

**Risto Hietala**

**MOBIILILAITEOHJELMAN SISÄLLÖN YKSILÖIMINEN  
NFC:N AVULLA**

**Case FinnCode**

**Opinnäytetyö  
CENTRIA-AMMATTIKORKEAKOULU  
Mediatekniikan koulutusohjelma  
Joulukuu 2017**

**TIIVISTELMÄ OPINNÄYTETYÖSTÄ**

<b>Yksikkö</b> Ylivieska	<b>Aika</b> Joulukuu 2017	<b>Tekijä/tekijät</b> Risto Hietala
<b>Koulutusohjelma</b> Mediatekniikka		
<b>Työn nimi</b> Mobiililaitteohjelman sisällön yksilöiminen NFC:n avulla		
<b>Työn ohjaaja</b> Hannu Puomio	<b>Sivumäärä</b> 21	
<b>Työelämäohjaaja</b> Vesa Haapaniemi		
<p>Opinnäyte työn aihe saatu FinnCode Oy:lle tehdystä Finncode Authentication-ohjelmistotalustasta. Opinnäytetyön aiheena on miten tuotteiden tunnistuksella NFC:n avulla voidaan antaa niille ohjelmallisesti lisäarvoa.</p> <p>Opinnäytetyön tavoitteena oli tutkia miten tuote voidaan tunnistaa NFC:n avulla. Työn tuloksena syntyi FinnCode Authentication –järjestelmä, jolla voidaan Android-käyttöjärjestelmän mobiililaitteissa, joissa on NFC-siru, varmistaa tuotteen aitous.</p>		

**Asiasanat**

Aitouden varmistaminen, Android, mobiililaitteet, NFC, väärennökset

## ABSTRACT

<b>CENTRIA UNIVERSITY OF APPLIED SCIENCES</b>	<b>Date</b> December 2017	<b>Author</b> Risto Hietala
<b>Degree programme</b> Mediatekniikka		
<b>Name of thesis</b> Individualizing mobile device programs with NFC		
<b>Instructor</b> Hannu Puomio	<b>Pages</b> 21	
<b>Supervisor</b> Vesa Haapaniemi		
<p>The subject of thesis came from Finncode Authentication software platform that was made for Finncode Oy. The subject of the thesis was to find out how the recognition of products with NFC can add value to them in terms of programs.</p> <p>The objective of the thesis was to research how to recognize a product with the help of NFC. As a result of this thesis Finncode Authentication platform was created. The platform can verify product authentication on Android devices with an NFC chip.</p>		

<p><b>Key words</b></p> <p>Authentication, Android, forgery, mobile devices, NFC</p>
--

## **KÄSITTEIDEN MÄÄRITTELY**

NFC

Near Field Communication. Lyhyen kantaman tiedonsiirtostandardi joka pohjautuu RFID-tekniikkaan.

## **ESIPUHE**

Haluaisin kiittää Finncode Oy:n henkilökuntaa. He mahdollistivat opinnäytetyön aiheen ja opettivat minulle paljon työelämästä ja ohjelmoinnista.

## **TIIVISTELMÄ**

## **ABSTRACT**

## **KÄSITTEIDEN MÄÄRITTELY**

## **ESIPUHE**

## **SISÄLLYS**

<b>1 JOHDANTO.....</b>	<b>1</b>
<b>2 LYHYEN KANTAMAN LANGATON TIEDONSIIRTOMENETELMÄ.....</b>	<b>2</b>
<b>2.1 NFC.....</b>	<b>2</b>
<b>2.2 NFC matkapuhelimessa.....</b>	<b>3</b>
<b>3 AITouden VARMISTAMINEN.....</b>	<b>4</b>
<b>3.1 Aitouden varmistus NFC:n avulla.....</b>	<b>6</b>
<b>3.2 Ohjelman yksilöinti tunnistetun NFC –tagin avulla.....</b>	<b>7</b>
<b>4 FINNCODE AUTENTIKOINTI.....</b>	<b>8</b>
<b>4.1 Yrityksen taustaa.....</b>	<b>8</b>
<b>4.2 FinnCode Authentication -järjestelmä käytössä.....</b>	<b>8</b>
<b>5 JOHTOPÄÄTÖKSET JA POHDINTA.....</b>	<b>14</b>

## **KUVIOT**

<b>KUVIO 1. Väärennöksiin ja piratismiin liittyviä tilastoja.....</b>	<b>4</b>
---	----------

## **KUVAT**

<b>KUVA 1. FinnCode –sovellus.....</b>	<b>9</b>
<b>KUVA 2. Reuhurinne Eläinlauluja –kirja.....</b>	<b>11</b>
<b>KUVA 3. Reuhurinne Ekstra –sovellus.....</b>	<b>12</b>
<b>KUVA 4. Dara –laukku.....</b>	<b>12</b>
<b>KUVA 5. Ami –laukku.....</b>	<b>13</b>

<b>LÄHTEET.....</b>	<b>15</b>
---------------------	-----------

# 1 JOHDANTO

Opinnäytetyön aiheena oli matkapuhelinten ja NFC:n käyttö aitouden varmistuksessa ja miten tästä saatua tietoa voidaan käyttää hyväksi. Työssä käsitellään miten erilaisia matkapuhelimet käsittelevät NFC:tä ja miten NFC:ltä saatuja tietoja voidaan käyttää aitouden varmistuksessa.

