

Relatório Projeto 2015 / 2016

Web NFC Authentication Use Case

21200094 – Ricardo Peres

Lisboa, Portugal

Janeiro de 2016

Universidade Lusófona de Humanidades e Tecnologias
Matemática – Ciências da Computação / Trabalho Final de Curso
Professor: Prof. José Faísca

1 Agradecimentos

Quero deixar um enorme agradecimento ao meu orientador de projeto, o Professor José Faísca, pela ajuda e apoio disponibilizados durante a execução do mesmo, tanto na vertente técnica como teórica, e também pela sugestão de um tema de enorme interesse.

Desejo também deixar um obrigado à comunidade open source em geral, por permitir que esta e outras inúmeras iniciativas tecnológicas possam surgir.

Comunidade para a qual, o Professor José Faísca me incentivou a dar atenção e a contribuir com a disponibilização deste mesmo projeto.

Index

| | |
|--------------------------------------|-------------------|
| 1 AGRADECIMENTOS..... | <u>2</u> |
| 2 RESUMO..... | 4 |
| 3 ABSTRACT..... | <u>5</u> |
| 4 INTRODUÇÃO..... | 6 |
| 5 FERRAMENTAS..... | 7 |
| 6 DESENVOLVIMENTO..... | 8, 9 |
| 7 FUNCIONAMENTO..... | 10, 11, 12 |
| 8 RESULTADOS..... | 13 |
| 9 DISCUSSÃO E CONCLUSÕES..... | 13 |
| 10 PONTOS NEGATIVOS..... | 14 |
| 11 REFERENCIAS..... | 15 |
| 12 GLOSSÁRIO..... | 16 |

2 Resumo

O objetivo deste projeto consiste em criar uma solução que permita que a autenticação em sites web se torne num processo mais seguro e cómodo para o utilizador.

Para tal, foi idealizado um método no qual, a autenticação é efetuada, usando a Web NFC API da W3C, juntamente com, a tecnologia de identificação por 2 fatores.

De forma a demonstrar o funcionamento do conceito, foi construído um protótipo de um recetor NFC que servisse de interface entre o dispositivo onde é apresentado um formulário de autenticação e um emissor NFC. Esse interface traduziu-se no desenvolvimento de, um portal web que disponibilizasse a identificação por 2 fatores como forma de autenticação, e de uma aplicação móvel geradora de tokens, os quais servirão para autenticar o utilizador no referido portal através do protótipo construído.

De forma a elucidar o leitor sobre os conceitos em causa no projeto, os mesmos serão de seguida explicados resumidamente.

NFC (em inglês, Near Field Communication) é, tal como o Wi-Fi e o Bluetooth, uma tecnologia de comunicação sem fios que permite a comunicação entre dois dispositivos, sem necessidade de qualquer ação para além da aproximação dos mesmos.

A identificação por 2 fatores é uma tecnologia que permite que a identificação de um utilizador seja efetuada através de duas componentes. Sucintamente, adiciona ao fator do método usual de autenticação um outro, e apenas a correta combinação de ambos garante que a autenticação será efetuada com sucesso. Embora esse fator adicional possa ser obtido de várias formas, uma das mais utilizadas é a resultante da aplicação do algoritmo TOTP (em inglês, Time-based One-time Password Algorithm), que a partir de um valor alfanumérico e um *timestamp* gera um valor numérico de 6 dígitos denominado **token**.

Por fim, outra tecnologia tida como referência, e na qual este projeto se caracteriza como um **use case** da mesma, é a Web NFC API da W3C, que consiste num conjunto de especificações que permitem desenvolver através de uma linguagem de desenvolvimento web (*Javascript*), sites capazes de emitir e rececionar dados transmitidos por NFC, desde que, o dispositivo anfitrião do browser desses mesmos sites possua essa mesma tecnologia de comunicação.

Nota: Foi tentado que todos os conceitos descritos no relatório fossem minimamente explicados.

As palavras a itálico são conceitos cuja sua descrição pode ser encontrada no capítulo 12 deste mesmo relatório.

