M800 SDK™ Software Development Kit

Strong Authentication for Mobile Apps

M8oo SDK™ is a library module very easy to be used for the development of mobile apps for **OTP** (One Time Password) Strong Authentication to web services. The mobile app developed with M8oo SDK is an OTP software token. By using M8oo SDK, in fact, the mobile app developer can implement easily mobile applications which the user can use to safely get the OTP codes.

M8oo SDK allows to integrate several kind of OATH token: TOTP, OCRA-1, 6 or 8 digit, SHA1 or SHA256 algorithms.

M8oo SDK together with **IAP8oo® Strong Authentication Server** (developed by IRETH) are the most reliable and secure solution to realize OTP tokens for mobile, cutting down the risks of on-line frauds and on-line attacks such as "Phishing" and "Man-In-The-Middle".

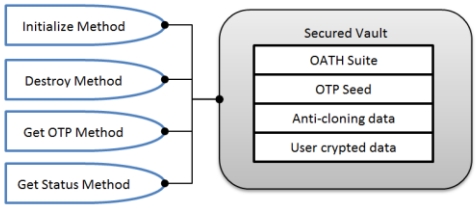
M8oo SDK is released for the most popular mobile operating systems (Android, iOS, Windows Phone), currently used by the most important brands such as Apple, Samsung, LG, Nokia, etc.

M8oo SDK grants the development of OTP apps with the very best security, **not clonable**: its technology allows, in fact, to develop OTP mobile apps univocally related to the mobile (smartphone) hardware, tracking the hardware's itself **fingerprint**.

M8oo SDK provides the same security level as OTP Displaycard/Token without their related costs (electronics&management).

M8oo SDK grants a very high security level for the sensitive data management. The sharing of secret keys used for the OTP code generation is absolutely safe thanks to the encrypted code which is mutually authenticated by IAP8oo® Server.
It is robust against reverse engineering and cracking.

M8oo SDK keeps the OTP generation data in a **specific encrypted Vault**. M8oo SDK allows the mobile app developer to access to use custom encrypted Vault in order to store further sensitive data in a very secure way.



- Complete & Easy-to-Use Primitive Functions
- Non Clonable
- Anti Frauds
- Safe Enrollment Process

How it works – 3 simple steps

1 – The Mobile App creates an OTP token by **M8oo SDK** on the mobile device, this token is not initialized yet
2- The OTP token will be initialized by receiving and validating two encrypted data packets provided by the IAP8oo® Authentication Server; these two packets are:
- Parameters for a safe communication between the OTP token and the IAP8oo® Authentication Server
- The Secret Keys which generate the OTP code. These keys will be safely stored within the OTP token of the mobile device.

3 – The Mobile App, when needed, requires the **M8oo SDK** to generate the OTP code in order to grant a Strong Authentication service.

The Mobile App can delete the installed OTP token and all its related data at any time by using the specific primitive function available from the **M8oo SDK**.

During the OTP token installation, the **M8oo SDK** scans the mobile device verifying eventual jailbreak conditions, the **M8oo SDK** alerts in case of not-secure environment, but the OTP token can be installed anyway if required by the user.

M8oo SDK quickly and reliably implements Strong Authentication functions within Mobile Apps with no need of any specialized technical skills about advanced security algorithms and protocols.

M8oo SDK perfectly suits Mobile Apps related to:

- E-banking
- E-commerce
- Remote Access (VPN)
- Remote Digital Signature

M8oo SDK is currently released for the following mobile operating systems:

- Android (version 4.0 or later)
- Apple iPhone iOS (version 7.x or 8.x)
- Windows Phone (version 7.x or later)

M8oo SDK supports the OATH standard authentication suite, with also PIN code (optional):

TOTP: Time Based OTP

OCRA: Challenge-Response Based OTP

iPhone

android

Windows Phone

ireth

Head Office: Via Capovilla, 73 – 36030 Villaverla (VI) | Headquarters: Via Genovesi, 19 - 10128 Torino
P. IVA 03245560242 Tel. +39 011 5089293 – Fax +39 011 5089999 info@ireth.net www.ireth.net