Työn aihetta minulle ehdotettiin työpaikallani FinnCode Oy:ssa. Aloitin aitouden tarkistukseen suunnitellun järjestelmän ohjelmoinnin ja suunnittelun ollessani työharjoittelussa keuhällä 2014. Järjestelmän kehitys jatkui Finncode Oy:n konkurssiin saakka syksyille 2017.

Aihe on valittu pitkäaikaisen työsuhteen aikana hyvin tutuksi tulleen järjestelmän takia. Aihetta on rajattu käsittelemään matkapuhelinten ja NFC:n osuutta järjestelmässä. Täten järjestelmässä käytettävää rajapintaa, joka siirtää tietoa palvelimille ja kyseisiä palvelimia käsitellään vähemmän.

Tämän opinnäytetyön tuloksena on FinnCode Oy:lle rakennettu aitouden varmennus-järjestelmä. Tähän järjestelmään kuului useita osia, mutta tämän opinnäytetyön yhteydessä käsitellään vain osia, joilla oli Finncode Oy:n ulkopuolisia asiakkaita.

Opinnäytetyön ensimmäisessä pääluvussa käsitellään NFC:tä yleisesti sekä miten matkapuhelimet tukevat NFC:n käsittelyä. Toisessa pääluvussa käsitellään miten aitous voidaan varmistaa eri menetelmillä sekä miten se voidaan todeta NFC:n avulla. Kolmannessa pääluvussa kerrotaan taustaa FinnCode Oy:sta sekä tarkemmin Finncodeille toteutetusta järjestelmästä.

## 2 LYHYEN KANTAMAN LANGATON TIEDONSIIRTOMENETELMÄ

### 2.1 NFC

NFC eli Near Field Communication on lyhyen kantaman langaton tiedonsiirtomenetelmä, jolla kaksi NFC -sirua voivat siirtää tietoa keskenään. Tiedonsiirron aloittavaa sirua kutsutaan aloitteentekijäksi ja tiedonsiirron määränpäänä olevaa sirua kohteeksi. NFC -sirut voidaan jakaa kahteen kategoriaan: passiivisiin ja aktiivisiin.

Passiiviset sirut eivät sisällä omaa virtalähdettä. Passiivisen sirun ja antennin yhdistelmää kutsutaan tagiksi. Passiivissa siruissa aloitteentekijä generoi radiotaajuuksisen kentän, joka siruun liitetyssä antennissa generoi sähkömagneettisen induktion avulla sirun tarvitseman sähköenergian.

Aktiiviset sirut sisältävät ulkoisen virtalähteen. Ulkoista virtalähdettä käytetään sirun toimintojen suorittamiseen. Tämä nopeuttaa sirun toimintaa, koska sirun ei tarvitse kerätä energiaa ulkopuolelta toimintaansa.

NFC Forum määritteli vuonna 2006 NFC -yhteensopivissa laitteissa ja tageissa käytettävät spesifikaatiot ja laitearkkitehtuurin. Spesifikaatiot sisältävät NFC -tiedonsiirrossa käytetyn protokollan LLCP (Logical Link Control Protocol), NDEF:n (Data Exchange Format) ja RTD:n (Record Type Definition) sekä neljä tagiformaattia.

NFC -tagilla olevaan muistiin voidaan kirjoittaa tietoa, joko bitti kerrallaan tai tieto voidaan kirjoittaa NFC -forumin määrittämänä NDEF -viestinä. NDEF -viestinä kirjoitettaessa voidaan viestin ohjausbittien avulla saada NFC -tagiin erikoisominaisuuksia. Tagista voidaan tehdä esimerkiksi käyntikortti, josta tieto menee suoraan matkapuhelimen yhteystietoihin.

Aloitteentekijän generoimaan kenttää käytetään antennin tarvitsemaan energiaan. NFC perustuu 13,56 MHz radiotaajuudella tapahtuvaan sähkömagneettiseen induktioon. Erona RFID -menetelmään on se, että NFC:ssä laite voi olla sekä lähettäjä, että vastaanottaja.



