RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo-SP, ano II, v.2, n. 2, jul./dez. 2022.

# NFC (Near Field Communication; Campo próximo de comunicação) entendimento e aceitação

*NFC understanding and acceptance (Near Field Communication)*

Sanderson Vinicius Pereira Fonseca[1]
Welton Gomes Azevedo[2]
Guilherme Bessa Alves[3]
Jonathan Costa Pereira Julio[4]
Prof. Luciano Pimenta Valadares (Orientador)[5]

Submetido em:18/08/2022
Aprovado em: 18/08/2022
Publicado em: 20/08/2022
DOI: 10.51473/rcmos.v2i2.341

**RESUMO**

Embora a dependência inevitável da humanidade com computadores não seja mais o que surpreende e admiram alguns, apesar de ser irreversível seu uso, há outros sistemas tecnológicos que passam despercebidos, como é o caso da popularização das interfaces de comunicação sem fio entre computadores. A adoção dessas interfaces sem fio está acontecendo em etapas e, curiosamente, o estilo de vida do indivíduo como um todo mudou, pois, a tecnologia NFC (Near Field Communication) permite a troca de informações de forma rápida e de curto prazo através de dispositivos compatíveis totalmente automático. Esse recurso pode ser usado com celulares, Tablets, cartões eletrônicos, tags ou qualquer dispositivo que possua tecnologia NFC. No entanto, a falta de informação sobre o dispositivo gera uma indagação de como adaptar o NFC e controlar a sua via? Uma vez que, esse mecanismo não apenas elimina a perda financeira do desgaste físico da interface e a consequente interrupção do serviço, como também possibilita que inúmeras aplicações exigem apenas um dispositivo ativo, marcando o próximo grande passo na propagação de interfaces de comunicação sem fio. Por essa razão, se faz necessário analisar como funciona a tecnologia via NFC. Visto que para o equilíbrio financeiro ou qualquer controle de comunicação sem fio, requer equilíbrio, não importando o quanto se é utilizado o sistema e sim, o controle efetivo do uso para que haja alcance dos objetivos em menos tempo e ao menor custo possível. Esse tipo de transferência, portanto, possibilita a troca de arquivos entre celulares, como fotos, vídeos, músicas, links de sites, dados criptografados, transações bancárias, podendo até substituir o uso de cartão de crédito.

**Palavras chaves:** Tecnologia NFC. Controle de acesso. Interfaces sem fio. Informações em curto prazo.

**ABSTRACT**

Although the inevitable dependence of humanity on computers is no longer what surprises and amazes some, despite its irreversible use, there are other technological systems that go unnoticed, such as the popularization of wireless communication interfaces between computers. The adoption of these wireless interfaces is happening in stages and, curiously, the individual's lifestyle as a whole has changed, for, NFC (Near Field Communication) technology allows the exchange of information in a fast and short-term manner through fully automatic compatible devices. This feature can be used with cell phones, tablets, electronic cards, tags, or any device that has NFC technology. However, the lack of information about the device generates a question of how to adapt NFC and control its path? This mechanism not only eliminates the financial loss from the physical wear and tear of the interface and the consequent interruption of service, but also makes it possible for countless applications to require only one active device, marking the next big step in the propagation of wireless communication interfaces. For this reason, it is necessary to analyze how NFC technology works. Since the financial balance or any control of wireless communication requires balance, it does not matter how much the system is used, but the effective control of the use, so that the objectives are reached in less time and at the lowest possible cost. This type of transfer, therefore, enables the exchange of files between cell phones, such as photos, videos, music, website links, encrypted data, banking transactions, and may even replace the use of a credit card.

**Keywords:** NFC technology. Access control. Wireless interfaces. Short term information.



1 Sanderson Vinicius Pereira Fonseca. sanderson.fonseca@es.estudante.senai.br
2 Welton Gomes Azevedo. welton.azevedo@es.estudante.senai.br
3 Guilherme Bessa Alves. bessaguilherme51@gmail.com
4 Jonathan Costa Pereira Julio. Jonathan.julio@es.estudante.senai.br
5 Luciano Pimenta Valadares. (Orientador). luciano.valadares@es.docente.senai.br

## 1 INTRODUÇÃO

Near Field Communication, mais conhecido como NFC, mudou a forma de trocar informações no dia a dia. Através dessa nova tecnologia é possível realizar pagamentos de forma aproximada, cujas informações podem ser transmitidas para outros dispositivos sem a necessidade de uma conexão com fios. Esse novo sistema permite que os dados sejam trocados de um dispositivo para outro sem intermediário de software só aproximando um dispositivo que contenha a tecnologia NFC em outro e a troca de dados acontece em fração de segundos. Essa técnica que visa a resolução de problemas surgiu no Japão entre 2002 e 2004 devido algumas empresas sentirem a necessidade de um dispositivo que transmitisse uma comunicação em curta distância, desenvolvendo o NFC.

