NFC USB Secure Dongle

Introduction

Multi-factor authentication (MFA) is an authentication method in which a user has granted access only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism:

- knowledge (something the user and only the user knows),
- possession (something the user and only the user has), and
- inherence (something the user and only the user is).

MFA for payments is defined in PCI DSS 3.2. standard issued by PCI Security Standards Council[1] and is **obligatory to all entities involved in payment card** processing, including merchants, processors, acquirers, issuers and service providers **and all other entities that store, process or transmit cardholder data or sensitive authentication data**. The standard updates are coming regularly also in response to major hacking incidents in the U.S. **Similar standards are used in other industry segments.**

In this document we describe NFC USB Secure dongle - a hardware device (USB key) developed by Logomotion and that enables MFA. We also describe examples of usage and benefits that it provides for various stakeholders. In the end of this document we show measurement results of NFC USB Secure dongle prototype and that are in line with particular standards of NFC Forum and Mobile NFC Association.

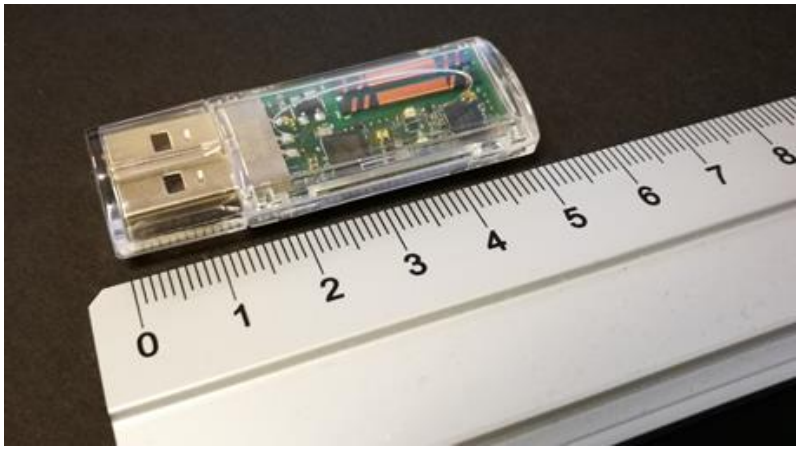
NFC USB Secure dongle basic functions

- **a multi-purpose, hardware based authentication device** for PC/notebook. As a possession factor it can be combined with knowledge factor (like password or PIN) and/or with inherence factor (typically biometric characteristics like fingerprints or face recognition). Because of its NFC antenna it can utilize inherence factor already used inside user's NFC enabled mobile phone. This will enable highly secure and user-friendly two or three factor authentication.
- **a contactless reader** attached to user's PC/notebook. By tapping a contactless chip plastic card to the NFC USB Secure dongle, sensitive data from the chip card can be securely transferred into the PC and used for various identification/authentication/authorization online use-cases.

[1] PCI DSS 3.2, February 2018

NFC USB Secure dongle description

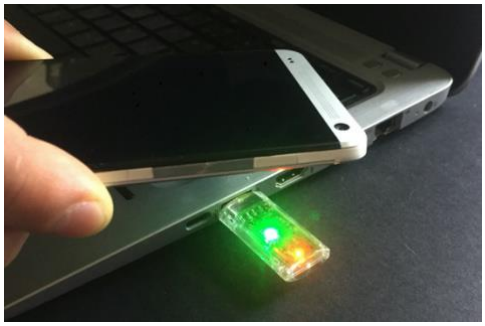
NFC USB Secure dongle is a standard USB-A key that fits computer ports. It contains NFC antenna enabling contactless usage. It comprises SE that generates, stores and protects secure keys and certificates and performs cryptographic operations and store other sensitive data (passwords, logins, user's identification etc.)

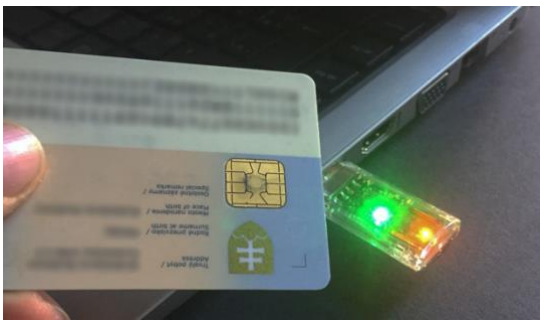


Picture: NFC USB Secure dongle prototype

Key features

* Tamper-proof secure element compliant with the Global Platform Card Secure Element standard
* High performance NFC module including patented miniature LGM antenna
* USB-A interface
* Miniature size, easy-to-use