## 2.2 NFC matkapuhelimessa

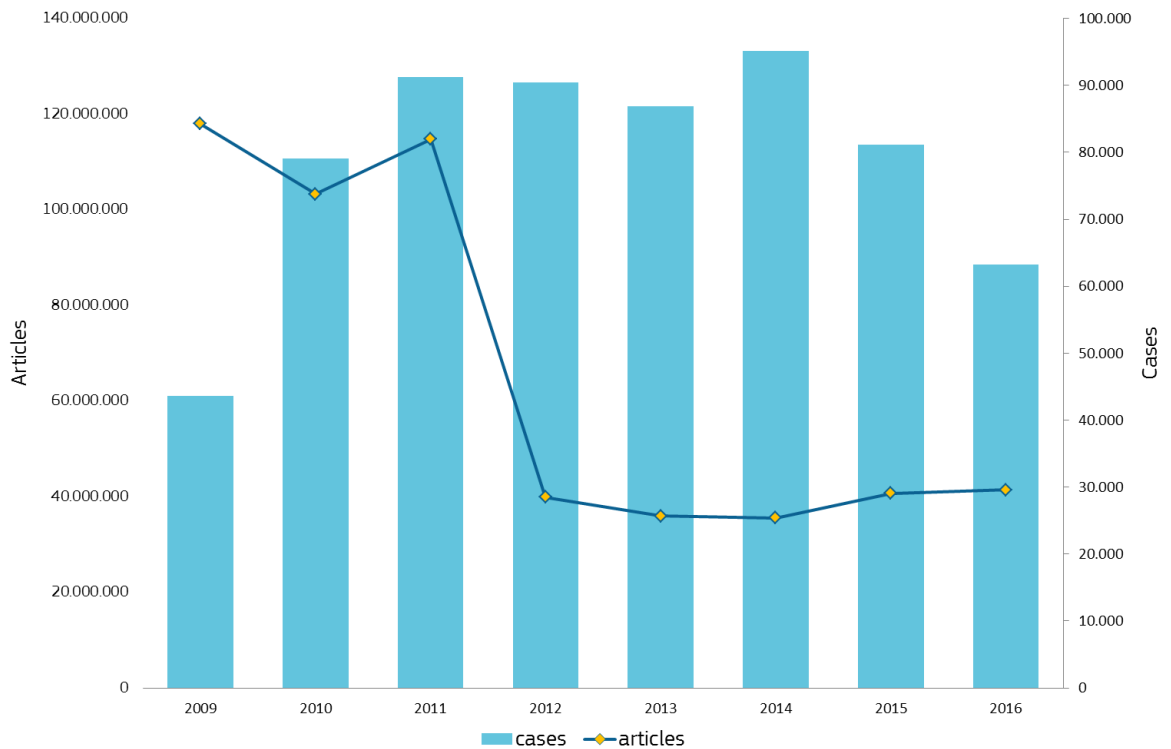
NFC -standardeissa on kolme tilaa: Card Emulation, Read/Write tai Peer to Peer -tila. Tällä hetkellä Android -käyttöjärjestelmä antaa suurimmat mahdollisuudet NFC:n hyväksikäyttöön matkapuhelinten käyttöjärjestelmistä. Windows Phone -käyttöjärjestelmään tuli 8.1-päivityksen mukana uusia ominaisuuksia NFC:n käyttöön. Tätä ennen sillä pystyi ainoastaan kirjoittamaan ja lukemaan NDEF-viestejä. Valitettavasti matkapuhelimia, joissa on uusia ominaisuuksia tukevia NFC-siruja ei ole vielä kovin paljoa markkinoilla. iPhone 6:ssa ja sen jälkeen ilmestyneissä iPhoneissa on mukana NFC -siru, mutta toistaiseksi Apple on antanut ainoastaan pääsyn lukemaan NDEF -viestejä. Apple haluaa tällä menetelmällä taata Apple Wallet:n turvallisuuden.

Korttiemuloinnissa puhelimen NFC-siru toimii NFC-tagina lukijalaitteelle. Tällöin matkapuhelimea voidaan käyttää esim. maksukorttina. Luku- ja kirjoitustilassa puhelin voi lukea ja kirjoittaa NFC-tageja. Tagilta voidaan lukea esim id-tieto, internet-osoite tai ohjata sovelluksen käynnistäminen. Peer to Peer -tilassa puhelin ja toinen laite avaavat yhteyden välilleen. Tämä mahdollistaa tiedonsiirron laitteiden välillä jotakin sovellusta varten.

NFC -standardin määritellyt NFC forum on standardoinut neljä tyyppiä NFC -tageille, NFC Forum Type 1-4, lisäksi matkapuhelimissa voidaan käyttää Mifare -standardia. Osa puhelimista tukee myös ISO 15693 -standardin tageja nimellä NFC-V. Tageja on saatavilla erillisillä asennusaloilla esim. tarroina, ulkotilan ja vaativien ympäristöjen tageina ja metallipinnoille sopivina tarroina.

Android-puhelimilla, joissa on NFC -siru voidaan käyttää ohjelmia, joilla voidaan syöttää NFC -tageille dataa bittivirtana. Tällä menetelmällä voidaan ohjata NFC -tagin sisäisiä toimintoja, kuten salausta ja tagin lukitusta salasanalla.

