Blockchain Security 2Go

Short Product Overview

Description

The Blockchain Security 2Go is a starter kit for development of secured blockchain applications like crypto currency wallets (e.g. Bitcoin, Ethereum) or eSignature/PKI. It supports the most important security functions on a highly fraud protected chip and provides dedicated APIs for an external communication via contactless interface to e.g. a NFC smartphone. An Android based API incl. example application is available on top of it.

The high security chip provided with the kit can be integrated into most common blockchain ecosystems to safeguard user credentials against various attacks like cloning, forgery etc. This emphasizes the security of the whole system in comparison with only software based solutions.

The starter kit contains

- 5 credit card sized ID1 cards based on ISO/IEC 7810 having a contactless interface and a Class 1 communication antenna based on ISO/IEC 14443.
- On-card software that supports commands for key-management, signature creation and PIN authentication.
- Open-source software that exemplifies how to integrate the features of the Blockchain Security 2Go cards in a real-world Blockchain system (e.g. sending cryptocurrencies or integrating the cards in a smart contract for eVoting). The software is hosted on GitHub https://github.com/Infineon/Blockchain.

Features

Hardware Features

- ID1 contactless card
- Supported interface: ISO/IEC 14443 (NFC)
- Cryptographic support: TRNG, ECC, AES

Software Features

- PIN Authentication
- Generate ECC keypair (secp256k1)
- Get Public Key
- Generate signature
- Encrypted keyload
- Storage of up to 255 keypairs
- Preloaded ECC curve (secp256k1) for e.g. Bitcoin, Ethereum

Applications

- Compatible to Android 6+
- Crypto currency wallet example
- eVoting example based on Ethereum

Example of open source android APP interaction with public APIs such as blockchain.info

Applications

Product name	**Blockchain Security 2Go**
Product description	Blockchain starter kit
Interfaces	ISO/IEC 14443
Memory	500kByte SOLID FLASH™ NVM 12kByte RAM
CPU	16-bit
Symmetrical cryptography	AES 256bit
Asymmetrical cryptography	ECC 256bit
Ambient temperature	-25 to + 85 °C (Chip) -25 to + 70 °C (ID1 card body)
Delivery forms	ID1 card(s)
Typical applications	Most common Blockchain applications like Bitcoin wallet, Ethereum smart contract, eSignature, Asset Management

For further information on technology, delivery forms and conditions please contact your nearest Infineon Technologies sales representative (www.infineon.com)

Edition 2019-03-14

Published by

Infineon Technologies AG

81726 München, Germany

Do you have a question about this document?

Email: erratum@infineon.com

Document reference

IMPORTANT NOTICE

The information given in this document shall in no event be regarded as a guarantee of conditions or characteristics (“Beschaffenheitsgarantie”) .

With respect to any examples, hints or any typical values stated herein and/or any information regarding the application of the product, Infineon Technologies hereby disclaims any and all warranties and liabilities of any kind, including without limitation warranties of non-infringement of intellectual property rights of any third party.

In addition, any information given in this document is subject to customer’s compliance with its obligations stated in this document and any applicable legal requirements, norms and standards concerning customer’s products and any use of the product of Infineon Technologies in customer’s applications.

The data contained in this document is exclusively intended for technically trained staff. It is the responsibility of customer’s technical departments to evaluate the suitability of the product for the intended application and the completeness of the product information given in this document with respect to such application.

For further information on the product, technology, delivery terms and conditions and prices please contact your nearest Infineon Technologies office (**www.infineon.com**).

WARNINGS

Due to technical requirements products may contain dangerous substances. For information on the types in question please contact your nearest Infineon Technologies office.

Except as otherwise explicitly approved by Infineon Technologies in a written document signed by authorized representatives of Infineon Technologies, Infineon Technologies’ products may not be used in any applications where a failure of the product or any consequences of the use thereof can reasonably be expected to result in personal injury.