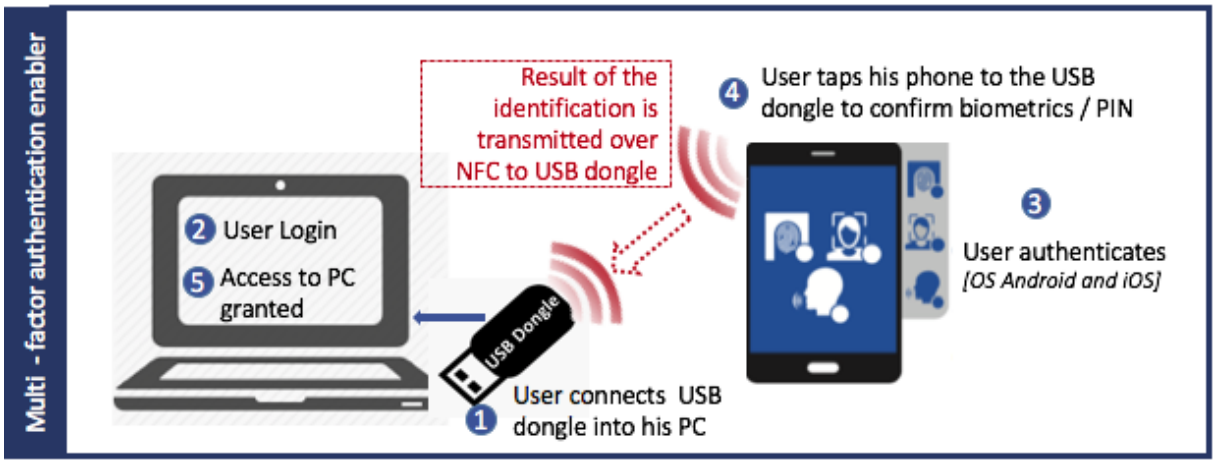
Pictures: NFC USB Secure dongle usage examples

Use-case examples

Hardware token & Multi-factor Authentication enabler

NFC USB Secure dongle is a possession device designed to be used as a **certificate-based PKI authentication token** (a hardware token). SE of NFC USB Secure dongle can store e.g. CC (client certificate), FIDO keys or RSA (public & private keys). This sensitive data never leaves the SE.

NFC USB Secure dongle enables to use biometric data / PIN that are already used in user's NFC enabled phone as a second-and/or third authentication factor for the user's PC. Biometric data/PIN is verified on a mobile phone via a standard BiometricPrompt API (OS Android) or TouchID/FaceID (iOS). A result of the verification (succeed, failed) is transferred through NFC channel from a mobile phone to NFC USB Secure dongle – during a tap of the mobile phone to the dongle. No biometric data / PIN are stored on NFC USB Secure dongle or in any database.



Picture: NFC USB Secure dongle used with NFC mobile phone for secure and easy two-or three factor authentication

