**UNIVERSIDADE FEDERAL DE SANTA CATARINA**
**INFORMÁTICA E ESTATÍSTICA**

Dayana Pierina Brustolin Spagnuelo

# PROTOCOLO FLEXÍVEL DE AUTENTICAÇÃO MULTI-FATOR: ESTUDO DE CASO PARA AMBIENTES DE TELEMEDICINA

Florianópolis(SC)

2013

Dayana Pierina Brustolin Spagnuelo

# PROTOCOLO FLEXÍVEL DE AUTENTICAÇÃO MULTI-FATOR: ESTUDO DE CASO PARA AMBIENTES DE TELEMEDICINA

Dissertação submetida ao Programa de Pós-Graduação em Ciências da Computação para a obtenção do Grau de mestre em Ciência da Computação.
Orientador: Prof. Ricardo Felipe Custódio, Dr.
Coorientador: Prof. Jean Everson Martina, Dr.

Florianópolis(SC)

2013

Catalogação na fonte elaborada pela biblioteca da
Universidade Federal de Santa Catarina

A ficha catalográfica é confeccionada pela Biblioteca Central.

Tamanho: 7cm x 12 cm

Fonte: Times New Roman 9,5

Maiores informações em:
http://www.bu.ufsc.br/design/Catalogacao.html

Dayana Pierina Brustolin Spagnuelo

**PROTOCOLO FLEXÍVEL DE AUTENTICAÇÃO MULTI-FATOR: ESTUDO DE CASO PARA AMBIENTES DE TELEMEDICINA**

Esta Dissertação foi julgada aprovada para a obtenção do Título de "mestre em Ciência da Computação", e aprovada em sua forma final pelo Programa de Pós-Graduação em Ciências da Computação.

Florianópolis(SC), 03 de Outubro 2013.

---

Prof. Ronaldo dos Santos Mello, Dr.
Coordenador

---

Prof. Ricardo Felipe Custódio, Dr.
Orientador

---

Prof. Jean Everson Martina, Dr.
Coorientador

**Banca Examinadora:**

---

Prof. Ricardo Felipe Custódio, Dr.
Presidente

---

Prof. Célio Vinicius Neves de Albuquerque, Dr.

Prof. Aldo von Wangenheim, Dr. rer.nat

Prof. Eros Comunello, Dr. rer.nat

Dedico este trabalho à minha mãe, Iraci, e em memória ao meu pai, Benitto.

## AGRADECIMENTOS

Gostaria de agradecer a todos aqueles que me ajudaram nesta etapa da minha vida. Porém seria impossível citar todos que, pouco ou bastante, contribuíram na finalização deste trabalho. Entretanto, algumas pessoas merecem ser citadas de forma a eternizar minha gratidão.

Primeiramente, gostaria de agradecer ao meu companheiro de todas as horas, Cezar Signori. Sem sua presença em minha vida seria impossível finalizar mais esta etapa. Ele esteve presente em todos os meus momentos baixos e de desânimo, sempre me ajudando a encontrar a solução para qualquer que fosse meu problema. Também esteve presente nos momentos altos e de alegria, contribuindo em cada pequena vitória durante o percurso. Ao Cezar Signori, agradeço por sua fundamental contribuição, e espero que a vida nos dê a oportunidade de compartilhar muitos outros momentos.

Gostaria também de agradecer a minha família por ter acreditado em mim e me apoiado sempre. Em especial, dedico esta dissertação em memória ao meu pai, Benitto, que me ensinou como ser uma pessoa melhor, mas infelizmente não pode estar presente para me ver alcançando mais esta conquista. Dedico também à minha mãe, Iraci, por ter superado os momentos difíceis de nossas vidas e ter atuado como pai e mãe nos últimos anos. Sem vocês eu não teria conseguido! Não esquecendo de citar a minha mais nova irmã Diane, que me ajudou a descansar nos finais de semana de comilança.

Não poderia deixar de agradecer aos colegas Thaís Idalino e Rafael Moser. Sem dúvidas, vocês contribuiram bastante com este trabalho, mas contribuiram ainda mais na minha formação como pessoa e pesquisadora. Agradeço também a Lucila Alosilla por sua enorme paciência e por estar sempre me auxiliando ao longo destes dois anos.

Por fim, agradeço ao meu Orientador Ricardo Custódio e Coorientador Jean Martina. Ambos me ajudaram a aperfeiçoar meu trabalho e me guiaram durante minha jornada acadêmica. Além do mais, abriram diversas oportunidades para mim dentro e fora do Laboratório de Segurança da Computação (LabSEC).

Todos vocês atuaram de forma essencial durante os últimos dois anos da minha vida, e por isso sou grata. Manterei guardadas em minha memória ótimas lembranças de meu mestrado.

*Isso de ser exatamente o que se é ainda vai nos levar além.*

Paulo Leminski

## RESUMO

Sistemas de telemedicina e telessaúde necessitam de serviços de autenticação fortes para garantir a identidade e a privacidade dos dados e, ao mesmo tempo, flexíveis para atender as necessidade de profissionais e pacientes. O foco deste trabalho é o processo de autenticação. Nós propomos um protocolo de autenticação multifator flexível e uma implementação do mesmo baseada em tecnologias de *web services* voltado ao ambiente de telessaúde. Este serviço faz uso de métodos escaláveis em um processo de autenticação de dois fatores. No novo modelo o usuário se autentica da mesma forma que fazia anteriormente e, em um segundo passo, informa algum dado que prove que ele tem a posse de determinado dispositivo único (token). Suas principais características são a flexibilidade de configuração dos mecanismos de autenticação, assim como o uso de um sistema robusto para o registro de eventos. Neste trabalho são tratados a engenharia de requisitos de segurança, e os detalhes da sua implementação. Também são discutidos sua adequação no ambiente de telemedicina e telssaúde e a integração do uso de diferentes métodos de autenticação.


**Palavras-chave:** Autenticação Multi-fator; Sistemas de Telemedicina; Sistemas de Telessaúde

## ABSTRACT

Telemedicine and telehealth systems require authentication services that are strong enough to ensure identification and privacy, and flexible to meet the needs of health professionals and patients. The focus of this work is the authentication process. We propose a multi-factor authentication protocol and an implementation based on web service technology for telemedicine environment. This service makes use of scalable authentication methods based on two-factor authentication mechanisms. In the new model users authenticate exactly the same way they use to do and, in a second step, they have to provide some information that proves that they possess some specific device (token). Its main characteristics are: flexibility of configuration for the authentication mechanisms, as well as the use of a robust system for recording events. In this dissertation we deal with the engineering requirements of the security system and the details of its implementation. We also discuss the efficacy and ease of use of different authentication methods.


**Keywords:** Multi-factor Authentication; Telemedicine Systems; Telehealth Systems

## LISTA DE FIGURAS

**SUMÁRIO**

# 1 INTRODUÇÃO

O crescente desenvolvimento da tecnologia da informação potencializou a utilização de meios eletrônicos para comunicação e prestação de serviços. E, neste âmbito, ambientes telemáticos ganham bastante destaque por apresentarem soluções viáveis para diversos tipos de problemas, incluindo os sociais. Similarmente, ambientes de telemedicina e telessaúde facilitam o acesso a serviços de saúde para pessoas que não poderiam tê-los da forma convencional, bem como simplificam o uso de tecnologia por profissionais da saúde (MARTÍNEZ et al., 2007).

Estes tipos de sistemas passaram a permitir a medicina à distância, tornando possível um paciente realizar seus exames na sua cidade e consultar especialistas geograficamente distantes. Desta forma, as situações existentes na medicina presencial se traduzem na medicina à distância através de um sistema de telemedicia e telessaúde.

No entanto, este crescimento não trouxe somente benefícios, ele também expôs a fragilidade que estes sistemas possuem em relação à segurança da informação. O processo de autenticação, por exemplo, pode ser responsável por diversos tipos de vulnerabilidades e até permitir o mal uso de credenciais se não for devidamente aplicado. Hoje em dia ainda vemos um cenário onde a maioria dos sistemas é baseado no modelo de autenticação baseado em usuário e senha simples. Este modelo, no entanto, não é considerado adequado em várias situações práticas, como por exemplo, em aplicações de telemedicina e telessaúde, por conta das fragilidades que possui.

Uma das principais fragilidades deste modelo é a possibilidade de personificação, que pode se dar por adivinhação ou cópia das credenciais de um usuário em determinado sistema. Sendo a segunda de mais fácil realização. Este tipo de ataque é bastante comum uma vez que os usuários normalmente não estão cientes das ameaças existentes, e acabam agindo de forma inadequada com relação às suas senhas. Muitos deles acabam anotando ou reutilizando suas senhas, por exemplo. Além do mais, considerando os avanços tecnológicos e a capacidade dos invasores crescendo cada vez mais, esta técnica tende a enfraquecer a segurança do sistema como um todo.

Este tipo de ameaça aumenta suas proporções se as informações contidas no sistema são sensíveis. Ou seja, informações que possuem grande importância em seu contexto e, normalmente, causam problemas quando divulgadas. Em sistemas de telessaúde, pela peculiaridade das informações gerenciadas, o roubo de identidade pode causar não somente o vazamento de informações privadas, mas diversas outras situações que não atendem ao interesse da relação médico/paciente. Desta forma o uso de um modelo de

autenticação mais seguro, com métodos mais fortes, torna-se impescindível para aumentar a segurança neste tipo de sistema. Uma importante característica a ser levada em consideração é que estes métodos devem interferir o mínimo possível na forma com que os usuários acessam ao sistema. Esta característica é importante pois diminui as chances de rejeição do modelo por parte dos usuários.

Por outro lado, métodos de autenticação considerados mais fortes requerem o uso de dispositivos criptográficos. Estes dispositivos, por sua vez, contém módulos de leitura que permitem sua utilização. Este tipo de módulo de leitura normalmente possuem baixa interoperabilidade. Ou seja, interferem diretamente na mobilidade e usabilidade dos sistemas que os utilizam. Dentro do ambiente de telemedicina ainda existe outro problema: um médico deve ser capaz de acessar o sistema de apoio a medicina à distância de qualquer lugar e a qualquer horário, pois qualquer impedimento pode significar risco à vida. Dessa forma, o modelo de autenticação deve ser forte o suficiente para garantir a segurança, mas não deve depender de processos que prejudicam a mobilidade e a usabilidade.

Neste trabalho propõe-se uma nova forma de autenticação flexível baseada em multiplos fatores que funciona como um *web service*. Embora o modelo permita a utilização de quantos métodos se desejar, acredita-se que apenas dois fatores sejam suficientes para aumentar a segurança do processo. Mais fatores podem tornar o processo de autenticação desnecessariamente complexo. Dessa forma, em nosso trabalho propõe-se que seja utilizado um segundo fator de autenticação, além do já existente (login e senha). Outra característica do modelo é a flexibilidade, que permite que usuários se autentiquem mesmo quando não estão de posse de algum dispositivo necessário.

O modelo proposto foi projetado baseado nas reais necessidades do Sistema Integrado de Telemedicina e Telessaúde de Santa Catarina (STT/SC), um projeto da Universidade Federal de Santa Catarina (UFSC) em parceria com a Secretaria do Estado de Saúde de Santa Catarina (SES/SC). Ao longo deste trabalho percebeu-se que as necessidades de usuários desse tipo de sistema são bastante distintas dos convencionais. Procurou-se portanto, uma solução de autenticação diferenciada baseada na posse de dispositivos comuns, como *smartphones*, telefones celulares, ou ainda telefonia fixa. O serviço *web* proposto atua na camada de autenticação do sistema de telessaúde, integrando diversos métodos de autenticação de segundo fator.

## 1.1 OBJETIVOS

O processo de acesso à sistemas computacionais se subdivide em: identificação, autenticação, autorização e registro de atividades. Neste trabalho, somente a etapa de autenticação é abordada. Os objetivos detalhados deste trabalho podem ser vistos nas subseções que seguem.

### 1.1.1 Objetivo Geral

Este trabalho tem por objetivo compreender melhor as necessidades reais do Sistema Integrado de Telemedicina e Telessaúde de Santa Catarina (STT/SC) e, a partir disso propor melhorias no processo de autenticação dos usuários através do projeto e do desenvolvimento de um novo modelo de autenticação. Este novo modelo deve respeitar a mobilidade dos seus usuários e a usabilidade do STT/SC.

### 1.1.2 Objetivos específicos

Os objetivos específicos deste trabalho são:

- Realizar uma revisão sistemática sobre modelos de autenticação utilizados em ambientes de telemedicina;
- Estudar a interação dos usuários com o STT/SC a fim de generalizar os principais casos;
- Projetar e desenvolver um gerador de senhas seguras a partir de um smartphone;
- Prover suporte para o envio de senhas de uso único através de mensagens de celular (SMS);
- Prover suporte para o mecanismo de reconhecimento de chamadas telefônicas;
- Projetar e desenvolver uma camada que gerencie mais de um método de autenticação;
- Realizar a integração da nova camada ao STT/SC;
- Avaliar a eficiência e o nível de segurança provido pela nova proposta.

## 1.2 LIMITAÇÕES DO TRABALHO

Estre trabalho propõe uma melhoria no processo de autenticação de usuários do Sistema Integrado de Telemedicina e Telessaúde de Santa Catarina, não tendo relação alguma com o processo de autorização. O processo de autorização é responsável por verificar se determinado usuário é autorizado a realizar determinada tarefa. Entende-se que a autorização é tratada pelo STT/SC. Da mesma forma, este trabalho propõe alternativas que visam diminuir as chances de sucesso de ataques como o roubo de identidade.

## 1.3 JUSTIFICATIVA

Atualmente, métodos de autenticação de usuários baseados em *login* e senha não são mais considerados adqueados para algumas aplicações. Um dos fatores que o torna inadequado é a facilidade com que se consegue copiar este tipo de senhas. A espionagem é uma das formas mais comuns de se obter a senha de um usuário. Esta técnica pode ser tão simples quanto observar uma pessoa digitando sua senha, ou complexas como implantar escutas em algum ponto entre o usuário e o sistema.

O levantamento feito por Silva (SILVA, 2007) ajuda a entender a fragilidade do modelo *login*/senha. O estudo teve por objetivo identificar os principais fatores que comprometem a memorização de senhas. Os resultados obtidos indicaram que, independente da idade e da escolaridade dos usuários, a quantidade de senhas é o fator que mais influencia no desempenho da memorização destas. Desta forma, os usuários tendem a dar preferência à escolha de senhas curtas. Ainda, quando da necessidade do uso de senhas longas e fortes, usuários tendem a usar a mesma senha em diversos sistemas. A associação de datas e números de telefone também constitui uma prática comum adotada pelos usuários no momento da definição de suas senhas. Todas estas práticas acabam facilitando os ataques.

Em se tratando do processo de autenticação de usuários como um todo, é possível diminuir esta fraqueza reduzindo a dependência da memória humana no processo. Por exemplo, utilizando dispositivos físicos ou até mesmo uma combinação destes com senhas memorizadas. Atualmente são conhecidos diversas formas de autenticar um usuário que podem ser combinadas entre si para prover maior confiabilidade ao sistema, porém, acredita-se que a combinação de muitas delas possam tornar o processo de autenticação demasiadamente trabalhoso.

Este trabalho é motivado pela hipótese de que é possível aumentar a segurança de um processo de autenticação e implementar autenticação de

dois ou mais fatores sem impedir ou atrapalhar o trabalho de um usuário em situações médicas emergenciais. Dessa forma, acredita-se que é possível permitir vários *tokens* de autenticação de tipos diferentes para um único usuário. Tornando o sistema inteligente o suficiente para permitir a autenticação de usuários da melhor forma possível. Ou seja, uma autenticação forte, mas simples. Da mesma forma, acredita-se que é possível que um usuário altere o modo de uma autenticação caso esteja impossibilitado de autenticar-se com o modo solicitado, sem impactar na segurança do processo.

Acredita-se também que é possível utilizar como *tokens* de autenticação dispositivos mais comuns, como *smartphones* ou *tablets*. Pois, além dos usuários já estarem habituados a utilizá-los, sua popularidade vem aumentando cada vez mais. Desta forma, se faz necessário dirigir um estudo cuidadoso acerca da melhor forma de combinação métodos de autenticação e quais métodos podem ser utilizados sem atrapalhar a interação dos usuários.

## 1.4 METODOLOGIA

Este trabalho inicia com a realização de uma revisão sistemática sobre modelos de autenticação utilizados em ambientes de telemedicina e telessaúde com objetivo de identificar o cenário atual, suas principais limitações e dificuldades. Além disto, visa-se também a descoberta de novos modelos de autenticação baseados em 2 fatores utilizando dispositivos móveis. A fim de identificar o problema comum existente nestes ambientes, é conduzida uma série de entrevistas com a equipe mantenedora do STT/SC, da qual é traçado um comparativo entre as necessidades locais e as necessidades apontadas nos trabalhos correlatos.

A partir da identificação do problema é proposto um novo modelo de autenticação que atenda principalmente as demandas locais do STT/SC, mas também as demandas comuns a outros sistemas de telemedicina e telessaúde. Uma vez definido o modelo, inicia-se a fase de projeto e desenvolvimento do protótipo deste novo modelo. Testes de validação quanto a confiabilidade do novo modelo e eficiência do processo de autenticação são realizados a partir do protótipo.

Com os resultados dos testes de validação inica-se a fase de desenvolvimento da versão final do novo modelo. A partir da versão final é realizada a integração no STT/SC e os testes de segurança e pesquisas de usabilidade para comprovação das hipóteses do trabalho.

## 1.5 CONTRIBUIÇÕES CIENTÍFICAS

Parte dos resultados deste trabalho foram publicados em artigo no *Fifth International Conference on eHealth Telemedicine, and Social Medicine (eTELEMED)*, realizado em Nice - França, nos dias 24 de fevereiro a 01 de março de 2013, com o título "*Multi-Factor Authentication in Telemedicine Systems*"(SPAGNUELO et al., 2013).

Parte da análise dos métodos de autenticação deste trabalho fizeram parte do trabalho "Um Levantamento de Métodos para Autenticação com Múltiplos Fatores"dentro do Programa de Gestão de Identidades (PGId) 2012 da Rede Nacional de Ensino e Pesquisa (RNP). O trabalho foi apresentado no *Workshop* de Gestão de Identidade, realizado em conjunto com o $12^o$ Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg).

Outra parte dos resultados deste projeto foram publicados no *Workshop* de Iniciação Científica, realizado em conjunto com o $12^o$ Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg), com o título "Senhas descartáveis em dispositivos móveis para ambientes de Telemedicina"(IDALINO; SPAGNUELO, 2012), tendo recebido menção honrosa.

## 1.6 ORGANIZAÇÃO DO TRABALHO

O restante deste trabalho está organizado da seguinte forma: uma breve discussão sobre métodos de autenticação de usuários é apresentada na Seção 2. A Seção 3 apresenta o STT/SC com detalhes sobre o seu modelo de autenticação, um levantamento dos trabalhos relacionados, e um estudo sobre diversas alternativas para se autenticar um usuário remotamente. Cada método é descrito de forma geral e avaliado em questões de segurança, custos de implementação e manutenção, e usabilidade. Na Seção 4 estão descritas as etapas de construção da proposta desde o levantamento de requisitos até a sua modelagem. Detalhes sobre a implementação do modelo proposto são apresentadas na Seção 5. A análise técnica dos métodos de autenticação do modelo proposto, bem como os resultados obtidos no teste com os usuários são apresentados na Seção 6. E, por fim, a Seção 7 contém as considerações finais do trabalho e sugestões de trabalhos futuros.

# 2 MÉTODOS DE AUTENTICAÇÃO

Este capítulo apresenta os conceitos básicos necessários para a compreensão deste trabalho. Inicialmente apresenta-se a definição de autenticação eletrônica, logo após as formas de um usuário apresentar suas credencias a um sistema computacional.

## 2.1 AUTENTICAÇÃO ELETRÔNICA

Autenticação eletrônica é o processo de estabelecer confiança em identidades apresentadas eletronicamente para sistemas de informação. O grande desafio em autenticações eletrônicas surge quando a autenticação é remota e o sistema precisa verificar a autenticidade da identidade apresentada por seus usuários através da internet.

No processo de autenticação eletrônica, cada usuário possui uma identidade eletrônica que lhes é atribuída dentro do sistema. Cada identidade é associada a credenciais únicas de autenticação, conhecidas somente pelo usário e que podem ser verificadas pelo sistema (BENANTAR, 2006). A forma de produzir e apresentar as credenciais a sistemas computacionais é chamada de fator.

### 2.1.1 Fatores de Autenticação

Dada a diversidade de sistemas de informação existentes, o projeto de um processo de autenticação pode ser bastante subjetivo. Sua eficácia não depende somente da sua segurança, mas também da aceitação por parte dos usuários, escalabilidade que suporte crescimento, interoperabilidade com futuros sistemas, etc. O processo de autenticação eletrônica pode ser realizado utilizando um fator ou vários deles em bloco, por exemplo.

Segundo o manual de autenticações para ambientes de *Internet Banking* do FFIEC (FFIEC, 2005), autenticações que dependem de mais de um fator são mais difíceis de se comprometer do que as que dependem de um único. Isto acontece porque logicamente é mais difícil fraudar ou roubar diversos *tokens* de autenticação do que um único. O sucesso deste tipo de processo de autenticação depende da prova de posse/conhecimento de todos os fatores exigidos.

De forma geral podemos definir fatores como sendo a informação utilizada para verificação da identidade de usuários em meios eletrônicos (MIL-

LER; VANDOME; MCBREWSTER, 2009). É praxe classificar os fatores em três categorias:

1. Algo que se sabe

   Nesta categoria a autenticação se dá através da apresentação ao sistema de algo que o usuário sabe e compartilha com o sistema. Quando se utiliza este fator, sistema e usuário compartilham um segredo conhecido somente pelos dois. Quando da autenticação, o usuário prova que conhece o segredo apresentando-o ao sistema. Nesta abordagem é necessário um compartilhamento do segredo prévio, que pode ser uma senha, uma frase ou até mesmo informações de cunho pessoal do próprio usuário.

