Autenticação de Usuários e Atestação de Dispositivos em Ambientes Urbanos usando TPM

Gustavo V. Monteiro[1], Ramon S. Araújo[1], Lyedson S. Rodrigues[1], Rafael A. Menezes[1], Paulo H. Maia[1], Rafael L. Gomes[1]

[1]Universidade Estadual do Ceará (UECE), Fortaleza, Ceará, Brasil.

{gustavo.cesar,ramon.araujo,lyedson.silva,

menezes.almeida}@aluno.uece.br,{pauloh.maia,rafa.lopes}@uece.br

Resumo. *A crescente necessidade de segurança digital tem impulsionado a adoção de mecanismos avançados de autenticação e atestação de dispositivos. Este trabalho propõe e implementa um sistema de autenticação que utiliza o Trusted Platform Module, ou Módulo de Plataforma Confiável (TPM), para garantir a vinculação entre um usuário e um dispositivo específico, reforçando a segurança do processo de login sem prejudicar a usabilidade. O servidor verifica a autenticidade das informações, garantindo que a autenticação ocorra apenas em dispositivos previamente autorizados e protegidos contra alterações não autorizadas. Os testes realizados avaliaram diferentes cenários, como erros de credenciais, alterações inesperadas nos Platform Configuration Registers, ou Registradores de Configuração de Plataforma (PCRs), e tentativas de autenticação em dispositivos não autorizados, demonstrando a eficácia da abordagem na proteção contra ataques e acessos indevidos.*

Abstract. *The growing need for digital security has driven the adoption of advanced authentication and device attestation mechanisms. This work proposes and implements an authentication system that utilizes the Trusted Platform Module (TPM) to ensure the binding between a user and a specific device, enhancing the security of the login process without compromising usability. The server verifies the authenticity of the information, ensuring that authentication occurs only on previously authorized devices, which are protected against unauthorized modifications. The conducted tests evaluated different scenarios, such as credential errors, unexpected changes in the Platform Configuration Registers (PCRs), and authentication attempts on unauthorized devices, demonstrating the effectiveness of the approach in protecting against attacks and unauthorized access.*

1. Introdução

A segurança digital tornou-se um aspecto fundamental na proteção de informações e no controle de acesso a sistemas corporativos. Mesmo após a pandemia de Covid 19, a tendência de trabalho remoto ainda permanece em alta, com cerca de $8,3\%$ dos brasileiros atuando nesta modalidade [Xavier et al. 2024, Portela et al. 2024b]. Juntamente com o crescimento do trabalho remoto (ou teletrabalho), os ataques cibernéticos aumentaram consideravelmente devido à grande quantidade de operações sensíveis sendo feitas de maneira digital, como transações bancárias, acessos a redes corporativas, dentre outras

operações [Silveira et al. 2023, Angafor et al. 2024]. Os ambientes urbanos são caracterizados por uma alta concentração de dispositivos conectados, redes compartilhadas e pontos de acesso públicos encontrados nas cidades, onde trabalhadores frequentemente realizam atividades profissionais em diferentes locais como cafés, espaços de *coworking* ou transporte público. Nessas situações, os dispositivos corporativos ficam mais vulneráveis a ameaças como ataques de rede, interceptação de credenciais e tentativas de alteração indevida no *firmware*, que são programas que controlam funções mais básicas de um dispositivo, ou *softwares* [Souza et al. 2024].

Uma das técnicas de segurança cruciais para esse contexto é a Autenticação. Autenticar um usuário e garantir que seu dispositivo não está comprometido de alguma forma é um desafio na segurança da informação, visto que a utilização de apenas métodos tradicionais, como email e senha, está sujeita a sofrer inúmeros tipos de ataques, incluindo *phishing* e vazamento de credenciais [Portela et al. 2023, Pinheiro et al. 2011]. Além do mais, é possível que algum ataque modifique o *firmware* do dispositivo, sendo quase impossível a detecção durante a execução do sistema operacional [Wang et al. 2021, Gomes et al. 2010].

Além disso, métodos de autenticação com múltiplos fatores adicionam uma certa complexidade no momento de um *login*, sendo até mesmo um fardo na experiência do usuário [Rekha et al. 2024]. A abordagem de utilizar a identidade do usuário atrelada a um dispositivo físico fornecido a ele pode oferecer uma experiência significativamente melhor, pois tem potencial de ser mais segura e conveniente. Portanto, garantir a segurança de uma autenticação sem prejudicar a usabilidade é um problema relevante que este trabalho busca abordar [Silva et al. 2023].

Adicionalmente, uma abordagem usada para dar suporte às soluções de segurança necessárias é o Trusted Platform Module, ou Módulo de Plataforma Confiável (TPM), que é um *chip* de segurança criado com o intuito de fornecer suporte criptográfico, inclusive com proteções a nível físico [Trusted Computing Group 2019b]. Para garantir a integridade e a autenticidade de um dispositivo, ele possibilita a geração e gerenciamento de chaves criptográficas, consegue oferecer proteção para credenciais contra acessos não autorizados, utilizando, por exemplo, um espaço de memória não volátil protegido por políticas que devem ser satisfeitas antes de obter acesso, além de também possibilitar a verificação do estado do sistema por meio de registradores que guardam medições de *software*, *hardware*, *firmware* e alguns outros componentes da máquina. Esses registradores são chamados de Platform Configuration Registers, ou Registradores de Configuração de Plataforma (PCRs) [Trusted Computing Group 2019a].

