STSW-ST25DV005

ST25DV-I2C cryptographic firmware for secure communications

Data brief

Features

- Encryption of the NFC communications between a smartphone (Android™ or iPhone) and an STM32 microcontroller (both ways)
- Fast communications over NFC, thanks to ST25DV-I2C Fast transfer mode
- AES and ECC cryptography
- Mutual authentication between the smartphone and the STM32 microcontroller
- Establishment of a unique AES session key
- Possibility to securely retrieve data, set device settings or update the firmware
- Based on STM32Trust security ecosystem

Description

The ST25DV-I2C CryptoDemo shows how to establish an NFC secure transfer channel between an STM32 and a smartphone (Android or iPhone), using the Fast transfer mode of ST25DV-I2C NFC tags.

This firmware (STSW-ST25DV005), an Android application (STSW-ST25003), an iOS application (STSW-ST25IOS003), a user manual and an application note are available on *www.st.com*.

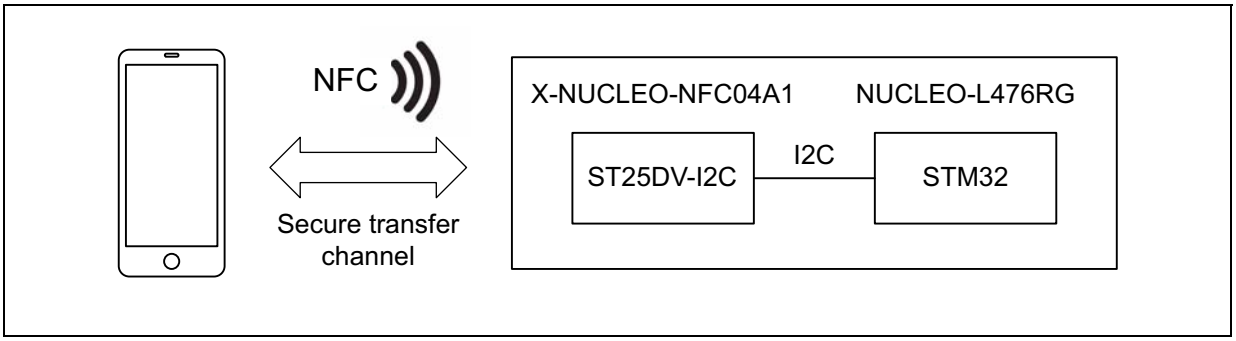
A NUCLEO-L476RG board together with an X-NUCLEO-NFC04A1 board is required to run the demonstration, which establishes a secure transfer channel.

STSW-ST25DV005 benefits from the STM32Trust protection by reusing the X-CUBE-SBSFU framework running on the STM32L476RG microcontroller.

Cryptography is used to perform mutual authentication and to encrypt the NFC communications.

This secure transfer channel can be exploited to send and retrieve data, for the device settings and to upload a new firmware. Only the granted user can communicate with the STM32 to perform these operations.

The communications between the microcontroller and the Android phone are encrypted both ways.



1 License scheme

The ST25DV-I2C CryptoDemo firmware is delivered under the SLA0052 software license agreement.

The software components provided in this package come with different license schemes, as shown in *Table 1*.

Table 1. ST25DV-I2C crypto firmware - License scheme

Component	Copyright	License
Project application	STMicroelectronics	ST proprietary
LibNDEF		ST proprietary
Menu demo		ST proprietary
Board support package (BSP)		ST proprietary
LibJPEG		ST Liberty SW License Agreement V2
HAL STM32L4		Open source BSD
STM32_Cryptographic		Image V2 (object release only)
STM32_Secure_Engine		Ultimate Liberty (source and object release)
Cortex®-M CMSIS	Arm®(1)	Open source BSD

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

2 Revision history

Table 2. Document revision history

Date	Revision	Changes
17-Apr-2020	1	Initial release.