2. Algo que se possui

   Nesta categoria a autenticação se dá através da prova de posse de determinado dispositivo físico, normalmente portátil. Este dispositivo é conhecido como *token*. Neste modelo, o usuário prova que tem a posse do dispositivo apresentando alguma informação que só seria possível obter através dele. *Tokens* podem ser tanto dispositivos comuns, como um celular ou *smartphone*, quanto dispositivos específicos, como *smart cards*.

3. Algo que se é

   Nesta categoria a autenticação se dá através da apresentação alguma característica única do usuário. O terceiro fator refere-se ao uso de características biológicas do usuário como prova da sua identidade. Nesta categoria pode-se utilizar características físicas do usuário, tais como impressões digitais, padrão de retina, imagem da face e voz.

Cada um dos fatores possuem vantagens e desvantagens, sendo bastante distintos um dos outros. Por exemplo, o primeiro fator pode ser facilmente implementado em sistemas computacionais, mas atualmente está bastante suscetível a ataques por cópia de senhas. Por outro lado, os fatores "Algo que se possui"e "Algo que se é"exigem o uso de dispositivos de leitura específicos e são mais difíceis de utilizar do que o modelo baseado em algo que o usuário sabe.

# 3 AUTENTICAÇÃO EM SISTEMAS DE TELESAÚDE

Este capítulo apresenta o Sistema Integrado de Telemedicina e Telessaúde de Santa Catarina (STT/SC), incluindo detalhes técnicos da implementação do seu modelo de autenticação de usuários. Apresenta também trabalhos correlacionados com objetivos similares aos deste trabalho.

## 3.1 SISTEMA INTEGRADO DE TELEMEDICINA E TELESSAÚDE

A telemedicina surgiu em meados dos anos 60 e, desde então, vem sido aplicada no auxílio a medicina a distância. Isto ocorre através da interconexão de regiões desprovidas de serviços de saúde qualificado com outras regiões com centros médicos mais desenvolvidos (MACEDO, 2008). De acordo com a *American Telemedicine Association* (ATA), Telemedicina pode ser definida como "o uso de informação médica veiculada de um local para outro, por meio de comunicação eletrônica, visando a saúde e educação dos pacientes e do profissional médico, para assim melhorar a assistência de saúde"(MACEDO, 2008).

De forma geral, no Brasil, ocorre uma centralização de profissionais da saúde em determinadas cidades, normalmente capitais. Mais especificamente em Santa Catarina, esta centralização ocorre nas cidades litorâneas. Devido a esta centralização, os pacientes de cidades do interior precisam ser transportados por meios terrestres ou aéreos, aumentando a demora e o custo do tratamento. Ainda por consequência da centralização ocorre a superlotação dos centros médicos, causando atraso no atendimento de pacientes (BARCELLOS, 2012).

No âmbito de soluções para este tipo de problemas de assistência de saúde podemos citar a Rede Catarinense de Telemedicia (RCTM) como um exemplo (CYCLOPS, 2010). A RCTM foi desenvolvida pela Universidade Federal de Santa Catarina (UFSC) em parceria com a Secretaria do Estado de Saúde de Santa Catarina (SES/SC), com objetivo de facilitar o acesso de exames médicos de média e alta complexidade em áreas menos desenvolvidas do estado.

O principal objetivo da RCTM era de estender a disponibilidade de equipamentos médicos tais como eletrocardiogramas, tomografia computadorizada e ressonância magnética para locais onde não existiam tais equipamentos. Esses equipamentos são caros, e exigem recursos humanos especializados para sua operação, normalmente não disponíveis em regiões distantes dos grandes centros urbanos. Um projeto piloto foi criado em 2005,

e começou interligando duas cidades do interior de Santa Catarina com a capital Florianópolis (WALLAUER et al., 2008). Desde 2005 até setembro de 2012, 293 novas cidades passaram a fazer parte do projeto, estando conectadas umas as outras através de um sistema baseado em *web* que oferece diagnósticos a distância de diversas modalidades. Além de oferecer também treinamento continuado para profissionais da saúde.

O Sistema Integrado de Telemedicina e Telessaúde de Santa Catarina (STT/SC) é um ambiente virtual de suporte a medicina, pertentencente à RCTM, que tem por objetivo facilitar o acesso a serviços de saúde específicos a pessoas que não podeiram tê-los da forma convencional. Os principais problemas que os usuários do STT/SC enfrentam são dificuldades de locomoção por conta de deficiências físicas, distância geográfica, e dificuldades financeiras (WANGENHEIM et al., 2012). O STT/SC disponibiliza, via web, imagens, sinais e laudos médicos gerados por instituições de saúde credenciadas distribuídas por todo o estado de Santa Catarina. Atualmente o sistema propicia uma média de 76.000 exames por mês e conta com mais de 3 milhões de exames e imagens armazenados desde 2005.

De forma geral pode-se descrever tecnicamente o STT/SC como um sistema *web* desenvolvido com a linguagem de programação PHP com auxílio do Framework Zend baseada na padrão de projeto *Model View Controller* (MVC), que utiliza diversos componentes da biblioteca Javascript Dojo e o banco de dados objeto relacional PostgreSQL.

O STT/SC conta com a colaboração de uma vasta equipe de profissionais de diversas áreas. Alguns deles são: médicos, dentistas, enfermeiros, técnicos da área de saúde, operadores de equipamentos médicos, administradores e técnicos de informática. Para autenticar estes profissionais, o STT/SC conta com um modelo de autenticação baseado em *login* e senha. Cada usuário do sistema recebe um identificador chamado *login* que é uma *string* única e exclusiva similar a uma credencial e que possui uma senha vinculada. A senha é também uma *string* e é conhecida somente pelo seu usuário. O sistema de autenticação funciona então como um desafio-resposta simples.

Para que ninguém além do usuário possa ter acesso a sua senha, nem mesmo os administradores ou desenvolvedores do portal, esta é guardada cifrada na base de dados. O algoritmo utilizado para cifrar a senha é o MD5 que é um algoritmo de resumo criptográfico unidirecional. Toda vez que um usuário tenta acessar o portal o mesmo fornece seu *login* e sua senha, o sistema aplica o algoritmo MD5 sobre a senha fornecida e então compara esta com a senha que encontra-se armazenada em sua base. O modelo assume que cada usuário possui uma senha e este é o único que a conhece, desta forma, se a comparação for efetivada então a resposta do desafio lançado pelo portal

está correta e a autenticação é efetuada.

Como o STT/SC é um sistema *web* quando um usuário tenta se autenticar seus dados (*login* e senha) são enviados pela rede. Como é possível observar o tráfego da rede e espiar o conteúdo que nela passa, se os dados para autenticação trafegassem em texto plano estariam vulneráveis a ataques. Para evitar que seja possível descobrir a senha de um usuário através deste tipo de ataque o STT/SC faz uso do protcolo SSL (do inglês *Secure Sockets Layer*). O protocolo SSL visa garantir a privacidade e a integridade dos dados autenticando as partes envolvidas na comunicação (neste caso cliente e servidor), e cifrando os dados transmitidos por estas, criando assim uma espécie de tunel seguro de dados.

## 3.2 TRABALHOS RELACIONADOS

Por se tratarem de sistemas que influenciam diretamente no andamento da sociedade, a segurança de sistemas de telessaúde tem ganhado a atenção de governos, provedores de saúde, centros de pesquisa e, por consequência, tem sido um assunto recorrente nas publicações de artigos científicos nos últimos anos.

O levantamento de artigos científicos relacionados foi realizado através de duas principais base de dados: *IEEEXplore* e *ACM Digital Library*. Em ambas as bases buscou-se pelas *strings* de busca "*health + authentication*", "*e-health + service + authentication*". Na primeira busca foram encontrados diversos trabalhos que foram selecionados a partir de seus títulos e resumo. O critério de exclusão adotado foi definido como qualquer artigo que não possuísse menção a melhorias no processo de autenticação tanto no título, quanto no resumo. Desta forma, os mais relevantes trabalhos foram selecionados. A partir desta seleção, uma avaliação mais criteriosa foi adotada, cada artigo foi lido por inteiro e somente os que não descreviam de forma detalhada as melhorias no processo de autenticação foram excluídos. A segunda parte do processo de seleção de artigos foi realizado através da busca pelas referências utilizadas nos trabalhos selecionados na primeira parte da busca, utilizando os mesmo critérios de exclusão. Ao todo, 6 principais trabalhos foram identificados. A fim de identificar trabalhos mais recentes, foram realizadas buscas em diversas plataformas sobre trabalhos relacionados com "*e-health system*", "*e-health service*", e "*telemedicine*" dos quais somente os que tinham menção a segurança da informação no título foram selecionados, e somente os que tinham menção ao processo de autenticação no resumo foram lidos por completo. Esta última busca resultou em outros 6 artigos, porém todos com pouca relevância pare o presente trabalho. O resultado desta revisão

é apresentado a seguir.

Foram encontrados diversos trabalhos cujo objetivo era de aumentar a segurança neste tipo de sistema (BARUA; LU; SHEN, 2011), (BARUA; MAHMOUD; SHEN, 2011), (BARUA et al., 2011a) e (DRIRA; RENAULT; ZEGHLACHE, 2012). Porém, de forma geral, a maioria deles se preocupa com a transmissão de dados entre componentes de um rede conhecida por WBAN. WBAN é o acrônimo para *Wireless Body Area Network*, e consiste em um conjunto de bio-sensores que ficam monitorando os sinais vitais de um paciente. Este tipo de rede surgiu na tentativa de migrar o hospital para um unidade virtual na casa do paciente. A integração deste tipo de rede com outros dispositivos wireless permite um monitoramento constante do paciente, até durante as atividades diárias deste. Os trabalhos neste sentido não serão apresentados pois possuem pouca ou nenhuma contribuição em questões de autenticação eletrônica de usuários.

Outros trabalhos que tratavam de alternativas de segurança em ambientes de telemedicina ou telessaúde eram voltados a segurança dos dados na nuvem, controle rigoroso de acesso a dados, e verificação de confiança entre os nós envolvidos (BARUA et al., 2011b) e (GUO et al., 2012). Estes trabalhos também não serão aqui tratados por trazerem pouca contribuição no escopo deste trabalho.

A maioria das propostas envolvendo modificações no processo de autenticação encontradas utiliza um segundo fator de autenticação e podem ser separadas em dois grandes grupos: baseadas em certificados digitais e baseadas em biometria. Somente um trabalho se diferencia dos demais (BOONYARATTAPHAN; BAI; CHUNG, 2009), e será tratado separadamente a seguir.

O trabalho de Boonyarattaphan, Bai e Chung é motivado pelo fato de que informações médicas pessoais são dados críticos no tratamento médico e precisam de privacidade e proteção (BOONYARATTAPHAN; BAI; CHUNG, 2009). Os autores propõem um *framework* seguro de alto custo-benefício para autenticação de usuários e transmissão de dados. No que tange a autenticação, foram propostas duas técnicas de autenticação baseada nos riscos da situação. Os autores definem três principais situações:

- Situações normais; Onde o paciente normalmente realiza exames de rotina.

- Situações anormais; Quando um paciente é encaminhado a um médico substituto ou é a primeira vez em que o paciente se consulta com determinado médico (ambas as situações são incomuns).

- Situações críticas. Quando o paciente encontra em situação médica

emergencial e algum cirurgião (normalmente não o mesmo médico que atende o paciente) precisa agir imediatamente.

Considerando cada uma das três situações os autores propuseram duas diferentes técnicas de autenticação adpatáveis ao risco da situação. São elas:

- Autenticação baseada em múltiplos fatores; Em situações normais o sistema exige que profissionais da saúde confirmem suas identidades apresentando somente um token. Em situações anormais o sistema exige múltiplos tokens. Neste trabalho, um token pode ser alguma credencial do hospital, algum documento pessoal, ou informações relacionadas ao *"social security number"*, que seria equivalente ao CPF no Brasil.

- Autenticação mútua; Em situações críticas os autores consideram importante autenticar as duas partes envolvidas no processo. Desta forma, previne-se que atacantes personifiquem um usuário válido para prover dados falsos, e também que atacantes consigam forjar o sistema de telesaúde, dificultando o roubo ou modificação de prontuários de pacientes.

O framework proposto pelos autores é baseado em serviços *web*. O sistema de e-Saúde fica logo acima do protocolo de *web service* (SOAP), na camada de aplicação. Neste trabalho percebe-se a preocupação dos autores em assegurar a independência do *framework* proposto com plataformas e linguagens de programação. A adoção de um protocolo de serviço *web* sobre HTTP possibilita tal independência.

### 3.2.1 Baseados em Certificados Digitais

O trabalho de Martinez et al. (MARTÍNEZ et al., 2007) visa apoiar o crescimento de sistemas de telessaúde e telegoverno através da proposta de soluções de segurança generalizáveis para estes dois tipos de sistemas. Segundo os autores, esses dois tipos de sistema possuem características bastante semelhantes. Ambos tem por objetivo facilitar o acesso a serviços básicos de saúde e sanitários por pessoas que não poderiam fazê-los da forma convencional, ou seja, pessoalmente. Os autores ressaltam que os requisitos de ambos devem ser tratados de forma global em uma primeira solução e depois personalizada, de forma a aumentar a reutilização dos serviços.

O principal requisito apontado neste trabalho é o cuidado com a segurança e proteção dos dados deste tipo de sistema. Desta forma, o trabalho tem por objetivo o projeto de um modelo de autenticação de autorização de

usuários que independa do sistema (telessaúde ou telegoverno). Neste trabalho os serviços de autenticação e autorização são tratados como serviços web. Assim consegue-se independência entre as regras de negócio dos sistemas da tecnologia de implementação utilizada nos serviços.

Para a autenticação de usuários, os autores indicam o uso de certificados digitais, embora permitam outras formas, como: usuário e senha somados a alguma informação de documentos de identificação do usuário. Em qualquer uma das duas formas, as mensagens transitam entre o cliente (sistema de telessaúde ou telegoverno) e o serviço web cifradas, para evitar que estes dados possam ser capturados por terceiros. Embora não fique claro no trabalho, acredita-se que a autenticação de usuários seja realizada através de um protocolo de desafio-resposta, onde o usuário é desafiado a assinar digitalmente algum tipo de desafio. Além do mais, também não é especificada a forma com que os pares de chaves relacionados a estes certificados são armazenados.

Com objetivos similares, Ahn and Shin (AHN; SHIN, 2002) propõem um *framework* de autenticação baseado em *tokens* criptográficos, que visa prover mais segurança a fim de proteger os dados deste tipo de sistema. O foco deste trabalho é o projeto de um *framework* capaz de autenticar fortemente um usuário de diferentes formas (através do uso de assinaturas, senhas ou biometria) e garantir acesso a seus dados. Neste trabalho, observa-se um empenho em abstrair as diferentes tecnologias de *smart cards* e *tokens* da camada de autenticação permitindo então a interoperabilidade entre diversos serviços diferentes relacionados a sistemas de telessaúde.

Ainda seguindo a mesma linha, Al-Nayadi and Abawajy (AL-NAYADI; ABAWAJY, 2007) propõem o projeto e a implementação de uma arquitetura de autenticação e autorização, também baseada em certificados digitais. Este trabalho visa integrar diferentes sistemas de telessaúde mantidos por diversas instituições com o objetivo de centralizar os dados de um determinado paciente.

Este modelo é baseado no fato de que cada sistema possui uma Autoridade Certificadora de Identidades (ACI) que distribui e assina os certificados de identidade dos seus usuários. Cada ACI confia nas demais, possibilitando assim a autenticação a sistemas remotos. A autenticação de usuários é feita através da verificação de confiabilidade de um certificado e da apresentação de uma senha. Embora o trabalho não disponibilize mais detalhes, acredita-se que a autenticação envolva um protocolo de desafio-resposta, similar ao apresentado no trabalho anterior.

O restante do trabalho trata somente da autorização de visualização de conteúdo de um paciente por um profissional da saúde. O termo autenticação é bastante confundido com utilização de um termo de consentimento que, neste trabalho, é um documento digital assinado por um paciente concedendo

acesso aos seus dados à profissionais de saúde.

### 3.2.2 Baseados em Biometria

Com uma abordagem diferenciada, Han et al. (HAN et al., 2006) propõem um *framework* de autenticação e autorização baseado em impressões digitais. O *framework* destina-se a reforçar o serviço de autorização do modelo de sistema de telessaúde de forma a garantir o acesso de seus usuários e, principalmente, que estes não tenham acesso a dados não autorizados. A autenticação fica por conta das impressões digitais somadas a um PIN. Os autores não comentam como ocorre a leitura das impressões digitais no *framework* proposto. Da mesma forma, não comentam qual o tipo de computador (convencionais, *tablets* ou *smartphones*) o *framework* foi projetado para. Fica subentendido que os usuários do sistema de telassaúde se autenticam através de um computador convencional equipado com uma leitora de impressões digitais portátil.

Em uma linha parecida, Garson e Adams (GARSON; ADAMS, 2008) propõem uma arquitetura de sistema de segurança de privacidade para e-hospital. No que diz respeito à autenticação, é apresentado um modelo baseado em impressões digitais e cartões de identificação por rádio-frequência - RFID (do inglês *Radio-Frequency IDentification*) que visa, além da autenticação de usuários, evitar que estes dados saiam do hospital, não sendo possível autenticar-se fora dele. A leitura de impressões digitais e dos cartões é feita através de leitoras já instaladas em um *tablet* especial que deve ser usado pelos usuários.

## 3.3 ESTUDO DE MÉTODOS DE AUTENTICAÇÃO

Esta seção é baseada no trabalho submetido ao Programa de Gestão de Identidades (PGId) 2012 da Rede Nacional de Ensino e Pesquisa (RNP), com o título ”Um Levantamento de Métodos para Autenticação com Múltiplos Fatores”.

Atualmente existem diversas alternativas de métodos de autenticação que garantem maior segurança aos usuários. Porém, muitas vezes este modelos possuem um alto custo de manutenção, ou sua implementação é inviável em determinados sistemas. Por exemplo, autenticações com biometria podem garantir um nível de segurança alto, porém é necessário a implantação de leitoras em todas os pontos de acesso. Além do mais, isto requer uma vigilância constante para garantir que o modelo está sendo utilizado de forma

correta. Por exemplo, existem casos registrados onde uma pessoa mal intencionada utilizou dedos falsos para se autenticar em nome de outras pessoas. Assim, este método de autenticação pode ser eficaz para autenticar usuários em lugares como prédios, porém, torna-se difícil de implementar em sistemas web.

Este estudo tem por objetivo geral o levantamento dos principais métodos de autenticação existentes atuamente. Também estudamos o nível de segurança provido por cada um deles, de forma a auxiliar a escolha dos métodos de autenticação utilizados no serviço de autenticação. Neste capítulo podemos ver a análise de cada método em relação a segurança dos tokens. Além disto, também são apresentadas as características de cada um dos métodos com relação a facilidade de uso, facilidade de implementação, custo e esforço de desenvolvimento e manutenção, dentre outros. O resultado deste estudo é um manual simples capaz de auxiliar na concepção de um modelo de autenticação eletrônica com requisitos bastante específicos, como no ambiente médico.

As análises de segurança deste estudo foram realizadas com base no Guia de Autenticação Eletrônica (BURR et al., 2011). O Guia será apresentado a seguir.

## 3.4 GUIA DE AUTENTICAÇÃO ELETRÔNICA

O Instituto Nacional de Padrões e Tecnologia (NIST em inglês) é uma agência federal não-regulatória do Departamento de Comércio dos Estado Unidos fundada em 1901. Sua missão é promover a inovação e a competição industrial evoluindo diversos padrões e tecnologias. Os laboratórios do NIST promovem pesquisas a nível mundial, alguma vezes em parceria com a indústria, que ajudam no avanço das tecnologias do país e ajudam empresas americanas a melhorar seus produtos e serviços.

Em dezembro de 2011 o Laboratório de Tecnologia da Informação (ITL em inglês) do NIST lançou a mais nova versão do Guia Eletrônico de Autenticação 800-63-1 (BURR et al., 2011). Este documento faz parte da série 800 que relata pesquisas e guias feitos pelo laboratório na área de segurança de sistemas de informação. Este documento contém recomendações para autenticações remotas de usuários sobre redes abertas, como a internet.

Este guia é completamente compatível com o Guia de autenticação eletrônica para agências federais do OMB (do inglês *Office of Management and Budget*), o OMB M-04-04 (OFFICE OF MANAGEMENT AND BUDGET, 2003). O guia do OMB define 4 níveis de confiança baseados nas consequências do uso indevido das credenciais de um usuário em um sistema.

O nível 1 é o mais baixo e o 4 é o mais alto, conforme as consequências tornam-se mais sérias o nível requerido de autenticação aumenta. O guia do OMB define 5 passos para a definição do nível de confiança requerido em um sistema:

1. Avaliação dos possíveis riscos;
2. Avaliação do nível de confiança exigido por cada risco;
3. Seleção da tecnologia de autenticação que satisfaça o requisito do nível de confiança;
4. Validação do nível de confiança oferecido pelo método escolhido;
5. Reavaliação periódica do sistema para atualização dos requisitos.

O documento 800-63-1 provê orientações para a realização do terceiro passo. Mais especificamente o documento especifica requisitos técnicos para cada um dos quatro níveis de confiança nas seguintes áreas:

- Registro e prova de identidade;
- Tokens;
- Mecanismos de gerenciamento de tokens e credenciais;
- Protocolos utilizados de suporte para os mecanismos de autenticação;
- Mecanismos de asserção utilizados para comunicar o resultado de uma autenticação.

## 3.5 MÉTODOS DE AUTENTICAÇÃO

Nesta seção serão apresentados detalhes dos métodos de autenticação estudados em questões de implementação, uso e segurança provida pelos mesmos com relação a área de *tokens*. Os métodos foram selecionados de forma a cobrir os mais comumente utilizados, suas variantes e alguma inovações na área.