Portanto, o aumento de redes sem fio e o desenvolvimento da miniaturização eletrônica abriram as portas para a adoção em massa de smartphones. Além de possibilitar a comunicação sem fio via NFC, o mesmo dispositivo pode substituir os cartões convencionais por pagamentos eletrônicos, onde em breve será possível efetuar pagamentos simplesmente aproximando o smartphone do receptor, de forma mais rápida e prática do que aquele usado hoje com cartões magnéticos ou com chip.

Por essa razão, a presente pesquisa tem por finalidade entender como se dá o uso da tecnologia via NFC, visto que, a humanidade ainda está dependente de interfaces de conexões sólidas onde alguns dispositivos eletrônicos que têm essa interface que lhe dá com muitas conexões e desconexões diariamente com o tempo passam por degradação mecânica sendo a principal causa de falha e mau funcionamento ocasionando prejuízos. Portanto, a presente pesquisa está dividida em três capítulos cujo primeiro: refere-se à tecnologia NFC; o segundo: a vantagem do NFC para os usuários; e, o terceiro: à adaptação de NFC em dispositivos.

## 2 A TECNOLOGIA NFC

A tecnologia NFC usa uma frequência de 13,56 MHz, largura de banda Até 424 Kbps para comunicação sem fio de curto alcance. O dispositivo precisa estar dentro de 4 cm de distância para iniciar a comunicação. Esta tecnologia é conhecida por funcionar com uma única aproximação para funcionar, ou seja, uma comunicação sem fio. Os dispositivos habilitados para comportar o sistema NFC são os novos Smartphones e Tablets que possuem antenas NFC em seus componentes. A fusão dessa tecnologia aumentou a popularidade do NFC, expandindo muito sua gama de aplicações. Os mais comuns hoje são usados para controlar o acesso ao transporte público e atrações de lazer e terminais de ponto de venda de cartão de crédito.

As tags NFC são chips de memória que podem ser incorporados, mais comumente encontrados em adesivos e cartões. Eles não possuem fonte de energia (passivos), então seu funcionamento depende de um leitor NFC e um campo magnético ativado pelo dispositivo móvel (ativo).

Para um dispositivo ser compatível com a tecnologia, ele deve conter uma antena NFC, que utiliza o protocolo de comunicação sem contato disposto na ISO 14443 (ORGANIZATION, 2003 p. 120). A necessidade de controlar o acesso aos eventos sempre existiu, por isso todo o processo desde a compra do ingresso até a entrada no evento é bem conhecido. Esse controle se desenvolve ao longo do tempo. Usar um smartphone e NFC para controlar o acesso a eventos é uma nova parte dessa inovação. Por ser relativamente novo, inclusive em outras áreas de aplicação, supõe-se que a maioria dos usuários seja inexperiente com a tecnologia.

A adoção de NFC em dispositivos móveis cresceu rapidamente e os fabricantes vêm adicionando a tecnologia aos designs de seus dispositivos móveis. Estima-se que cerca de 400 milhões de dispositivos móveis equipados com NFC tenham sido vendidos em todo o mundo, e esse número deve chegar a mais de um bilhão em 2022.



### 2.1 Vantagens do uso do NFC (Near Field Communication)

As principais vantagens para os usuários finais que utilizam NFC são: fácil conexão, transações rápidas e fácil compartilhamento de dados. Um dos fundamentos da segurança da informação é baseado na integridade, que visa garantir

que um documento não altere seu conteúdo após sua assinatura. Para fazer isso, o sistema deve ser capaz de detectar alterações não autorizadas no conteúdo. O objetivo é que o destinatário verifique se os dados não foram modificados indevidamente.

Segundo (Bruce Schneier, 1996) Existem várias técnicas para assegurar a integridade dos dados, uma delas se chama Hash ou Hash sum, que se baseia na criação de uma sequência de símbolos única baseada no documento ou conjunto de dados.

