Audit certificate

Android and iOS mobile applications STID MOBILE ID + Web Platform

Phonesec

Version

Audit period	Mars 2018	
Auditor	Younes Benzagmout @Phonesec	Security expert
Validation	Pascal CAPUANO @Phonesec	Fraud and security projects director
Place	France	

Phonesec est une entreprise labélisée France Cybercecurity

1. Scope and overall testing conditions

The scope of the service is defined by the functionalities accessible via the STID MOBILE ID applications which versions are **1.0.8 (0.8) for the iOS platform, and v1.1.129d for the Android platform**. The web platform also included in the perimeter was, during the test period intended to security acceptance, and was compliant with the upcoming public platform.

This certificate introduces the methodology and an overall assessment based on the audit results

2. Methodology

The application was subjected to a static and a dynamic analysis, including a flow analysis. Due to the application functionalities, the following test plan has been approved. Each test can itself be based on one or several controls depending on particular requirements.

2.1. Static analysis

1	Installation package
2	Queries on database
3	Interfaces recall
4	Clipboard
5	Cyphering algorithms
6	Hashing algorithms
7	Securing the cyphering keys
8	handling the cyphering keys
9	Code obfuscation
10	Verification of the signature certificat

2.2. Dynamic analysis

1	Sensitive data in memory
2	Sensitive data in preference file
3	Sensitive data in database
4	Creation of files containing sensitive data
5	Authentication
6	Authorisations
7	Strength of the authentication scheme
8	Control of authentication
9	Control of authorisations
10	Identication
11	Strength of the session identifier
12	Data submitted to interfaces
13	Access to application interfaces
14	Use of web components
15	Data logging
16	Managing exceptions
17	Caching pictures

18	Temp files
19	Exposition of sensitive fields
20	Autocorrecting
21	Strength of the cyphering keys
22	Controling system (root / jailbreak)
23	Access to personal data
24	Webview usage
25	Application debugging
26	Application Backup

2.3. Flow analysis

1	Securing data transmitted over the network (flow)
2	SSL Pinning
3	Certificate validity

2.4. Forensic analysis

1	Information accessible once installed

2.5. Web server application test method

The web application has been subjected to a security analysis including all Top 10 OWASP (www.owasp.org) vulnerability check. None of them was or discovered neither remained without a relevant correction.

Tests
Test 1 : Cookies entropy
Test 2 : Cookies security options
Test 3 : Cross Site-Scripting
Test 4 : Session fixation
Test 5 : CRLF injection
Test 6 : Cross Site Request Forgery - CSRF
Test 7 : Communication protection
Test 8 : Force brute mechanisms
Test 9 : Directory listing
Test 10 : Users enumeration
Test 11 : Denial of access
Test 12 : Password policy
Test 13 : Disclosing technical information
Test 14 : SQL injection

Tests
Test 15 : File Upload
Test 16 : Cross Site-Flashing
Test 17 : Insecure Direct Object Reference
Test 18 : Patch management
Test 19 : http headers security

3. Assessment

Because the application enables to open physical accesses, sensitivity is high de facto. Phonesec is used to test numerous mobile applications of which the required security level is high, in the same or similar business sectors.

The 3 tested applications offers security guaranties which are in the top end of mobile applications in terms of security protections. The audit does not reveal security breaches which would be directly exploitable, enabling to confirm a high security level regarding the application target and the security requirements.

4. About Phonesec

These audits were performed by PHONESEC on behalf of STID.

PHONESEC is an independent French company created in 2002, France CyberSecurity certified. It specializes in information security consulting and engineering and combating fraud in new technologies. Its current clients include 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, Cdiscount, Sanofi, Allianz, and many other worldwide companies.

Contact
PHONESEC
27 boulevard Charles Moretti
13014 Marseille
France

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