3 Abstract

The objective of this project is to create a solution that allows authentication to web sites to become a safer and more convenient process for the user.

To this end, a method was devised in which the authentication is performed using the API W3C Web NFC together with the factors of 2 identification technology.

In order to demonstrate the functioning of the concept, it built a prototype of a NFC receiver to serve as the interface between the device where a authentication form and a NFC transmitter is displayed. This interface has resulted in the development of a web portal that dispose the second identification factors such as authentication, and a mobile application generating tokens, which serve to authenticate the user in said portal through built prototype.

In order to elucidate the reader about the concepts involved in the project, they will be briefly explained below.

NFC (in English, Near Field Communication) is such as Wi-Fi and Bluetooth, a wireless communications technology that allows communication between two devices without the need for any action beyond the approach of the same.

Identification by two factors is a technology that allows identifying a user is performed by two components. Briefly, adds to the usual method of factor authentication one another, and just the right combination of both ensures that authentication is successfully performed. While this additional factor can be obtained in several ways, the most widely used is that resulting from the application of TOTP algorithm (in English, time-based one-time password Algorithm), which from an alphanumeric value and a *timestamp* generates a value 6-digit number called **token**.

Finally, another technology taken as a reference, and in which this design is characterized as a **use case** of the same is the web NFC API W3C, which is a set of specifications that allow the development via a web development language (*JavaScript*), sites capable of sending and receive data transmitted by NFC, since the host device browser of those sites have the same communication technology.

Note: We tried all the concepts described in the report were minimally explained.

The words in italics are concepts which your description can be found in Chapter 12 of this same report.

4 Introdução

A atual demanda por tecnologia que possa ajudar tem vindo a assumir um crescimento exponencial. Desde sensores biométricos, ao uso de protocolos de segurança específicos, e a outra tecnologia de vanguarda, o número de soluções é incontável.

No entanto, muita dessa tecnologia está disponível apenas a troco de valores monetários elevados, o que a torna pouco acessível ao utilizador comum.

Existem no entanto várias alternativas que podem adicionar segurança no acesso a dados de utilizadores. Este projeto apresenta um conceito que é de fácil implementação, e poderia agilizar, acelerar e aumentar a segurança num comum processo de autenticação web.

O processo é trivial. Munido com um smartphone, uma aplicação específica e um adaptador NFC, o utilizador poderá ter essa mesma segurança na sua navegação habitual pela web sem grandes custos nem complexidade.

De seguida será explicado o desenvolvimento e aplicação deste mesmo processo.

5 Ferramentas

Para a realização deste projeto, foi necessário empregar, simultaneamente, soluções de software e de hardware.

Relativamente à vertente de software, a linguagem de programação utilizada foi, maioritariamente **Java** (versão 8.0.60), para o desenvolvimento da aplicação móvel e do portal web, sendo que neste foi escolhido, **JavaServer Pages** para a criação do frontend, **MariaDB** como solução de armazenamento e **Apache Tomcat** como servidor aplicacional.

De referir que a aplicação móvel é um *fork* da aplicação **Google Authenticator** e, de forma a afastar a possibilidade de ambiguidade em relação ao nome, a aplicação móvel desenvolvida no escopo deste projeto, será referida como **Forked_Authenticator**.

A linguagem de programação **C** foi também usada no projeto, mais especificamente, na programação do microcontrolador do protótipo de recetor NFC.

Na vertente de hardware, para a construção de um protótipo de recetor NFC, foi utilizado um Arduino Uno e um módulo NFC.



