Logit: W3 Report ToC

Malik Koljenović; **04.04.2017**
Faza: ToC

1. Uvod
2. Razrada i specifikacija problema
3. Pregled postojećih tehničkih rješenja i literature
    a. Kontrola pristupa
        i. Metode utvrđivanja identiteta
            1. Višefaktorno utvrđivanje identiteta
        ii. Upravljanje autorizacijama
    b. Web i IoT kao platforma za kontrolu pristupa
        i. Kriptografija javnog ključa i mrežni protokoli
        ii. Web prakse za kontrolu pristupa
            1. ?? OpenID, Shibboleth, eduroam, SAML, OpenAthens, LDAP ...
        iii. Android platforma
            1. Prednosti i nedostaci
            2. Sigurnosne mogućnosti platforme
            3. NFC i komunikacijske mogućnosti
    c. Primjena NFC tehnologije u sistemima kontrole pristupa
        i. Opšte karakteristike NFC tehnologije
        ii. Komponente NFC sistema
        iii. Područje primjene
        iv. Implementacijski pristupi
    d. Sigurni element i pametne kartice
        i. Opšte karakteristike
        ii. Osobine implementacije
            1. SIM kartice
            2. ID kartice
            3. Platne kartice
            4. USB SE (YubiKey, SmartCard-HSM)
            5. Android SE i HCE
            6. HSM i Distribuirani sigurni element
    e. Relevantni standardi i specifikacije
        i. RSA PKCS# set
        ii. ITU-T X.509
        iii. ISO 14443
        iv. ISO 7816-4
        v. NFC Forum NDEF i Tag specifikacije
        vi. Proizvođačke specifikacije (NXP)

4. Prijedlog i obrazloženje rješenja
    a. Pregled komponenti rješenja
    b. Komponente sistema
        i. Android uređaj
        ii. Čitač* / Pisač*
        iii. Aplikacijska komponenta
        iv. ISM (Integrated Security Module)
5. Arhitektura sistema
    a. Opšti pregled arhitekture sistema
    b. Sigurnosna arhitektura
        i. Detaljan opis dijelova sistema od posebnog značaja
    c. Android aplikacija za bilježenje prisustva
        i. Detaljan opis dijelova koda od posebnog značaja
    d. Sigurnosna analiza sistema
6. Projektna dokumentacija
    a. Specifikacija zahtjeva
    b. Arhitektura korisničkog interfejsa
    c. Arhitektura baze podataka
    d. Mrežna arhitektura
7. API Dokumentacija
8. Korisničko uputstvo
9. Zaključak
10. Literatura

Apstrakt

Uvod

U okruženju u kom se većina komunikacija odvija elektronski za očekivati je da se i evidentiranje prisustva može raditi na ovaj način. Međutim, postoje otvorena pitanja pogodnosti i sigurnosti elektronskog evidentiranja. NFC može biti osnova za siguran i jednostavan sistem. Kako savremeni mobilni uređaji uglavnom imaju NFC oni mogu biti iskorišteni kao sredstvo prijavljivanja i vođenja evidencije bez potrebe za dodatnim karticama i čitačima.

Razrada i specifikacija problema

Potrebno je napraviti Android aplikaciju koja omogućava evidentiranje prisustva upotrebom NFC tehnologije. Aplikacija treba da bude jednostavna za upotrebu i zaštićena od zloupotreba.

U radu je potrebno objasniti šta se podrazumjeva pod pojmom evidencija prisustva i koja su otvorena pitanja elektronskog vođenja ove evidencije.

- Pregled postojećih tehničkih rješenja i literature
  - Kontrola pristupa
    - Metode utvrđivanja identiteta
      - Višefaktorno utvrđivanje identiteta
    - Upravljanje autorizacijama
  - Web i IoT kao platforma za kontrolu pristupa
    - Kriptografija javnog ključa i mrežni protokoli
    - Web prakse za kontrolu pristupa
      - ?? OpenID, Shibboleth, eduroam, SAML, OpenAthens, LDAP ...
    - Android platforma
      - Prednosti i nedostaci
      - Sigurnosne mogućnosti platforme
      - NFC i komunikacijske mogućnosti
  - Primjena NFC tehnologije u sistemima kontrole pristupa
    - Opšte karakteristike NFC tehnologije
    - NDEF
    - Tags
      - Type 4 Tag
    - Komponente NFC sistema
    - Područje primjene
    - Implementacijski pristupi

Android SE i HCE [ASEHCE]

Android does not offer APIs for directly communicating with a secure element itself.