O apelo da segurança para todos os tipos de transações levou ao desenvolvimento de sistemas que utilizam a tecnologia NFC, pois suas propriedades fornecem inerentemente um nível adicional de segurança nos sistemas em que é aplicada. No caso de substituição do cartão, evita "ataques de retransmissão", que ocorrem quando as comunicações com o cartão inteligente são retransmitidas a longas distâncias através de canais de dados alternativos. Dentre os diferentes tipos de sistemas, um deles se refere à autenticação, que leva a entrada de eventos na aplicação de controle. Embora não seja totalmente à prova de fraude.

Nos EUA e no Japão, a tecnologia tem sido usada para comprar passagens de trem, ingressos para eventos e até pagar compras. No sistema de metrô de Tóquio, você pode comprar uma passagem simplesmente segurando seu telefone próximo ao portão. Essa simples função mudou a forma como as viagens domésticas, além de aumentar a confiança na tecnologia.

**2.2 A adaptação de NFC em dispositivos**

A implementação de serviços de computação móvel utilizando a tecnologia NFC depende dos mecanismos de segurança para sua operação. As técnicas descritas permitem a criação de soluções funcionais, mas possuem limitações de usabilidade ou segurança. Portanto, é importante que haja protocolos de autenticação amigáveis e seguros entre dispositivos móveis e servidores que possuem o sistema NFC.

Esses protocolos são chamados de Protecting Touch (PT), PT1 é usado para tags de armazenamento NFC, enquanto PT2 usa tags de processador MIFARE DESFire. Em relação ao primeiro protocolo, ele funciona com qualquer tag de armazenamento e pode ser utilizado como fator de autenticação. Esta etiqueta é usada para armazenar uma chave de autenticação que associa o aplicativo a outro.

O material criptográfico armazenado no smartphone é usado para vincular o conteúdo da etiqueta à instância do aplicativo instalado. Este material pode ser simétrico ou Assimétrico para criptografar e autenticar mensagens NDEF.

Os dados do PT1 são condicionados em mensagens NDEF e podem ser armazenados em qualquer tipo de tag NFC. A carga útil OTK Payload do registro único (OTK) contém o identificador de usuário (IDuser) onde uma chave de índice de contador (CT OTK), e a chave de uso único (kOTK). A carga útil do registro é criptografada e contém um código de verificação de mensagem. A criptografia e a autenticação de mensagens são feitas usando chaves conhecidas do aplicativo e armazenado em (key vault) implementado no sistema operacional. Um vetor de inicialização aleatório para encadear blocos de cifras é mantido na memória do aplicativo.

Assumindo que o IDuser é de 4 bytes para CT OTK, já o comprimento do kOTK é de 32 bytes, e a criptografia é AES-128 e a codificação da mensagem de autenticação é HMAC-SHA-256 (32 bytes), a carga útil do registro OTK ocupará 80 bytes. E depois será necessário acrescentar um cabeçalho NDEF do tipo "fkaway.br:ptotk" com um nome do registro OTK que pode caber em 100 bytes, embora que o registro HMAC-SHA-512 e AES-256, cabe em 130 bytes.

As tags NFC podem conter um registro NDEF onde acionará o dispositivo automaticamente, por meio do Android Application Record (AAR) conforme a imagem abaixo.

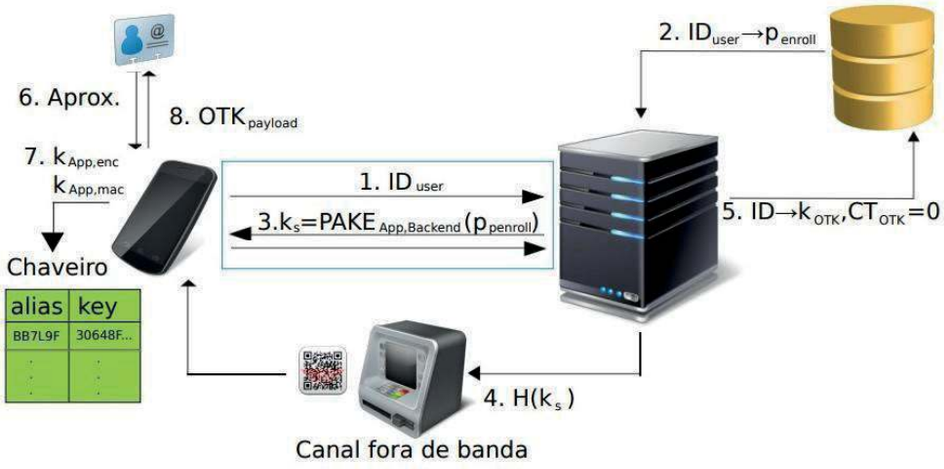


Figura 23 – Cadastramento inicial de etiqueta do Protecting Touch 1

Durante o registro inicial da tag, o aplicativo gera um novo par de chaves e os armazena em seu chaveiro, dessa forma o protocolo de inicialização é acionado pelo usuário onde será inserido no IDuser (eu identificador) e no Pen Roll (senha).