Dentro deste contexto, este trabalho propõe um sistema de autenticação, baseado no TPM, onde não apenas um usuário se autentica de maneira tradicional, com o uso de email e senha, como também o dispositivo que ele usa deve ser um dispositivo específico e de uso exclusivo dele, além de também ser feita a verificação da integridade do mesmo. Esse processo visa garantir que a identidade do usuário esteja vinculada ao dispositivo utilizado para acessar um serviço, por exemplo, uma rede ou aplicação corporativa. A ideia é fortalecer o processo de *login* em ambientes corporativos, onde notebooks e outros dispositivos são fornecidos pela empresa para que um colaborador realize suas atividades de maneira remota, protegendo-os contra acessos indevidos e roubos de credenciais.

A solução oferece uma camada extra de proteção contra ataques comuns, como o roubo de credenciais, *phishing* e uso indevido de dispositivos. Ao exigir que tanto o usuário quanto o dispositivo estejam previamente provisionados e íntegros, o sistema bloqueia tentativas de acesso não autorizadas mesmo que um invasor tenha obtido a senha do usuário. Isso é especialmente relevante em contextos de trabalho remoto em ambientes urbanos, onde dispositivos corporativos estão mais expostos. Além disso, a solução mantém a usabilidade, uma vez que o processo de *login* permanece simples para o usuário final, sendo similar ao tradicional, mas com verificações de segurança ocorrendo de forma transparente em segundo plano.

Dentre as principais contribuições, destacam-se: (i) Implementação de um fluxo de provisionamento, no qual chaves criptográficas são geradas pelo TPM e associadas ao usuário; (ii) Implementação de um mecanismo de autenticação que utiliza *quotes* do TPM para verificar a integridade do dispositivo antes de conceder acesso, sem prejudicar a usabilidade; e, (iii) Avaliação da solução em diferentes cenários, demonstrando sua robustez contra tentativas de fraude, como o uso de dispositivos não autorizados ou alterações inesperadas nos registros dos PCRs do TPM.

O restante deste artigo está organizado da seguinte forma: Na Seção 2 são apresentados trabalhos relacionados; na Seção 3 é detalhada a proposta; na Seção 4 são descritos os experimentos realizados e os resultados obtidos; e na Seção 5 são apresentadas as conclusões e direções para pesquisas futuras.

2. Trabalhos Relacionados

Nesta seção serão apresentados alguns trabalhos que envolvem o *chip*, destacando alguns aspectos importantes para levar em consideração sobre o uso de TPM nas mais diversas aplicações.

No trabalho de Ioos *et al.* [2021], o autor descreve como o TPM pode ser utilizado para proteger a autenticação Secure Shell, ou Shell Seguro (SSH), especialmente a chave privada, contra acessos não autorizados. O trabalho detalha o processo de configuração, uso e segurança do TPM em conjunto com SSH, além de responder questões importantes, como a impossibilidade de comprometer o sistema apenas roubando o banco de dados SQLite que é utilizado, já que o mesmo é mantido criptografado usando chaves derivadas do TPM. O trabalho mostra bem como funciona o armazenamento seguro de chaves do TPM, já que o autor usa um simulador de TPM, o que lhe permite extrair a chave simétrica usada para criptografar a parte privada das chaves geradas pelo *chip*, o que, por sua vez, dá a essas chaves a característica de apenas poderem ser utilizadas pelo próprio dispositivo que as criou.

Reineh *et al.* [2016] abordam o uso de TPM em dispositivos móveis para aumentar a segurança e a usabilidade de aplicativos sensíveis, como os de transações bancárias. O trabalho propõe uma estrutura que utiliza o TPM para autenticação e atestação remota, substituindo credenciais do usuário por atestações baseadas no dispositivo, porém, como geralmente dispositivos móveis não possuem TPMs físicos, o trabalho se limita ao uso de TPM em *software*, que não oferece o mesmo nível de proteção de um TPM físico devido à potencial vulnerabilidade do *kernel* ou de outros componentes do sistema em que o *software* opera. O interessante aqui é perceber como os PCRs são usados de maneira específica para a necessidade, provando a flexibilidade dos recursos disponíveis nos

TPMs.

Hosseinzadeh *et al.* [2019] discutem como o TPM ajuda a mitigar possíveis ataques que ocorrem na nuvem. Isso mostra que, utilizando a nuvem, é possível criar um ambiente para garantir a confiança em um computador que pode ser certificado e evitar vários tipos de ameaças. Esses ataques são categorizados e descritos como ataque de rede, ataque de aplicação, provedor de serviços em nuvem malicioso/não confiável, ataques ao *back-end* da nuvem, adulteração de dados e vazamento de dados. Este trabalho ajuda a evidenciar o quanto TPM é flexível e eficiente para garantir a segurança em ambientes variados, incluindo a nuvem.