Arduino Uno



Module NFC PN532



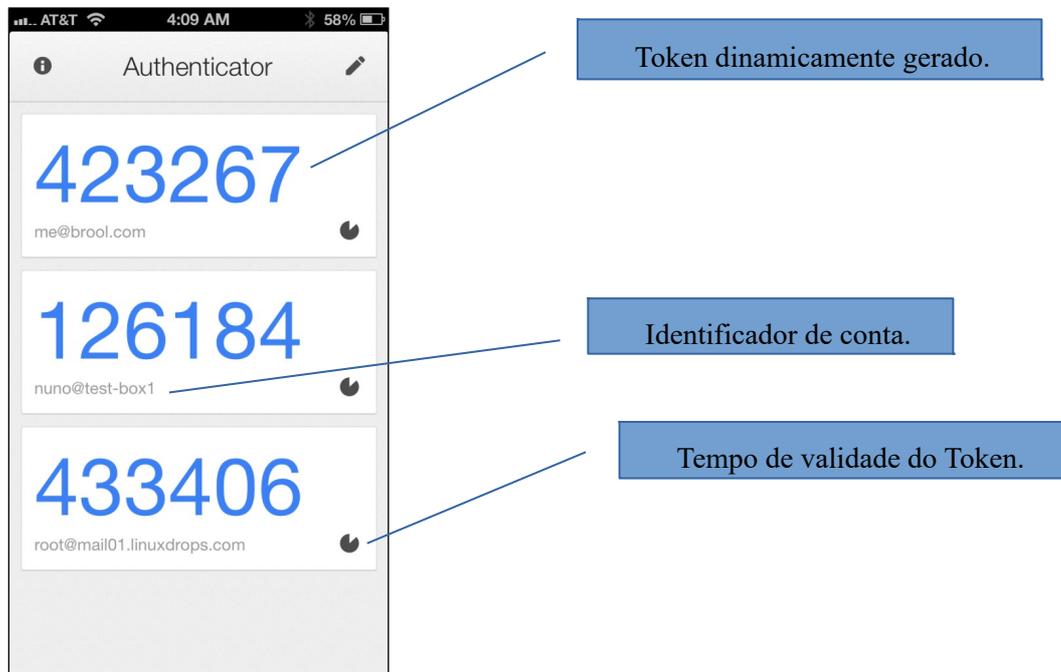
NFC key tag

- **Arduino Uno:** Plataforma de código-aberto para o desenvolvimento de projetos de eletrónica. Consiste numa placa com um circuito programável, complementado com um *IDE*, permitindo desenvolver soluções com relativa facilidade e rapidez;
- **Módulo NFC PN532:** Apesar da grande utilidade do Arduino Uno, o mesmo não possui nenhum interface NFC, sendo necessário recorrer a hardware extra, de forma a colmatar esse handicap. Este módulo adiciona ao Arduino a capacidade de processar informação transmitida por dispositivos NFC;
- **NFC key tag:** Chip emissor NFC que contém uma “mensagem” (token). Apesar do formato acima ser o de porta-chaves, podem assumir múltiplas formas tais como, cartões, adesivos, entre outros;

De forma a realizar testes durante o desenvolvimento, foi necessário um chip emissor NFC que pudesse interagir com o protótipo, e transmitir os seus dados para o portal web.

Forked_Authenticator

Existe atualmente disponível, no Google Play, uma aplicação de nome Google Authenticator (<https://github.com/google/google-authenticator-android.git>), cuja função é disponibilizar ao utilizador, os tokens necessários para aceder às suas diferentes contas.



Na aplicação original do Google, o utilizador ao configurar uma nova conta, tem a hipótese de escolher entre duas formas de gerar tokens, por contador incremental (algoritmo HOTP), ou por *timestamp* (algoritmo TOTP). Este projeto contempla exclusivamente apenas a segunda opção.

O que distingue a aplicação Forked_Authenticator da aplicação original do Google, é o facto de a primeira poder emitir por NFC o token gerado para um qualquer recetor com essa mesma tecnologia.

Para o projeto é útil pois desta forma, o token será transmitido para o formulário de login no browser do dispositivo onde o utilizador está a efetuar a autenticação.

A adição do suporte NFC na aplicação Forked_Authenticator foi possível graças à API NFC disponibilizada pelo Google no desenvolvimento de soluções em linguagem Java para o sistema operativo Android.