Para a boa compreensão deste capítulo, é necessário conhecer alguns termos específicos utilizados na análise dos métodos de autenticação estudados. São eles:

**Definição 1** *Entropia: É a quantidade de incerteza no valor de uma senha. Em outras palavras, entropia expressa a quantidade de informação produzida, em média, para cada letra de um texto. A entorpia é expressa em bits. Para senhas aleatórias de k bits é dito que a sua entropia é de $2^k$ bits.*

*Para senhas selecionadas por usuários, o cálculo é expresso em termos da probabilidade de cada letra assumir um determinado valor. Assim, a entropia de senhas escolhidas pelo usuário é menor que a de senhas aleatórias. Uma vez que é assumido que usuários escolhem palavras existententes no vocabulário, pode-se presumir que uma determinada letra assume probabilidades maiores para determinados valores quando posicionada logo após letras específicas, aumentando assim a previsibilidade. É bastante difícil definir a entropia de senhas escohidas pelo usuário, dado que estas não possuem distribuição não uniforme dos caracteres, característica presente nas senhas aleatórias. Uma definição matemática aproximada de entropia pode ser vista abaixo:*

$$H(X) := -\sum_{x} P(X = x) log_2 P(X = x)$$

*Onde $P(X = x)$ é a probabilidade da variável X ter o valor x. Sendo assim, a entropia está diretamente relacionada com dificuldade de um atacante adivinhar uma senha. Ou seja, quanto maior a entropia, maior a dificuldade no ataque. Porém, percebe-se que, em senhas escolhidas pelo usuário, a maior dificuldade está em descobrir os primeiros caracteres da senha, sendo assim, estes caracteres contribuem mais para a entropia geral da senha. Isto ocorre uma vez que, dado uma determinada sequência de caracteres, é menor a quantidade de possíveis valores para o próximo caractere para que a senha continue com valor semântico, Em contrapartida, o primeiro caractere pode ser qualquer um e ainda é possível se obter uma sequência com valor semântico. Desta forma, é importante ressaltar que, embora a entropia cresça conforme a quantidade de caracteres de uma senha aumenta, este crescimento não é linear.*

*Para a melhor compreensão deste trabalho, a entropia foi traduzida em questões de tamanho de senha. Esta tradução foi realizada com auxílio da tabela de correlação de entropia de uma senha e seu tamanho fornecida pelo guia do NIST.*

**Definição 2** *Alfabeto completo: Definido pelos 94 caracteres imprimíveis da codificação de 7 bits ASCII. Este alfabeto é baseado no alfabeto inglês.*

### 3.5.1 Usuário e senha

O método de autenticação baseado em usuário e senha é hoje o mais difundido. Desde simples *web sites* até os mais complexos sistemas de auxílio a gerência de empresas utilizam este método por ter grande aceitação entre os usuários. A combinação é simples: um usuário se identifica utilizando um nome de usuário e confirma sua identidade provando que conhece um segredo previamente combinado: a senha. Diversas modificações foram propostas no modelo para acrescentar mais segurança ao processo ou melhorar a sua usabilidade, dentre estas se destacam:

**PIN** - do inglês *Personal Identification Number*, é uma adaptação do modelo para ser utilizado em telefones celulares, onde os teclados são numéricos e o fornecimento de dados é difícil. Neste modelo a senha é uma sequência de números, normalmente de tamanho reduzido, cujo objetivo é melhorar a experiência do usuário quando da entrada dos dados.

***Pass-Phrase*** - é uma adaptação do modelo cujo objetivo é aumentar o nível de segurança e também facilitar a memorização. Neste modelo as senhas são longas, dificultando ataques de força bruta, e com valor semântico, facilitando assim a memorização.

***Fast word*** - é outra adaptação do modelo para melhorar a experiência do usuário em telefones celulares (JAKOBSSON; AKAVIPAT, 2011). A proposta deste modelo é se utilizar dos métodos de auto correção, já existentes nos celulares, para facilitar a digitação da senha. Neste modelo a senha é composta de algumas palavras sem correlação, ou seja, que dificilmente seriam encontradas em textos na mesma ordem em que se encontram na senha.

**Senhas aleatórias** - é uma adaptação que visa aumentar a segurança do processo fazendo com que os usuários não utilizem senhas passíveis de engenharia social (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 1993). Neste modelo o sistema gera aleatoriamente senhas através da concatenação de sílabas, de forma a montar senhas pronunciáveis porém sem valor semântico. Sendo assim as senhas são aleatórias, porém, mais fácil de memorizar.

#### 3.5.1.1 Análise de segurança

O nível de segurança provido pelos modelos de senhas memorizadas são baseados no tamanho das senhas, podendo variar entre o nível 1 e 2 segundo o NIST. Para senhas comuns escolhidas pelo usuário, o tamanho deve ser pelo menos 6 caracteres. Com este tamanho o nível de segurança garantido pelo método é 1. Ainda de acordo com o NIST, para garantir o nível 2

de segurança com senhas comuns, o tamanho deve ser igual ou superior a 8 caracteres. O método de *Pass-Phrase* e *Fast word* seguem a mesma lógica por serem ambos passíveis de ataques de dicionário. O Pass-Phrase, no entanto, possui a característica de senhas longas, sendo mais difícil atacá-lo com sucesso.

Para o modelo baseado em PINs, as senhas devem ser geradas aleatoriamente com 4 ou mais dígitos para atingir o nível 1 de segurança, e com 6 ou mais para o nível 2. Alternativamente, PINs escolhidos pelos usuários devem possuir pelo menos 10 dígitos para atingirem o nível 1 e 15 para o nível 2.

O modelo baseado em senhas randômicas não necessita de senhas com tamanhos tão grandes uma vez que é imune a ataques de dicionário. Neste modelo, senhas de 4 caracteres já atingem o nível 2 de segurança.

Todos os modelos devem implementar um mecanismo que limite o número de tentativas falhas a 100 ou menos em um período de 30 dias. Embora um mecanismo que faça a verificação mensalmente se encaixe nos requisitos, ele não é ideal. Um mecanismo como este, idealmente, deve limitar o número de tentativas falhas a 3 por dia, ou 5 a cada 2 dias e, caso atinja este limite, o usuário deve ter seu acesso bloqueado, por exemplo.

#### 3.5.1.2 Avaliação geral

- Facilidade de uso: métodos baseados em usuário e senha são os mais amplamente utilizados em sistemas atualmente. O conceito é simples de entender, o nome de usuário é a identificação, e a senha é a forma mais simples de provar sua identidade. Além do mais, estes conceitos sempre estiveram inseridos na vida dos usuários. A dificuldade de utilização deste método aumenta quando tratamos de senhas longas. Usuários tem dificuldades em memorizar senhas muito longas, e essa dificuldade aumenta principalmente quando tratamos de senhas longas e aleatórias.

- Segurança: segundo o NIST o nível de segurança deste método pode chegar a 2, porém devemos considerar a dificuldade de memorização dos usuários em conta. Por causa desta dificuldade, os usuários tendem a utilizar senhas curtas, quando possível, anotá-las em bilhetes, celulares, guardá-las em e-mails, além de reutilizá-las em outros sistemas. Estes comportamentos por parte do usuário tornam mais fácil o ataque e mais severa sua consequência. Uma vez que a reutilização de senhas é bastante comum, se um atacante consegue obter uma senha do usuário, ele possui grande chance de conseguir atacar outros sistemas também.

- Implementação: este método possui uma implementação bastante simples e barata. Para implementá-lo é necessário considerar as duas etapas envolvidas: inicialização e autenticação. A autenticação é simples e igual em todas as variações, envolve somente a verificação de existência do nome de usuário e, caso exista, a comparação entre a sua senha e a senha fornecida. A etapa de inicialização difere entre as senhas aleatórias e as outras variações. Nas aletaórias o sistema deve enviar, idealmente, por meio de um canal seguro a senha escolhida, e, se possível, um canal diferente do canal principal. Nas outras variações é necessário implementar um formulário que o usuário irá preencher para escolher sua senha. Todas as variações devem implementar o devido filtro para as senhas, por exemplo, o formulário de escolha de um PIN só deve aceitar senhas numéricas. É recomendado que as senhas sejam guardadas cifradas ou que se guarde somente o seu resumo criptográfico para evitar ataques ao próprio sistema. Também recomenda-se que as mensagens de falha de autenticação não descrevam se a falha ocorreu na verificação do nome de usuário ou da senha, pois isto pode facilitar ataques.

- Custo: para implementar este método o custo e o esforço são muito baixos, envolvem apenas o desenvolvimento do formulário simples e a implementação do método de envio de senhas aleatórias. Este último pode ser mais custoso dependendo do canal utilizado. O custo/esforço de manutenção é praticamente inexistente, uma vez que os componentes envolvidos são em software. O custo/esforço para o ususário final é bastante pequeno também. Por ser um modelo amplamente utilizado, usuários já estão habituados com ele, portanto seu uso é intuitivo, além de envolver somente a inserção de uma senha por parte do usuário, que é uma operação simples.

### 3.5.2 Lista de senhas únicas

A lista de senhas únicas é um método de autenticação simples e de fácil uso, consiste em uma cartela/livro que contém um determinado número de senhas, normalmente numéricas, de natureza aleatória enumeradas previamente conhecidas pelo sistema. O uso deste método consiste em um desafio-resposta onde o usuário primeiramente se identifica perante o sistema. Em seguida, o sistema desafia o usuário solicitando uma das senhas de forma aleatória, e o usuário prova ter a posse da cartela/livro lhe enviando a senha. Uma característica importante do modelo é que cada senha é utilizada uma única vez, sendo necessária a troca de cartela/livro quando este acaba. Outra

característica importante do modelo é que cada cartela/livro é única, ou seja, não existe outro usuário com uma igual. Este método é bastante utilizado em bancos, combinado a outros *tokens*, por aumentar a segurança do processo assegurando que o usuário é quem se diz ser através da posse da cartela/livro.

#### 3.5.2.1 Análise de segurança

Segundo o NIST, este método de autenticação tem nível de segurança 2 com relação ao token. Porém, há casos onde alguns requisitos devem ser cumpridos. Em casos onde as senhas possuam entropia de, pelo menos, 64 bits, ou seja, 20 caracteres quando for formada somente por números e 10 caracteres quando formada pelo alfabeto completo, nenhum requisito complementar é obrigatório. Em casos onde se deseja uma senha menor, 6 caracteres quando for numérica e 4 quando quando for formada pelo alfabeto completo, por exemplo, é necessário implementar um mecanismo similar ao apresentado em 3.5.1 - Usuário e senha.

#### 3.5.2.2 Avaliação geral

- Facilidade de uso: embora este método não seja muito comum, sua utilização é simples. Não envolve memorização e a única tarefa que o usuário executa é a cópia de uma senha do cartão/livro para o sistema.

- Segurança: embora o nível de segurança definido pelo NIST para tokens deste tipo seja de apenas 2, ele possui algumas características importantes quanto a segurança. Pelo fato das senhas deste modelo serem de natureza aleatória, ataques de predição de senhas tem menores chances de sucesso. Além disso, cada senha é utilizada uma única vez, tornando-se inválida logo após o seu uso, o que dificulta ainda mais um ataque. Desta forma, por mais que o nível de segurança seja o mesmo de um método baseado em usuário e senha, com uma senha grande, pode-se considerá-lo mais seguro por tais características. Por outro lado, o token neste modelo é físico, sendo passível de outros tipos de ataques físicos, ou até mesmo de perdas e esquecimentos.

- Implementação: a implementação deste método exige a impressão de cartelas/livros e um gerenciamento bastante robusto destes. O sistema de gerenciamento das cartelas/livros deve verificar quantas senhas ainda não foram utilizadas e, caso este valor seja próximo de zero, enviar uma nova cartela/livro ao usuário. O sistema deve garatir que o usuário não

será prejudicado caso sua nova cartela/livro demore para chegar. Além disto é necessário implementar alternativas para os casos de roubo ou perda de cartelas. Esta opção deve ser controlada por algum outro token, preferencialmente que seja um fator diferente do principal, para evitar que seja roubado/perdido também. A implementação deste método também exige que o processo de autenticação aconteça de fato em duas etapas: identificação e autenticação. Na identificação o sistema identifica o usuário que deseja se autenticar, escolhe uma das senhas (numeradas) da cartela/livro dele, e a envia como um desafio. Na autenticação o usuário vê o número da senha escolhida na cartela/livro e a copia para o sistema, que verifica se a senha confere, e se conferir, autentica o usuário. A escolha das senhas pode ser simplesmente aleatória, sorteando sempre uma que ainda não foi utilizada, ou sequencial, com uma sequência pré-definida, normalmente diferente da apresentada no cartão.

- Custo: para o usuário o sistema é bastante trivial e o maior esforço envolvido é para transcrever uma senha da cartela para o sistema. A implementação deste método, porém, envolve a adoção de mecanismos que verifique sempre se uma cartela está próxima de acabar e antecipe o envio de uma nova cartela, além de prover alguma alternativa para os casos de roubo ou perda. Além do mais, deve ser responsável por selecionar a próxima senha a ser utilizada. A manutenção do modelo envolve o envio contínuo de cartelas/livros para os usuários.

#### 3.5.2.3 Informações adicionais

Uma forma de implementar este método é baseado na RFC4226 (M'RAIHI et al., 2005).

### 3.5.3 Contrassenha

O modelo de contrassenha enviada pelo sistema também é um modelo bastante simples, que consiste na geração de uma senha de natureza aleatória, normalmente alfanumérica, a cada vez que o usuário tentar se autenticar. Esta senha é enviada ao usuário através de um segundo canal de comunicação, ou seja, um canal diferente do canal utilizado para comunicação entre o usuário e o sistema. Para minimizar as chances de ataques, estas senhas possuem um tempo de vida curto e são utilizadas uma única vez.

A Figura 1 apresenta esquematicamente o processo de autenticação de

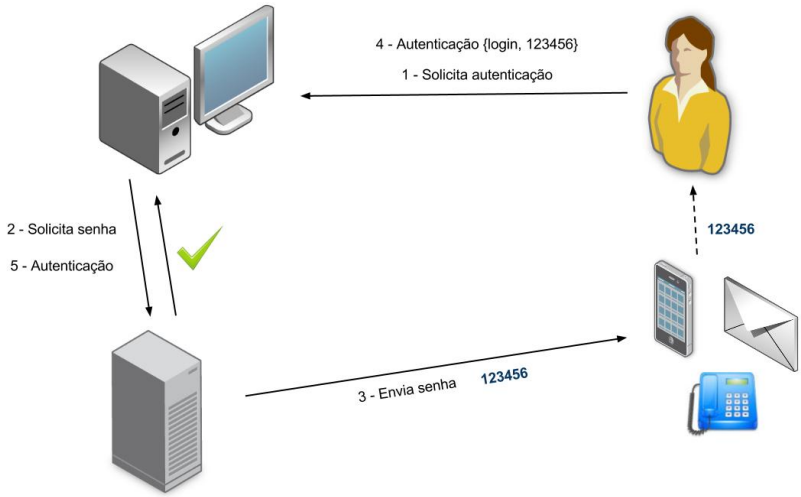


Figura 1: Processo de identificação e autenticação do método de Contrassenhas

usuários utilizando o modelo de contrassenhas. Em um primeiro momento o usuário informa ao sistema que deseja se autenticar (passo 1). Neste momento o usuário também se identifica perante ao sistema. Logo após, nos passos 2 e 3, o sistema recupera o número de telefone do usuário (já cadastrado), gera uma nova senha, e a envia. Por fim, quando o usuário recebe a senha ele a apresenta ao sistema para que este comprove sua identidade (passos 4 e 5).

Os canais de comunicação utilizados neste modelo podem ser:

**SMS** - neste canal o usuário recebe uma mensagem de texto através de SMS (*Short Message Service*) em seu celular pessoal com a senha que deve ser utilizada na autenticação. Contrassenhas enviadas por este canal exigem que o usuário tenha cadastrado previamente o seu telefone celular, e são taxadas pela prestadora de serviços telefonicos utilizada. Possui a vantagem de utilizar um canal diferente do principal, e de utilizar uma tecnologia já conhecida pelos usuários.

**Telefonema** - este canal é bastante parecido com o SMS e possui as mesmas vantagens citadas, porém, neste, o usuário recebe uma chamada telefônica e ouve a sua senha. Também exige o cadastro prévio do número telefônico (seja celular ou fixo) e também é tarifado. Entretanto, este modelo possui outra vantagem: a autenticação geográfica quando utilizado com telefones fixos. Um usuário com um telefone fixo cadastrado deve estar no local onde o telefone está instalado para receber a sua senha e conseguir acessar o

sistema.

**E-mail** - este canal é uma alternativa aos outros pois evita a tarifição. Neste modelo o usuário recebe um e-mail contendo a senha que será utilizada na autenticação.

#### 3.5.3.1 Análise de segurança

Por serem tokens que se utilizam de um canal diferente do utilizado na autenticação, os modelos baseados em SMS e Telefonema podem atingir o nível 2 de segurança. Para atingi-lo é necessário cumprir um destes dois requisitos: as senhas envolvidas devem possuir entropia de, pelo menos, 64 bits, ou seja, 20 dígitos (quando forem somente numéricas) ou 10 caracteres quando forem compostas pelo alfabeto completo; ou devem possuir 20 bits de entropia, ou seja, 6 dígitos (quando forem somente numéricas) ou 4 caracteres quando forem compostas pelo alfabeto completo. Neste último ainda é necessário implementar um mecanismo similar ao apresentado em 3.5.1 - Usuário e senha.

Já o modelo baseado em contrassenhas por e-mail utiliza o mesmo canal utilizado para realizar a autenticação e não possui as mesma características dos outros dois. Embora não se encaixe em nenhum dos *tokens* definidos pelo guia do NIST, pode-se assumir que atinja um nível similar aos outros dois modelos de contrassenhas pelas suas similaridades. Porém, recomenda-se o uso dos dois primeiros antes do uso do método de contrassenha por e-mail, pois estes se utilizam de um canal diferente do principal e, portanto, são mais difícies de serem atacados.

#### 3.5.3.2 Avaliação geral

- Facilidade de uso: embora este método ainda não seja muito comum, sua utilização é simples. Não envolve memorização e a tarefa que o usuário tem que executar é a cópia de uma senha recebida via SMS, telefonema ou *e-mail*. Porém, como o serviço de SMS não possui garantia de tempo de entrega de mensagens, o método de contrassenha por SMS pode aumentar significativamente o tempo do processo de autenticação.

- Segurança: embora o nível de segurança definido pelo NIST para os *tokens out of band* (via SMS e via telefonema) seja de apenas 2, o fato de utilizarem um canal diferente do canal principal é bastante importante pois dificultam os ataques de intercepção. Especialmente nestes

dois modelos, o *token* utilizado é de uso pessoal, e ataques físicos como roubos são facilmente percebidos pelo usuário, que pode tomar as devidas atitudes para minimizar as consequências o mais rápido possível. Além do mais, em todos os três modelos as senhas são de natureza aleatória, dificultando também ataques de adivinhação.

- Implementação: a implementação deste método pode exigir a instalação de infra-estrutura para que se possa fazer o envio das contrassenhas. Para o modelo de contrassenha enviada por telefonema é necessário ter-se acesso a infra-estrutura telefônica. Para o modelo de contrassenhas enviadas via SMS pode-se utilizar infra-estrutura VoIP ou GSM. Para o último modelo de contrassenhas é necessário um servidor de *e-mail*. Neste modelo o processo de autenticação deve acontecer de fato em duas etapas: identificação e autenticação. Na identificação o sistema identifica o usuário que deseja se autenticar, gera uma senha aleatória e a envia para o usuário através do canal definido previamente. Na etapa de autenticação o usuário lê a senha recebida e a copia para o sistema, que é reponsável pela sua verificação.

- Custo: do ponto de vista do usuário, os sistemas de contrassenhas são triviais e o maior esforço envolvido é para copiar uma senha. O desenvolvimento, porém, é mais custoso, pois envolve os custos de adquirir e operar a infra-estrutura necessária. Além disso, a implementação em software não é tão trivial quanto a dos métodos de atenticação apresentados anteriormente. Neste método, por exemplo, é necessário o desenvolvimento de componentes complexos, como o responsável pelo envio de senhas por tons telefônicos. A manutenção deste método envolve basicamente os gastos com as tarifas de SMS e ligações telefônicas.

### 3.5.4 Identificação de chamadas

Neste método, o usuário que deseja se autenticar realiza uma chamada telefônica para o sistema. O servidor de recebimento de chamadas identifica o número do telefone que originou a chamada e o registra em um banco de dados. Para prosseguir com a autenticação, o sistema verifica se o usuário que está tentando se autenticar já realizou a ligação conferindo o número telefônico que este possui cadastrado. Cada ligação possui um tempo curto de validade para minimizar a janela de tempo de ataques. Toda vez que um usuário realiza a ligação, até que ele efetivamente se autentique, existe uma janela de tempo que poderia ser aproveitada por atacantes. Além do mais, se o usuário realiza a ligação mas não finaliza a autenticação por algum mo-

tivo, isto dá ao atacante maiores chances de sucesso em um ataque. Por isso cada chamada tem um tempo de vida útil pequeno, assim a janela de ataque diminui, bem como as chances de um ataque com sucesso. Além do mais, quando um usuário se autentica com sucesso, o sistema remove o registro da ligação para evitar que se reutilize a mesma ligação válida em mais de uma autenticação. Neste método, também percebemos a vantagem da autenticação geográfica. Caso o telefone utilizado para realizar a ligação seja um telefone fixo, temos a certeza de que a chamada foi originada do local onde a linha está instalada. Este método, embora se utilize do canal telefônico, não possui tarifação para o sistema, somente o usuário é tarifado.

Este método só funciona corretamente no Brasil, uma vez que a arquitetura de Rede pública de telefonia comutada (PSTN, do inglês *Public switched telephone network*) adotada em nosso país não permite a forja de identificadores de chamadas. No modelo brasileiro, os identificadores são atribuidos à chamada pela operadora, e não pelo telefone que a originou. Assim, mesmo que se tente alterar o identificador, a operadora o sebrescreverá pelo número correto.

A Figura 2 apresenta o processo de autenticação de um usuário utilizando o método de identificação de chamadas telefônicas. Em um primeiro momento o usuário informa ao sistema que deseja autenticar-se (passo 1). Neste momento o usuário também se identifica perante ao sistema. O sistema solicita que o usuário faça uma chamada telefônica para determinado telefone (passo 2). Assim que o usuário realiza a ligação (passo 3), esta chamada é registrada e o sistema é informado (passo 4). Por fim, com o registro das ligações recebidas, o sistema consegue verificar os identificadores de chamada e autenticar o usuário (passo 5).