Na referência [Fiolhais and Sousa 2023], os autores estudam a viabilidade de incorporar algoritmos criptográficos que sejam resistentes a ataques quânticos no TPM. Mais especificamente, o trabalho explora a possibilidade de integração de algoritmos como Kyber e Dilithium para garantir segurança futura contra computação quântica. Os resultados indicaram que esses algoritmos podem sim substituir métodos tradicionais, como RSA, permitindo a continuidade da robustez do TPM em cenários emergentes. Além disso, também é enfatizada a necessidade de mudanças nas arquiteturas existentes com o objetivo de lidar com os desafios trazidos pelo avanço da computação quântica.

Kim *et al.* [2024] estudam o uso do TPM em sistemas de defesa. O estudo evidencia a importância desse tipo de módulo de segurança baseado em *hardware* para impedir tanto ataques lógicos quanto físicos, deixando clara a capacidade que o TPM tem de fornecer um ambiente confiável para armazenamento de chaves criptográficas e outras operações críticas de segurança. O artigo também analisa a adoção do TPM em diferentes setores da indústria e destaca a necessidade de padronizar e aprimorar a tecnologia para que possa ser possível obter uma maior compatibilidade e eficiência em sistemas modernos. Similarmente, Zeitouni *et al.* [2024] propõem melhorias no gerenciamento de integridade de dados utilizando TPM em ambientes virtualizados. A pesquisa busca evitar sobrecarga do TPM físico quando se têm muitas máquinas virtuais utilizando um vTPM através da introdução de um mecanismo de escalonamento de requisições.

A partir desta revisão da literatura, observa-se que, embora existam trabalhos significativos na área, ainda há uma lacuna importante no desenvolvimento de soluções de segurança que possam habilitar autenticação e atestação com TPM. Diferente dos trabalhos anteriores, a presente pesquisa se destaca ao oferecer uma solução que combina segurança e eficiência de forma integrada, considerando não apenas a implementação teórica, mas sua aplicação prática em cenários reais.

3. Proposta

A solução proposta visa aumentar a segurança do processo de *login* em ambientes corporativos, vinculando a identidade do usuário a um dispositivo específico. Por meio do uso do TPM, o sistema garante não apenas que o usuário está inserindo as credenciais corretas, mas também que o dispositivo utilizado está íntegro e não sofreu alterações indevidas, como modificações em *firmware* ou *software*. A solução se divide em duas fases e seis entidades, sendo uma delas o usuário. As fases da solução são:

- **Provisionamento de chaves e certificados:** o dispositivo irá gerar as chaves Local Attestation Key, ou Chave de Atestação Local (LAK) e Local Device Identity, ou Identidade de Dispositivo Local (LDEVID), usando TPM e

irá solicitar a emissão de um certificado para as ambas. Esse processo acontecerá internamente na empresa/entidade que irá fornecer o dispositivo para o usuário, portanto parte-se do pressuposto que não haverá tentativas de fraude, não sendo feitas as verificações necessárias para constatar que uma chave realmente foi gerada por um TPM (normalmente presente em provisionamentos remotos [Trusted Computing Group 2021]).

- **Autenticação e Atestação:** o usuário tentará se autenticar, usando o dispositivo que lhe foi dado, com suas credenciais. É nesta fase que os dados serão verificados e, tanto a identidade do usuário e do dispositivo, quanto a saúde do dispositivo, serão testados.

3.1. Arquitetura da Solução

A solução desenvolvida possui duas fases e seis entidades. Durante a fase de provisionamento, é assumido que o dispositivo esteja em uma rede privada e segura, portanto, como já citado anteriormente, os processos e verificações necessárias para o provisionamento seguro de forma remota não são seguidos, e não estão no escopo deste trabalho. É possível visualizar a arquitetura da fase de provisionamento na Figura 1.

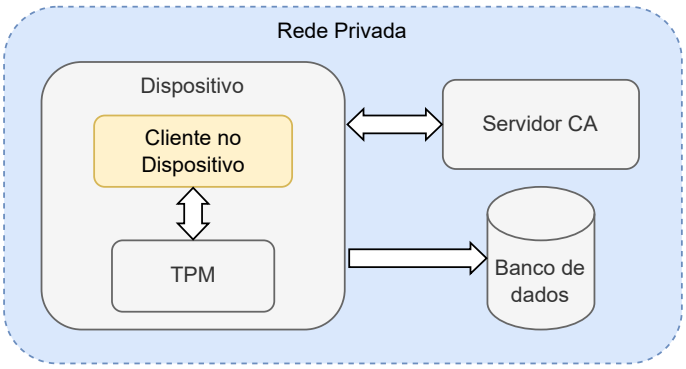

Figura 1. Arquitetura alto nível da fase de provisionamento

Já na fase de autenticação, o Certificate Authority, ou Autoridade Certificadora (CA), não se faz presente, pois seu papel é apenas emitir os certificados para as chaves do TPM. A arquitetura da fase de autenticação pode ser observada na Figura 2. As entidades presentes na solução são:

- **Autoridade Certificadora (CA):** um servidor que irá realizar a assinatura dos certificados para as chaves do TPM durante a fase de provisionamento.
- **Usuário:** quem vai inserir os dados de email e senha, necessários para realizar a autenticação em questão.
- **Agente de *Login*:** aplicação que receberá os dados de entrada vindos do usuário, no caso, email e senha, e irá repassá-los para o Cliente em execução no dispositivo. Ao receber a entrada do usuário, o agente irá: (1) Solicitar um *nonce* para o servidor de autenticação/atestação; (2) Solicitar a geração do *quote* via TPM para o dispositivo, repassando o *nonce* recebido juntamente do email e senha coletados.
- **Cliente no Dispositivo:** um serviço que estará no dispositivo do usuário para receber os dados do Agente de *Login* e gerar o *quote*. São realizadas duas funções, uma sendo executada apenas uma vez e a outra de fato permanecendo em execução

em segundo plano. A primeira função é usada apenas no momento de provisionar as chaves e certificados, que deve ser um processo feito em uma rede local e segura, pois o procedimento não considera as verificações necessárias para garantir que as chaves utilizadas realmente são de um TPM legítimo, pois não estão no escopo deste projeto. A segunda função é de fato um serviço que ficará em execução constante, e tem como objetivo receber os dados de entrada do usuário no agente de *login* e gerar um *quote* via TPM usando a chave de atestação gerada na primeira fase.

- **Servidor de Autenticação/Atestação:** um servidor que irá fazer a geração dos *nonces*, para evitar ataques de *replay*, que consistem na reutilização de uma mensagem válida por parte de um atacante, e irá realizar a verificação de todos os dados de autenticação e atestação do usuário e do dispositivo a fim de garantir a autenticidade e integridade.
- **Banco de Dados:** uma aplicação de banco de dados comum para armazenar dados dos usuários, dispositivos e *nonces*.

A arquitetura projetada permite que o sistema funcione com segurança mesmo quando os dispositivos estão fora da infraestrutura da empresa. A separação clara de funções entre os componentes e a utilização do TPM para garantir integridade e identidade tornam a solução robusta contra ataques, sem comprometer a experiência do usuário. Além disso, a estrutura modular facilita a expansão futura para diferentes aplicações e cenários de uso.

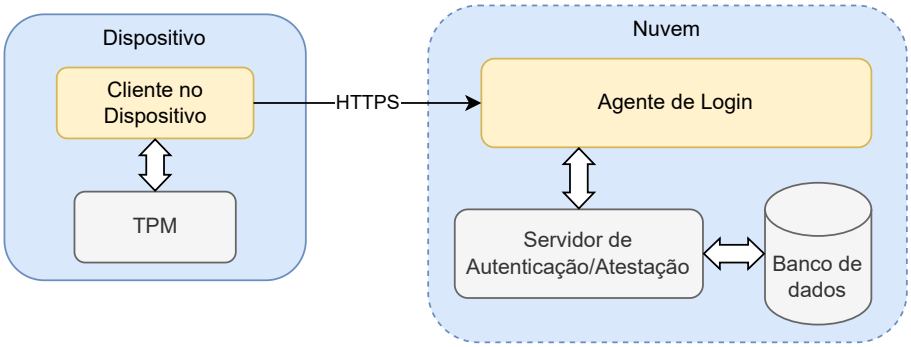

Figura 2. Arquitetura alto nível da fase de autenticação

3.2. Fases da solução

A solução proposta por este trabalho se divide em duas fases principais: a Fase de Provisionamento e a Fase de Autenticação. Durante a fase de provisionamento, as chaves criptográficas são geradas diretamente no TPM presente no dispositivo. Primeiramente, é criada a Endorsement Key, ou Chave de Endorso (EK), usada exclusivamente para derivar as demais chaves, que são a LAK e a LDEVID. Cada uma dessas chaves é gerada seguindo um *template* padronizado pelo Trusted Computing Group. Após a criação, o dispositivo gera um Certificate Signing Request, ou Solicitação de Assinatura de Certificado (CSR), contendo a chave pública correspondente. Esse CSR é enviado para um CA, que emite certificados digitais específicos para essas chaves, atrelando-as de maneira inequívoca ao dispositivo e ao usuário.

No momento da autenticação, o servidor de autenticação gera um *nonce*, que é um número aleatório com validade temporal, enviado ao dispositivo junto às credenciais do

usuário. O dispositivo então utiliza o TPM para criar um *quote*, que consiste em uma assinatura criptográfica gerada usando a chave LAK. O *quote* incorpora a *hash* criptográfica que combina email, senha e o *nonce* recebido, além dos valores atuais dos PCRs. Este procedimento garante que os dados transmitidos sejam únicos para cada autenticação, impedindo ataques de *replay* e validando simultaneamente a integridade do dispositivo. A seguir, essas fases serão detalhadas.