Código fonte disponível em <https://gitlab.com/ulht/authenticator.git>

Portal web

O portal web é simplesmente um pequeno website, o qual foi desenvolvido para se puder demonstrar o conceito a funcionar. Permite que um utilizador se registe e efetue logins através da identificação por 2 fatores em conjunto com a tecnologia NFC do seu dispositivo onde a aplicação Forked_Authenticator está instalada.

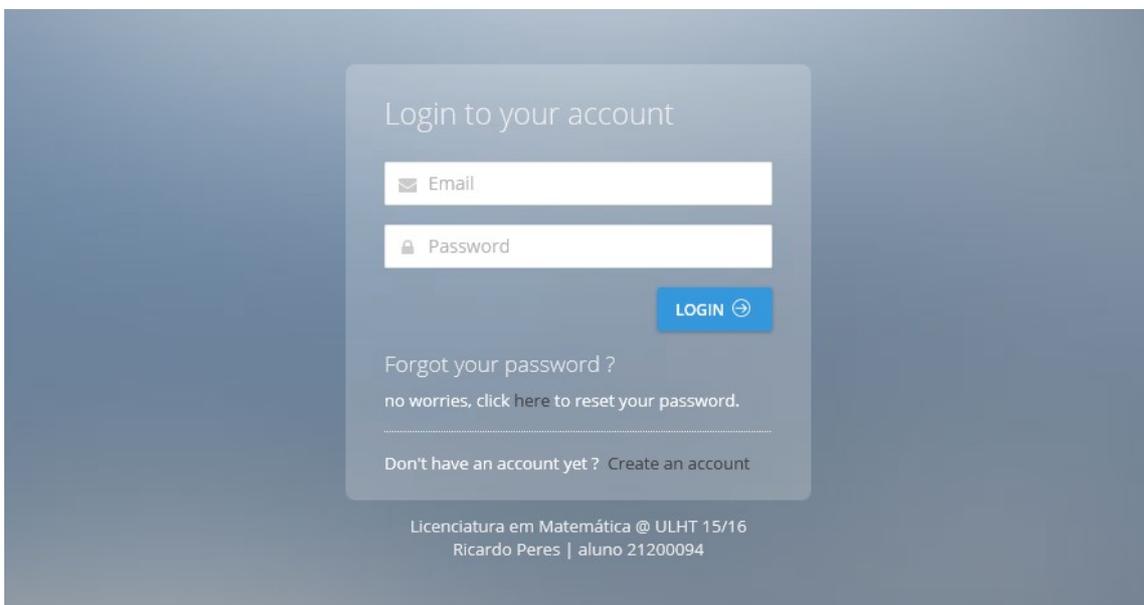
Código fonte disponível em <https://gitlab.com/ulht/portal.git>

7 Funcionamento

Para exemplificar o funcionamento, considere-se um utilizador que acede pela primeira vez ao portal web e decide adicionar ao seu registo e aos seus posteriores logins, a identificação por 2 fatores.

Registo

O utilizador acede, via browser, ao portal através do endereço http://123.456.789.101/web_portal onde lhe será apresentada a seguinte página web:



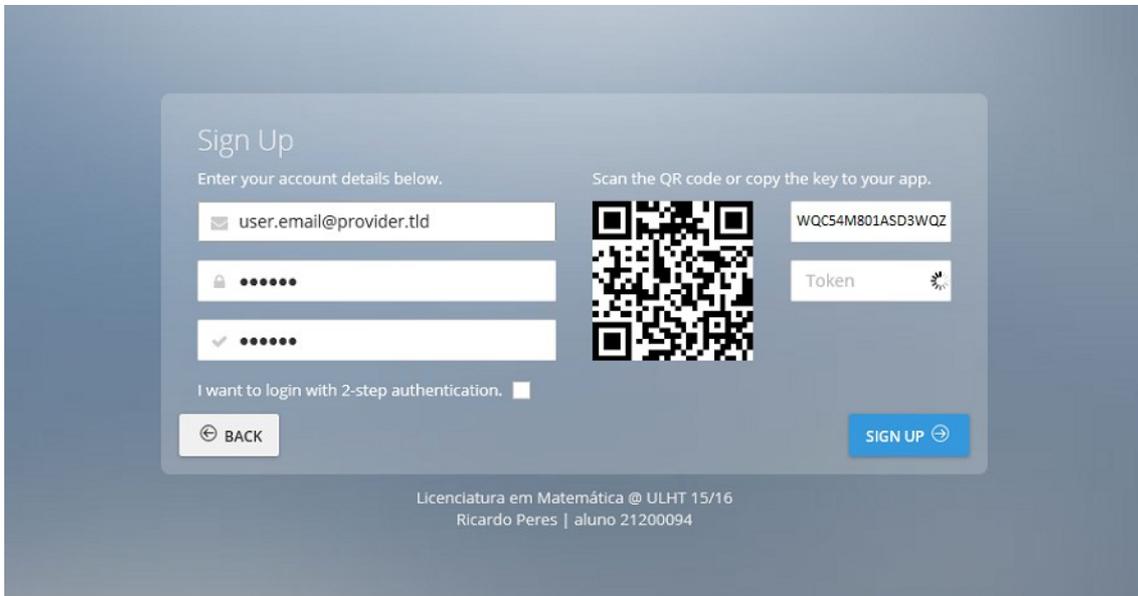
De seguida, irá escolher a opção **Create an account**, e seleciona a checkbox **I want to login with 2-step authentication**.



Deverão ser preenchidos os campos, **Email**, **Password**, e a confirmação da mesma.

O utilizador poderá verificar que, ao preencher o campo **Email**, é dinamicamente gerado um valor alfanumérico de 16 dígitos no campo superior direito do formulário, e simultaneamente, o código QR sofrerá alterações até o utilizador finalizar o preenchimento do campo **Email**.

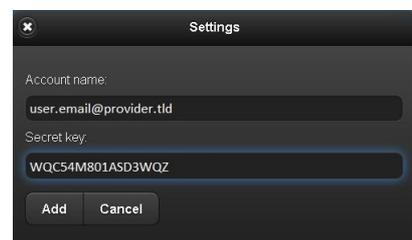
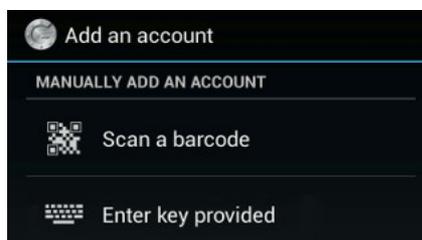
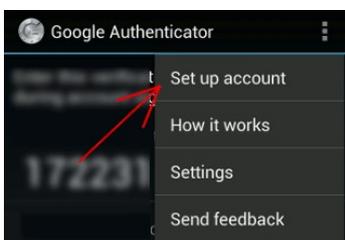
Após isso, o utilizador terá de configurar uma nova conta na aplicação Forked_Authenticator.



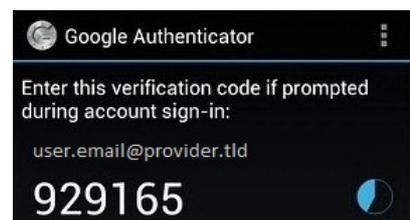
Para tal, poderá proceder de duas formas: introduzir manualmente na aplicação o valor alfanumérico gerado ou alternativamente, com uma aplicação de scan, focar o código QR obtido, o que automaticamente solicitará à aplicação Forked_Authenticator a criação de uma nova entidade. Independentemente da forma escolhida, a aplicação Forked_Authenticator é notificada de uma nova entidade e é iniciada a geração de tokens de autenticação para a conta em causa.

Para finalizar o processo de registo com a identificação por 2 fatores, basta introduzir no campo **Token** do formulário no portal web, o valor do token gerado na aplicação Forked_Authenticator.

A seqüência abaixo demonstra a configuração necessária.



