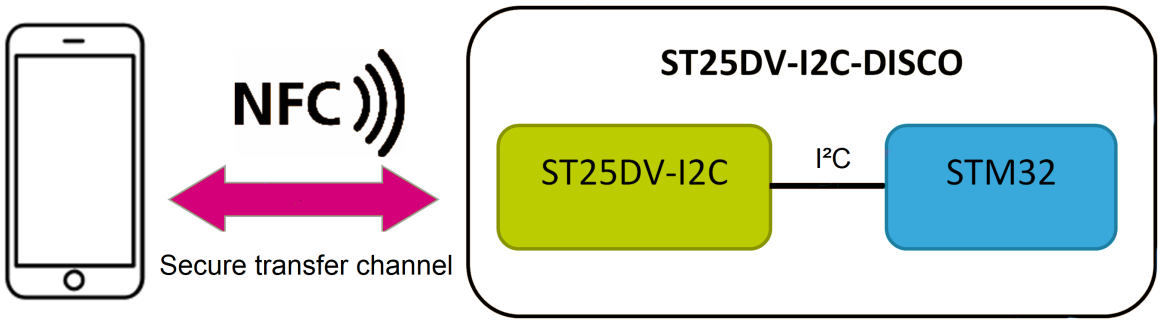
STSW-ST25003

Data brief

ST25DV-I2C CryptoDemo Android application



Product status link
STSW-ST25003

Features

- Encryption of all NFC bidirectional communications between an Android™ phone and an STM32 microcontroller
- Fast communications over NFC, using ST25DV fast transfer mode
- AES and ECC cryptography
- Mutual authentication between the Android phone and the STM32 microcontroller
- Establishment of a unique AES session key
- Encryption can be used to retrieve data, set device settings or update the firmware securely

Description

The ST25DV-I2C CryptoDemo Android application shows how to establish a secure transfer channel over NFC, between an STM32 microcontroller and an Android smartphone. It uses the fast transfer mode (FTM) feature of the ST25DV-I2C NFC Tag.

The items available for this demonstration are: this Android application (STSW-ST25003), the firmware (STSW-ST25DV003), a user manual (UM2575), and application note (AN5323). An ST25DV-I2C-DISCO board is required to run the demonstration.

This demonstration establishes a secure transfer channel by using cryptography to perform mutual authentication and to encrypt the communications over NFC. This secure transfer channel is used during the demonstration to securely send and retrieve data, perform the device settings, and upload new firmware.

Only the granted user may communicate with the STM32 microcontroller to perform these operations. All the communications are encrypted between the microcontroller and the Android phone in both ways, so that the user can configure the product or retrieve data securely.

1 License

STSW-ST25003 is delivered under software license agreement SLA0052.
The software components provided in this package come with different license schemes as shown in Table 1.

Table 1. Software component license agreements

Software component	License type	License details
Graphview	Apache License, Version 2.0	https://github.com(1)
HKDF		
TIMBER		
Conscrypt		
commons-lang		https://mvnrepository.com(2)

1. *Search for the component in the Git repository.*
2. *Search for the proper version of the component in the MVN repository.*

STSW-ST25003 runs with a 32-bit microcontroller based on the Arm® Cortex®-M4 CPU with FPU high-performance microcontroller.

Note: Arm is a registered trademark of Arm Limited (or its subsidiaries) in the US and/or elsewhere.

Revision history

Table 2. **Document revision history**

Date	Version	Changes
13-Jun-2019	1	Initial release.

Contents

1 License 2
Revision history 3
Contents 4
List of tables 5

List of tables

Table 1. Software component license agreements 2
Table 2. Document revision history 3

IMPORTANT NOTICE – PLEASE READ CAREFULLY

STMicroelectronics NV and its subsidiaries (“ST”) reserve the right to make changes, corrections, enhancements, modifications, and improvements to ST products and/or to this document at any time without notice. Purchasers should obtain the latest relevant information on ST products before placing orders. ST products are sold pursuant to ST’s terms and conditions of sale in place at the time of order acknowledgement.

Purchasers are solely responsible for the choice, selection, and use of ST products and ST assumes no liability for application assistance or the design of Purchasers’ products.

No license, express or implied, to any intellectual property right is granted by ST herein.

Resale of ST products with provisions different from the information set forth herein shall void any warranty granted by ST for such product.

ST and the ST logo are trademarks of ST. For additional information about ST trademarks, please refer to www.st.com/trademarks. All other product or service names are the property of their respective owners.

Information in this document supersedes and replaces information previously supplied in any prior versions of this document.

© 2019 STMicroelectronics – All rights reserved