### 3 AITOU DEN VARMISTAMINEN



KUVIO 1. Väärennöksiin ja piratismiin liittyviä tilastoja (European Commission 2017)

Tuotteiden väärentämisessä liikkuu maailmalla paljon rahaa. Yhdysvaltain hallitus arvioi väärennettyjen tuotteiden markkina-arvoksi 500 miljardia dollaria vuonna 2008 ja noin 600 miljardia vuonna 2012 (Chaudhry & Zimmerman 2013, 9). Euroopan komission tilastoissa vuonna 2016 tullissa oli pysäytetty yli 41 miljoonaa kappaletta väärennetyiksi epäiltyjä tavaroita joiden yhteisarvo oli yli 672 miljoonaa euroa (European Commission 2017). Monenlaisia tuotteita väärennetetään. Väärennöksiä on jokapäiväisistä tuotteista kuten hammasharjoista aina kalliiseen elektroniikkaan ja muotituotteisiin. Myös lääkkeiden väärentäminen on yleistynyt. Yleensä väärennettyjen tuotteiden halvempi hinta saa ihmiset ostamaan niitä. Ihmiset myös usein tietävät ostavansa väärennetyin tuotteen, mutta eivät välitä siitä.

Väärennetyillä tuotteilla on kuitenkin useita haittapuolia, joita useimmat niiden ostajat eivät ota huomioon. Yleensä väärennettyjen tuotteiden taustalla on järjestäytynyt rikollisuus. Myös väärennetyjen tuotteiden laatu on yleensä paljon huonompi kuin aitojen.

Väärennösten havaitsemiseen on kehitetty monenlaisia menetelmiä. Menetelmät voidaan toteuttaa kahdella eri tavalla. Tuotteen tekeväälle yritykselle halvempi tapa on kiinnittää tuotteeseen jonkinlainen aitouden osoittava merkki. Tässä menetelmässä kuluttaja itse vastaa aitouden varmistuksesta. Tästä menetelmästä yleisin toteutus on tuotteessa oleva hologrammi. Yritykselle kalliimpi tapa on varmistaa tuotteen aitous lähettämällä yrityksen ylläpitämään järjestelmään kysely, onko tuote aito.

Hologrammipohjainen aitouden varmistus on ollut pitkään yksi eniten käytetyistä menetelmistä tuotteiden aitouden varmistuksessa. Nykyään kuitenkin hologrammin valmistustekniikka on yleistynyt, joten tuotteiden väärentäjien on mahdollisuus tehdä omat hologramminsa. Tässä menetelmässä tuotteen aitouden varmistus on kuluttajan vastuulla. Kuluttajan pitää itse tarkistaa, että tuotteessa oleva hologrammi täsmää yrityksen hologrammin kanssa. Tämä menetelmä on erittäin yleinen musiikin ja tietokoneohjelmien aitouden varmistuksessa.

Numerosarjaan pohjautuvat menetelmät ovat myös yleisiä. Tuotteessa oleva numerosarja lähetetään joko nettisivulle tai tekstiviestinä yrityksen palveluun, joka lähettää takaisin tiedon tuotteesta. Numerosarja voidaan yleensä tarkistaa vain kerran, joten myöhemmin tuotetta myydessä tuotteen aitoutta ei voida tarkistaa uudelleen. Mikäli numerosarjan voi käyttää uudelleen on aitouden varmistus paljon epävarmempi, sillä samaa numerosarjaa voidaan siten käyttää väärennetyissä tuotteissa.

Viiva- ja QR-koodeihin pohjautuvat menetelmät antavat mahdollisuuden käyttää matkapuheliimiin tarkoitettuja sovelluksia aitouden varmistukseen. Tässä menetelmässä on sama ongelma kuin numerosarjoissa, eli menetelmä on helppo kopioida. Huonona puolena on, että kuluttaja tarvitsee viivakoodinlukuohjelman tai tuotteen valmistaneen yrityksen erikoisohjelman aitouden varmistukseen.

Teollisuudessa voidaan käyttää viivakoodien apuna erikoispaperia, jonka aitous voidaan testata kemikaalien avulla. Tämä ei kuitenkaan toimi hyvin kuluttajatuotteissa, koska aitouden varmistukseen vaaditaan erikoisvälineitä.

RFID:seen pohjautuvat menetelmät ovat paljon varmempia kuin muut menetelmät, mutta RFID -tagien lukemiseen tarvitaan yleensä erikoislaite, mikä tekee tästä menetelmästä enemmän teollisuuteen soveltuvan. Tästä poikkeuksena ovat NFC -standardiin pohjautuvat RFID -tekniikkaa käyttävät tagit, joista tarkemmin seuraavassa luvussa.

### **3.1 Aitouden varmistus NFC:n avulla**

Aitouden varmistus NFC:n avulla voidaan toteuttaa monella tavalla. Tämä opinnäytetyö käsittelee pääasiassa NFC -tageihin pohjautuvia ratkaisuja.