3.2.1. Fase de Provisionamento

A Fase de Provisionamento tem a função de criar, registrar e associar os elementos necessários para o funcionamento da solução. Esta fase é executada uma única vez por dispositivo, além de dever ser feita de maneira local e controlada, ou seja, em um ambiente que deva ser seguro, como a rede privada de uma empresa, e deve ser executada por um colaborador responsável. O processo consiste na realização das seguintes etapas:

- **Geração de chaves no TPM**: São criadas as chaves criptográficas específicas no TPM, que no caso são a LAK e a LDEVID, respectivamente a chave de atestação e a chave de identificação. A geração da LDEVID está sendo realizada como uma preparação para um futuro uso do protocolo Mutual Transport Layer Security, ou Segurança da Camada de Transporte Mútua (mTLS), porém para a prova de conceito sua utilização não foi feita.
- **Criação de CSR (PKCS #10)**: Um CSR é gerado pelo dispositivo para cada chave gerada, contendo informações sobre a chave pública. O CSR é utilizado para solicitar um certificado digital ao CA.
- **Assinatura pelo CA**: O CSR é enviado ao CA, que emite um certificado digital correspondente à chave pública do dispositivo.
- **Registro no banco de dados**: As informações do dispositivo, incluindo o certificado das chaves e valores de PCRs, e dados do usuário, como *email*, nome e senha, são armazenadas em um banco de dados. Esse registro associa o usuário ao dispositivo de maneira única.

Essa fase prepara o ambiente para que o dispositivo e o usuário possam ser autenticados e atestados com segurança durante a fase de autenticação, que é o foco principal deste trabalho. O fluxo completo da fase de provisionamento pode ser visto na Figura 3.

3.2.2. Fase de Autenticação

A Fase de Autenticação é o momento em que o sistema realiza a autenticação do usuário com base nos dados provisionados na fase anterior. Esta fase ocorre toda vez que o usuário tenta acessar o sistema e segue os seguintes passos:

- **Inserção de credenciais**: O usuário insere suas credenciais (email e senha) no agente que contenha o formulário para autenticação.
- **Solicitação de um *nonce***: O agente de *login* solicita um *nonce* para o Servidor de Autenticação/Atestação. Esse *nonce* recebe um tempo de validade, então caso esse tempo exceda, a autenticação não será permitida.

