STID

Audit certificate

Android and iOS mobile applications STID MOBILE ID

PHONESEC

Version

Audit period	April 2017		
Auditor	Benjamin NABET @Phonesec	Security expert	
Validation	Pascal CAPUANO @Phonesec	Fraud and security Project Director	
Lieu	France		

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 **1.0.3 (025) for the iOS platform, and 1.0.83 for the Android 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	Webview VS user entries
5	Webviews VS contents (such as Javascript)
6	Clipboard
7	Cyphering algorithms
8	Hashing algorithms
9	Securing the cyphering keys
10	Sharing the cyphering keys
11	Sensitive data hard coded in the application
12	Personal or private data
13	Code obfuscation
14	Anti-recompilation mechanism
15	Root detection mechanism

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	Storage of the session identifier
13	Data submitted to interfaces
14	Access to application interfaces
15	Use of web components
16	Data logging
17	Creation of temp files
18	Storage of data in memory
19	Exposition of sensitive fields
20	Autocorrecting
21	Strength of the cyphering keys
22	Securing data transmitted over the network (flow)
23	Flow protection

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 STID Mobile ID application offers security guaranties which are in the top end of mobile applications (on the basis of the static and dynamic analysis). 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. A propos de 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