Teknisesti helpoin tapa toteuttaa aitouden varmistus, on kirjoittaa NFC -tagille teksti, joka on yksilöllinen eri tageissa. Vertaamalla tätä tekstiä tietokannassa olevaan voidaan tuotteen aitous varmistaa. Tässä menetelmässä etuna on tagien edullisuus ja aitouden varmistukseen käytettävän järjestelmän yksinkertaisuus. Tagit ovat edullisempia, koska niissä ei tarvitse olla edistysellisiä ominaisuuksia ja tagien valmistaja voi kirjoittaa tageissa olevat tekstit jo valmistusvaiheessa.

Tämä menetelmä on kuitenkin helposti murrettavissa, sillä tagissa oleva teksti on helppo lukea millä tahansa NFC:n lukuohjelmalla ja teksti on helppo kirjoittaa mille tahansa muulle NFC -tagille. Tämä menetelmä on siten verrattavissa QR -koodilla toteutettuun aitouden varmistukseen.

Menetelmää voidaan parantaa paljon käyttämällä hyväksi NFC -tagin yksilöllistä id:tä. Jokaiselle NFC -tagien valmistajalle on annettu oma alueensa, jolta he voivat tehdä id:tä. On kuitenkin olemassa laitteita, kuten Proxmark III, jotka on suunniteltu emuloimaan NFC -tageja. Näillä laitteilla voidaan kopioida ja emuloida NFC -tagia täydellisesti. Tällä tavoin myös yksilöllinen id voidaan väärentää. Valmistajille annettu id -numeroiden avaruus on myös rajallinen, joten valmistajat saattavat tulevaisuudessa käyttää id:t uudelleen.

Varmennusta voidaan parantaa käyttämällä NFC -tagien lukuun omaa ohjelmaa. Tällöin voidaan käyttää hyväksi NFC -tageissa olevan mikrosirun sisäisiä komentoja, jotka vaihte-

levat valmistajan ja tagi-tyypin mukaan. Tämän menetelmän murttamiseen joudutaan kopioidaan NFC -tagilla oleva siru kokonaisuudessaan. Koska sirujen valmistukseen vaaditaan erikoistunut laitteisto, on tämä hyvin kallista.

Markkinoilla on myös olemassa NFC -tageja, joiden ominaisuuksiin kuuluu tietojen salaus. Tällöin NFC -tagia ei voida lukea tai kirjoittaa, jos sitä ei ensin avata koodiavaimella. Tässä menetelmässä kuitenkin on vaikeutena, että on pidettävä myöskin listaa nfc:n liittyvästä koodiavaimesta.

### **3.2 Ohjelman yksilöinti tunnistetun NFC –tagin avulla**

Sen jälkeen kun NFC-tagin aitous on varmistettu yhdellä tai useammalla edellä mainitulla keinolla, voidaan siitä saatua tietoa käyttää mobiililaitteen ohjelmassa. Voidaan esimerkiksi hakea palvelimelta tieto, mikä tuote on yhdistetty tagiin kuten Finncode Authentication-sovelluksessa tai mitkä tiedostot on yhdistetty tagiin kuten Otavan äänikirjat-sovelluksessa.

Toisin kuin sisäänkirjautumiseen pohjautuvissa järjestelmissä tuotteen ostaneen asiakkaan tietoja ei välttämättä tarvita, joten menetelmä on asiakkaan tietoturvan kannalta parempi. Valmistajan kannalta järjestelmä takaa heille, että koska sovelluksen käyttöön vaaditaan fyysinen NFC -tagi, että ohjelman käyttäjällä on todella kyseinen tuote, eikä kyseessä ole vain tiettyä sisäänkirjautumistietoa käyttävä käyttäjä, sillä kyseinen kirjautumistieto voidaan jakaa erittäin helposti.

Tuotteen tunnistuksen avulla voidaan tuottaa monenlaista lisäsisältöä tuotteeseen liittyen. Esimerkiksi tuotteen käyttöohjeet ja ostotiedot voidaan saada helposti. Myös mahdolliset tuotteen takaisinkutsut tai käyttöohjeiden muutokset voidaan toteuttaa nopeasti, sillä tuotteen omistaja saa uudet tiedot heti kun hän lukee tuotteen seuraavan kerran.

## **4 FINNCODE AUTENTIKOINTI**

### **4.1 Yrityksen taustaa**

FinnCoden taustalla on RE-AD niminen yritys, jonka yksi palveluista on tuotteiden tunnistus NFC:n avulla ja niiden huoltotietojen näyttäminen tämän jälkeen. Yrityksen perustajien käydessä yrittäjille tarkoitetulla matkalla Brysseliin, oli EU:n piratismiin vastaisen toiminnasta vastaavan henkilön, joka oli ehdottanut heille, että järjestelmää voisi soveltaa tuotteen aitouden varmistamiseen.

