des opérations de login, les validations des transactions et OATH

- L'application récupère les éléments de customisation (couleur, image, …), et ferme la connexion
- La demande peut être faite à l'utilisateur de changer le mot de passe de protection de ses clés.

FS2 : Vérification de l'opération par l'application cliente (service bancaire)

Le service web consulté par l'utilisateur (service bancaire par exemple) fait appel au serveur ActivID AS afin de demander la vérification de l'opération effectuée. Le serveur ActivID AS enverra une notification PUSH à l'utilisateur, obtiendra sa réponse, et la transmet ensuite au service web consulté vi la Message Queue.

Cette Message Queue correspond à des notifications JMS OOB transférées par un agent Apache ActiveMQ. L'authentification et le contrôle d'accès au niveau de la MQ reposent sur 2 librairies : JAAS Dual Authentication Plug-In (permet une authentification soit par login/mot de passe, soit par certificat), et Simple Authorization Plugin (gestion des droits lecture / écriture et admin sur les différents topics de la MQ).

FS3 : Vérification de l'opération par le serveur ActivID AS

Le serveur ActivID AS envoie des demandes sur le terminal mobile de l'utilisateur, afin d'obtenir son autorisation pour effectuer une action. Le terminal mobile aura au préalable été associé au compte de l'utilisateur. Le serveur ActivID AS doit s'assurer que la décision reçue provient bien de l'utilisateur concerné (grâce aux dispositifs cryptographiques mis en place).

FS4 : Stockage des clés sur le terminal mobile et sur le serveur ActivID AS.

Des clés de chiffrement assurant le bon fonctionnement et la confidentialité du service sont stockées sur le terminal mobile. Sur iOS, la clé de protection du terminal est stockée dans le service KeyChain. Les autres clés sont stockées dans une base de données chiffrée. Sous Android, la clé de protection du terminal est stockée à l'aide du hardware disponible (TEE). Toutes les autres clés sont stockées dans le Keystore BouncyCastle de type 'UBER'.

FS5 : Log des opérations effectuées et stockage sur le serveur ActivID AS.

Les opérations effectuées sur le serveur ActivID AS sont logués, et stockés de manière à ce que des utilisateurs non autorisés ne puissent pas y avoir accès. Ces logs sont protégés en intégrité : des numéros séquentiels sont attribués aux enregistrements, afin de détecter la suppression d'une ligne. Et chaque ligne est protégée en intégrité par un HMAC.

7.2 Couverture des besoins de sécurité

7.2.1 Menaces - biens sensibles

	Configuration	Données utilisateur	Mot de passes	Informations sur les sessions ouvertes	Secrets cryptographiques	Validation des opérations	Nature et description des opérations	Logs du serveur ActivID AS
M1 : Dénis de service	X				X	X		
M2 : Vol d'informations de connexion			X	X	X	X		
M3 : Divulgation de données utilisateur		X	X					X
M4 : Divulgation des opérations d'un utilisateur							X	X
M5 : Bypass de l'authentification		X				X	X	
M6 : Bypass de la vérification d'opération						X		
M7 : Divulgation de la configuration	X							

M8 : Modification de la configuration	X							

Tableau 2 : Récapitulatif des menaces sur les biens sensibles

7.2.2 Fonctions de sécurité - menaces

	M1 : Dénis de service	M2 : Vol d'informations de connexion	M3 : Divulgation de données utilisateur	M4 : Divulgation des opérations d'un utilisateur	M5 : Bypass de l'authentification	M6 : Bypass de la vérification d'opération	M7 : Divulgation de la configuration	M8 : Modification de la configuration
Fonctions de sécurité								
FS1 : Communications sécurisées	X	X	X	X	X	X	X	X
FS2 : Vérification de l'opération par l'application cliente						X		
FS3 : Vérification de l'opération par le serveur ActivID						X		
FS4 : Stockage des clefs sur le terminal et sur le serveur ActivID AS	X	X	X					
FS5 : Log des opérations effectuées et stockage sur le serveur ActivID AS.							X	X
Hypothèses								
H1 : Environnement physique sécurisé	X							
H2 : Administrateurs de confiance	X		X	X	X	X	X	X
H3 : Navigateurs à jours et fonctionnels		X					X	
H4 : Postes utilisateurs / admin sécurisés		X	X				X	
H5 : Services périphériques sécurisés		X	X				X	
H6 : Terminaux mobiles sûrs	X	X	X	X				
H7 : Vol de terminal détecté immédiatement	X	X	X	X				
H8 : Délivrance au bon utilisateur		X	X	X				

Tableau 3 : récapitulatif des fonctions de sécurité et hypothèses contrant les menaces.