#### 3.5.4.1 Análise de segurança

Embora este método não se encaixe em nenhum dos *tokens* definidos pelo NIST, ele possui bastante similaridades com *tokens out of band*. Neste modelo a comunicação é inversa, o usuário a inicia, ao invés do sistema, como nos outros modelos deste tipo de *token*, porém pode-se observar que a maioria das características permanecem iguais. A principal diferença entre os modelos é a ausência do segredo utilizado para provar a posse do dispositivo que, neste caso, não é necessária uma vez que a própria chamada a prova. Desta forma, podemos dizer que este modelo atinge um nível similar ao de *tokens out of band*.

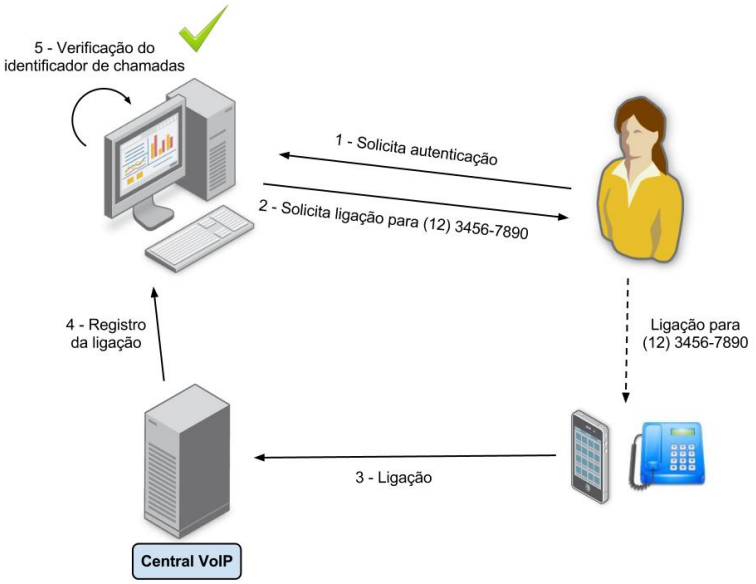


Figura 2: Processo de autenticação do método de Identificação de chamadas

#### 3.5.4.2 Avaliação geral

- Facilidade de uso: embora este método não seja comum, sua utilização pode ser facilmente explicada através de tutoriais. Na primeira vez que o usuário for se autenticar, é necessário explicar o método passo a passo, porém, acredita-se que seja de fácil utilização, dado que somente envolve uma ligação telefônica, tarefa que os usuários já sabem fazer.

- Segurança: a avaliação de segurança deste método é bastante subjetiva, dado que não há um *token* ao qual este método se encaixe, estando relacionada às suas características. A característica do telefone ser um objeto de uso pessoal, por exemplo, torna o modelo um pouco mais seguro, uma vez que seria bastante difícil um atacante obtê-lo sem ser percebido. Porém, quando o telefone cadastrado é um telefone fixo, tanto residencial quanto comercial, é comum que mais de uma pessoa tenha acesso a este, facilitando possíveis ataques. Porém, os telefones fixos ainda trazem uma característica importante, que é a localização geográfica onde o usuário está tentando se autenticar, que pode ser utilizada como um fator de autenticação.

- Implementação: a implementação deste método exige acesso a uma infra-estrutura de VoIP. A central VoIP deve ser programada com um *script* que roda a cada ligação recebida. O *script* deve registrar o identificador de chamadas da ligação recebida em uma base de dados que o sistema possua acesso. Desta forma, o sistema consegue verificar se o usuário que diz ter ligado realmente o fez, e se o tempo de validade da ligação não expirou. Para que se possa prover um bom serviço, o ideal seria possuir diversas centrais VoIP autorizadas. Assim o problema de linhas ocupadas seria amenizado. A implementação deste método na camada do sistema deve ser feita em duas etapas: identificação e autenticação. Na identificação o sistema solicita que o usuário realize uma chamada para um determinado número telefônico. Na autenticação o sistema realiza a verificação da chamada e do tempo de validade, e caso ambos sejam válidos, o usuário se autentica com sucesso.

- Custo: neste modelo as operações tem custo financeiro para o usuário. Cada ligação pode ser tarifada de diferentes formas, dependendo da companhia que esteja provendo o serviço telefônico. Para o sistema as ligações são gratuitas. Somente há o custo de manutenção da infra-estrutura. A implementação deste modelo não é simples, pois envolve o desenvolvimento de componentes complexos, como por exemplo, os

scripts que rodam na central VoIP para o reconhecimento e registro dos identificadores de chamadas.

### 3.5.5 One-Time Password

O método de autenticação baseado em OTP (*One-Time Password*) consiste em dois geradores de senhas sincronizados. O primeiro é um dispositivo único e intransferível que fica de posse do usuário e o outro é o servidor de autenticação. Os geradores geram senhas pseudo-aleatórias, normalmente de 6 dígitos, que são utilizadas somente uma única vez. Logo após o seu uso elas se tornam inválidas.

Os geradores são inicializados com um segredo compartilhado que é conhecido somente por estes, e é utilizado para gerar as senhas, juntamente com um outro fator que pode ser de tempo ou evento. Quando baseados em tempo, os geradores possuem um relógio e estes devem estar sincronizados. O sincronismo é necessário para que novas senhas sejam geradas automaticamente em um determinado intervalo de tempo (normalmente 30 segundos) e se tornam inválidas após isto. Quando os geradores são baseados em eventos, as senhas são geradas somente quando o usuário solicita, e o controle é feito através de um contador.

O método ainda prevê uma janela de ressincronização, que consiste em verificar uma determinada quantidade de OTPs futuros e passados para fazer com que os geradores se ressincronizem. A ressincronização só ocorre no servidor de autenticação. O servidor verifica a diferença cronológica ou do contador entre a OTP recebido e o OTP gerado, e passa a levar em consideração esta diferença nas próximas autenticações. A janela de ressinronização tem um valor determinado pelo servidor de autenticação. A janela deve ser pequena o suficiente para não permitir ataques e, ao mesmo tempo, grande o suficiente para previnir problemas com geradores válidos.

Existem muitas implementações disponíveis do OTP. Entre as que usam somente software, uma das mais conhecidas é o Google Authenticator. Já implementações em hardware há vários fornecedores de tokens.

O Google Authenticator (Google Inc., 2012) é um aplicativo disponível nas plataformas Android, iOS e Blackberry. É um *token* gerador em software e, por conta disso, a inicialização do segredo compartilhado é feita online. Possui uma interface de fácil uso e a vantagem de que os usuários já estão, normalmente, habituados com o uso de seus *smartphones*.

*Tokens* em *hardware* possuem uma arquitetura dedicada à geração de senhas OTP. Normalmente são inicializados somente uma vez. Portanto o compartilhamento do segredo pode ser feito *offline* no momento da fabricação.

#### 3.5.5.1 Análise de segurança

Segundo o NIST, o *Google Authenticator* pode ser classificado como um dispositivo de senha únicas de somente um fator. Isto significa que ao se autenticar com uma senha de uso único (*One-Time Password*), o usuário está provando somente a posse do dispositivo (um único fator). De acordo com o NIST, este tipo de dispositivo pode atingir até o nível de segurança 2. Para isso, é necessário que o tempo de vida útil de cada senha descartável seja na ordem de minutos. Embora não esteja definido no guia, assume-se que este requisito seja relativo somente ao OTP baseado em tempo, uma vez que não é possível verificar a vida útil de um OTP baseado em contador. Outro requisito necessário neste modelo é o uso de um servidor de autenticação, em questões de *hardware*, validado pelo FIPS 140-2 nível 1 ou maior (NIST, 2002).

A avaliação do modelo baseado em hardware específico é similar, porém pode atingir o nível 4 de segurança se cumprir alguns outros dois requisitos. O primeiro exige a validação do próprio dispositivo gerador pelo FIPS 140-2 em nível 2 ou nível maior e com segurança física validada em nível 3 ou nível maior. O segundo é uma redução do tempo de vida de uma senha para menos de 2 minutos.

#### 3.5.5.2 Avaliação geral

- Facilidade de uso: este método é de simples utilização para os usuários que já estão habituados com *smartphones*. Envolve somente a geração de uma senha (quando o OTP for baseado em contador) e a cópia desta senha, normalmente de 6 dígitos, para o sistema.

- Segurança: embora a variação de OTP utilizando *Google Authenticator* não atinja o mesmo nível de segurança do *token* em *hardware*, deve-se destacar suas características importantes. Por ser um aplicativo de *smartphone*, a primeira característica importante é a pessoalidade deste tipo de dispositivo. Ou seja, os usuários não utilizam seus *smartphones* somente para fazer ligações, mas sim para diversas tarefas do seu dia a dia, mantendo-os sempre por perto. Esta característica é importante pois dificulta alguns ataques. Por exemplo, o ataque de roubo do dispositivo se torna muito mais perceptível pois os usuários acabam tendo mais cuidado com seus *smartphones*, por serem peça importante no seu dia a dia. Mesmo em casos onde o roubo é bem sucedido, os usuários perceberiam logo que foram roubados, e tomariam as devidas providências rapidamente, minimizando ou até mesmo anulando as

consequências do ataque ao sistema.

- Implementação: a implementação em nível de software pode ser considerada simples. Para que o método opere corretamente é necessário implementar funções capazes de gerar as mesmas senhas do cliente dado o segredo compartilhado e supondo que ambos estejam sincronizados. Porém, em ambos os modelos, baseado em tempo ou em contador, é necessário prever a ressincronização entre cliente e servidor, uma vez que relógios não são precisos e que o contador pode ser facilmente dessincronizado quando não utilizado corretamente.

- Custo: quando utiliza-se o Google Authenticator, o custo do método pode ser quase nulo, tendo-se somente custo com a manutenção dos componentes de software. Quando utiliza-se token em hardware, existe o custo de fabricação/compra dos dispositivos e do envio dos mesmos, podendo ser bastante elevado dependendo do nível de segurança dos *tokens*.

#### 3.5.5.3 Informações adicionais

Embora o *Google Authenticator* seja utilizado nos sistemas do Google, como contas de *e-mail*, é possível utilizá-lo em outros sistemas, uma vez que seu código fonte é aberto e o aplicativo é ditribuído gratuitamente. De forma geral as implementações deste modelo seguem as RFCs 6238 (M'RAIHI et al., 2011a) e 4226 (M'RAIHI et al., 2005).

### 3.5.6 Tiqr

O Tiqr (SURFnet, 2013) é um método de autenticação baseado em código de barras bidimensionais conhecidos como *QR Code*. É um aplicativo disponível para as plataformas Android e iOS baseado nos padrões abertos do OATH (*Open Authentication Initiative*) de autenticação. Ele utiliza o protocolo OCRA de desafio-resposta (M'RAIHI et al., 2011b). O processo envolve duas etapas: inicialização e autenticação. Para a inicialização, o usuário fornece alguns dados pessoais, como usuário e nome, que são registrados no sistema. Logo após o fornecimento destes dados, o sistema gera um nova chave hexadecimal, associa-a ao usuário, e a compartilha com o usuário através de um *QR Code*. O usuário efetua a leitura desta chave com o aplicativo já instalado no seu *smartphone*, e protege esta com um PIN de 4 dígitos. A Figura 3 mostra os passo necessários para autenticação com o Tiqr. A autenticação


Fonte: (SURFnet, 2013)

Figura 3: Processo de autenticação do método Tiqr

inicia com a leitura de um *QR Code* (passo 1). Este contém uma informação sobre o sistema para que se possa identificar qual chave utilizar (passo 2), e um desafio, que consiste em uma sequência alfa-numérica aleatória. Logo após, o usuário deve entrar com um PIN (passo 3) que desbloqueia o aplicativo. A resposta ao desafio é a cifra da sequência aleatória com a chave do usuário, utilizando o método de cifra simétrica AES 256-bits. O envio da resposta é feito através da internet e leva junto a credencial do usuário. Quando o sistema recebe a resposta e consegue verificá-la, a página que o usuário está visualizando se atualiza e este consegue acessar o sistema (passo 4).

#### 3.5.6.1 Análise de segurança

O Tiqr pode ser classificado como um dispositivo criptográfico multi-fator de acordo com o guia do NIST. Isso ocorre uma vez que o aplicativo opera com o protocolo desafio-resposta utilizando cifra simétrica, o que o caracteriza como dispositivo criptográfico. O multi-fator se refere ao fato do aplicativo ser bloqueado por um PIN, ou seja, quando um usuário se autentica utilizando este método ele prova a posse do dispositivo com o aplicativo instalado (primeiro fator, algo que o usuário possui) e também que ele conhece o PIN para o desbloqueio do mesmo (segundo fator, algo que o usuário conhece). Este tipo de *token* pode atingir o nível 3 de segurança com relação ao *token*, porém é necessário cumprir dois requisitos. O primeiro diz respeito a validação do *token* em FIPS 140-2 nível 1 ou maior. O segundo diz respeito

a força do desafio, que deve possuir no mínimo 20 dígitos ou 10 caracteres quando formado por um alfabeto completo.

#### 3.5.6.2 Avaliação geral

- Facilidade de uso: este método é de simples utilização para os usuários que já estão habituados com *smartphones*. Envolve a leitura de *QR Codes* com o aplicativo.

- Segurança: similarmente ao *token* gerador de OTPs *Google Authenticator*, o Tiqr também possui características importantes que deve-se destacar. A primeira delas é a pessoalidade dos *smatphones*, similarmente ao citado em 3.5.5 - *One-Time Password*. A segunda característica importante é a utilização de um PIN no aplicativo não permitindo a utilização sem o seu conhecimento, esta característica é a responsável pela diferença entre os níveis de garantia do *Google Authenticator* e o Tiqr.

- Implementação: como o aplicativo que roda no *smartphone* do usuário está pronto e atualmente já é distribuído, a implementação deste método diz respeito somente a camada do servidor. Esta implementação pode ser considerada simples, uma vez que somente envolve o desenvolvimento de um componente que adote o protocolo OCRA de desafio-resposta. Este protocolo é bastante similar ao de geração de OTP baseado em contador, utilizando a palavra de desafio como o contador e a chave previamente compartilhada.

- Custo: para o sistema o custo é praticamente nulo, uma vez que somente se gasta com a manutenção dos componentes de software. Porém, para o usuário o modelo pode ter um custo, pois toda vez que o usuário deseja se autenticar, o aplicativo utiliza a rede do aparelho para enviar, via internet, a resposta ao desafio. Ou seja, se não houver uma rede sem fio disponível no momento da autenticação, o usuário deverá utilizar o seu pacote de dados de sua operadora para o envio.

### 3.5.7 Desafio resposta - chave assimétrica

Um dos mais conhecidos protocolos em Desafio-Resposta utilizando chaves assimétricas é o *Public-key Needham-Schroeder* (NEEDHAM; SCHROEDER, 1978). Os autores propõem um protocolo de desafio-resposta en-

volvendo duas partes (A e B) e um servidor confiável que armazena as chaves públicas dos envolvidos. Em um primeiro passo do protocolo é feito o compartilhamento de chaves públicas das partes envolvidas. Logo após, A (primeira parte) gera um *nonce* (um número aleatório grande utilizado uma única vez), cifra com a chave pública de B e o envia. Ao receber, B consegue decifrar o *nonce*. B então gera um segundo *nonce*, e o envia cifrado com a chave pública de A, juntamente com o primeiro *nonce*. A então decifra o segundo *nonce* e o envia de volta, encerrando o protocolo. A prova da identidade, neste caso, se dá no momento em que cada parte devolve o *nonce* gerado pela outra parte decifrado. Os *nonces* não são utilizados e nem distribuídos fora do protocolo, desta forma, cada parte só poderia consegui-lo através da decifragem, utilizando a sua chave privada. O fato do *nonce* ser aleatório ajuda a combater ataques de *replay*.

Como deseja-se autenticar somente os usuários, é possível reduzir o protocolo a dois passos: a geração e envio do *nonce* por parte do sistema; a resposta ao desafio por parte do usuário. Neste trabalho considera-se que as chaves privadas possam estar armazenadas das seguintes formas: em *software*, em *smartcards*, ou em *tokens*.

#### 3.5.7.1 Análise de segurança

Segundo o NIST este método pode atingir um nível de segurança até 4, dependendo de algumas caracterísitcas físicas do *token*. Quando o *token* é mais simples ele atinge o nível 2, mas ainda assim é necessário validá-lo no FIPS 140-2 no nível 1 ou maior, e o desafio (*nonce*) enviado ao usuário deve possuir, pelo menos, 64 bits de entropia, ou seja, 20 dígitos se for somente numérico ou 10 caracteres se for formado por um alfabeto completo. Para atingir o nível 4 o *token* deve ser validado pelo FIPS 140-2 no nível 2 ou maior, com segurança física FIPS 140-2 nível 3 ou maior, além de ser necessário a utilização de outro fator para ativá-lo, e não ser permitido a exportação da chave privada. Mesmo neste caso, o desafio também deve possuir, pelo menos, 64 bits de entropia.

#### 3.5.7.2 Avaliação geral

- Facilidade de uso: por utilizar *tokens* não muito comuns, este método pode ser de difícil utilização para os seus usuários. Quando as chaves estão em *software*, o sistema deve disponibilizar um módulo para auxiliar o usuário na tarefa de responder ao desafio. Outra alternativa é o

usuário utilizar-se de ferramentas que o auxilie. Porém isso exigirá algum conhecimento técnico. Quando as chaves estão em *smartcards* ou *tokens* criptográficos, a utilização dos mesmos irá depender de leitoras devidamente instaladas e/ou da instalação correta de drivers.

- Segurança: quando o par de chaves está armazenado em *software*, a segurança deste *token* pode ser similar à provida pelo método de autenticação baseado em usuário e senha comum. Isto porque a chave privada do par é protegida por um segredo, ou seja, se a ferramenta utilizada para dar suporte não for segura, pode-se atacar o sistema com ataques de dicionário ou força bruta. Este fato explica porque os *tokens* mais simples possuem somente nível 2 de segurança. Os *smartcards* e *tokens* proveem um nível maior de segurança, uma vez que não se conhece forma de retirar a chave privada dos mesmos ou cloná-la de alguma forma.

- Implementação: a implementação deste método é simples. Na camada do sistema deve-se implementar um módulo capaz de gerar sequências numéricas aleatórias com tamanho grande o suficiente. Além disso, o sistema de ser capaz de decifrar uma mensagem cifrada com a sua chave pública.

- Custo: quando o par de chaves é armazenado em software o custo do modelo é quase nulo, envolvendo somente custos com a manutenção dos componentes de software. Quando o par de chaves é armazenado em smartcards ou tokens criptográficos, o custo é mais elevado, pois envolve o custo de fabricação/compra dos dispositivos, além dos custos de distribuição dos mesmos.

### 3.5.8 Biometria

Em métodos baseados em biometria, as características físicas de um indivíduo são analisadas para assegurar que este é quem afirma ser. O método exige que cada usuário faça um cadastro prévio de uma característica física que o sistema tenha suporte. Este pode ser: voz, impressão digital, iris, retina, face, etc. O método consiste na leitura de determinada característica física através de leitoras específicas. Como os padrões de biometria dos usuários cadastrados já estão registrados no sistema, se estes coincidirem então a autenticação ocorre com sucesso, caso contrário, ela falha. De acordo com Schneier (SCHNEIER, 1999), há diversas formas de atacar métodos de autenticação baseados em biometria. O autor ainda afirma que este método

só funciona bem se o sistema puder verificar duas propriedades: 1 - se a característica biometrica veio da pessoa correta no momento da verificação; 2 - se a biometria apresentada confere com a armazenada pelo próprio sistema.

#### 3.5.8.1 Análise de segurança

O guia do NIST define como *tokens* de autenticação eletrônica aqueles que contém um segredo. Embora características biométricas sejam únicas e pessoais, não se pode dizer que são secretas. Impressões digitais ficam marcadas em diversos objetos que as pessoas tocam, por exemplo. Devido a isso, o NIST recomenda o uso de biometria somente para a identificação de usuários. O guia do NIST não define um tipo de *token* para a biometria, e nem um nível de segurança. Dessa forma, sua avaliação é bastante subjetiva. Atualmente os métodos de falsificação de características biométricas estão bastante sofisticados, e cada vez mais baratos. Por exemplo, já é possível comprar pela internet um dispositivo capaz de falsificar uma impressão digital. Além disto, os índices de falsos positivos das leitoras deste tipo ainda são bastante altos, adicionando um percentual de incerteza nas autenticações.

#### 3.5.8.2 Avaliação geral

- Facilidade de uso: o seu uso é complicado quando utilizado para autenticação remota, pois envolve a instalação correta de leitora de características biométricas, que muitas vezes não é uma tarefa trivial. Além do mais, quando tratamos deste tipo de autenticação, as leitoras mais comuns são as de impressão digital, limitando então as variações. Quando utilizado em autenticações locais, como em edifícios, pode-se dizer que sua utilização é simples, basta ensinar os usuários uma única vez.

- Segurança: como mencionado, biometria não é indicada para autenticação de usuários em ambiente computacionais pois não constitui uma informação secreta. Apesar deste método possuir algumas características importantes, como a unicidade, e o fato do usuário ser o próprio "*token*", o guia do NIST não define um nível de segurança para este.

- Implementação: a implementação deste método não pode ser considerada trivial, uma vez que envolve a comunicação com os drivers das leitoras biométricas para que se possa verificar as características de

uma pessoa. Esta tarefa é especialmente complicada pois não existe um padrão para os dados lidos entre fabricantes.

- Custo: o custo deste método é elevado e envolve os custos de compra das leitoras biométricas, e o custo de manter vigilantes para garantir que o processo está sendo bem executado durante todo o tempo. Além disto, normalmente as leitoras de mais qualidade também são as leitoras mais caras, portanto o custo do modelo aumenta conforme a necessidade de segurança do processo aumenta.

Na Tabela 1 podemos ver a sumarização do estudo realizado. A tabela apresenta os níveis de garantia possíveis de alcançar em cada um dos métodos, e os requisitos necessário para atingi-los.

Neste capítulo foi apresentado um estudo dos métodos de autenticação mais comuns atualmente, com o objetivo de analisá-los segundo o nível de segurança provido por cada um. Além disso, um estudo sobre as características com relação a facilidade de uso, facilidade de implementação e custo/esforço de desenvolvimento e manutenção também foi apresentado.