Kesällä 2014 alettiin kehittämään järjestelmää, jolla voitaisiin NFC:tä hyväksikäyttäen varmistaa tuotteen aitous. Järjestelmän kehittäjäksi perustettiin uusi yhtiö nimellä FinnCode Oy. Tarkoituksena rakentaa järjestelmä, jossa yritykset voisivat luoda järjestelmään tuotteet ja saada niiden myynnistä reaaliaikaista tietoa ja myöhemmin lähettää asiakkailleen tarjouksia ja mainoksia järjestelmän kautta. Järjestelmän avulla yritykset myös voivat saada ensimmäistä kertaa tietoa, myös sen jälkeen kun asiakas on myynyt tuotteen edelleen. Tämän avulla yritykset voivat saada arvokasta tietoa siitä, mitä tuotteille tapahtuu niiden elinkaaren aikana. Järjestelmä myös antaa valmistajille tietoa, missä kaupoissa tuotetta on myyty ja mihin maihin.

### **4.2 FinnCode Authentication -järjestelmä käytössä**

FinnCode Authentication on tuotteiden aitouden tarkistamiseen suunniteltu järjestelmä, jonka pääosana on tällä hetkellä Android -käyttöjärjestelmälle tehty sovellus, jolla Android -matkapuhelimella voidaan tarkastaa NFC -tagi lukemalla tuotteen aitous. Tulevaisuudessa järjestelmään on tarkoitus lisätä Iphone ja Windows Phone versiot ohjelmasta, mutta toistaiseksi teknisten rajoitusten takia, niitä ei voida tehdä. Ohjelmasta on tehty Iphone -versio, mutta toistaiseksi ohjelmassa on ainoastaan kuluttajalle rekisteröityjen tuotteiden näyttö. Uusissa iOS -versioissa on alkeellinen NFC:n lukuominaisuus, mutta esimerkiksi yksilöllisen id:n lukeminen ei onnistu.



# Finncode Authentication

FinnCode Ltd Elämäntapa

★★★★★ 8

3 PEGI 3

Sisältää mainoksia

Tämä sovellus on yhteensopiva joidenkin laitteidesi kanssa.

Asennettu



Finncode is a cutting-edge system that helps to authenticate things that matter to you. Utilizing unique NFC (Near Field Communication) technology, Finncode can register your valuables and store the information safely to our cloud service. This eliminates the need to register your products by mailing coupons, registering to multiple services and storing all those papers and brochures.

KUVA 1. Finncode sovellus (Google Play 2017a)

Järjestelmän perustana on MySQL -tietokanta, johon tuotteet on talletettu. Järjestelmä on kirjoitettu pääasiassa Perl -ohjelmointikielellä. Internet -sivuston pohjaksi valittiin Perl pohjainen Dancer 2 -kehitysympäristö. Järjestelmään luotiin internetin kautta käytettävä ohjausjärjestelmä, jolta järjestelmään voidaan lisätä uusia tuotteita ja järjestelmässä olevien tuotteiden tietoja muuttaa. Matkapuhelin-ohjelmien ja tietokannan välistä yhteyttä hoitaa Perl -ohjelmointikielellä kirjoitettu rajapinta, joka lähettää ja vastaanottaa tietonsa JSON -formaattissa.

Android -sovelluksen ensimmäisessä versiossa tuotteen aitous tarkistettiin lukemalla NFC -tagille kirjoitettu teksti ja lukemalla NFC -tagin uniikki ID. Nämä tiedot lähetettiin rajapintaan ja siellä suoritettiin tarkistus, vastaavatko NFC-tagin tiedot tietokannassa olevia tietoja. Aitouden tarkistus on kuitenkin tällä menetelmällä epätäydellinen. Myöhemmin tähän versioon lisättiin tagin sisäisiä ominaisuuksia hyväksi käytävä uniikin ID:n lukutoiminto, jossa tarkistetaan, että luettava NFC -tagi on varmasti tietynlainen.

Seuraavassa versiossa otettiin käyttöön modernimmalla NFC -tagilla ominaisuutena oleva tagin lukitseva ominaisuus. Tällöin NFC -tagilla olevat tiedot voidaan lukea vain FinnCode Authentication -ohjelmalla, koska vain sen kautta tagi saa tarvitsemansa avauskoodin. Tällöin tagin sisällä olevan tiedon kopioiminen vaikeutuu huomattavasti. Tässä versiossa myös tagin sisältämä tieto vaihdettiin jokaisen luvun yhteydessä. Tällä saadaan aikaiseksi se, että maailmassa voi olla vain yksi aito kappale tiettyä tagia. Tähän tekniikkaan kuitenkin liittyy tiettyjä ongelmia. Testeissä havaittiin, että käyttäjillä oli usein vaikeuksia saada luettua tagia, sillä kenttäolosuhteissa tagin lukemiseen, tietojen hakuun ja tagin uudelleenkirjoittamiseen menee useita sekunteja, käyttäjä yleensä poisti matkapuhelimen pois NFC:n lukualueelta liian nopeasti.