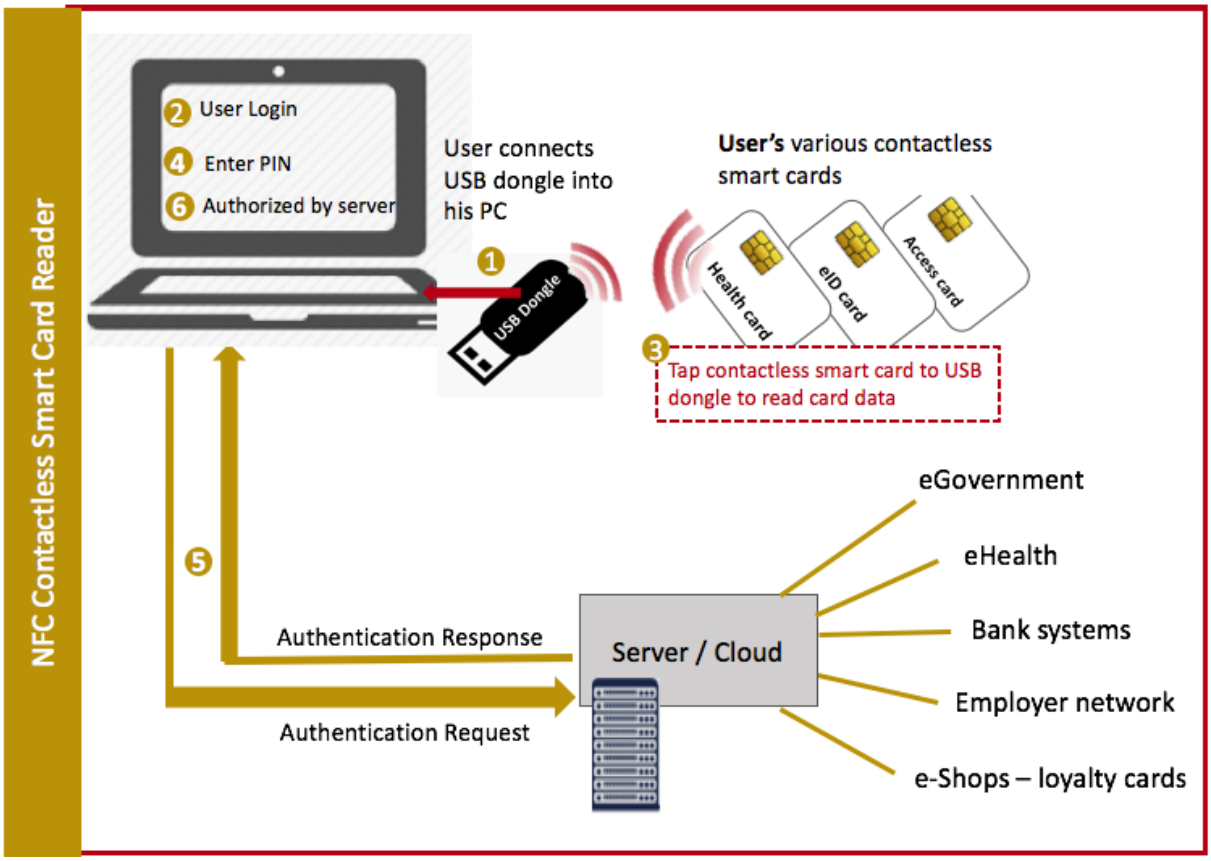
- ***Step 1.*** A user connects NFC USB Secure dongle to PC via USB
- ***Step 2.*** A user starts login process in desired application
- ***Step 3.*** To access PKI certificate from USB dongle's secure element, a user is asked to perform the second step of authentication. A user identifies himself on his mobile phone, typically by unlocking phone screen by his fingerprint (alternatively by screen pattern, PIN or password).
- ***Step 4.*** Tapping his mobile phone to NFC USB Secure dongle, a user adds 2nd factor of MFA (inherence – biometrics or knowledge – PIN).
- ***Step 5.*** Access to PS is enabled.

NFC Contactless smart card reader

NFC USB Secure dongle has embedded miniature NFC antenna that works as a reader of contactless chip cards. NFC USB Secure dongle can be used in eGovernment, Banking & Payment, eHealth, Access Control, Network Security, e-Purse & Loyalty, Transportation etc.

NFC USB Secure dongle will enable to securely communicate with the chip (SE) of the contactless smart card.

Solution for Key management and end-to-end online authentication solution is independent on NFC USB Secure dongle and is out of scope of this document. NFC USB Secure dongle is a hardware that enables to deploy various end-to-end authentication solutions.



Picture: NFC USB Secure dongle used as NFC contactless smart card reader of various contactless chip cards (and optional secure and easy two-or three factor authentication)

- ***Step 1.*** A user connects NFC USB Secure dongle to his PC via USB.
- ***Step 2.*** Starts login process at desired application.
- ***Step 3.*** User taps contactless smart card to the NFC USB Secure dongle

- ***Step 4.*** To access PKI certificate a user is asked to perform the second step of authentication – e.g. to enter PIN.
- ***Step 5.*** Authentication request/response session by particular server
- ***Step 6.*** The user's PC is authorized to access the particular server and to start secure communication with the server

Applications

NFC USB Secure dongle can attract **banks, government, big enterprises, wallet providers, cryptocurrency providers, e-shop etc.** – using it **in various** applications:

- access control, including remote access, network access, password management, network login, as well as advanced applications including digital signature, data and email encryption and other advanced services based on Public Key Infrastructure (PKI). It can also serve as "locker" to the computer's data or to transmit data from/to industrial devices.