Para analisar os métodos quanto ao nível de segurança provido utilizou-se do Guia de Autenticação Eletrônica (documento 800-63-1) do NIST, que classifica os *tokens* de autenticação em quatro níveis, sendo 1 o nível mais baixo e 4 o mais alto. Para as outras características foram realizados estudos de caso com os métodos de autenticação, onde a avaliação foi baseada em fatores mais subjetivos.

Ao final do estudo concluiu-se que não existe um método de autenticação que possua um alto nível de segurança, baixo custo de implantação e que seja de fácil utilização. Todos os métodos estudados apresentaram, pelo menos, uma das três características prejudicadas. Desta forma, para cada sistema, deve-se estudar as características desejadas e escolher o método de autenticação que mais perfeitamente se enquadra.

Tabela 1: Tabela com níveis de garantia dos métodos de autenticação

| Método | Nível | Requisitos Específicos | Requisitos comuns |
|---|---|---|---|
| Usuário e senha | 1 | 6 caracteres | Limitar as tentativas falhas a 100 por mês, com verificações mais frenquentes (diarias) |
| | 2 | 8 caracteres | |
| PIN | 1 | 4 dígitos aleatórios, ou 10 escolhidos pelo usuário | |
| | 2 | 6 dígitos aleatórios, ou 15 escolhidos pelo usuário | |
| Pass-Phrase | 2 | 8 caracteres | |
| Fast word | 1 | 6 caracteres | |
| | 2 | 8 caracteres | |
| Senha randômica | 2 | 4 caracteres | |
| Lista de senhas únicas | 2 | 6 digitos ou 4 caracteres | |
| | | 20 digitos ou 10 caracteres | - |
| Contrassenha - SMS | 2 | 6 digitos ou 4 caracteres | Limitar as tentativas falhas a 100 por mês, com verificações mais frenquentes (diarias) |
| | | 20 digitos ou 10 caracteres | - |
| Contrassenha - Telefonema | 2 | 20 digitos ou 10 caracteres | - |
| | | 6 digitos ou 4 caracteres | Limitar as tentativas falhas a 100 por mês, com verificações mais frenquentes (diarias) |
| Contrassenha - e-mail | - | - | - |
| Identificação de chamadas | - | - | - |
| OTP - Google Authenticator | 2 | Servidor de autenticação validado em FIPS 140-2 nível 1 | Tempo de vida das senhas na ordem de minutos |
| OTP - Hardware | 4 | Hardware validado em FIPS 140-2 nível 2 ou mais, com segurança física FIPS 140-2 nível 3 ou mais | |
| | | Tempo de vida das senhas com menos de 2 minutos | |
| Tiqr | 3 | Validação FIPS 140-2 nível 1 ou mais | Desafio com 20 dígitos ou 10 caracteres |
| Desafio resposta - Chaves assimétricas | 2 | Validação FIPS 140-2 nível 1 ou mais | |
| | 4 | Validação FIPS 140-2 nível 2 ou mais, com segurança FIPS 140-2 nível 3 ou mais | |
| Biometria | - | - | - |

# 4 PROTOCOLO DE AUTENTICAÇÃO MULTI-FATOR FLEXÍVEL

Este capítulo descreve o protocolo de autenticação multifator flexível e uma implementação do mesmo. A implementação do protocolo foi adicionada como um componente de autenticação do Sistema Integrado de Telemedicina e Telessaúde de Santa Catarina. São também apresentados os resultados da fase de concepção do projeto, do levantamento de requisitos, descrição de arquitetura do software e implementação.

O projeto contou com a colaboração de uma equipe de desenvolvimento de aplicativos móveis e *web* composta por dois alunos de graduação. Sendo estes guiados pela autora tanto na concepção de ideias e gerenciamento do projeto, quanto no desenvolvimento dos aplicativos e da plataforma *web*.

Para a realização deste projeto adotou-se a metodologia de Processo Unificado (RUP, do inglês *Rational Unified Process*) (JACOBSON; BOOCH; RUMBAUGH, 1999) adaptada. A metodologia foi mantida nas suas fases iniciais de concepção e elaboração do projeto, mas tomou uma face mais ágil durante a construção do software, se adaptando melhor a equipe de desenvolvimento. Para o desenvolvimento utilizou-se a metodologia ágil SCRUM (SCHWABER; SUTHERLAND, 2012), com iterações de 1 a 2 semanas e incrementais.

O Processo Unificado determina que a fase inicial (concepção) seja feita através de reuniões entre o cliente (no contexto deste trabalho consideramos o STT/SC como o cliente) e os desenvolvedores. Seu resultado é um documento com a visão geral do sistema (WAZLAWICK, 2010). Esta fase foi executada com a inserção de um membro da equipe desenvolvedora (a autora deste trabalho) durante 1 mês no ambiente de desenvolvimento do STT/SC (cliente). Esta fase fez com que compreendessemos melhor o atual processo de autenticação do sistema e as necessidades dos usuários com relação a assistência e treinamentos.

A segunda etapa do projeto (ainda na fase de concepção) foi o levantamento dos requisitos funcionais e não funcionais. Esta etapa foi realizada em reuniões periódicas entre a equipe desenvolvedora deste projeto e dois membros da equipe desenvolvedora do STT/SC, além da presença de um dos coordenadores do mesmo. O levantamento de requisitos foi feito incrementalmente, em reuniões semanais, onde as equipes traziam suas preocupações e discutiam os requisitos do projeto. O processo de levantamento de requisitos é descrito na seção seguinte.

## 4.1 LEVANTAMENTO DE REQUISITOS

Foi utilizado o STT/SC como base para melhor compreender os requisitos de um modelo de autenticação no contexto médico. Além disso, foram levados em consideração as características encontradas nos trabalhos relacionados. Esta seção trata dos requisitos de um modelo de autenticação para o contexto médico. Os requisitos comuns a todos os projetos de modelo de autenticação não serão tratados aqui.

Neste capítulo usaremos os termos ”profissional médico”ou ”médico”para designar o usuário de um sistema de telemedicina com requisitos de autenticação distintos dos tradicionalmente encontrados em sistemas de autenticação computacionais. Apesar de se referir a usuário ”médico”e tratar dos requisitos de forma a focar no contexto médico, os resultados do nosso trabalho podem ser usados por quaisquer outras aplicações com necessidades similares. Ou seja, aplicações que possuam dados sensíveis e que necessitam flexibilidade e mobilidade na autenticação, por exemplo, *web banking*.

Os requisitos tratados nesta seção são requisitos suplementares, que, de acordo com Wazlawick (WAZLAWICK, 2010), são ”todo tipo de restrição tecnológica ou lógica que se aplica ao sistema como um todo, e não apenas a funções individuais”. Optou-se iniciar o levantamento por estes requisitos por serem de natureza limitante.

As reuniões com a equipe do STT/SC mostraram que existem cenários onde usuários (normalmente médicos especialistas laudadores) precisam ter acesso ao sistema de computadores fora do hospital, por exemplo, quando eles estão viajando. Desta forma, o primeiro requisito encontrado diz respeito a possibilitar a mobilidade dos médicos. Assim, tais profissionais devem poder se autenticar tanto no hospital, quanto a partir de qualquer outro local, através da *internet*. O sistema de autenticação deve ser seguro o suficiente para que o profissional médico consiga se autenticar, sem comprometer a sua mobilidade.

Nos primeiros trabalhos relacionados apresentados percebe-se uma preocupação com a interoperabilidade entre sistemas. Os modelos propostos são baseados em certificados digitais, e em modelos como estes faz-se necessária a utilização de leitoras de *smart tokens* para realizar de autenticações. Leitoras como estas possuem baixa interoperabilidade entre sistemas operacionais. Além do mais, os dispositivos como notebooks, *tablets* e *smartphones*, utilizados para acessar o STT/SC, normalmente não dispõem de leitoras deste tipo. Desta forma, a utilização de leitoras de *tokens* criptográficos acabam prejudicando uma das principais características dos sistemas *web*: a mobilidade.

Uma das alternativas para resolver o problema das leitoras é utilizar

certificados e chaves em *software* (também citado nos trabalhos apresentados), que mantém o modelo interoperável e móvel, porém diminuem o nível de segurança que se pode prover. Uma vez que, dependendo da forma com que o par de chaves é armazenado, o esforço computacional empregado para obter a chave privada é similar ao de ataque de um modelo que se utiliza de senha simples, uma vez que esta somente é protegida por uma senha.

Outros trabalhos relacionados apresentados seguem outra linha utilizando-se de biometria como o segundo fator de autenticação. A leitura de uma impressão digital também é feita através de um *hardware* específico que possui problemas similares aos das leitoras de *smart tokens*. Neste modelo um usuário comum (paciente/médico) é forçado a utilizar um computador que satisfaça todos os requisitos operacionais de instalação da leitora, que, normalmente, são mais restritivos do que os de leitoras de *smart tokens*. Além do mais, biometria ainda possui uma taxa de falsos positivos e negativos mais alta do que o aceitável. Ou seja, os casos onde uma impressão digital inválida é aceita, e onde uma impressão válida é rejeitada acontecem em uma frequência mais alta do que o aceitável.

O sistema de autenticação não deve restringir ou bloquear o trabalho de um profissional de saúde, por que isso pode por a vida de pacientes em risco. Além do mais, um usuário deve ser capaz de acessar o sistema de telemedicina de qualquer computador ou dispositivo móvel, desde que este possua conexão com a *internet*. Por causa desta exigência foi possível identificar o primeiro requisito: mobilidade. Para cumprir com o requisito ”mobilidade”a adoção de métodos de autenticação que requeiram *hardware* criptográfico, e que precisem de leitoras específicas, como *smart card* e biometria, é inviabilizada. Normalmente este tipo de leitora possui baixa compatibilidade com diferentes dispositivos (computadores, *tablets* e *smartphones*).

Além do mais, percebeu-se que há casos onde o acesso ao sistema é urgente e, nesses casos, o usuário não deve ter seu acesso negado. Assim, da mesma forma que o dispositivo utilizado para acessar o sistema não pode ser limitante, os dispositivos utilizados como fatores de autenticação também não o podem. E este foi o segundo requisito do modelo de autenticação encontrado: flexibilidade.

*Tokens* criptográficos são dispositivos muito específicos, e podem ser mais facilmente perdidos ou esquecidos quando comparados a outros dispositivos de maior valor agregado. Desta forma, neste trabalho procura-se evitar a utilização de *hardwares* específicos e tenta-se substituí-los por outros dispositivos de uso diário, como celulares e *smartphones*. Além do mais, o requisito de flexibilidade também diz respeito a usuários serem capazes de acessar o sistema mesmo quando eles não estão em posse de qualquer dispositivo requerido. O modelo deve prever esse tipo de situação e oferecer alternativas.

Tabela 2: Requisitos suplementares de um modelo de autenticação

| **Requisito Suplementar** | **Descrição** |
|---|---|
| Mobilidade | O modelo de autenticação deve manter a mobilidade dos usuários, sem interferir ou bloquear o trabalho dos profissionais de saúde. Nenhuma tecnologia que impeça ou atrapalhe o uso do sistema deve ser utilizada. |
| Flexibilidade | O modelo de autenticação deve prover alternativas para usuários que não estão de posse de qualquer tipo de *token* exigido. |

Um resumo dos requisitos suplementares é apresentado na Tabela 2.

O levantamento de requisitos se estendeu por mais duas iterações com incrementos de requisitos funcionais e não-funcionais. Estas iterações são apresentadas nas próximas duas sub-seções.

### 4.1.1 Iteração 1: Biblioteca de Autenticação

Além dos dois requisitos apresentados na seção anterior, foram considerados os requisitos comuns a projetos de processos de autenticação, que não serão detalhados por serem de conhecimento geral, mas serão apresentados adiante. A partir destes desenvolveu-se uma primeira proposta: uma biblioteca de *software* dedicada a autenticação de usuários.

Os requisitos comuns a outros projetos não serão tratados separadamente pois são bastante intuitivos, como: autenticar usuários; verificar credenciais; etc. Além do mais, eles serão apresentados juntamente com os requisitos específicos deste trabalho ao decorrer da seção.

A primeira proposta prevê o desenvolvimento de uma biblioteca de *software* responsável por prestar serviços em um processo de autenticação. Para tal, a biblioteca disponibiliza um conjunto de métodos de autenticação. Neste modelo fica a cargo do sistema a forma com que estes métodos são utilizados.

Todos os métodos de autenticação envolvidos nesta proposta são utilizados como um segundo fator da autenticação, ou seja, no novo modelo o usuário se autentica da mesma forma que fazia anteriormente e, num segundo passo, informa algum dado que prove que ele tem a posse de determinado dispositivo único (*token*). Os métodos de autenticação utilizados foram selecionados de forma a não atrapalhar a característica de mobilidade do STT/SC,

Tabela 3: Requisitos funcionais da biblioteca de autenticação

| **Requisito Funcional** | **Descrição** |
|---|---|
| Autenticar um usuário. | A biblioteca deve ser capaz de autenticar um usuário. |
| Permitir a alteração do modo de autenticação de um usuário. | A biblioteca deve permitir que um usuário altere o método de autenticação solicitado caso este esteja impossibilitado de autenticar-se com o atual. |
| Permitir a alteração da política de autenticação do sistema. | A biblioteca deve prover meios para alterar a forma com que os métodos de autenticação são exigidos (prioridades e agrupamentos). |
| Permitir a priorização de modos de autenticação do sistema. | A biblioteca deve prover meios para alterar a ordem em que os métodos de autenticação são exigidos (prioridades). |

ou seja, cumprir com o primeiro requisito. Desta forma, foi necessário utilizar *tokens* comuns como *smartphones* e telefones fixos ao invés de *tokens* criptográficos. Além disso, não são utilizados métodos de autenticação dependentes de hardware de leitura como *smart cards* e biometria de forma geral.

Desta forma, cada usuário do sistema passa a se autenticar não somente com a sua senha, mas também um segundo fator escolhido de uma lista de fatores disponibilizados pela biblioteca e de acordo com a sequência especificada pelo sistema. Para isto, se fez necessário criar o que chamamos neste trabalho de política de autenticação do sistema. A política é uma lista de métodos de autenticação ou agrupamentos dos mesmos, ordenados pela sua prioridade no sistema. Ou seja, quando o sistema possui uma política definida, o usuário se autentica com o método de autenticação definido como o mais prioritário, e que tende a ser o método considerado mais seguro. Nesta proposta, ainda é possível exigir que o usuário se autentique com uma combinação de mais de um método, desde que a política especifique um agrupamento (sub-conjunto) de métodos de autenticação como o mais prioritário.

A Tabela 3 descreve os requisitos funcionais identificados nesta primeira proposta, enquanto a Tabela 4 descreve os requisitos não-funcionais.

Mesmo quando a forma de autenticação definida como a mais prioritária é realizada através da utilização de um dispositivo comum, como um *smartphone*, não se pode assumir que todos os usuários do sistema possuem tal dispositivo a sua disposição quando da autenticação. Desta forma, um usuário que não o possuir não deve ser prejudicado. Para que isso não

Tabela 4: Requisitos não-funcionais da biblioteca de autenticação

| Requisito Não-Funcional | Descrição |
|---|---|
| A biblioteca deve suportar múltiplas formas de autenticação. | A biblioteca deve disponibilizar alternativas de autenticação para casos onde o usuário está impossibilitado de autenticar-se com outro método. |
| A biblioteca deve ser desenvolvida na linguagem PHP. | A biblioteca deve ser desenvolvida da linguagem de programação PHP, de forma a prover total integração com o STT/SC. |

aconteça, a biblioteca prevê a alteração do método de autenticação para um menos prioritário (que normalmente depende de outro tipo de dispositivo) sem impactar na autenticação do usuário. Por exemplo, inicialmente é utilizado um segundo fator de autenticação que se vale de um dispositivo como um *smartphone*. Na medida que o usuário médico não dispõe do dispositivo, ele ainda pode relaxar o requisito, usando outro segundo fator. E, em último caso, o usuário não realiza o segundo passo da autenticação, ou seja ele se autentica utilizando somente seu *login* e senha que já foram fornecidos no primeiro passo. Portanto, o modelo preserva a característica de mobilidade e de flexibilidade do sistema, não impedindo o acesso dos seus usuários, conforme definido no requisito ”Flexibilidade”.

O cenário apresentado acima cumpre os requisitos citados anteriormente e se adequa bem a casos onde o usuário não tem como usar o seu *smartphone*. Porém, não se adequa muito bem a casos onde o usuário faz acessos constantes ao sistema, uma vez que isso implica na mudança de método de autenticação em cada acesso. Estas preocupações com a usabilidade do sistema foram levantadas na segunda iteração da etapa do levantamento dos requisitos. A segunda iteração desta etapa é descrita na seção seguinte.

### 4.1.2 Iteração 2: Serviço de Autenticação

Na segunda iteração do processo de levantamento de requisitos surgiu a preocupação com a usabilidade do sistema. Quando os sistemas eletrônicos adotam processos muito complexos e burocráticos a tendência é que os seus usuários acabem rejeitando-os (ALZOMAI et al., 2008). Por vezes, o sistema acaba caindo em desuso por falta de usabilidade. Desta forma, adicionou-se aos requisitos suplementares (limitantes) a usabilidade. O modelo deve se adaptar aos usuários, interferindo o mínimo possível na rotina atual destes. A

Tabela 5: Requisitos específicos de um modelo de autenticação em ambientes médicos

| **Requisito Suplementar** | **Descrição** |
|---|---|
| Mobilidade | O modelo de autenticação deve manter a mobilidade do sistema de telemedicina, sem interferir ou bloquear o trabalho dos profissionais de saúde. Nenhuma tecnologia que impeça ou atrapalhe o uso do sistema deve ser utilizada. |
| Flexibilidade | O modelo de autenticação deve prover alternativas para usuários que não estão de posse de qualquer tipo de *token* exigido. |
| Usabilidade | O modelo deve se adaptar aos usuários, interferindo o mínimo possível na rotina atual destes. |

Tabela 5 mostra os requisitos suplementares da iteração 2.

Nesta iteração foi concebido o segundo modelo de forma a atender não somente aos requisitos definidos para o primeiro, como também a se preocupar com o impacto na usabilidade do sistema. Para tal foi concebida uma nova estratégia: cada usuário possui uma lista de métodos de autenticação habilitados. Desta forma o usuário mantém desabilitado os métodos que utilizam dispositivos que ele não possui, e evita a alteração do método em cada autenticação. Este novo modelo passou a guardar um volume de informações muito maior com a inclusão dos usuários e das diversas combinações de métodos de autenticações que estes podem possuir. Desta forma, deixou de se comportar como uma biblioteca, pois possuía contexto próprio.

Neste trabalho optou-se por seguir com a abordagem de serviço *web* de autenticação para tornar a solução independente do STT/SC. Ao mesmo tempo, ainda é possível utilizá-lo localmente com políticas de acesso restritas, fazendo-o agir como um *framework* local.

A alteração para um serviço *web* de autenticação ainda trouxe algumas vantagens além da melhoria na usabilidade. Com a nova abordagem passa a ser possível utilizar o modelo em qualquer sistema, sem depender de linguagem e arquitetura de *software*, bastando implementar uma chamada a um *web service* seguindo padrões de protocolos recomendados pela W3C (do inglês *World Wide Web Consortium*) (World Wide Web Consortium, 2013). Além disso, nesse modelo, a mudança do método de uma autenticação é um processo esporádico, e é registrado pelo serviço. Assim, o sistema utiliza este registro da forma que preferir, podendo até bloquear o acesso de um usuário,

Tabela 6: Requisitos funcionais do serviço de autenticação

| **Requisito Funcional** | **Descrição** |
|---|---|
| Autenticar um usuário. | O serviço deve ser capaz de autenticar um usuário. |
| Permitir a alteração automática do modo de autenticação. | O serviço deve alterar automaticamente o método de autenticação caso o usuário não consiga autenticar-se com o atual. |
| Permitir a alteração do modo de autenticação pelo usuário. | O serviço deve permitir que um usuário altere o método de autenticação solicitado caso este esteja impossibilitado momentaneamente de autenticar-se com o atual. |
| Permitir a alteração da política de autenticação do sistema. | O serviço deve prover meios para alterar a forma com que os métodos de autenticação são cobrados (prioridades e agrupamentos). |
| Permitir a priorização de modos de autenticação do sistema. | O serviço deve prover meios para alterar a ordem em que os métodos de autenticação são cobrados (prioridades). |
| Cadastro e manutenção de usuários. | O serviço deve prover meios para (des)associar usuários aos métodos de autenticação que estes estão habilitados a utilizar. |
| Registrar formas de acesso de um usuário. | O serviço deve registrar que um usuário alterou o método de autenticação solicitado para um menos prioritário. |

se for detectado um possível ataque.

A tabela 6 descreve os requisitos funcionais identificados no segundo modelo, enquanto a tabela 7 descreve os requisitos não-funcionais.

Outra vantagem deste modelo sobre o primeiro é a automatização da mudança de método de autenticação. O *web service* utiliza a política e a lista de métodos que o usuário possui para montar uma terceira lista com a intersecção das duas ordenadas da mesma forma que a política. Além da predição do método, baseado nesta terceira lista, ainda é possível analisar se os métodos que dependem de acesso à internet estão online, evitando tentativas que resultariam em falha. Dessa forma, cada um dos três requisitos suplementares foi abordado neste modelo. A mobilidade e a flexibilidade são características herdadas do primeiro modelo e o impacto na usabilidade é reduzido através do uso de uma lista de métodos de autenticação.

Tabela 7: Requisitos não-funcionais do serviço de autenticação

| **Requisito Não-Funcional** | **Descrição** |
|---|---|
| O serviço deve suportar múltiplas formas de autenticação. | O serviço deve disponibilizar alternativas de autenticação para casos onde o usuário está impossibilitado de autenticar-se com outro método. |
| O serviço deve funcionar como um *web service*. | O serviço deve ser desenvolvido utilizando protocolos de *web service*, de forma a prover total integração com o STT/SC. |

## 4.2 MÉTODOS DE AUTENTICAÇÃO

Neste trabalho, propomos o uso de três métodos de autenticação: a) One-time Password; b) Contrassenha via SMS; e c) Identificação de chamadas telefônicas. Esses métodos foram escolhidos devido aos fatores usabilidade, maior nível de segurança e de baixo custo, conforme o estudo realizado que apresentado no Capítulo 3. Embora o último método pareça ferir o requisito de mobilidade, este foi escolhido por dois principais motivos: 1) sem perda de nenhuma des suas características, o método pode ser utilizado com telefones celulares, sem interferir em nada no requisito de mobilidade; 2) embora requeira infraestrutura bastante parecida, este método apresenta uma vantagem estratégica sobre o baseado em contrassenhas via SMS em questões de custo. Uma vez que o sistema não precisa executar nenhuma chamada, o custo de sua manutenção é bastante menor.