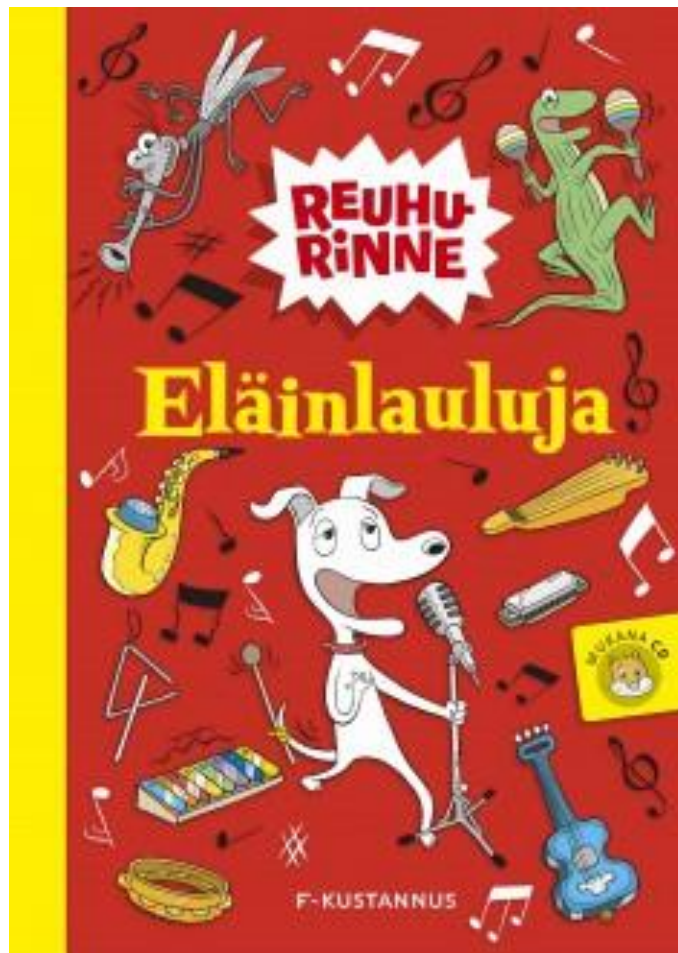
Suurin osa järjestelmän halunneista yrityksistä päätyi lopulta versioon, jossa NFC -tagille kirjoitetaan tagille yksilöllinen viesti ja ohjelma lukee sen lisäksi NFC:n uniikin ID:n. Näiden tietojen pohjalta palvelimella määritetään tuotteen aitoutta. Tämä ei ole varmin mahdollinen menetelmä, mutta tämä on yrityksille helpoin käyttää.

Finncode Authentication -palvelusta tehtiin myös versio, jossa tuotteen aitouden varmistuksen jälkeen saatiin tuotetietojen lisäksi tuotteen huoltotiedot. Järjestelmään tehtiin yritysten käyttöön ohjelma, jolla he voivat lisätä NFC:n lukemalla huoltotietoja ja huoltoon liittyvien osien tietoja. Näin kuluttajat voivat NFC:n lukemalla saada tietoja omaan tuotteeseensa liittyvistä huolloista ja huoltoihin liittyvistä osista. Myös tuotteen ja huolto-osien takuutiedot saa kätevästi ohjelmasta. Järjestelmään oli tarkoituksena lisätä myös muuta tietoa tuotteista, kuten vaatteiden pesutiedot, jotka yleensä ovat tiivistettynä vaatteeseen liitettävässä lipukkeessa.



Android -sovelluksessa on tori, jossa kuluttajat voivat myydä heille rekisteröityjä tuotteitaan. Tämän avulla tuotteen valmistaja saa tietoa jälleenmyyntimarkkinoilta, mistä he eivät yleensä ennen saaneet tietoa. Iphone -sovelluksessa asiakkaat voivat ainoastaan tarkastella omistamiensa tuotteiden tietoja ja päivittää tuotteensa päiväkirjaa.

Myöhemmin järjestelmään kehitettiin tuotteen tunnistukseen pohjautuvia muita sovelluksia. Järjestelmään lisättiin muun muassa aikakorttijärjestelmä, tuotteiden paketointiin liittyvät tiedot sekä äänikirjat. Näistä ainoastaan äänikirja-sovelluksiin tuli kaupallista sisältöäkin. Otavalle tehtiin ensin Reuhurinne -lastenkirjoihin pohjautuvan sovelluksen, jossa Reuhurinne Eläinlauluja -kirjaan lisättiin kannen sisään NFC -tagi, jolta pystyi Android -sovelluksen avulla kuuntelemaan kirjaan liittyvät laulut. Myöhemmin Otavalle tehtiin Otavan äänikirjat -sovellus, johon liittyviä NFC -tagin sisältäviä kortteja voi ostaa kaupoista. Näissä sovelluksissa tuotteen aitous tarkastetaan, jonka jälkeen kyseiseen kirjaan kuuluvat äänitiedostot voi kuunnella sovelluksella.



KUVA 2. Reuhurinne Eläinlauluja -kirja (Otava 2017)



KUVA 3. Reuhurinne Ekstra -sovellus (Google Play 2017b)

Finncode Authentication -järjestelmä otettiin käyttöön muutamiin tuotteisiin eri valmistajilla. Tunnetuin ja eniten käytössä näistä olivat järjestelmän esittelykäyttöön paljon käytetyt Aki Choklat:n suunnittemat Dara ja Ami -laukut, joihin oli lisätty järjestelmään liittyvä NFC-tagi.