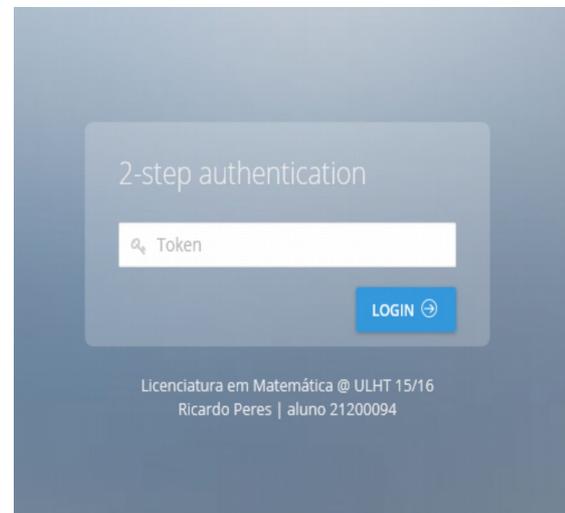
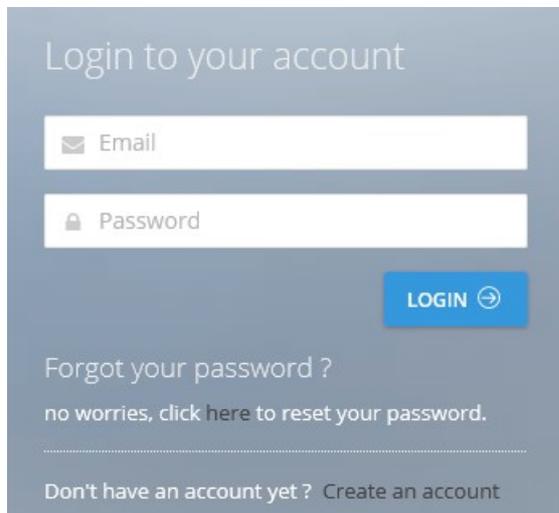
O utilizador está assim, pronto para efetuar o seu login no portal web.



Login

Após o registo com sucesso no portal web, o utilizador está apto a efetuar o login no mesmo.

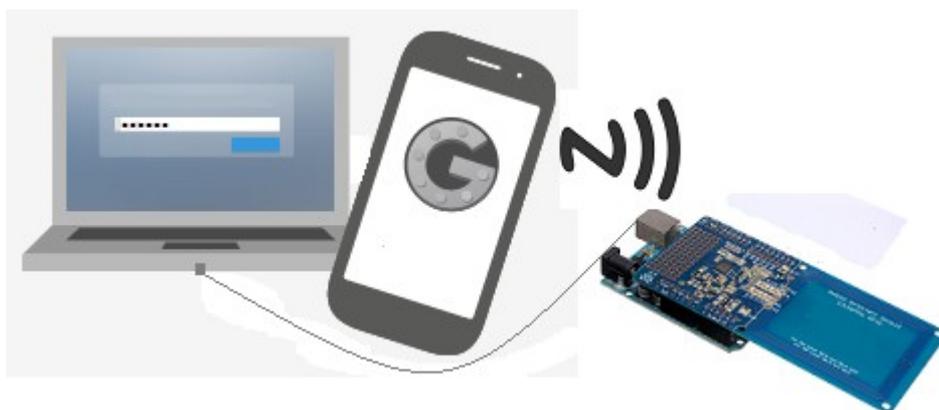
Irá inicialmente, introduzir o email e password, e após a confirmação dos mesmos, ser-lhe-á pedido um código de 6 dígitos de modo a finalizar a autenticação.



Código que está a ser gerado dinamicamente na aplicação Forked_Authenticator do utilizador.

Presentemente, o utilizador consulta a sua aplicação geradora de tokens, e simultaneamente, introduz o mesmo no formulário do portal.

Sendo a comodidade um objetivo desta prova de conceito, a mesma pode ser bem identificada neste passo, no qual, o utilizador deixa de ter necessariamente de aceder à aplicação Forked_Authenticator para consultar o token gerado. Ao invés de isso, o token será introduzido no respetivo campo do portal web por NFC, necessitando apenas de, aproximar o dispositivo NFC.



O utilizador finaliza assim, o seu processo de autenticação através da identificação por 2 fatores, e tem acesso ao seu espaço de utilizador no portal.