- *One-Time Password*: Para este trabalho foi desenvolvido um aplicativo pelo Laboratório de Segurança em Computação (LabSEC) com base no *Google Authenticator* (IDALINO; SPAGNUELO, 2012). O Google *authenticator* é um *Single-factor OTP device*, que utiliza senhas únicas para provar a posse de um *smartphone*. Segundo o Guia do NIST, este tipo de *token* atinge o nível 2 de garantia/segurança. Porém, como o aplicativo LabSEC *authenticator* foi alterado para utilizar um PIN para o seu desbloqueio, podemos considerar este *token* como *Multi-factor OTP device*. De acordo com o NIST, dispositivos que se utilizam de mais de um fator podem ser considerados mais seguros. Neste caso, o nível de segurança sobe para 3 pois o *token* combina um PIN (algo que se sabe) com a prova de posse do dispositivo (algo que se possui). Por se utilizar de *smartphone*, nenhuma infra-estrutura física é adicionada ao processo quando os usuários já os possuem. Além do mais, este método possui a vantagem de não utilizar o pacote de dados do

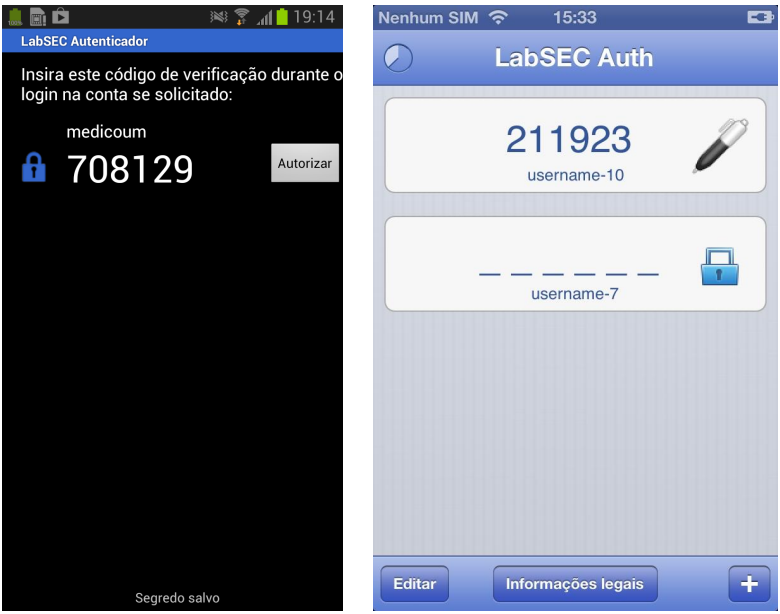


Figura 4: LabSEC Authenticator versão Android e iOS

*smartphone* do usuário, sendo completamente *offline* e gratuito. Imagens do aplicativo podem ser vistas na Figura 4.

- Contrassenha via SMS: Similarmente ao método anterior, o método de contrassenhas pode atingir o nível 3 se o celular for bloqueado por PIN. Este método não exige que os usuários possuam *smartphones* para sua utilização; celulares comuns já são suficientes. Além disto, este é um token *Out of Band* que, segundo o manual de Autenticação para *Internet Banking*, pode ser definido como sendo uma técnica de autenticação que permite que a identidade do usuário que originou a operação possa ser verificada por meio de um canal diferente. O fato deste método ser *Out of band* é bastante importante pois faz com que um possível atacante tenha que dominar dois diferentes canais de comunicação para realizar o ataque. Neste caso, um ataque é muito mais complexo e mais difícil.

- Identificação de chamadas telefônicas: O método de autenticação através de chamadas telefônicas também é *Out of Band*. Embora este método

não não seja explicitamente classificado pelo documento do NIST, podemos classificá-lo com um nível bastante próximo ao do método anterior, uma vez que o modelo de ataque de ambos é muito similiar. A vantagem deste método está em não exigir um tipo de dispositivo específico, bastando somente a posse de uma linha telefônica e de um telefone. O fato do usuário ter executado uma chamada para um dos números autorizados do sistema é a própria prova da posse do *token* do segundo fator, neste caso um celular ou telefone fixo. Outra vantagem é o baixo custo do método, tanto para o sistema, quanto para os usuários, que por vezes acabam não pagando pelas ligações.

## 4.3 MODELAGEM

A especificação do serviço web de autenticação foi feita em duas etapas: a modelagem de processos de negócio; e a modelagem de *software* em si. Para cada uma das modelagens utilizou-se uma notação diferente. A primeira mais direcionada as funcionalidades do serviço, descreve o modelo de negócios. A segunda, mais voltada a componentes de *software* e a forma com que estes se comunicam para atender as funcionalidades definidas pela primeira modelagem.

Os processos de negócio foram modelados utilizando a notação BPMN (do inglês *Business Process Model and Notation*) (Object Management Group, Inc., 2011a). Segundo a própria documentação da notação, o principal objetivo da BPMN é prover uma documentação de fácil compreensão, tanto para usuários quanto para analistas. Os diagramas que utilizam a notação BPMN descrevem os passos necessários para realizar determinadas tarefas, sem se preocupar com a informatização do processo.

A modelagem de software foi realizada utilizando-se diagramas de classes e de atividades da linguagem UML (do inglês *Unified Modeling Language*) (Object Management Group, Inc., 2011b). Esta modelagem, embora implemente os processos de negócio descritos na primeira, difere da primeira pois descreve em detalhes os elementos de software e a interação entre estes.

As seções seguintes descrevem melhor cada uma das modelagens.

### 4.3.1 Modelagem de negócio

O principal modelo mostra o processo de autenticação de um usuário de forma geral e pode ser visto na Figura 5. Em um primeiro momento, o usuário deve se identificar perante o sistema. Conhecendo o usuário, o

sistema pode então verificar quais métodos de autenticação este está habilitado a utilizar, e quais destes estão disponíveis. Ou seja, se algum destes métodos depender da internet, pode-se verificar se este está online. Com esta informação, o serviço consegue filtrar os métodos de autenticação passíveis de utilização. Estes métodos são ordenados da mesma forma que a política do sistema, ou seja, ao final define-se uma lista de métodos de autenticação disponíveis ordenados pela sua prioridade. Logo em seguida o usuário é requisitado a realizar autenticação com o método mais prioritário da lista gerada. Caso o usuário esteja possibilitado de autenticar-se com este método, então o processo de autenticação é iniciado. Caso contrário, o usuário solicita a alteração do método de autenticação para um menos prioritário. Este último passo é repetido até que o usuário esteja possibilitado de autenticar-se. O último passo do processo é a verificação das credenciais apresentadas, caso sejam válidas o usuário se autentica com sucesso.

Neste processo destacam-se dois importantes passos. O primeiro deles é o passo de identificação do usuário. Embora somente a apresentação de algo (alguma informação) que identifique o usuário seja suficiente, aconselha-se a realizar uma autenticação simples com nome de usuário e senha, de forma a transformar o processo em uma autenticação de múltiplas etapas. O segundo é a verificação da possibilidade do usuário se autenticar com o método mais prioritário. A primeira característica importante é que esta tarefa é executada pelo usuário. Neste ponto o serviço já verificou se os métodos que o usuário possui cadastrados estão tecnicamente disponíveis (online). Desta forma, a degradação só ocorrerá se o usuário não estiver, momentaneamente, possibilitado de autenticar-se com o método sugerido. Ao usuário é imputado a resposabilidade sob o método de autenticação escolhido. O sistema de autenticação simplesmente informa ao usuário o método de autenticação mais seguro e apropriado. Se o usuário decidir não seguir esta recomendação, deve estar ciente das possíveis consequências desse ato. Sendo a principal delas o possível bloqueio do usuário. A possibilidade de se usar um método mais simples de autenticação existe para os casos emergenciais, onde o acesso ao sistema é necessário mas o usuário não está com o *token* exigido. Porém, por ser uma degradação de prioridade, toda vez que um usuário a solicita, ela é registrada pelo serviço, e esta é a segunda característica importante deste passo. O serviço permite que o sistema defina quais comportamentos são toleráveis, garantindo a flexibilidade do modelo. Neste caso, o sistema define quantas degradações podem ser realizadas antes do bloqueio do usuário.

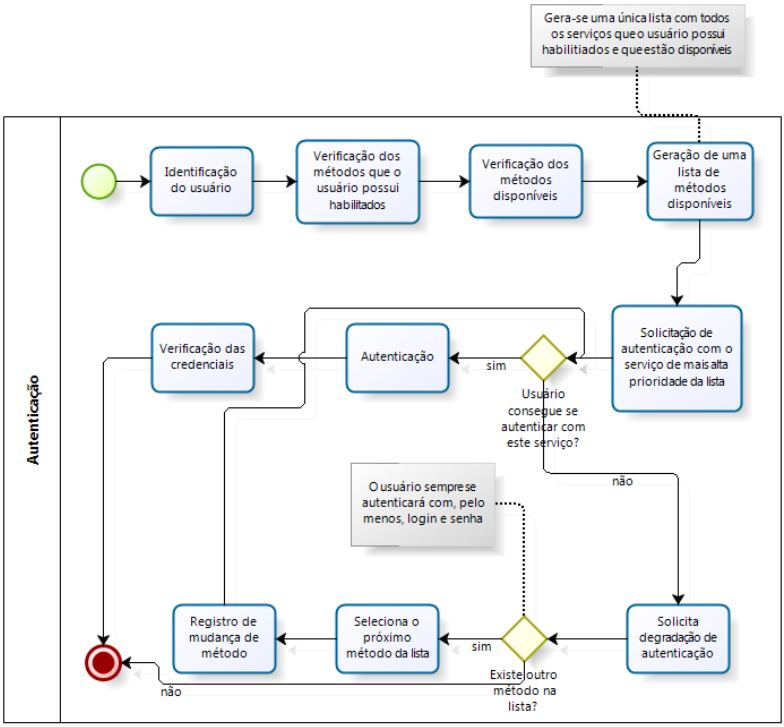


Figura 5: Fluxograma de autenticação de um usuário

### 4.3.2 Modelagem de software

A modelagem de *software* iniciou com uma primeira versão do diagrama de classes. Nesta primeira versão definiu-se o modelo de dados e as classes responsáveis pelo funcionamento do serviço: *Authenticator* e *ServiceManager*. O diagrama de classes pode ser visto na Figura 6.

O modelo de dados inclui os modelos de usuários (*Users*), dos métodos de autenticação que o serviço dispõe (*AuthTypes*), da política (*Policy*), dos métodos de autenticação habilitados para cada usuário (*UserAuthType*) e dos registros de eventos relativos a autenticação (*Logs*).

O modelo da política guarda, além de um combinado de métodos de autenticação ordenados pela prioridade, a quantidade máxima (*maxWeakAuth*) de degradação de método de autenticação tolerada. Esta quantidade é definida pelo sistema e ajuda a garantir a flexibilidade sem prejudicar a segurança. Ou seja, o sistema define uma quantidade de autenticações não prioritárias que um usuário pode realizar sem caracterizar um ataque. Cada usuário possui a contagem de quantidade de vezes que reduziu a prioridade da autenticação (*weakAuthCounter*). Quando um usuário atinge o número máximo de reduções, o serviço avisa o sistema. Cabe ao sistema definir qual medida será tomada. Esta pode ser desde a reinicialização da contagem, até o bloqueio definitivo do usuário.

A contagem de redução de prioridade somente ocorre quando o usuário solicita a redução. Ou seja, é em relação aos métodos que o usuário possui habilitados (dados do modelo *UserAuthType*). Se o serviço automaticamente reduz a prioridade porque o usuário não possiu habilitado o método mais prioritário, a contagem não é realizada.

O serviço possui o registro de todos os métodos de autenticação (*AuthTypes*) que este dá suporte. Cada método de autenticação possui um nome (*name*) que o identifica, um endereço (*address*) que é usado somente para métodos de autenticação que dependem de serviços *online*, e um sinalizador que indica se o método está habilitado ou não (*enabled*). O sistema deve definir quais métodos de autenticação estão habilitados. Ou seja, que estão disponíveis para ser utilizados por seus usuários.

Por fim, o serviço também possui registro de todos os eventos relacionados com a autenticação (*Logs*). Cada registro possui o identificador do usuário que realizou o evento (*userId*), uma mensagem (*message*) que descreve o evento, a estampa de tempo do horário em que o evento aconteceu (*timestamp*), e um código (*code*) que classifica o evento em tipos. Os tipos de eventos podem ser desde emergenciais, onde não é possível utilizar serviço de autenticação, até informativas.

O funcionamento do serviço depende diretamente das classes *Authen-*

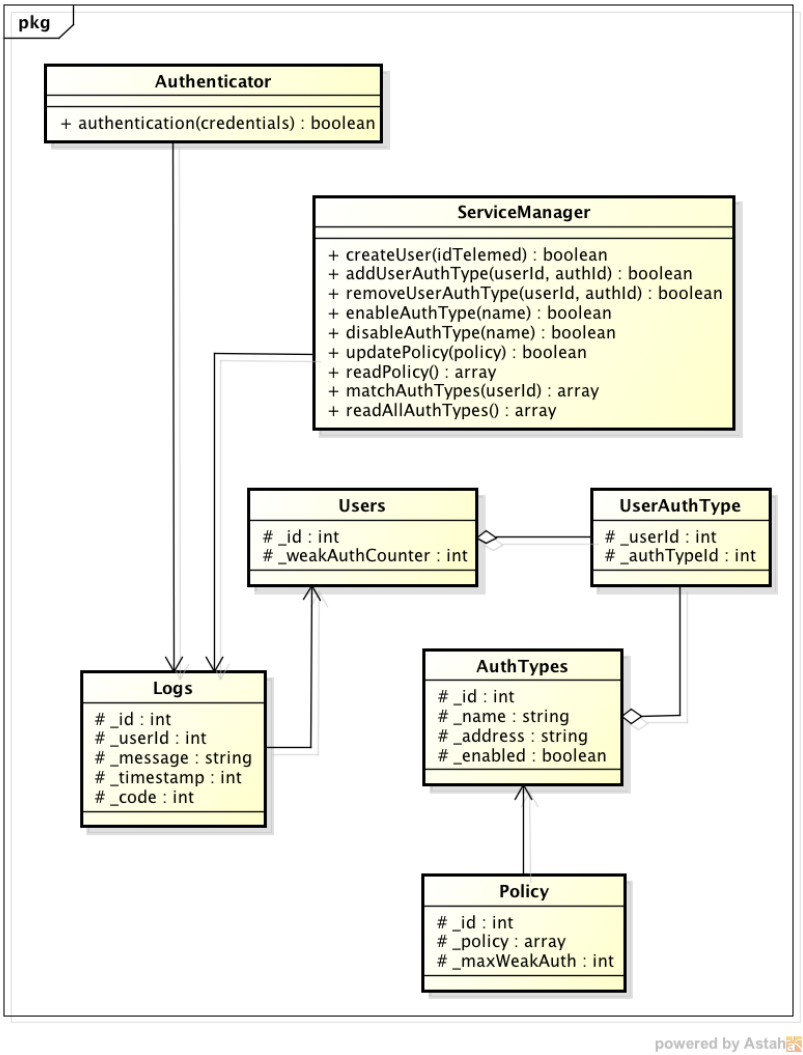


Figura 6: Diagrama de classes do serviço

*ticator* e *ServiceManager*. A primeira é responsável pela autenticação usuários em si. A segunda dá suporte as atividades de manutenção do serviço, como o cadastro de novos usuários (*createUser*), a habilitação e desabilitação de métodos de autenticação (*enableAuthType* e *disableAuthType*), e a alteração da política (*updatePolicy*). Além disto, a classe *ServiceManager* também é responsável pela geração da lista de métodos de autenticação disponíveis para cada usuário (*matchAuthTypes*).

O funcionamento do serviço de autenticação de usuários pode ser visto na Figura 7. Neste diagrama é apresentado o processo completo de autenticação, e como o sistema de telemedicina interage com cada uma das classes definidas. Em um primeiro momento o usuário realiza uma autenticação simples, com seu usuário e senha. Quando o STT/SC recebe estas credenciais, além de realizar a primeira etapa da autenticação, ele também identifica o usuário que está realizando o processo. Desta forma, o STT/SC consegue solicitar ao *ServiceManager* a lista de métodos de autenticação que este usuário específico está habilitado a utilizar.

A segunda etapa da autenticação inicia quando o STT/SC recebe a lista solicitada. O sistema de Telemedicina solicita que o usuário autentique-se com o primeiro método da lista (mais prioritário). Quando o usuário está impossibilitado de autenticar-se com o método solicitado, ele informa o sistema e, então, a mudança é realizada. Este processo é repetido até que o usuário consiga se autenticar. Por fim, quando a segunda etapa da autenticação é realizada o *Authenticator* é utilizado. Quando este recebe uma solicitação de autenticação, ele verifica com o *ServiceManager* se esta é uma autenticação menos prioritária. Caso seja, o *ServiceManager* a registra no contador de autenticações fracas do usuário (*weakAuthCounter*).

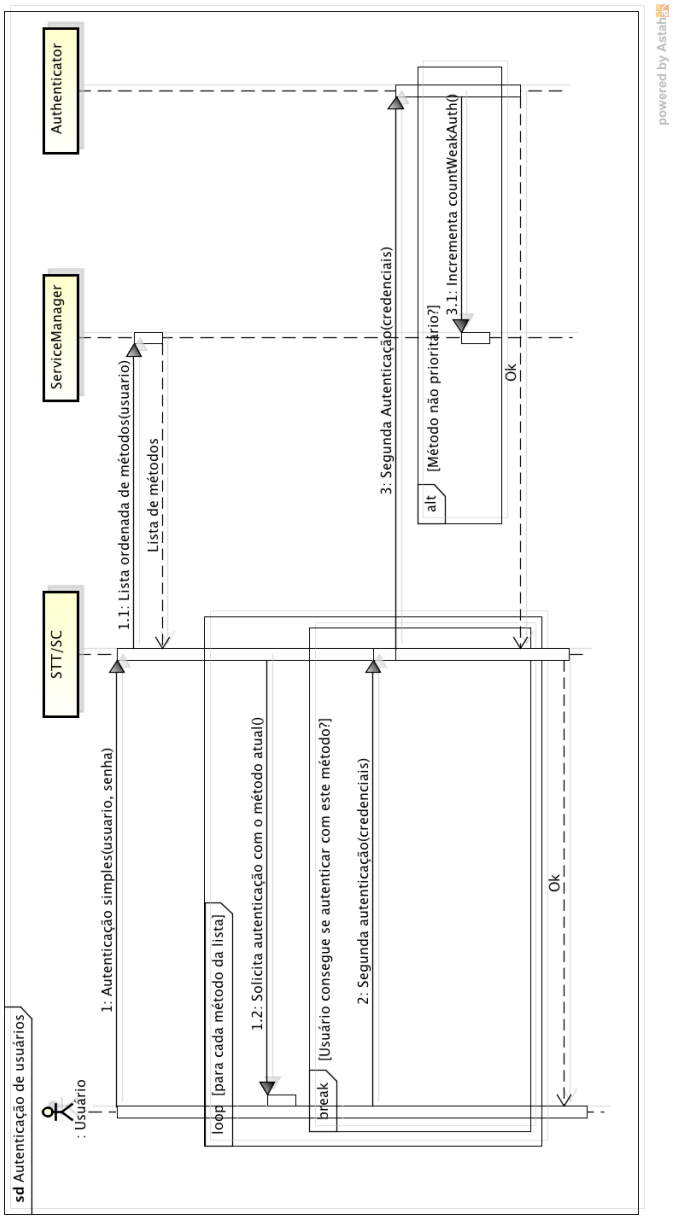


Figura 7: Diagrama de sequência do processo de autenticação de um usuário

O modelo proposto foi implementado como um *web service* seguro baseado nos padrões de Chamada de Procedimento Remoto (RPC, do inglês *Remote Procedure Call*). Os detalhes desta implementação serão tratados no capítulo seguinte.

# 5 IMPLEMENTAÇÃO DO PROTOCOLO MULTI-FATOR FLEXÍVEL

O serviço foi construído com base nos padrões de Chamada de Procedimento Remoto (RPC) (BIRRELL; NELSON, 1984). De acordo com os autores, o RPC é baseado na observação de que chamada de procedimentos são mecanismos bem conhecidos para transferência de controle e dados em programas rodando em um único computador. A proposta do RPC é estender este mecanismo para transferência de controle e dados pela *internet*. Similarmente a chamadas de procedimento locais, quando uma RPC é requisitada, o ambiente que chama normalmente é suspenso até que receba uma resposta. O ambiente que recebe a chamada executa o procedimento solicitado e retorna o resultado pela *internet*.

Na implementação foi utilizado o XML-RPC, um padrão simples de RPC, que provê um mecanismo baseado em XML e HTTP. XML-RPC surgiu em 1998 e desde então se mostrou bastante estável. Neste padrão, a natureza da requisição e a respostas das chamadas são codificadas em um XML. Ou seja, o cliente especifica o nome do procedimento e os parâmetros em um XML de requisição, e o servidor retorna tanto falhas quanto respostas no XML de resposta (CERAMI, 2002). Os parâmetros do XML-RPC são uma lista simples de tipos e conteúdos. Não há a noção de objetos neste modelo. *Structs* e *arrays* são os tipos mais complexos existentes.

Ao mesmo tempo que o XML-RPC pode parecer meio limitado para algumas aplicações, sua simplicidade acaba sendo uma grande vantagem no universo computacional (CERAMI, 2002). O fato do objetivo do serviço ser somente a autenticação de usuários contribuiu bastante na escolha do protocolo de serviço a ser utilizado. O uso de um protocolo mais simples evita transformar a autenticação de usuários, que carregam somente suas credenciais, em um processo complexo e demorado.