KUVA 4. Dara -laukku (Aki Choklat 2017a)



KUVA 5. Ami -laukku (Aki Choklat 2017b)

Finncode Authentication -tageja oli myös eräissä italialaisen suunnittelijan Francesca Castagnacci:n suunnittelemissa kengissä. Käytössä järjestelmä havaittiin hieman vaikeaksi toteuttaa, sillä tuotteiden rekisteröinti asiakkaille tapahtui myyjän toimesta. Tämä tarkoitti sitä, että tuotteita valmistavan yrityksen täytyi kouluttaa tuotteidensa myyjät käyttämään Finncoden toteuttamaa yrityksillä tarkoitettua sovellusta, jolla tuotteet voitiin rekisteröidä. Tämä rekisteröintiprosessi myös aiheuttaa myyjille ylimääräistä työtä ja asiakkaille pidemmän ostoprosessin.

## 5 JOHTOPÄÄTÖKSET JA POHDINTA

Älypuhelimien ja langattoman internetin yleistymisen ovat luoneet uuden mahdollisuuden valmistajille luoda yhteyksiä kuluttajiin. Valmistajat kuitenkin tarvitsevat jonkinlaisen tavun yksilöidä tuotteitaan, että he voivat antaa parempaa palvelua. NFC -pohjainen tuotteiden autentikointi on yksi vaihtoehto, jolla tämä voidaan toteuttaa. Kuluttajille on kuitenkin tarjottava jotain muutakin kuin pelkkä tuotteen aitouden ja tietojen esittäminen. Suurin osa kuluttajista ei ole kiinnostunut siitä, onko tuote aito vai ei. Heitä kiinnostaa enemmän tuotteen hinta, mikä väärennetyissä tuotteissa on yleensä halvempi kuin aidoissa.

Tulevaisuudessa tuotteiden aitouden varmistamisesta tulee entistä tärkeämpää. Erityisesti lääkkeiden aitouden varmistamiseen tullaan tulevaisuudessa panostamaan paljon. Tällä hetkellä lääkeväärennöksiä on Suomessa ja EU-jäsenvaltioissa havaittu vasta vähän, mutta kehitysmaissa väärennöksiä saattaa olla markkinoilla olevista lääkkeistä jopa 10-30% (Lääkealan turvallisuus- ja kehittämiskeskus Fimea [www-sivusto](http://www.fimea.fi)). Lääkkeiden väärennöksissä vaarat kuluttajalle ovat huomattavasti suuremmat kuin esim. vaatteiden. Mikäli Finn-code Authentication -järjestelmällä voitaisiin esimerkiksi lääkkeiden aitouden varmistuksen lisäksi antaa vaikka hälytyksiä jotka muistuttavat ottamaan lääkkeitä. Tämä olisi erityisen tärkeää huonomuistisille ihmisille.

Järjestelmän pääpaino pitäisi tulevaisuudessa toistaiseksi keskittää tarjoamaan enemmän lisäpalveluja tuotteille, kuin antamaan tuotteen aitoustietoa. Nykyinen kuluttajakulttuuri ei ole vielä sellainen, että tuotteen aitouden toteaminen olisi tuotteen oston kannalta tärkeää.

## LÄHTEET

Aki Choklat. 2017a. Dara absinthe. Saatavissa <http://www.akichoklat.com/shop/dara-absinthe>. Luettu 20.12.2017

Aki Choklat. 2017b. Ami onyx black. Saatavissa <http://www.akichoklat.com/shop/ami-onyx-black>. Luettu 20.12.2017

Chaudhry, P.E. & Zimmerman. A 2013. Protecting Your Intellectual Property Rights.

European Commission. 2017. IPR Infringements: Facts and figures. Saatavissa [https://ec.europa.eu/taxation\\_customs/business/customs-controls/counterfeit-piracy-other-ipr-violations/ipr-infringements-facts-figures\\_en](https://ec.europa.eu/taxation_customs/business/customs-controls/counterfeit-piracy-other-ipr-violations/ipr-infringements-facts-figures_en). Luettu 20.12.2017

Fimea. 2017. Lääkeväärennökset. Saatavissa [http://www.fimea.fi/vaestolle/laakkeiden\\_turvallisuus/laakevaarennokset](http://www.fimea.fi/vaestolle/laakkeiden_turvallisuus/laakevaarennokset). Luettu 23.12.2017

Google Play. 2017a. Finncode Authentication. Saatavissa <https://play.google.com/store/apps/details?id=finncode.app>. Luettu 20.12.2017

Google Play. 2017b. Reuhurinne Ekstra. Saatavissa <https://play.google.com/store/apps/details?id=com.finncode.reuhurinne>. Luettu 20.12.2017

Otava. 2017. Reuhurinne eläinlauluja. Saatavissa <https://otava.fi/kirjat/9789511303879>. Luettu 20.12.2017