O aplicativo inicia a interação com o servidor enviando um IDuser e Indica que um novo rótulo, App æ Server: IDuser, está registrado. Depois o servidor carrega a senha de registro de seu banco de dados (usando baseado em IDuser) e a fase de autenticação começa. Se não houver correspondência a comunicação com o aplicativo será encerrada. Portanto, o aplicativo e o servidor realizam uma troca de chave, autenticada pela Pen Roll (senha) (Aplicativo+Servidor: ks = PAKEApp, Backend (Penroll).

Se a senha de registro não for considerada forte o suficiente, em alguns cenários de aplicação, a fase de autenticação pode ser realizada por meio de um canal fora de banda. Para isso, tanto o servidor quanto a aplicação geram um hash através da chave compartilhada ks, para que o servidor passe o hash para o aplicativo através do canal fora de banda. O aplicativo compara os hashes para verificar se está se comunicando diretamente com o servidor. Esse canal fora de banda pode ser uma máquina de caixa eletrônico, que exibe o hash na forma de um código de resposta rápida (QR) legível pelo aplicativo e solicita ao usuário resultados de verificação e, uma vez logado, usa seu cartão de conta bancária e senha. O aplicativo e o servidor contam até zero e obtêm KOTK da chave de sessão. O servidor armazena uma chave de uso único e um contador inicial em seu banco de dados.

O usuário aproxima a etiqueta NFC depois de ter sido instruído a fazer o processo pelo app. Em seguida, o aplicativo gera novas chaves simétricas como kApp,mac e kApp,enc em seu chaveiro. Se ele não suportar rapidamente será gerado um novo par de chaves assimétricas. E assim, as chaves aleatórias temporárias kApp, mac e kApp,enc são geradas, criptografadas onde será armazenado na memória do aparelho. Depois o mesmo aplicativo gera um novo registro - OTK e IDuser, que nada mais é que o contador de índice de chave inicial juntamente com chave de uso único ambos criptografadas para adicionar código de verificação de mensagens através das chaves simétricas ou assimétricas temporárias e o envia para armazenamento na etiqueta.

Aplicativo + Etiqueta: OTK Payload



O protocolo de autenticação é iniciado aproximando-se a etiqueta NFC ao dispositivo móvel. Isso pode acontecer depois que o aplicativo instrui o usuário a se aproximar do rótulo, quando o usuário toca no rótulo, mesmo que o aplicativo não esteja em execução.


Figura 24 – Operação do Protecting Touch 1

O aplicativo lê a mensagem NDEF da etiqueta NFC e extrai o registro OTK.

Aplicativo + Etiqueta: OTK Payload

## CONCLUSÃO

Este trabalho apresenta um método de aplicação da tecnologia NFC a um sistema de cobrança, controle de passagens ou controle de acesso. Uma das prioridades do trabalho é avaliar a aceitação da tecnologia NFC entre os usuários brasileiros. Os resultados mostram que o modelo proposto e a tecnologia NFC são bem aceitos em todos os aspectos. Devido à pequena amostra de usuários avaliados, a aceitação observada deve ser considerada apenas como um indicador da alta aceitação da tecnologia NFC no mercado brasileiro para controle de acesso em qualquer tipo de empreendimento. Atualmente, a tecnologia NFC é usada principalmente para pagamentos sem contato, permitindo que smartphones sejam usados como cartões de crédito tornando o processo mais seguro. O sistema não tem só essa função, pelo contrário, o NFC tem outras funcionalidades, sendo muito útil entender suas funcionalidades no celular. Atualmente está se tornando popular no Brasil.

Portanto, pode-se entender que o NFC foi projetado para transmissão de dados via ondas eletromagnéticas de forma distanciada entre o dispositivo.

O recurso também possui velocidades de transferência mais baixas em comparação com o Bluetooth. Por outro lado, as vantagens são o emparelhamento quase instantâneo e o baixo consumo de energia. Dessa forma, a tecnologia é considerada segura justamente por operar em distâncias menores. Assim, o NFC é uma tecnologia prática e com muitas possibilidades de uso.