Como na resto da *internet*, a publicação de um *web service* significa que é possível ter controle do ambiente do servidor, mas não necessariamente do cliente e do canal (CERAMI, 2002). Desta forma, o uso de HTTPS foi necessário para evitar que as credenciais de usuários trafegassem na rede desprotegidos durante as comunicações entre o STT/SC e o *web service*. Optou-se utilizar o HTTPS mutualmente autenticado para evitar que atacantes façam operações em nome do STT/SC, assim somente sistemas autorizados conseguem se comunicar com o serviço e, neste contexto, somente o STT/SC é autorizado.

As chamadas de procedimentos de autenticação de usuários são compostas pelo nome do procedimento, um identificador do usuário e alguma

informação que prove a posse de um token, ou seja, normalmente uma senha. Com estas informações é montado um XML no padrão do XML-RPC, que é enviado pela rede, do cliente para o servidor do serviço *web*. Um exemplo de um XML de chamada é apresentado a seguir.

```
<!--?xml version="1.0"?-->
<methodcall>
  <methodname>
    cs.otpAuthentication
  </methodname>
  <params>
    <param>
      <value><int>123</int></value>
    </param>
    <param>
      <value><int>123456</int></value>
    </param>
  </params>
</methodcall>
```

As respostas de cada procedimento de autenticação foram definidas como uma tupla de 3 valores: um valor booleano que indica se a autenticação ocorreu com sucesso; uma mensagem de texto que contém a causa de possíveis falhas; e um código numérico que identifica esta mensagem. O código numérico possui 3 dígitos sendo o primeiro **6** quando tudo ocorreu com sucesso, e **7** quando ocorreu algum problema. Os dois outros dígitos são identificadores sequenciais. Um exemplo de XML de resposta é apresentado a seguir.

```
<methodresponse>
 <params>
  <param>
    <value><array>
      <data>
        <value><boolean>0</boolean></value>
        <value><int>724</int></value>
        <value>
          <string>
            Username or OTP incorrect!
          </string>
        </value>
      </data>
    </array></value
 </params>
```

```
16 </methodresponse>
```

A figura 8 mostra a estrutura de camadas do serviço *web* de autenticação. Uma versão mais completa do diagrama de classes pode ser visto na Figura 9.

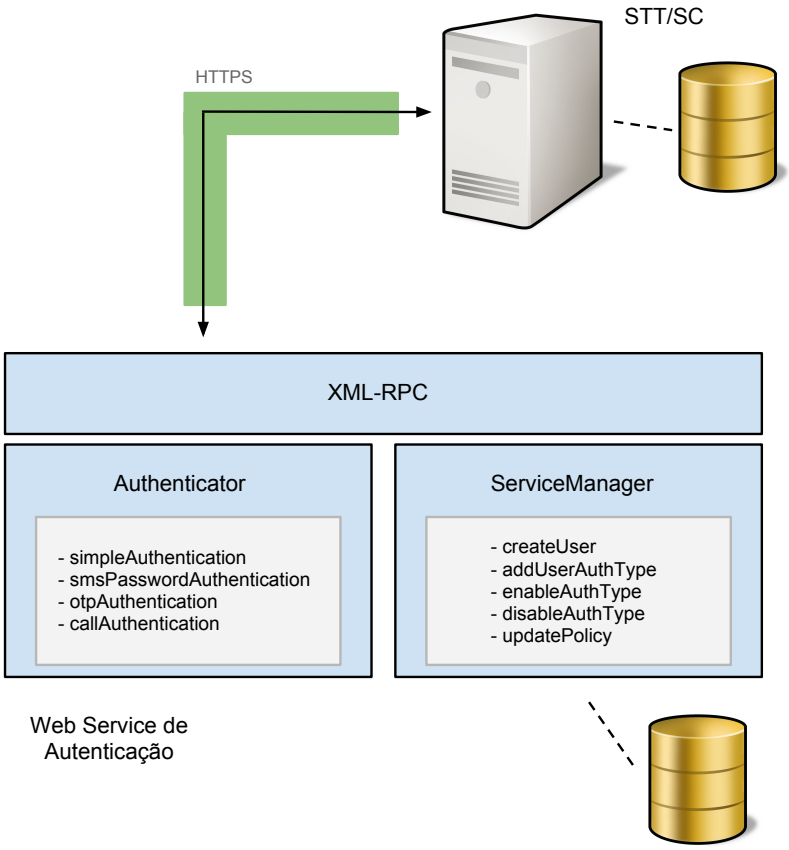


Figura 8: Diagrama de camadas do serviço de autenticação

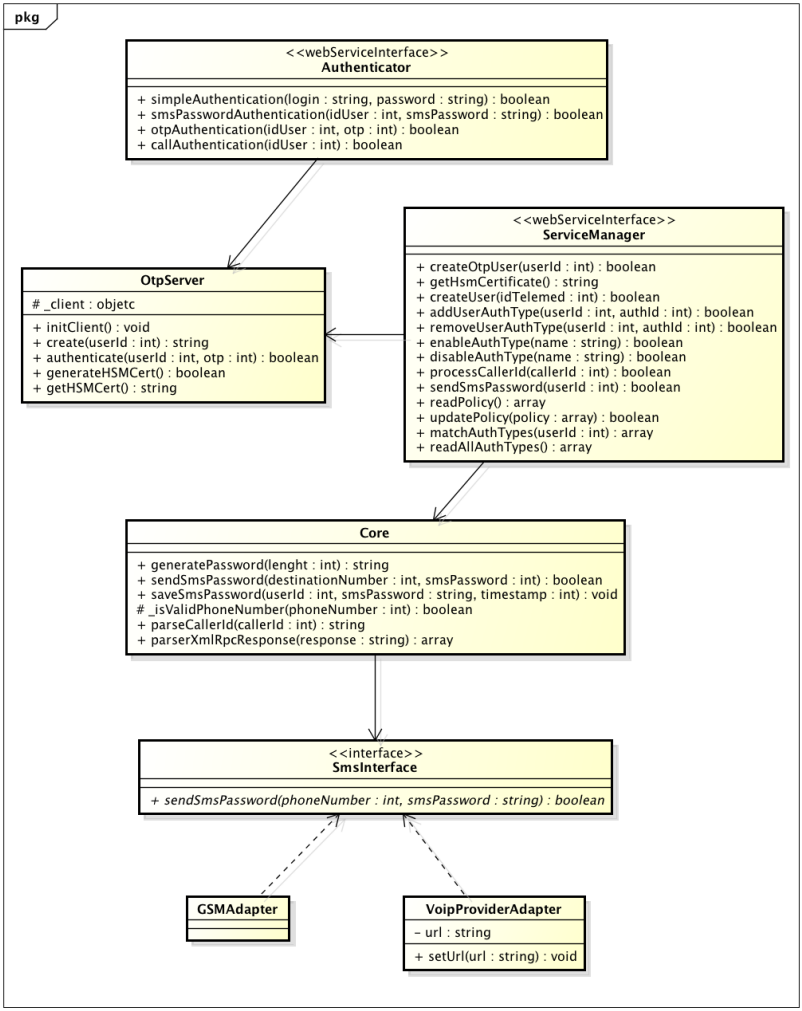


Figura 9: Diagrama de classes do serviço web

# 6 ANÁLISE

Neste capítulo apresenta-se uma análise dos aspectos de segurança e de usabilidade de cada uma das técnicas de autenticação. Também é apresentada uma análise baseada nos aspectos gerais do modelo proposto.

## 6.1 ANÁLISE DOS MÉTODOS DE AUTENTICAÇÃO

No modelo de *One-Time Passwords* utilizamos *smartphones* como geradores de senhas. Por serem dispositivos de uso pessoal, usuários já estão habituados com suas interfaces e formas de interação. Por conta disso, este modelo não causa grande impacto sobre a usabilidade do STT/SC.

*One-Time Passwords* são bastante comuns e muito bem aceitos em ambientes bancários por se tratarem de ambientes com operações de alto risco. Similarmente a ambientes bancários, operações em sistemas de telessaúde também podem ser consideradas de alto risco, uma vez que um ataque pode significar risco à vida. Desta forma a utilização de OTPs em um sistema como este se justifica.

Segundo o manual de autenticação para *Internet Banking* (FFIEC, 2005) geradores de senhas são seguros pela natureza sensível ao tempo ou sincronizada da autenticação. Ainda segundo o manual de autenticação, a aleatoriedade, imprevisibilidade, e a singularidade do OTPs aumentam substancialmente a dificuldade de um atacante obter uma senha. Além disto, o processo de geração de um OTP é *offline* e ataques virtuais só poderiam ser realizados quando a senha for utilizada. Como após sua utilização os OTPs são invalidados, as chances de sucesso de um ataque deste tipo são bastante baixas.

O ataque por adivinhação também possui uma chance de sucesso bastante pequena. Segundo a RFC 4226 (M'RAIHI et al., 2005) a probabilidade de sucesso de uma adivinhação é de:

$$Sec = \frac{s.v}{10^{Digit}}$$

A probabilidade se dá em função do tamanho **s** da janela de ressincronização prevista pelo método, da quantidade **v** de tentativas que um atacante pode fazer ao sistema antes de ser bloqueado, e da quantidade de dígitos que possui o OTP.

Pelo fato de *smartphones* serem de natureza muito pessoal, ataques físicos como roubo seriam facilmente percebidos. Ao contrário de ataques

virtuais, estes normalmente não são discretos, e o usuário, sabendo do ataque e das suas consequências, pode tomar as devidas providências para amenizá-lo. Por exemplo, realizar o cancelamento ou bloqueio temporário de sua conta.

*Smartphones* são aparelhos sofisticados e caros. Desta forma o modelo de autenticação de Contrassenha via SMS vem como uma alternativa de abrangência muito maior que o de OTP. Segundo a Anatel (Agência Nacional de Telecomincações, 2012), a quantidade de contas móveis em maio de 2012 no Brasil é de mais de 254 milhões. Quantia esta maior que o número de habitantes no Brasil que, de acordo com o último Censo (IBGE, 2010), é de cerca de 190 milhões. Desta forma, uma das vantagens do modelo é o fato de que grande parte dos usuários já possui celular. Além do mais, normalmente usuários de celulares já estão habituados com o sistema de SMS.

De acordo com Alzomai et al. (ALZOMAI et al., 2008), a principal vantagem de se utilizar uma autenticação baseada em SMS é que mensagens enviadas passam pela rede de telefonia móvel, que é separada e independente da internet. De acordo com Josang, Zomai e Suriadi (JØSANG; ZOMAI; SURIADI, 2007), a segurança de esquemas como este está baseada na assunção que é difícil para um atacante roubar o celular de uma pessoa ou atacar a rede de telefonia móvel. As chances de sucesso de um ataque por adivinhação são similares às apresentadas no modelo baseado em OTP uma vez que a característica de aleatoriedade também está presente neste modelo.

O modelo de SMS porém possui um custo elevado para o sistema de telemedicina. Cada autenticação requer o envio de uma mensagem e, conforme a quantidade de acessos aumenta, o custo de mantenimento do modelo também aumenta. Como uma alternativa a este custo elevado foi apresentado o terceiro modelo, baseado em chamadas telefônicas.

O modelo baseado em chamadas telefônicas possui as mesmas características do modelo SMS: utiliza-se de dispositivos que os usuários já possuem e já conhecem; utiliza uma rede independente da internet; e possui um nível de segurança também similar. A primeira vantagem deste modelo em relação ao de SMS é que não possui custos para o sistema de telemedicina, e também pode ser um método sem custos para os usuários, dependendo do contrato com a operadora.

## 6.2 ANÁLISE DO MODELO PROPOSTO

O nível de segurança do modelo está bastante atrelado ao nível de segurança provido por cada um dos métodos que este utiliza. Porém os métodos apresentados são somente um dos fatores utilizados na autenticação

dos usuários. De acordo com Petro, Me e Strangio (PIETRO; ME; STRANGIO, 2005), um atacante que conseguisse quebrar algum dos métodos apresentados com sucesso ainda não teria acesso ao sistema de telessaúde sem conhecer as credenciais de login do usuário. Além disso, o modelo apresentado dá ao sistema a liberdade de definir como utilizar os métodos, de forma que se pode exigir a utilização de mais de um por vez, aumentando ainda mais a dificuldade de um ataque.

Como o modelo prevê um processo de autenticação completamente separado das regras de negócio do sistema de telessaúde, é possível aplicá-lo não somente no *login*, mas em áreas críticas do sistema. Ao se aumentar o número de fatores utilizados em uma autenticação, ou a quantidade de sessões que exigem autenticações, aumenta-se o nível de segurança, porém perde-se em usabilidade. De acordo com Alzomai et al. (ALZOMAI et al., 2008), quando usuários encontram tarefas de segurança frustrantes, estes tendem a contorná-las ou ignorá-las. Desta forma, a flexibilidade do modelo mostra-se como uma importante característica, pois permite que o sistema defina onde deseja utilizá-lo, e como utilizá-lo.

A primeira versão do web service foi instalada em uma versão teste do STT/SC. Com auxílio da Secretaria de Saúde do Estado de Santa Catarina, amostras de usuários de diversos municípios foram submetidos a um teste de usabilidade. Com o teste foi obter indicadores para inferência em 3 quesitos: facilidade de uso; segurança; e complexidade do processo. Os quesitos facilidade de uso e complexidade do processo, embora pareçam contraditórios, foram assim definidos na tentativa de identificar se o processo está muito longo e burocrático. Por mais que cada passo do processo seja simples, um processo muito longo pode desmotivar usuários a utilizar o modelo. O quesito de segurança foi assim definido para tentar identificar se os usuários entendem o porque das modificações no processo e se estes se sentem mais seguros com o novo modelo.

O teste foi realizado da seguinte forma: um agente da Secretaria de Saúde do Estado visitava uma instituição (normalmente hospital) parceira do STT/SC, e apresentava o novo modelo para alguns usuários. Em um primeiro momento os usuários realizavam a autenticação com um usuário de teste já cadastrado. Logo em seguida cada um deles era instruído a realizar o cadastro de um novo usuário. Cada usuário respondeu um questionário baseado na Escala de Usabilidade do Sistema (BROOKE, 1996). Este questionário consiste em 17 afirmações que o usuário deve indicar o grau de concordância. Cada afirmação pode ser respondida com um grau de 1 a 5, onde 1 representa a discordância total, e 5 a concordância total. O questionário pode ser visto no Anexo A.

O questionário proposto por John Brooke possui somente 10 afirmações

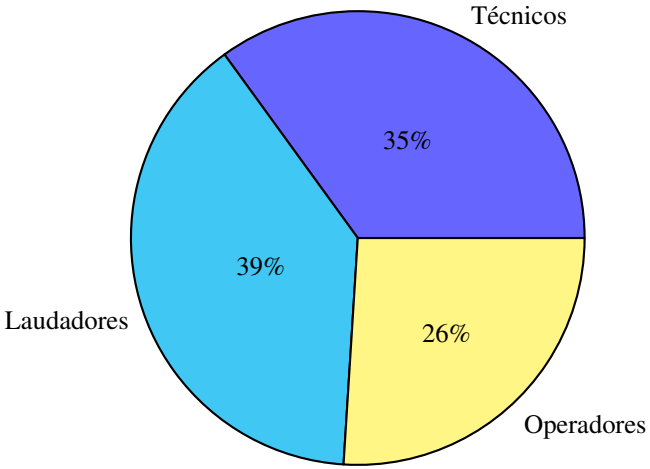


Figura 10: População por perfil

bastante genéricas. Em nosso questionário, foram adicionadas 7 afirmações mais específicas sobre a segurança do processo e a utilização do software do celular (quando necessário). A adição destas afirmações visava, além da própria avaliação, correlacionar alguns comportamentos dos usuários com outras questões do seu cotidiano. Por exemplo, os itens 16 e 17 do questionário, ”Eu considero que conheço novas tecnologias”e ”Eu já conhecia outros sistemas com tecnologias similares”respectivamente, foram assim colocados para tentar relacionar a facilidade de uso do sistema com conhecimentos prévios dos usuários.

A avaliação foi realizada com o apoio de 23 usuários utilizando o método de autenticação baseado em OTP. Estes usuários foram classificados de duas formas diferentes: por idade e por perfil da profissão. A classificação por idade foi feita em duas classes: usuários com até 40 anos; e usuários com 41 anos ou mais. A classificação por perfil da profissão foi feita em três classes: laudadores (em geral médicos e dentistas); operadores (técnicos administrativos, jornalistas e técnicos de informática); e técnicos (enfermeiros, técnicos de enfermagem e técnicos que operam aparelhos de exames). Cada uma das classificações pode ser melhor vista nas Figuras 10 e 11.

Para realizar uma análise comparativa foram definidos valores esperados para cada um dos três quesitos. Para facilidade de uso, espera-se que os usuários mantenham-se na casa da concordância. Desta forma, o valor esperado foi definido como 5. Para a segurança espera-se o mesmo comportamento dos usuários. Assim, o valor esperado para este quesito também

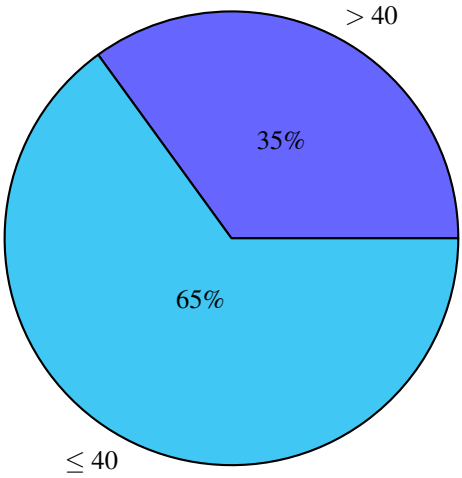


Figura 11: População por faixa etária

foi definido como 5. Quanto a complexidade do processo, espera-se que os usuários mantenham-se na casa da discordância. Assim, o valor esperado foi definido como 1.

A análise é uma comparação entre as respostas para cada um dos grupos de afirmações por perfil de profissão. A tabela 8 mostra os resultados desta análise. Nesta tabela podemos observar que o perfil dos Laudadores e Operadores possuem comportamentos bastante similares, ambos se mantiveram na casa da concordância quanto a facilidade de uso e a segurança do modelo, e na casa da discordância quando questionados sobre a complexidade. Além do mais, estes resultados ficaram suficientemente próximos dos resultados esperados. Os usuários com perfil de Técnico obtiveram uma avaliação pior. Pode-se observar a tendência ao neutralismo nos quesitos de facilidade de uso e complexidade (valores próximos a 3). Embora estes valores ainda estejam na casa da concordância para a facilidade de uso, e discordância para a complexidade, acredita-se que esta classe de profissionais necessite de mais atenção no treinamento de utilização do novo modelo. A Figura 12 mostra graficamente os resultados obtidos.

A mesma análise foi realizada com a classificação dos usuários por idade. A Tabela 9 mostra os resultados desta análise. Nesta tabela observamos um comportamento bastante próximo do esperado nos participantes com até 40 anos de idade. Já os usuários com mais de 40 anos apresentaram resultados que, embora ainda próximos aos esperados, são piores do que

Tabela 8: Análise bivariada por perfil profissional

| **Grupo** | **Laud.** | **Oper.** | **Técn.** | **Valor esperado** |
|---|---|---|---|---|
| Facilidade de uso | 4,51 | 4,35 | 3,9 | 5 |
| Sergurança | 4,28 | 4,42 | 4,13 | 5 |
| Complexidade | 1,29 | 1,20 | 2,28 | 1 |

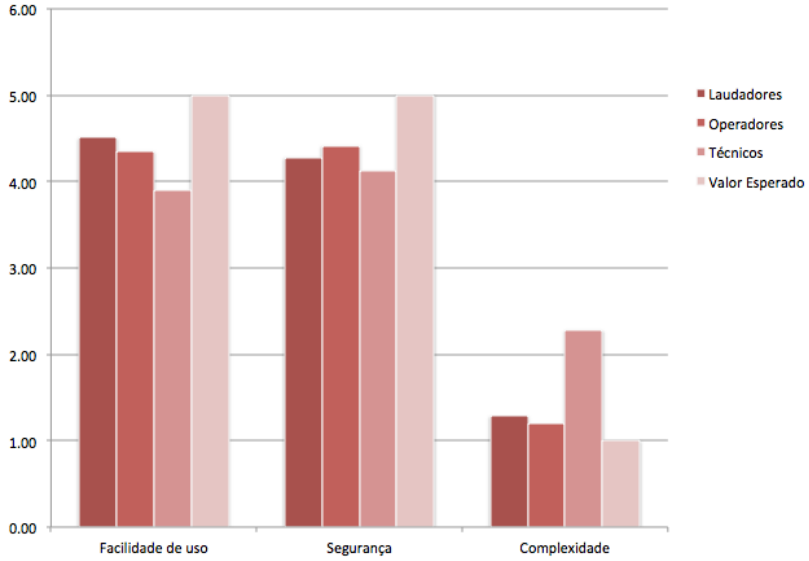


Figura 12: Gráfico de barras da análise bivariada por perfil

Tabela 9: Análise bivariada por faixa etária

| **Grupo** | $\leq 40$ | $> 40$ | **Valor esperado** |
|---|---|---|---|
| Facilidade de uso | 4,39 | 4 | 5 |
| Sergurança | 4,57 | 3,69 | 5 |
| Complexidade | 1,40 | 2 | 1 |

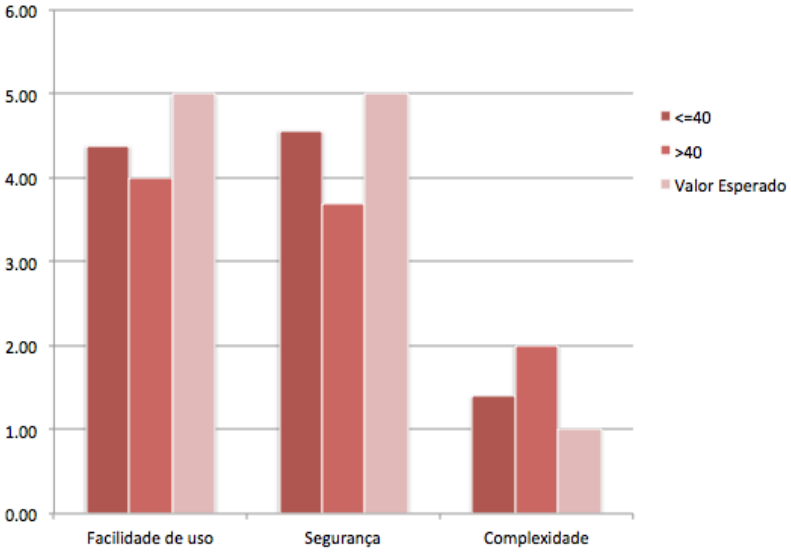


Figura 13: Gráfico de barras da análise bivariada por faixa etária

a primeira classe. Esta diferença é facilmente percebida na Figura 13. Da mesma forma, acredita-se que usuários nesta faixa etária necessitam de mais atenção no treinamento de utilização do novo modelo.