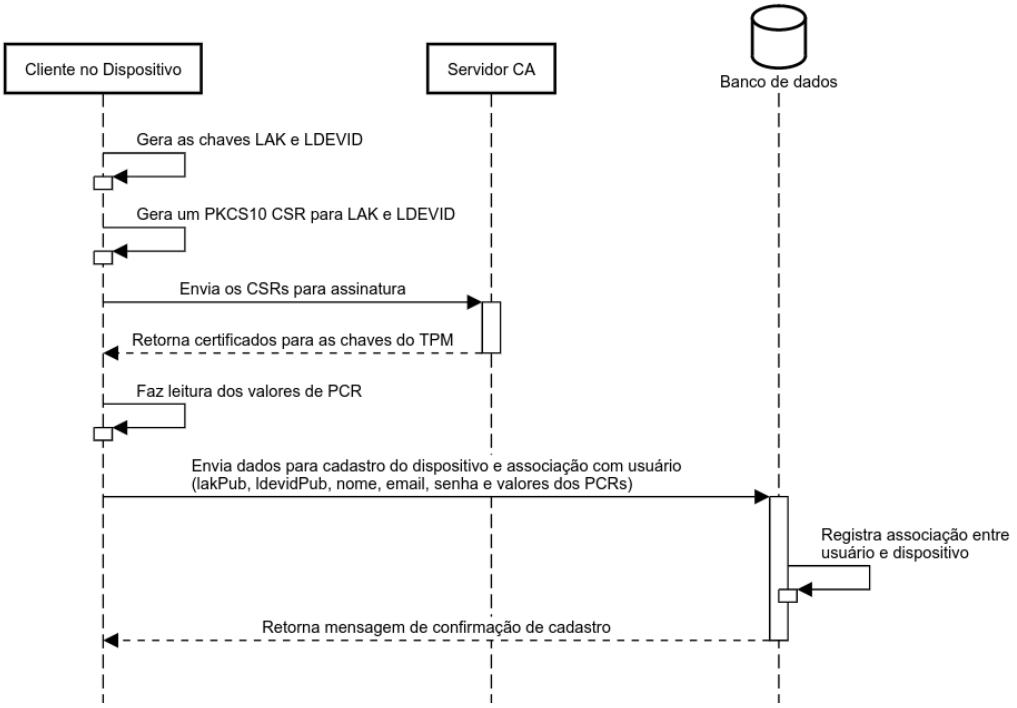

Figura 3. Fluxo de provisionamento

- **Envio ao dispositivo**: As credenciais inseridas, juntamente do *nonce*, são enviadas para o Cliente que fica em execução no dispositivo.
- **Geração do *quote***: O dispositivo gera um *quote* usando o TPM, onde a *hash* do email, senha e *nonce* será inserida no campo de dado extra.
- **Envio ao servidor**: As credenciais do usuário, o *quote*, juntamente de sua assinatura, e outras informações relevantes são enviadas ao servidor.
- **Verificação pelo servidor**: O servidor valida as informações recebidas. Ele verifica a autenticidade do *quote*, a validade das credenciais do usuário e do *nonce*, e garante que o dispositivo está íntegro e de fato pertence ao usuário.
- **Resultado da autenticação**: Caso todas as verificações sejam feitas com sucesso, o acesso ao sistema é autorizado. Caso contrário, o acesso é negado e o motivo é informado ao usuário.

Essa fase garante que a autenticação e a atestação ocorram de forma segura e que apenas um usuário, em posse de um dispositivo atrelado a ele, e que esteja em um estado confiável, possa acessar o sistema. O fluxo completo da Fase de Autenticação pode ser observado na Figura 4.

4. Experimentos

Esta seção apresenta os resultados do sistema de autenticação e atestação baseado em TPM. Os resultados foram analisados tendo como base os objetivos da solução, incluindo a geração e gerenciamento das chaves do TPM, a execução das duas fases principais, que são a de provisionamento e autenticação, além da verificação da segurança e eficiência do sistema, testando, por exemplo, o que acontece quando se erra a senha, quando há alguma alteração nos PCRs que não estava prevista, ou então quando um usuário tenta se autenticar com um dispositivo que não foi o destinado a ele.