The Android Keystore system lets you store cryptographic keys in a container to make it more difficult to extract from the device. Once keys are in the keystore, they can be used for cryptographic operations with the key material remaining non-exportable. Moreover, it offers facilities to restrict when and how keys can be used, such as requiring user authentication for key use or restricting keys to be used only in certain cryptographic modes. See Security Features section for more information.

The Keystore system is used by the KeyChain API as well as the Android Keystore provider feature that was introduced in Android 4.3 (API level 18). This document goes over when and how to use the Android Keystore provider.

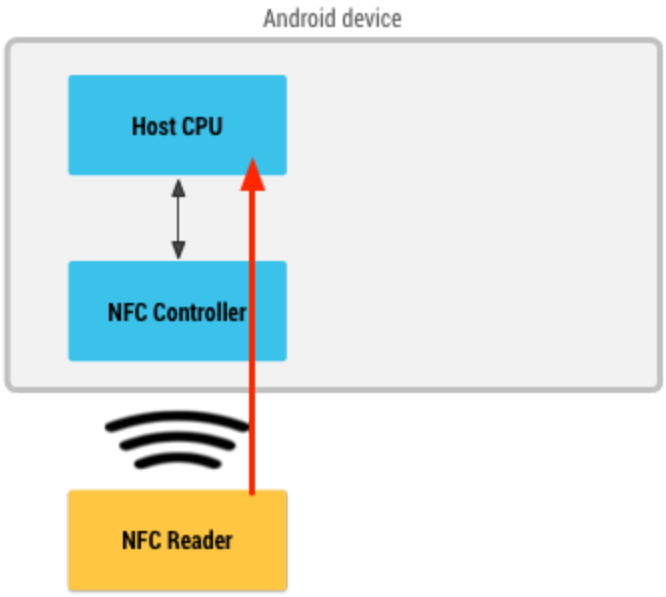
Android Keystore system protects key material from unauthorized use. Firstly, Android Keystore mitigates unauthorized use of key material outside of the Android device by preventing extraction of the key material from application processes and from the Android device as a whole. Secondly, Android KeyStore mitigates unauthorized use of key material on the Android device by making apps specify authorized uses of their keys and then enforcing these restrictions outside of the apps' processes.

Key material of Android Keystore keys is protected from extraction using two security measures:
Key material never enters the application process. When an application performs cryptographic operations using an Android Keystore key, behind the scenes plaintext, ciphertext, and messages to be signed or verified are fed to a system process which carries out the cryptographic operations. If the app's process is compromised, the attacker may be able to use the app's keys but will not be able to extract their key material (for example, to be used outside of the Android device).
Key material may be bound to the secure hardware (e.g., Trusted Execution Environment (TEE), Secure Element (SE)) of the Android device. When this feature is enabled for a key, its key material is never exposed outside of secure hardware. If the Android OS is compromised or an attacker can read the device's internal storage, the attacker may be able to use any app's Android Keystore keys on the Android device, but not extract them from the device. This feature is enabled only if the device's secure hardware supports the particular combination of key algorithm, block modes, padding schemes, and digests with which the key is authorized to be used. To check whether the feature is enabled for a key, obtain a KeyInfo for the key and inspect the return value of KeyInfo.isInsideSecurityHardware().

HCE
Many Android-powered devices that offer NFC functionality already support NFC card emulation. In most cases, the card is emulated by a separate chip in the device, called a secure element. Many SIM cards provided by wireless carriers also contain a secure element.

Android 4.4 introduces an additional method of card emulation that does not involve a secure element, called host-based card emulation. This allows any Android application to emulate a card and talk directly to the NFC reader. This document describes how host-based card emulation (HCE) works on Android and how you can develop an app that emulates an NFC card using this technique.

When an NFC card is emulated using host-based card emulation, the data is routed to the host CPU on which Android applications are running directly, instead of routing the NFC protocol frames to a secure element. Figure 2 illustrates how host-based card emulation works.



The HCE architecture itself provides one core piece of security: because your service is protected by the BIND_NFC_SERVICE system permission, only the OS can bind to and communicate with your service. This ensures that any APDU you receive is actually an APDU that was received by the OS from the NFC controller, and that any APDU you send back will only go to the OS, which in turn directly forwards the APDUs to the NFC controller.

The core remaining piece is where you get your data that your app sends to the NFC reader. This is intentionally decoupled in the HCE design: it does not care where the data comes from, it just makes sure that it is safely transported to the NFC controller and out to the NFC reader.

For securely storing and retrieving the data that you want to send from your HCE service, you can, for example, rely on the Android Application Sandbox, which isolates your app's data from other apps. For more details on Android security, read Security Tips.