Ainda foram realizadas análises de correlção de Pearson entre os dados obtidos. Esta análise visa descobrir se há correlação linear entre as respostas de cada participante. Ou seja, se os participantes responderam a duas afirmativas com graus sempre semelhantes, a análise de Pearson irá apontar uma correlação positiva alta. Se os participantes respondem a duas afirmativas sempre com graus inversos (na casa da discordância para uma e de concordância para a outra), então a análise irá apontar uma correlação negativa alta. Caso contrário, a correlação será baixa.

A primeira dessas análises de correlação foi realizada entre as afirmativas ”3 - Eu achei o sistema fácil de usar”e ”16 - Eu considero que conheço

novas tecnologias". O objetivo desta análise é verificar se os participantes do teste não tiveram dificuldades com o modelo por conhecerem bem novas tecnologias. O grau de correlação entre estas duas afirmativas foi de -0,083, com um grau de explicação 0,68%. Ou seja, neste caso a correlação é negativa e bastante baixa, tendo apresentado somente 0,68% de usuários com uma avaliação de afirmação sendo influenciada pela outra.

A segunda análise de correlação foi realizada entre as afirmativas "3 - Eu achei o sistema fácil de usar"e "17 - Eu já conhecia outros sistemas com tecnologias similares". Nesta comparação visa-se observar se conhecimentos de outros sistemas similares auxiliaram os usuários a não encontrar dificuldade no uso do novo modelo. O grau de correlação obtido nesta avaliação foi de 0,19, com um grau de explicação 3,61%. Nesta caso a correlação é um pouco maior e positiva, porém ainda é considerada baixa, com somente 3,61% de usuários com uma avaliação de afirmação sendo influenciada pela outra.

As duas análises de correlação apresentaram resultados bastante diferentes dos esperados. Em geral, espera-se que a facilidade de uso esteja bastante relacionada a quão bem o usuário conhece da tecnologia utilizada. A correlação de Pearson define que graus entre 0 e 0,30 (positivo ou negativo) indicam uma correlação fraca. Os dois resultados apresentaram graus de correlação dentro deste intervalo, quebrando o estigma que se tinha no início do projeto. Estes resultados também ajudam a validar nossa proposta, uma vez que a facilidade de uso pouco tem a ver com conhecimentos prévios dos usuários. Acredita-se que este fator possa facilitar a aceitação do novo modelo.

De forma geral, os resultados obtidos foram bastante satisfatórios. A maioria dos participantes do teste concordam que o modelo proposto é fácil de utilizar. As respostas para a categoria Complexidade reafirmaram a primeira conclusão, a maioria dos participantes discorda que o modelo é muito complexo, fato que impacta diretamente na facilidade de uso. As respostas para a última categoria também são bastante importantes. Em geral os participantes consideraram o modelo de autenticação proposto neste trabalho mais seguro que o atual. Este fator pode ser utilizado como motivador para a aceitação do modelo proposto no sistema. Uma vez que os usuário sentem-se mais seguros utilizando o modelo proposto, não é necessário muito esforço para empregá-lo.

# 7 CONSIDERAÇÕES FINAIS

Neste trabalho apresentou-se um modelo de autenticação baseado em *web service* seguro. Este modelo é voltado às necessidades de segurança de sistemas do STT/SC, que contém informações de alto valor agregado. Para que se cumpra com os principais requisitos que este tipo de sistema exige, o modelo se utiliza de autenticação de múltiplos fatores. Isto é feito através de um conjunto de métodos de autenticação que podem ser combinados de forma a prover mais confiabilidade ao processo.

A proposta de um novo modelo de autenticação foi baseada nos pontos fortes de cada modelo já existente voltada para o ambiente médico encontrado na literatura. Também foram utilizadas as características consideradas negativas de cada modelo encontrado. Estas foram evitadas em nosso trabalho.

Além dos modelos já existentes, realizou-se um estudo direcionado a forma com que o STT/SC é utilizado, de forma a entender melhor os requisitos neste tipo de projeto. A partir deste estudo, foi possível generalizar os principais casos e determinar algumas características necessárias para o novo modelo.

Nosso modelo opera como um *web service* e, portanto, não impõe aos sistemas limitações tecnológicas, como linguagem de implementação específica. Além do mais, não requer o uso de *tokens* criptográficos, podendo ser facilmente integrado a diversos sistemas. Em nosso modelo, optou-se pelo uso de métodos de autenticação simples, baseados em *tokens* comuns.

O primeiro método escolhido para implementação foi o baseado em OTP. Com este método, foi possível transformar um *smartphone* em um gerador de senhas seguras (de uso único). Neste método, o único dispositivo exigido é o próprio *smartphone* do usuário.

Como uma alternativa para usuários que não possuem *smartphone*, foi desenvolvido um método de contrassenha enviada via SMS. Através deste, foi possível prover suporte ao envio de senhas de uso único ao usuário através de um canal diferente da internet. Neste método, o único dispositivo exigido é um celular comum. Desta forma, este modelo possui uma abrangência maior.

Uma terceira alternativa foi implementada para prover mais flexibilidade ao modelo. O método de reconhecimento de chamadas telefônicas foi implementado como uma alternativa ao sistema, pois possui um custo de manutenção mais baixo. Neste método, um usuário é identificado através de uma ligação que este realiza a partir do seu telefone. Neste método, somente é necessário uma linha telefônica e um telefone previamente cadastrado, não importando a natureza deste último.

A flexibilidade do modelo proposto é dada pelos métodos de autenticação

escolhidos. Cabe ao sistema determinar a forma com que seus usuários irão se autenticar, podendo flexibilizar a escolha do método de autenticação dependendo da situação. Além do mais, o sistema pode definir a prioridade de cada método no processo de autenticação, e também definir em quais áeras do sistema será exigida a autenticação de usuários. Desta forma, cabe ao serviço verificar as credenciais fornecidas, sem interferir nas regras de negócio do sistema. Sua característica de alta interoperabilidade e sua eficácia puderam ser mostradas através de uma versão operável do serviço; a proposta encontra-se implementada e integrada ao STT/SC.

Nossa análise demonstrou que o modelo proposto se adequa bem à sistemas de telemedicina e telessaúde uma vez que provê flexibilidade e consegue se moldar de forma a suprir as necessidades do sistema, por mais específicas que estas sejam. Nesta análise, incluímos as principais características dos sistemas, que são a facilidade de uso e a segurança. A complexidade das atividades relacionadas com a autenticação também foi analisada como uma forma de reafirmar o facilidade de uso. Os testes com os usuários mostraram que, de forma geral, os usuários não tiveram dificuldade para utilizar o novo modelo e que compreenderam para que serviam as novas funcionalidades.

Além do mais, a análise demonstra que houve também um aumento no nível de segurança do processo de autenticação do STT/SC. Isso pode ser visto através da avaliação dos métodos pelos níveis de segurança do NIST. Antes, o processo atingia o nível 1 utilizando o método baseado em login e senha simples. Utilizando o modelo proposto é possível atingir o nível 3.

A análise ainda mostrou que o modelo cobre os principais ataques envolvendo o processo de autenticação. Ao utilizar diferentes métodos de autenticação de segundo fator, além de prover um sistema financeiramente adaptável ao cenário requerido, ainda é possível flexibilizar o processo de autenticação ao usuário e ao sistema. Ainda nesse âmbito, é possível prover propriedades de autenticação não existentes na maioria dos outros sistemas, tais como a garantia de autenticação geográfica, baseada no uso do identificador de chamadas de um sistema de telefonia fixa.

Como forma de melhorar o serviço de autenticação proposto sugere-se a adição de novos métodos de autenticação. Nossos próximos passos na melhora dos mecanismos de autenticação são a inclusão de um sistema criptográfico baseado em identidades (*identity based encryption*) para permitir a autenticação de usuários não cadastrados no sistema e a implementação de um sistema de envio de senha de uso único (OTP) através de tons telefônicos para eliminar a janela de tempo de ataques existente no modelo atual. Desta forma o usuário precisa entrar com o OTP recebido pelo telefone para se autenticar, não sendo mais possível somente se utilizar de uma ligação válida

para tentar um ataque. Por fim, outra proposta é a de que o ambiente autentique o usuário. Isto pode ser feito levando em conta a presença do usuário em determinado ambiente, através da percepção de que algum dispositivo de sua posse esteja conectado a uma rede *wifi*, por exemplo.

# REFERÊNCIAS BIBLIOGRÁFICAS

Agência Nacional de Telecomincações. *Quantidade de Acessos/Plano de Serviço/Unidade da Federação*. 2012. http://sistemas.anatel.gov.br/.

AHN, G.-J.; SHIN, D. Towards scalable authentication in health services. In: *Enabling Technologies: Infrastructure for Collaborative Enterprises, 2002. WET ICE 2002. Proceedings. Eleventh IEEE International Workshops on*. [S.l.: s.n.], 2002. p. 83 – 88. ISSN 1080-1383.

AL-NAYADI, F.; ABAWAJY, J. An authentication framework for e-health systems. In: *Signal Processing and Information Technology, 2007 IEEE International Symposium on*. [S.l.: s.n.], 2007. p. 616 –620.

ALZOMAI, M. et al. Strengthening sms-based authentication through usability. In: *Parallel and Distributed Processing with Applications, 2008. ISPA '08. International Symposium on*. [S.l.: s.n.], 2008. p. 683 –688.

BARCELLOS, C. L. *Concepção, desenvolvimento e implantação de uma ferramenta para uso de laudo estruturado no padrão DICOM SR em sistemas de telemedicina de larga escala*. 2012.

BARUA, M. et al. Secure and quality of service assurance scheduling scheme for wban with application to ehealth. In: *Wireless Communications and Networking Conference (WCNC), 2011 IEEE*. [S.l.: s.n.], 2011. p. 1102–1106. ISSN 1525-3511.

BARUA, M. et al. Peace: An efficient and secure patient-centric access control scheme for ehealth care system. In: *Computer Communications Workshops (INFOCOM WKSHPS), 2011 IEEE Conference on*. [S.l.: s.n.], 2011. p. 970–975.

BARUA, M.; LU, R.; SHEN, X. Health-post: A delay-tolerant secure long-term health care scheme in rural area. In: *Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE*. [S.l.: s.n.], 2011. p. 1–5. ISSN 1930-529X.

BARUA, M.; MAHMOUD, M.; SHEN, X. Astp: Agent-based secure and trustworthy packet-forwarding protocol for ehealth. In: *Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE*. [S.l.: s.n.], 2011. p. 1–5. ISSN 1930-529X.

BENANTAR, M. *Access Control Systems: Security, Identity Management and Trust Models*. Springer, 2006. ISBN 9780387004457. <http://books.google.com.br/books?id=dpjsXA5SPPwC>.

BIRRELL, A. D.; NELSON, B. J. Implementing remote procedure calls. *ACM Trans. Comput. Syst.*, ACM, New York, NY, USA, v. 2, n. 1, p. 39–59, fev. 1984. ISSN 0734-2071. <http://doi.acm.org/10.1145/2080.357392>.

BOONYARATTAPHAN, A.; BAI, Y.; CHUNG, S. A security framework for e-health service authentication and e-health data transmission. In: *Proceedings of the 9th international conference on Communications and information technologies*. Piscataway, NJ, USA: IEEE Press, 2009. (ISCIT'09), p. 1213–1218. ISBN 978-1-4244-4521-9. <http://dl.acm.org/citation.cfm?id=1789954.1790254>.

BROOKE, J. SUS: A quick and dirty usability scale. In: JORDAN, P. W. et al. (Ed.). *Usability evaluation in industry*. London: Taylor and Francis, 1996.

BURR, W. E. et al. *SP 800-63-1. Electronic Authentication Guideline*. Gaithersburg, MD, United States, 2011.

CERAMI, E. *Web Services Essentials*. 1st. ed. Sebastopol, CA, USA: O'Reilly & Associates, Inc., 2002. ISBN 0596002246.

CYCLOPS. *Sistema Catarinense de Telemedicina e Telessaúde*. 2010. https://www.telemedicina.ufsc.br/rctm.

DRIRA, W.; RENAULT, E.; ZEGHLACHE, D. A hybrid authentication and key establishment scheme for wban. In: *Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on*. [S.l.: s.n.], 2012. p. 78–83.

FFIEC. Authentication in an internet banking environment. http://www.ffiec.gov/press/pr101205.htm. Outubro 2005.

GARSON, K.; ADAMS, C. Security and privacy system architecture for an e-hospital environment. In: *Proceedings of the 7th symposium on Identity and trust on the Internet*. New York, NY, USA: ACM, 2008. (IDtrust '08), p. 122–130. ISBN 978-1-60558-066-1. <http://doi.acm.org/10.1145/1373290.1373306>.

Google Inc. *Google Authenticator*. 2012. http://code.google.com/p/google-authenticator.

GUO, L. et al. User-centric private matching for ehealth networks - a social perspective. In: *Global Communications Conference (GLOBECOM), 2012 IEEE*. [S.l.: s.n.], 2012. p. 732–737. ISSN 1930-529X.

HAN, S. et al. A framework of authentication and authorization for e-health services. In: *Proceedings of the 3rd ACM workshop on Secure web services*. New York, NY, USA: ACM, 2006. (SWS '06), p. 105–106. ISBN 1-59593-546-0. <http://doi.acm.org/10.1145/1180367.1180387>.

IBGE. *Sinopse do Censo Demográfico 2010*. 2010.

IDALINO, T. B.; SPAGNUELO, D. Senhas descartáveis em dispositivos móveis para ambientes de telemedicina. In: *SBSeg 2012 WTICG*. http://sbseg2012.ppgia.pucpr.br/: [s.n.], 2012.

JACOBSON, I.; BOOCH, G.; RUMBAUGH, J. The unified software development process–the complete guide to the unified process from the original designers. *Rational Software Corporation, US*, 1999.

JAKOBSSON, M.; AKAVIPAT, R. *Rethinking passwords to adapt to constrained keyboards*. 2011. <http://www.markus-jakobsson.com/fastwords.pdf>.

JØSANG, A.; ZOMAI, M. A.; SURIADI, S. Usability and privacy in identity management architectures. In: *Proceedings of the fifth Australasian symposium on ACSW frontiers - Volume 68*. Darlinghurst, Australia, Australia: Australian Computer Society, Inc., 2007. (ACSW '07), p. 143–152. ISBN 1-920-68285-X. <http://dl.acm.org/citation.cfm?id=1274531.1274548>.

MACEDO, D. D. J. de. *Um estudo de estratégias de sistemas distribuidos aplicadas a sistemas de telemedicina*. 2008.

MARTÍNEZ, J.-F. et al. Security services provision for telematic services at the knowledge and information society. In: *Proceedings of the 2007 Euro American conference on Telematics and information systems*. New York, NY, USA: ACM, 2007. (EATIS '07), p. 41:1–41:7. ISBN 978-1-59593-598-4. <http://doi.acm.org/10.1145/1352694.1352736>.

MILLER, F.; VANDOME, A.; MCBREWSTER, J. *Digital Identity: Digital, Authentication, E-Authentication, Entity, Federated Identity, Future of Identity in the Information Society, Global Trust Center, Identity (social Science)*. VDM Publishing, 2009. ISBN 9786130223403. <http://books.google.com.br/books?id=u_zPQgAACAAJ>.

M'RAIHI, D. et al. *HOTP: An HMAC-Based One-Time Password Algorithm*. IETF, dez. 2005. RFC 4226 (Informational). (Request for Comments, 4226). <http://www.ietf.org/rfc/rfc4226.txt>.

M'RAIHI, D. et al. *TOTP: Time-Based One-Time Password Algorithm*. IETF, maio 2011. RFC 6238 (Informational). (Request for Comments, 6238). <http://www.ietf.org/rfc/rfc6238.txt>.

M'RAIHI, D. et al. *OCRA: OATH Challenge-Response Algorithm*. IETF, jun. 2011. RFC 6287 (Informational). (Request for Comments, 6287). <http://www.ietf.org/rfc/rfc6287.txt>.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. *Federal Information Processing Standards Publication 181, Standard for Automated Password Generator (APG)*. out. 1993. <http://www.itl.nist.gov/fipspubs/fip181.htm>.

NEEDHAM, R. M.; SCHROEDER, M. D. Using encryption for authentication in large networks of computers. *Commun. ACM*, ACM, New York, NY, USA, v. 21, n. 12, p. 993–999, dez. 1978. ISSN 0001-0782. <http://doi.acm.org/10.1145/359657.359659>.

NIST. *Security Requirements for Cryptographic Modules*. [S.l.], dez. 2002. (FIPS PUB, v. 140-2). <http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>.

Object Management Group, Inc. *Business Process Model and Notation (BPMN)*. 2011. Http://www.omg.org/spec/BPMN/2.0/. (formal/2011-01-03).

Object Management Group, Inc. *OMG Unified Modeling LanguageTM (OMG UML), Infrastructure*. 2011. Http://www.omg.org/spec/UML/2.4.1/. (formal/2011-08-05).

OFFICE OF MANAGEMENT AND BUDGET. *E-Authentication Guidance for Federal Agencies OMB-M-04-04*. dez. 2003. <http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf>.

PIETRO, R. D.; ME, G.; STRANGIO, M. A two-factor mobile authentication scheme for secure financial transactions. In: *Mobile Business, 2005. ICMB 2005. International Conference on*. [S.l.: s.n.], 2005. p. 28 – 34.

SCHNEIER, B. Inside risks: the uses and abuses of biometrics. *Commun. ACM*, ACM, New York, NY, USA, v. 42, n. 8, p. 136–, ago. 1999. ISSN 0001-0782. <http://doi.acm.org/10.1145/310930.310988>.

SCHWABER, K.; SUTHERLAND, J. *SCRUM*. 2012. Http://www.scrum.org/.

SILVA, D. R. P. da. *A memória humana no uso de senhas*. Tese (Doutorado) — Pontifícia Universidade Católica do Rio Grande do Sul, 2007.

SPAGNUELO, D. P. B. et al. Multi-factor authentication in telemedicine systems. In: *eTELEMED 2013, The Fifth International Conference on eHealth, Telemedicine, and Social Medicine*. http://www.iaria.org/conferences2013/eTELEMED13.html/: [s.n.], 2013.

SURFnet. *tiqr*. 2013. https://tiqr.org/.

WALLAUER, J. et al. Building a national telemedicine network. *IT Professional*, IEEE Computer Society, Los Alamitos, CA, USA, v. 10, p. 12–17, 2008. ISSN 1520-9202.

WANGENHEIM, A. von et al. User satisfaction with asynchronous telemedicine: A study of users of santa catarina system of telemedicine and telehealth. *Telemed J E Health*, v. 18, n. 5, p. 339–46, 2012. ISSN 1556-3669.

WAZLAWICK, R. *Análise e Projeto de Sistemas de Informação Orientados a Objetos, 2E*. [S.l.]: Elsevier Brasil, 2010.

World Wide Web Consortium. *W3C*. 2013. http://www.w3.org/.

# ANEXO A – Escala de Usabildade do Sistema

UNIVERSIDADE FEDERAL DE SANTA CATARINA

INCoD
Instituto Nacional para Convergência Digital

# Escala de Usabilidade do Sistema

**System Usability Scale - SUS**



Nº do Participante:_____

| | Discordo totalmente | | | | Concordo totalmente |
|---|---|---|---|---|---|
| 1. Eu acho que gostaria de usar esse sistema frequentemente. | 1 | 2 | 3 | 4 | 5 |
| 2. Eu achei o sistema desnecessariamente complexo. | 1 | 2 | 3 | 4 | 5 |
| 3. Eu achei o sistema fácil de usar. | 1 | 2 | 3 | 4 | 5 |
| 4. Eu acho que eu precisaria de ajuda de um técnico para ser capaz de usar o sistema. | 1 | 2 | 3 | 4 | 5 |
| 5. Eu achei que as funções do sistema estavam bem integradas. | 1 | 2 | 3 | 4 | 5 |
| 6. Eu achei que havia muitas inconsistências no sistema. | 1 | 2 | 3 | 4 | 5 |
| 7. Eu acho que a maioria das pessoas aprenderia a usar esse sistema rapidamente. | 1 | 2 | 3 | 4 | 5 |
| 8. Eu achei o sistema muito incômodo de usar. | 1 | 2 | 3 | 4 | 5 |
| 9. Eu me senti muito confiante usando o sistema. | 1 | 2 | 3 | 4 | 5 |
| 10. Eu precisei aprender muitas coisas antes de conseguir usar o sistema. | 1 | 2 | 3 | 4 | 5 |

| | Discordo totalmente | | | | Concordo totalmente |
|---|---|---|---|---|---|
| 11. Eu me senti mais seguro utilizando o sistema. | 1 | 2 | 3 | 4 | 5 |
| 12. Eu entendi para que servem as novas funcionalidades do sistema. | 1 | 2 | 3 | 4 | 5 |
| 13. O sistema não alterou a forma como eu trabalho. | 1 | 2 | 3 | 4 | 5 |
| 14. Eu achei o software da plataforma móvel fácil de interagir. | 1 | 2 | 3 | 4 | 5 |
| 15. Eu acredito que meu dispositivo móvel é mais seguro do que minha estação de trabalho. | 1 | 2 | 3 | 4 | 5 |
| 16. Eu considero que conheço novas tecnologias. | 1 | 2 | 3 | 4 | 5 |
| 17. Eu já conhecia outros sistemas com tecnologias similares. | 1 | 2 | 3 | 4 | 5 |