Um exemplo que já está sendo utilizado em larga escala no Brasil é o uso de NFC para pagamento de passagens de ônibus e metrôs. Em São Paulo, algumas cidades, como São Paulo, começaram a oferecer a possibilidade de pagar os ônibus diretamente com cartão de crédito ou até mesmo um smartphone com NFC. Basta tocar na máquina, sem necessidade de digitar uma senha, como qualquer outro cartão de ônibus. NFC é uma tecnologia que anda de mãos dadas com a Internet ou IoT (Internet of Things; internet das coisas) que é um conceito que significa transformar os objetos cotidianos em objetos inteligentes e conectados. Trata-se de torná-lo mais fácil de usar e mais prático no trabalho diário. O NFC é justamente a capacidade de conectar objetos a uma rede e permitir a comunicação entre eles.

## REFERÊNCIAS

ABDUL, D. S.; ELMINAAM, H. M. A. K.; HADHOUD, M. M. Performance **evaluation of symmetric encryption algorithms.** Communications of the IBIMA, v. 8, 2009.

BARCLAYS. **Contactless Mobile.** 2012.. Accessed: 2015-09-30.

BOULOS, M., WHEELER, S., TAVARES, C., JONES, R., How smartphones are changing the face of mobile and participatory healthcare: an overview, with example from eCAALYX, **BioMedical Engineering OnLine,** Vol. 10, 2011.

BURKE, B. **RESTful Java with JAX-RS.** [S.l.]: O'Reilly Media, 2010.

CEIPIDOR, U. B., et al., NFC: **Integration between RFID and Mobile, state of the art and future developments**, Emerging Technologies for Radiofrequency Identification, p.78-81, 2008.

FIDO Alliance.**FIDO NFC Protocol Specification v1.0.** 2015. Implementation Draft.

FIDO Alliance.U.B., MEDAGLIA, C.M., MARINO, A., MORENA, M., SPOSATO, S., MORONI, A., Di ROLLO, P., MORGIA, M.La, **Mobile ticketing with NFC management for transport companies.** Problems and solutions, 5th International Workshop on Near Field Communication (NFC), 2013.

CHEN, L. Recommendation for key derivation using pseudorandom functions. **NIST special publication**, v. 800, p. 108, 2008.

CHOU, W. **Elliptic curve cryptography and its applications to mobile devices.** 2003.

COSKUN, V.; OK, K.; OZDENIZCI, B. **Professional Application Development for Android.** [S.l.]: Wrox, 2013.

COSKUN, V.; OK, K.; OZDENIZCI, B. **Professional NFC application development for Android.** [S.l.]: John Wiley & Sons, 2013.

GALITZ, W.O., **The essential guide to user interface design: an introduction to GUI design principles and techniques**, John Wiley & Sons, Inc., 3ª ed., 2007.

IGOE, T, JEPSON, B., BEGINNING. **NFC: near field communication with Arduino, Android, Phonegap**, O'Reilly Media, Inc., p.11–15, 2014.

MADLMAYR, G., LANGER J., KANTNER. C., SCHARINGER, J., **NFC Devices: Security and Privacy, Third International Conference on Availability, Reliability and Security**, ARES 08. 2008.

MATOS, A. V. Desenvolvimento **de um protótipo de aplicação para um dispositivo com sistema operacional Android para a gestão de um evento por um produtor.** Universidade Tecnológica Federal do Paraná, 2012. Dissertação (Pós-graduação para Especialização em Tecnologia Java). Disponível em: http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/830/1/CT_JAVA_VII_2012_19.PDF. Acesso em 17 jun. 2022.

NFC-FORUM. **NFC and Contactless Technologies.** Disponível em: http://nfc-forum.org/what-is-nfc/about-the-technology/. Acesso em 15 jun. 2022.

ORGANIZATION, I. S. **International standard ISO/IEC 14443.** Technical Specification. 2003, p.18

POURGHOMI, P., SAEED, M. Q., GUINEA, G. Secure **Cloud-based NFC Mobile Payment Protocol.** Disponível em https://eprint.iacr.org/2014/538.pdf. Acesso em 25 de outubro de 2022.

ROLAND, M., **Software Card Emulation in NFC-enabled Mobile Phones:** Great Advantage or Security Nightmare? Fourth International Workshop on Security and Privacy in Spontaneous Interaction and Mobile Phone Use (IWSSI/SPMU), Newcastle, UK, 2012.

SCHNEIR, B., **Applied Cryptography**, 2ªed., Mountain View, p.14-15, 1996.

VISA, pay. **Wave for Mobile**, Disponível em: https//www.developer.visa.com/paywavemobile. Acesso em 20 jun. 2022.