Better security measures for smartphones, ENISA has created a SMAShiNG new tool!

ENISA releases SMAShiNG – SMArtphone Secure developmeNt Guidelines – an online tool that maps security measures for smartphone guidelines. The tool supports developers to build secure mobile applications.

Published on February 12, 2019



© Copyright: Shutterstock

Tagged with

* [Internet of things](https://www.enisa.europa.eu/search?Subject%3Alist=Internet%20of%20things)

The [SMAShiNG tool](https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/smartphone-guidelines-tool" \t "_self) supports developers to build secure mobile applications. It is technologically agnostic, hence can be applied to all mobile applications developed for any operating system on the market nowadays

New developments in both software and hardware area have resulted into new significant threats for the mobile computing environment, highlighting the need for a tool to help the developers’ community. SMAShiNG touches upon crucial security measures such as:

* User authentication;
* Sensitive data protection;
* Secure software distribution;
* Device and application integrity;
* Protection from client side injections;
* Correct usage of biometric sensors.

SMAShiNG makes it easier for the developers’ community to follow guidelines, by selecting only the ones that are relevant to them. The tool allows for selecting security measures associated with a specific domain and export them as a checklist to follow in the design phase, based on the requirements of the developer.

The security measures featured by SMAShiNG are defined in the [ENISA Smartphone Secure Development Guidelines](https://www.enisa.europa.eu/publications/smartphone-secure-development-guidelines-2016) report, which provides a guide for developing secure mobile applications.

The release of SMAShiNG is an important part of ENISA’s continuous work in promoting the ‘security-by-design’ principle, by which strong cybersecurity is built into products as early as the design phase, easing the burden of EU citizens to secure their devices and products.

SMAShiNG complements the work done by ENISA in this area, such as the[recently launched online tool for IoT and Smart Infrastructures](https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot/good-practices-for-iot-and-smart-infrastructures-tool)and the [privacy enhancing technologies (PETs) knowledge management and maturity assessment](https://www.enisa.europa.eu/publications/pets-maturity-tool).

ENISA aims to implement a series of enhancements and to broaden the scope of this tool, in order to facilitate users’ live interaction with security recommendations through a visualised and interactive page.