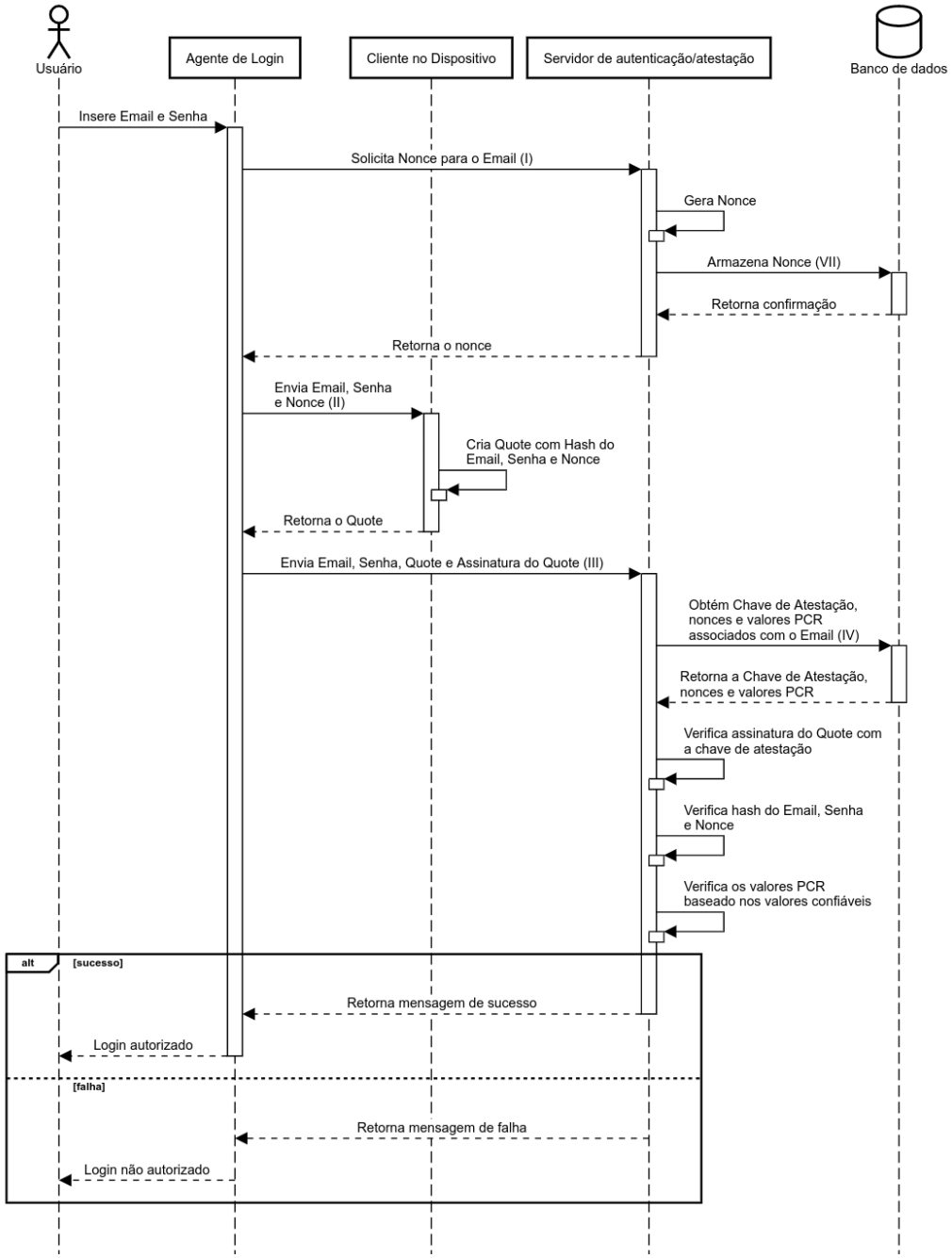

Figura 4. Fluxo de autenticação e atestação

4.1. Resultados

O sistema foi testado para garantir a correta geração e armazenamento das chaves geradas pelo TPM, assim como a possibilidade de utilizar as chaves depois de salvas no disco. Durante o provisionamento, foram geradas as seguintes chaves:(A) **EK**: Utilizada apenas para gerar a LAK e LDEVID, não foi utilizada para nenhuma verificação, pois não é do escopo deste trabalho; (B) **LAK**: Criada para possibilitar a assinatura dos *quotes*, permitindo a verificação da integridade do dispositivo por meio dos PCRs.; e, (C) **LDEVID**: Criada para estabelecer conexão mTLS com o servidor. Como explicado anteriormente, para a prova de conceito foi implementada a comunicação usando o Hy-

pertext Transfer Protocol, ou Protocolo de Transferência de Hipertexto (HTTP), mas na eventual implantação do sistema em algum ambiente real é indispensável utilizar mTLS [Ferreira et al. 2024, Portela et al. 2024a].

Os testes mostraram que as chaves permaneceram protegidas, mesmo após salvas no disco, graças ao processo de criptografia que as chaves privadas sofrem por parte do TPM antes de serem salvas, e que as operações de assinatura utilizando essas chaves ocorreram conforme esperado. Com isso, é possível criar quantas chaves forem necessárias, sem a limitação da memória do *chip*.

Nas Figuras 5 e 6 são apresentados o intervalo de confiança de 95% para os tempos de execução medidos para a geração, respectivamente, das chaves EK, LAK e LDEVID. Foram coletadas 10 amostras, e em cada uma as três chaves foram geradas usando *templates* padrões, como especificado em [Trusted Computing Group 2024] para a EK e em [Trusted Computing Group 2021] para LAK e LDEVID. A barra vertical representa o intervalo de confiança, enquanto o círculo central indica a média dos tempos coletados.

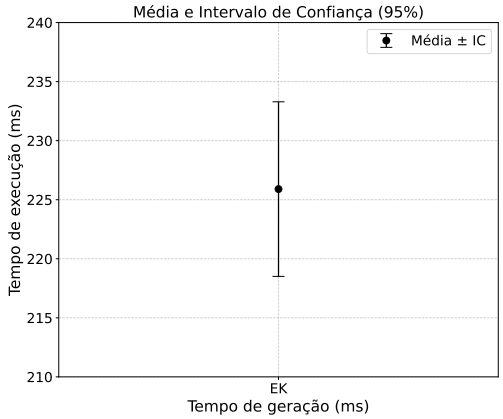

Figura 5. Intervalo de Confiança para os Tempos de geração da EK

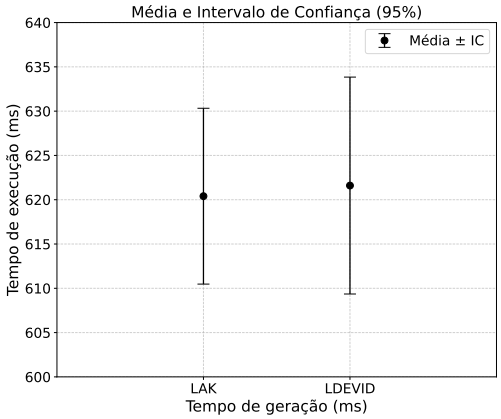

Figura 6. Intervalo de Confiança para os Tempos de geração da LAK e LDEVID

A fase de provisionamento foi avaliada considerando os seguintes aspectos: (a) **Geração do CSR**: A solicitação para emissão de certificado para as chaves do TPM foi corretamente gerada por parte do dispositivo e assinada pelo Servidor CA; (b) **Registro no Banco de Dados**: As informações do usuário e do dispositivo foram armazenadas no banco de dados, estabelecendo corretamente uma relação entre o usuário e o dispositivo.

Os testes demonstraram que todas as etapas do provisionamento foram feitas com sucesso, garantindo a correta associação entre usuário e dispositivo, de modo que não seja possível o usuário se autenticar com um dispositivo que não foi atrelado a ele.

Na Figura 7, é apresentado o intervalo de confiança de 95%, usando as mesmas 10 amostras, para os tempos de execução da Fase de Provisionamento. A barra vertical representa o intervalo de confiança, enquanto o círculo central indica a média dos tempos.

