Infineon ID Key S USB – SLC38DUA800A8

Description

- Combination of a Secure Element and a USB-serial bridge, delivered as a System-in-Package (SiP).
- Optimized for multi-application USB security devices and security tokens.

Features

Secure Element

- SOLID FLASH™ dual-interface, contact-based and contactless security crypto controller
- 32-bit architecture based on the 100MHz clocked Arm® SecurCore® SC300 enhanced by Infineon Technologies' cache and security technology
- Supported interfaces: UART, contactless interface (RFI), NFC, I2C target, and GPIO
- 800 kB user SOLID FLASH™ NVM
- 24 kB user RAM
- Certification level: CC EAL 6+ (high)
- NFC

USB-serial bridge

- USB 2.0 Full-Speed Interface with on-chip clock recovery and on-chip USB voltage regulator
- Cortex M0 (48 MHz)
- 32 kB flash memory, 4 kB SRAM
- Supported interfaces: USB 2.0 Full-Speed, I2C controller, CAPSENSE™, and SWD

Applications

- Authentication
- FIDO security keys for device-bound passkeys
- Digital Signature
- Encryption
- Logical and physical access
- Software protection and management
- Cold wallets / cryptocurrency hardware wallet

Parameters

Product name	Infineon ID KEY S USB – SLC38DUA800A8
Product description	System-in-package comprising a SOLID FLASH™ 32-bit security crypto controller and a USB-serial bridge in one single package optimized for multi-application USB devices
Interfaces and protocols	UART, ISO/IEC7816, GPIO, I2C, ISO/IEC 14443, for both type A and/or type B, ISO/IEC 18092 (NFC passive mode), CAPSENSE™, SWD, USB 2.0
Secure Element CPU Memory Symmetrical cryptography Asymmetrical cryptography	 32-bit Arm® SecurCore® SC300 (100 MHz) 800 kB SOLID FLASH™ NVM, 24 kB RAM DES, Triple DES, AES up to 256-bit RSA up to 4096-bit, ECC up to 521-bit
USB-serial bridge CPU Memory	 Cortex® M0 (48 MHz) 32 kB flash NVM, 4 kB SRAM
Ambient temperature	-25 to + 85 °C
Contact and dual interface package delivery forms	SMD package VQFN-28-4 (4x4x0.85 mm)
Typical applications	multi-application USB security devices and security tokens
Compliance	CC EAL6+ (high) Hardware prepared for FIPS 140-3 composite certification BSI AIS20/31 RNG (PTG.2, PTG.3, DRG.3, DRG.4)

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

Published by
Infineon Technologies AG
Am Campeon 1-15, 85579 Neubiberg
Germany

© 2023 Infineon Technologies AG
All rights reserved.

Public

Date: MM/2024

Please note!
This Document is for information purposes only and any information given herein shall in no event be regarded as a warranty, guarantee or description of any functionality, conditions and/or quality of our products or any suitability for a particular purpose. With regard to the technical specifications of our products, we kindly ask you to refer to the relevant product data sheets provided by us. Our customers and their technical departments are required to evaluate the suitability of our products for the intended application.

We reserve the right to change this document and/or the information given herein at any time.

Additional information
For further information on technologies, our products, the application of our products, delivery terms and conditions and/or prices, please contact your nearest Infineon Technologies office (www.infineon.com).

Warnings
Due to technical requirements, our 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 us in a written document signed by authorized representatives of Infineon Technologies, our products may not be used in any life-endangering applications, including but not limited to medical, nuclear, military, life-critical or any other applications where a failure of the product or any consequences of the use thereof can result in personal injury.

Scan QR code and explore offering
www.infineon.com