8 Resultados

Em termos de rapidez, a solução apresentada consome significativamente menos tempo que a usual, na qual o token de autenticação tem de ser introduzido manualmente. Após uma série de simulações, observa-se uma redução de 22 segundos no tempo médio de autenticação.

Outro resultado, o qual já previsível foi, de o token de autenticação necessário para um login com sucesso, nunca ser revelado visualmente pelos dispositivos intervenientes durante todo o processo.

9 Discussão e Conclusões

Os resultados obtidos após a conclusão do projeto, revelam que a solução apresentada é uma opção viável para ser implementada como uma medida adicional de segurança e comodidade num processo de autenticação.

Dos benefícios inicialmente indicados como principal razão para adoção deste conceito, a questão da segurança veio-se a revelar crucial, dado que, o facto de durante todo o processo de autenticação, o token não ser revelado visualmente, diminui as hipóteses de roubo do mesmo.

Um outro benefício, é a comodidade que adiciona ao processo de autenticação com identificação por 2 fatores, dado que liberta o utilizador de vários passos atualmente necessários. Remove a possibilidade de má introdução do token no formulário de login por parte do utilizador, isto é, exclui o inevitável erro humano, e remove também a possibilidade de má introdução por lentidão no tempo de inserção do token no formulário.

10 Pontos Negativos

Como referido anteriormente, o objetivo inicial do projeto foi cumprido.

No entanto, o produto final é unicamente um protótipo, como tal, ao ponto de vista estético não foi dada relevância, sendo que por isso, seria um ponto a melhorar, de forma a ser uma solução apelativa ao utilizador comum.

Uma questão também importante de referir, é o facto de a tecnologia NFC não estar a ter a receção esperada como inicialmente previsto. Presentemente, os dispositivos que incluem nativamente tecnologia NFC, são na sua maioria, caros. Uma alternativa a esses mesmos dispositivos, é o uso de pequenos objetos (por ex.: porta-chaves, cartões, adesivos, entre outros) contendo chips, como emissores NFC. No entanto nestes mesmos objetos, a geração de tokens é muito menos dinâmica, pois obriga a uma reprogramação do chip de cada vez que se pretenda alterar o token.

Por fim, a tecnologia de identificação por 2 fatores, é usada apenas por uma minoria dos utilizadores, e ainda menos são, os portais web que a disponibilizam como medida adicional à autenticação, seja por desconhecimento da existência da mesma, ou por pouca comodidade na sua implementação.

A realidade é que atualmente, a segurança embora sendo um assunto de alta importância, ainda poucos lhe dão o devido valor. Dito isto, a adoção deste conceito, apesar de tecnologicamente possível, tem obstáculos que provavelmente a dificultarão num futuro próximo.

11 Bibliografia

- Site oficial da Web NFC API: <https://w3c.github.io/web-nfc>
- Site oficial da comunidade Web NFC: <https://www.w3.org/community/web-nfc>
- Site oficial do Arduino: <https://www.arduino.cc>
- Site da Mozilla sobre a Web API NFC:
https://developer.mozilla.org/en-US/docs/Web/API/NFC_API

12 Glossário

- **timestamp** – cadeia de caracteres que especifica a hora e/ou data de um certo evento.
- **Javascript** – linguagem de programação interpretada, usada maioritariamente no desenvolvimento web, para interação no lado do cliente.
- **JavaServer Pages** – tecnologia de desenvolvimento de conteúdos web dinamicamente gerados. A sua popularidade deve-se ao facto do suporte que tem para trabalhar sobre Servlets (classes Java).
- **MariaDB** – base de dados relacional. É um fork (ver abaixo) da base de dados MySQL.
- **fork** – desenvolvimento de um projeto com base em código fonte de um projeto já existente.
- **IDE** – em inglês, “Integrated Development Environment”, é um software que aumenta a produtividade na criação de aplicações, reunindo num pacote as ferramentas necessárias para o rápido desenvolvimento de programas escritos em uma ou várias linguagens de programação.