STID

Certificat d’audit

Applications mobiles Android et iOS **STID MOBILE ID**

PHONESEC

Note de version

Dates d'audit	Avril 2017		
Auditeur	Benjamin NABET @Phonesec	Expert sécurité	
Validation	Pascal CAPUANO @Phonesec	Directeur des projets fraude et sécurité	
Lieu	France		

1. Périmètre et conditions générales des tests

Le périmètre de la prestation est défini par le lot de fonctionnalités accessibles via l'application **STID MOBILE ID en version 1.0.3 (025) de production pour la plateforme iOS, et 1.0.83 de production pour la plateforme Android**.

Ce certificat présente la méthodologie et l'appréciation globale des résultats d'audit.

2. Méthodologie de l'audit

L'application a profité d'une analyse statique et d'une analyse dynamique, flux inclus. Au regard des fonctionnalités de l'application, le plan de test ci-après a été retenu. Chaque test fait l'objet d'un ou plusieurs contrôles selon les exigences de l'analyse.

2.1. Analyse statique

1	Package d'installation
2	Requêtes sur la base de données
3	Appels aux interfaces
4	Rôle des Webview vis-à-vis des entrées utilisateurs
5	Rôle des Webviews vis-à-vis de contenus tels que Javascript ou autre
6	Utilisation du clipboard
7	Algorithmes de chiffrement
8	Algorithmes de hachage
9	Sécurisation de la clé de chiffrement
10	Partage de la clé de chiffrement
11	Recherche de données sensibles codées en dur dans l'application
12	Données personnelles ou privés
13	Obfuscation du code
14	Mécanisme anti-recompilation
15	Mécanisme de détection du root

2.2. Analyse dynamique

1	Stockage de données sensibles en mémoire
2	Stockage de données sensibles dans des fichiers de préférence
3	Stockage dans des bases de données
4	Création de fichiers contenant des données sensibles
5	Exécution de l'authentification
6	Exécution des autorisations
7	Robustesse du schéma d'authentification
8	Contrôle de l'authentification
9	Contrôle des autorisations

10	Identification
11	Robustesse de l'identifiant de session
12	Stockage de l'identifiant de session
13	Données soumises aux interfaces
14	Accès aux interfaces de l'application
15	Utilisation de composants web
16	Logue de données
17	Création de fichiers temporaires
18	Création de fichiers temporaires
10	Stockage de données en mémoire
20	Exposition de champs sensibles
21	Autocorrection
22	Robustesse des clés de chiffrement
23	Sécurisation des données sensibles transitant sur le réseau (flux)
24	Mécanismes de protection protocolaires (flux)

3. Appréciation

Dans la mesure où l'application permet d'ouvrir des accès physiques, la sensibilité est de facto élevée. Phonesec test de nombreuses applications mobiles dont le niveau de sécurité requis est élevé, dans le même secteur d'activité ou pour des secteurs d'activités comparables.

L'application de STID présente des garanties de sécurité qui la situe dans la frange haute des applications mobiles (sur la base des analyses statiques et dynamique effectuée). L'audit ne révèle pas de faille directement exploitable, ce qui permet de positionner le niveau de sécurité de l'application à un niveau élevé pour le domaine d'application et les exigences de protection.

4. A propos de Phonesec

Cette étude a été réalisée par la société PHONESEC pour le compte de STID.

PHONESEC est une société française indépendante créée en 2002, labellisée France Cybersecurity. Ses spécialités sont le conseil et l'ingénierie dans la sécurité de l'information ainsi que la lutte contre la fraude dans les nouvelles technologies. Ses références actives sont entre autres les sociétés Bouygues Télécom, Gemalto, la GSMA, H3G, Orange Group, Price Minister, mutuelle France Plus, Caisse d'Epargne, Gendarmerie Nationale, Eurocopter, Samsung, SFR, TCL, Vodafone Group, VSC Technologies, CMA CGM, Showroomprivé, Snef, et de nombreuses autres.

Contact
PHONESEC
27 boulevard Charles Moretti
13014 Marseille
France

Site Internet : http://www.phonesec.com
Email : contact@phonesec.com