Example for healthcare

Access control and authentication is the third from eleven the most important challenges in eHealth[2]. The greatest vulnerabilities in data security are sharing data between third parties and insiders (breaches by employees) and unauthorized access on data over the network. At the same time a user-friendly system is of great importance.

Authentication is the initial stage of the user's validation in order to determine their identity which is necessary to ensure that they are authorized to access the system. Some of the main requirements for a secure access to patients 'data include:

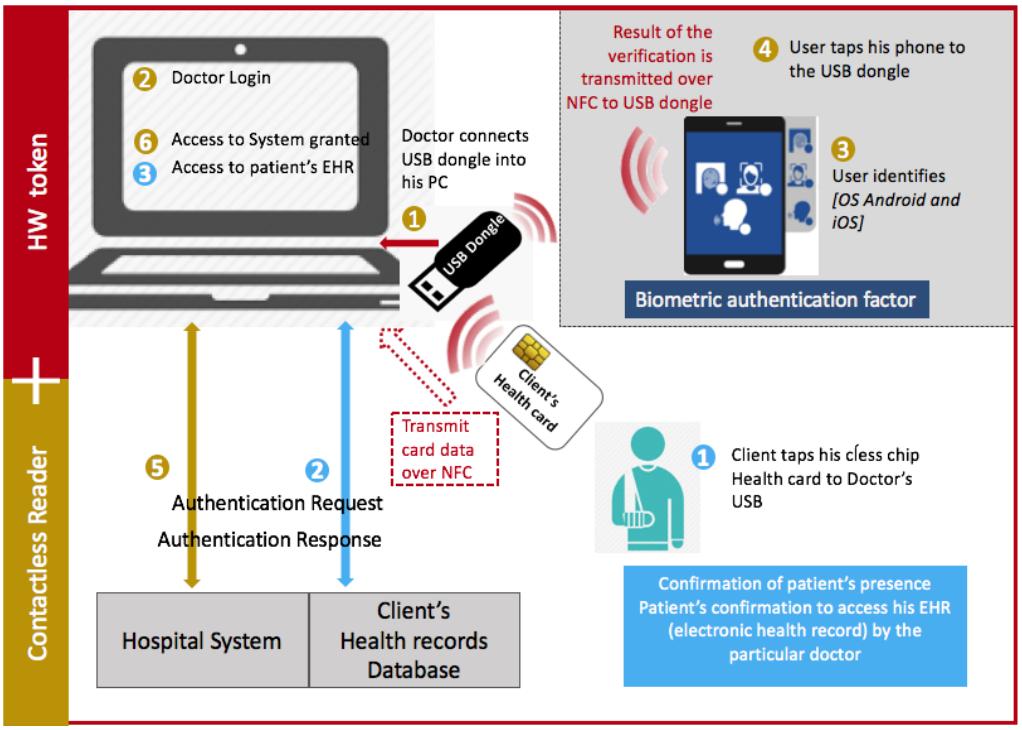
- access to the system permitted only where there is a "legitimate relationship" between the system user and the patient;
- registration of all users with a central authority to obtain a smartcard and a pass code (chip and pin)
- deployment of a multi-factor authentication methods

NFC USB Secure dongle can be issued to doctors as a HW token (contains smartcard chip). While inserted into doctor's PC/laptop and after a login confirmed by PIN it will determine identity to ensure they are authorized to access the system.

NFC USB Secure dongle enables to use doctor's biometrics from his NFC mobile smartphone (iOS and Android) – as additional authentication factor (optional).

NFC USB Secure dongle can read patient's contactless health smart card that will confirm patient's physical presence and his approval to access his EHR (electronic health record) by particular doctor.

[2] Security and Resilience in eHealth Infrastructures and Services.pdf. www.enisa.europa. euEuropean Union Agency For Network And Information Security



Picture: NFC USB Secure dongle used as HW token and contactless reader of various contactless chip cards (and optional secure and easy two-or three factor authentication)

Benefits and advantages

Unlike usual hardware authentication tokens (smart card readers, USB tokens), NFC USB Secure Dongle provide contactless functionality – it can be connected directly to a PC and it can work also as a miniature NFC reader.

In contrast to software tokens, the credentials and private keys are stored on a tamper-proof hardware secure element and therefore cannot be duplicated. Private keys never leave secure element. Secure element contains a certified microcontroller and embedded software so it can protect digital identities and is vital to ensure digital security and privacy.