Relevantni standardi i specifikacije

- RSA PKCS# set
- ITU-T X.509
- ISO 14443
- ISO 7816-4
- NFC Forum NDEF i Tag specifikacije
- Proizvođačke specifikacije (NXP)

Potrebno je objasniti šta je NFC i kako radi.

Prijedlog i obrazloženje rješenja
- Pregled komponenti rješenja
- Komponente sistema
  - Android uređaj
  - Čitač* / Pisač*
  - Aplikacijska komponenta
  - ISM (Integrated Security Module)

Potrebno je teoretski objasniti kako je moguće napraviti siguran elektronski sistem evidentiranja prisustva zasnovan na NFC koji je lak za upotrebu.

The following conventions and notations apply in this document unless otherwise stated.
• Binary numbers are represented by strings of digits 0 and 1 shown with the most significant bit (msb) on the left, the least significant bit (lsb) on the right, and a “b” added at the end.
Example: 11110101b
• Hexadecimal numbers are represented by using the numbers 0 to 9 and the characters A – F, and adding an “h” at the end. The Most Significant Byte (MSB) is shown on the left and the Least Significant Byte (LSB) on the right.
Example: F5h
• Decimal numbers are represented as is (without any trailing character).
Example: 245

Arhitektura sistema
- Opšti pregled arhitekture sistema
- Sigurnosna arhitektura
  - Detaljan opis dijelova sistema od posebnog značaja
- Android aplikacija za bilježenje prisustva
  - Detaljan opis dijelova koda od posebnog značaja
- Sigurnosna analiza sistema

Projektna dokumentacija
- Specifikacija zahtjeva
- Arhitektura korisničkog interfejsa
- Arhitektura baze podataka
- Mrežna arhitektura

U sklopu rada potrebno je napraviti praktičnu izvedbu sistema koji omogućava korisnicima koji imaju mobilne uređaje sa NFC da se pomoću njih registruju i potvrde prisustvo.
Ovaj sistem treba biti zaštićen od zloupotreba.

API Dokumentacija

Korisničko uputstvo

Zaključak

Prokomentarisati iskustva stečena tokom praktične realizacije i dati savjete za buduće izvedbe.

Skracenice

[ACTIVITY] NFC Activity Specification, Latest version NFC Forum
[DIGITAL] NFC Digital Protocol Technical Specification, Version 1.0, NFC Forum
[ISO/IEC_7816-4] ISO/IEC 7816-4:2005 Identification cards - Integrated circuit cards - Organization, security and commands for interchange, Second edition, January 15, 2005
[NDEF] NFC Data Exchange Format (NDEF), Version 1.0 NFC Forum
[RFC2119] Key words for use in RFCs to Indicate Requirement Levels, RFC 2119 S. Bradner, March 1997 Harvard University
[T4TOP_V1.0] Type 4 Tag Operation Technical Specification, Version 1.0, NFC Forum

APDU
Application Protocol Data Unit
C-APDU
Command APDU
CC
Capability Container
DF
Directory File
EF
Elementary File (file identifier)
Lc
Length command
Le
Length expected
LSB
Least significant byte
lsb
Least significant bit
MLc
Maximum data Length C-APDU
MLe
Maximum data Length R-APDU
MSB
Most significant byte
msb
Most significant bit
NDEF
NFC Data Exchange Format
R-APDU
Response APDU
RF

Radio Frequency
RFU
Reserved for future use
ISO-DEP Protocol
The half-duplex block transmission protocol as defined in [DIGITAL].
NFC Forum Device
A device that supports the following modus operandi: Initiator, Target, and Reader/Writer. It may also support Card Emulator. In this document, the NFC Forum Device is always using the Reader/Writer modus operandi (for more information, see [DIGITAL]).
NFCDevVNo
Mapping version number implemented in the NFC Forum Device.
T4VNo
Mapping version numbers implemented in the Type 4 Tag Platform.
Type 4 Tag Platform
A legacy platform supporting a subset of a Technology (also called Technology Subset), which uses a particular subset of NFC – Type A technology or NFC- Type B technology, including anticollision (for more information, see [DIGITAL]).
NDEF application
The logical, higher-layer application on an NFC Forum Device using NDEF to format information for exchange with other NFC Forum Devices or NFC Forum Tags. Also user application or NDEF user application.
NDEF message
The basic message construct defined by this specification. An NDEF message contains one or more NDEF records (see section 2.3.1).
NDEF record
An NDEF record contains a payload described by a type, a length, and an optional identifier (see section 2.3.2).
NDEF short record
An NDEF record with the SR flag set to 1; the PAYLOAD_LENGTH field in short records is a single octet allowing payloads or chunks of up to 255 bytes to be carried (see section 3.2.4).
NDEF record chunk
An NDEF record that contains a chunk of a payload rather than a full payload (see section 2.3.3). Each record chunk carrying a portion of the chunked payload, except the last record of each chunked payload, has its CF flag set to 1.
NDEF payload
The application data carried within an NDEF record.
NDEF chunked payload
Application data that has been partitioned into multiple chunks each carried in a separate NDEF record, where each of these records except the last has the CF flag set to 1. This facility can be used to carry dynamically generated content for which the payload size is not known in advance or very large entities that don't fit into a single NDEF record. Chunked payloads are not intended to support multiplexing or streaming of content and

such use is deprecated. (See section 2.3.3.)

NDEF payload length

The size of the payload in a single NDEF record indicated as the number of octets (see section 2.4.1).

NDEF payload type

An identifier that indicates the type of the payload. This specification supports URIs [RFC 3986], MIME media type constructs [RFC 2616], as well as an NFC-specific record type as type identifiers (see section 2.4.2).

NDEF payload identifier

An optional URI that can be used to identify a payload (see section 2.4.3).

NDEF generator

An entity or module that encapsulates application-defined payloads within NDEF Messages.

NDEF parser

An entity or module that parses NDEF messages and hands off the payloads to an NDEF application.

User Application

See NDEF Application.

NFC

Popis tabela

Popis listinga

Popis grafika

Literatura

[ASEHCE] https://developer.android.com/guide/topics/connectivity/nfc/hce.html

[ISO/IEC 18092] ISO/IEC 18092, “Information Technology- Telecommunications and information exchange between systems- Near Field Communication - Interface and Protocol (NFCIP-1)”.
[NFC RTD] “NFC Record Type Definition (RTD) Specification”, NFC Forum, 2006.
[RFC 1700] Reynolds, J. and J. Postel, “Assigned Numbers”, STD 2, RFC 1700, October 1994.
[RFC 1900] B. Carpenter, Y. Rekhter, “Renumbering Needs Work”, RFC 1900, IAB, February 1996.
[RFC 2046] N. Freed, N. Borenstein, “Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types” RFC 2046, Innosoft, First Virtual, November 1996.
[RFC 2047] K. Moore, “MIME (Multipurpose Internet Mail Extensions) Part Three: Message Header Extensions for Non-ASCII Text”, RFC 2047, University of Tennessee, November 1996.
[RFC 2048] N. Freed, J. Klensin, J. Postel, “Multipurpose Internet Mail Extensions (MIME) Part Four: Registration Procedures”, RFC 2048, Innosoft, MCI, ISI, November 1996.
[RFC 2119] S. Bradner, “Key words for use in RFCs to Indicate Requirement Levels”, RFC 2119, Harvard University, March 1997. http://www.apps.ietf.org/rfc/rfc2119.html
[RFC 2616] R. Fielding, J. Gettys, J. C. Mogul, H. F. Nielsen, T. Berners-Lee, “Hypertext Transfer Protocol -- HTTP/1.1”, RFC 2616, U.C. Irvine, DEC W3C/MIT, DEC, W3C/MIT, W3C/MIT, January 1997.
[RFC 2717] R. Petke, I. King, “Registration Procedures for URL Scheme Names”, BCP: 35, RFC 2717, UUNET Technologies, Microsoft Corporation, November 1999.
[RFC 2718] L. Masinter, H. Alvestrand, D. Zigmond, R. Petke, “Guidelines for new URL Schemes”, RFC 2718, Xerox Corporation, Maxware, Pirsenteret, WebTV Networks, Inc., UUNET Technologies, November 1999.
[RFC 2732] R. Hinden, B. Carpenter, L. Masinter, “Format for Literal IPv6 Addresses in URL's”, RFC 2732, Nokia, IBM, AT&T, December 1999.
[RFC 3023] M. Murata, S. St. Laurent, D. Kohn, “XML Media Types” RFC 3023, IBM Tokyo Research Laboratory, simonstl.com, Skymoon Ventures, January 2001.
[RFC 3986] T. Berners-Lee, R. Fielding, L. Masinter, “Uniform Resource Identifiers (URI): Generic Syntax”, RFC 3986, MIT/LCS, U.C. Irvine, Xerox Corporation, January 2005. http://www.apps.ietf.org/rfc/rfc3986.html
[URI SCHEME] List of Uniform Resource Identifier (URI) schemes registered by IANA is available at:http://www.iana.org/assignments/uri-schemes