Compared to pure password authentication and authentication using data stored on server side; NFC USB Secure dongle used for authentication prevents from:

- Forgetting/steeling/loosing/duplication of passwords. It enables password-less login
- Hacking data from servers and huge investment on server's data security. It enables to store sensitive data on client's side inside a HW tamper-proof SE or to read sensitive data stored on an independent carrier (contactless chip card) over NFC –thus no need to store such data on server side

NFC USB Secure dongle is inline with security requierements on IT systems, services and applications that requieres high privacy and confidentiality of sensitive data. It can prevent the greatest vulnerabilities in data security – sharing data between third parties and insiders and prevention of unauthorized access on data over the netwok – by securing multi-factor authentication and access control.

NFC USB Secure dongle – alternative features

NFC USB Secure dongle with the embedded fingerprint sensor allows using without NFC phone – a user is asked to present a finger to scan directly on NFC USB Secure dongle.

NFC USB Secure dongle with microUSB/USB-C connector can be used with a smartphone for mobile authentication services requiring hardware authentication tokens.

Picture: NFC USB Secure dongle with fingerprint reader

NFC USB Dongle Prototype

NFC USB Dongle prototype was designed to demonstrate the performance and size of the LGM miniature antenna system. NFC USB Dongle can use various vendors' components. We have designed prototypes based on NXP and SONY technologies.

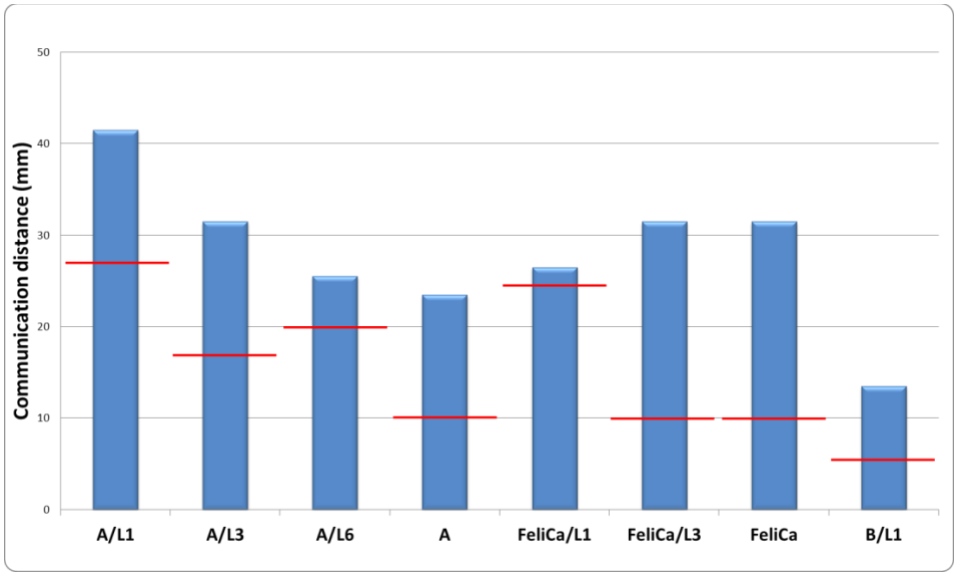
NFC USB Dongle Prototype comprises 2 LGM antennas 18 x 1.75 x 0.8 mm, 1 miniature planar antenna, matching circuits and NFC Controller and a Cypress USB Controller.

Figure 2: NFC USB Dongle Prototype

Communication Distance Measurement Results

MoNA NFC tag	MoNA Requirement [mm]	NFC USB Dongle Prototype [mm]
TypeA_L1	27	41,5
TypeA_L3	17	31,5
TypeA_L6	20	25,5
TypeA	10	23,5
FeliCa_L1	25	26,5
FeliCa_L3	10	31,5
FeliCa	10	31,5
TypeB_L1	5	13,5

Note 1: Distances were measured from the enclosure of the USB Dongle Prototype cover
Note 2: MoNA NFC tags are defined by Mobile NFC Association



Summary

NFC USB Secure dongle is a hardware token that identifies PC/notebook user and that enables additional authentication factor (existing biometric/PIN data) used in user's NFC enabled mobile phone. In addition, it provides NFC smart card reader functionality with encryption mechanisms for reading contactless smart cards.

Logomotion has developed NFC USB Secure dongle prototypes to demonstrate the idea and to confirm strong NFC antenna performance – that directly influence positive customer's experience with contactless communication.