A fase de autenticação foi avaliada desde a inserção dos dados por parte do usuário até cada verificação realizada pelo servidor. Os resultados observados incluem:(1) **Geração do *quote***: O TPM gerou corretamente o *quote*, assinando corretamente com a

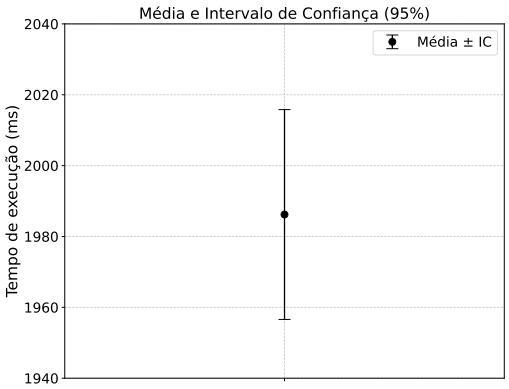

Figura 7. Intervalo de Confiança para os Tempos de Execução da Fase de Provisionamento

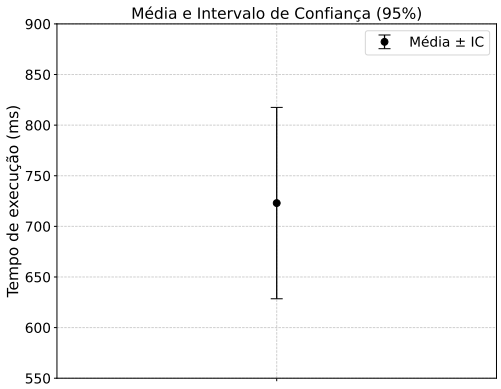

Figura 8. Intervalo de Confiança para os Tempos de Execução da Fase de Autenticação

chave LAK, sendo assim possível atestar o estado dos PCRs e também garantir a frescura dos dados graças ao *nonce*; e, (2) **Validação no Servidor**: O servidor conseguiu validar a combinação de email e senha do usuário, além de verificar a assinatura do *quote* e o próprio *quote*, incluindo os valores de PCR e o campo extra, que deve possuir a *hash* da concatenação do email, senha e *nonce*, tudo isso utilizando a chave de atestação pública que está devidamente atrelada ao usuário no banco de dados, garantindo assim a integridade do dispositivo antes de conceder a autorização.

A análise mostrou que a autenticação do usuário, juntamente com a vinculação ao dispositivo, funciona corretamente e oferece maior segurança do que métodos tradicionais baseados apenas em senha, já que, além da própria identidade do usuário, é garantido que o dispositivo por ele utilizado está em um estado confiável.

Na Figura 8, é apresentado o intervalo de confiança de 95%, também de 10 amostras, para os tempos de execução da Fase de Autenticação. A barra vertical representa o intervalo de confiança, enquanto o círculo central indica a média dos tempos coletados.

4.2. Segurança e Robustez da Solução

Além dos testes funcionais, foram realizados alguns experimentos para verificar o comportamento do sistema na eventualidade de cenários adversos. Os experimentos foram:

- **Erro na senha**: Quando um usuário inseriu uma senha incorreta, o sistema seguiu o comportamento esperado de rejeitar a autenticação sem a necessidade de verificar o restante dos dados, como o *quote*. Isso contribui para um tratamento mais ágil dos casos de falha.
- **Alteração nos PCRs**: Ao forçar uma mudança nos valores dos PCRs, fazendo com que os dados presentes no *quote* não coincidam com aqueles esperados pelo servidor, a autenticação foi negada. Esse comportamento demonstra que o sistema é capaz de detectar modificações no dispositivo corretamente e prevenir autenticações indevidas.

- **Uso de um dispositivo não autorizado**: Quando um usuário tentou se autenticar em um dispositivo diferente do que foi fornecido para ele, o servidor rejeitou a autenticação ao verificar que a chave de atestação do dispositivo não correspondia ao esperado, o que implica que a verificação da assinatura do *quote* falhou. Esse teste confirma que a solução impede o uso de dispositivos que não foram designados para um determinado usuário.

Os testes mostraram que o sistema é resiliente a ataques comuns e garante que apenas as combinações corretas de usuário e dispositivo, desde que estejam em um estado confiável, possam realizar a autenticação com sucesso.

4.3. Discussão Final

Os testes realizados demonstraram que a solução implementada atende aos requisitos de segurança e autenticidade esperados. A implementação do TPM permitiu que a autenticação de um usuário fosse vinculada ao dispositivo, aumentando a confiabilidade do processo. Todo esse ganho em segurança e praticidade veio ao custo de um tempo consideravelmente baixo de processamento, tanto para a fase de provisionamento, com a geração de chaves criptográficas e inserção de dados em um banco, mas principalmente para a fase de autenticação, que é a etapa onde o usuário, de fato, perceberia o impacto de um tempo de execução muito alto. Com a média de tempo por volta de $725\ ms$, o usuário facilmente mal perceberia que está ocorrendo toda uma série de verificações para ampliar sua segurança digital.

Vale ressaltar, também, que a capacidade de perceber qualquer alteração não autorizada e/ou prevista nos valores dos PCRs abre uma infinidade de possibilidades de casos de uso para os PCRs, uma vez que, apesar de alguns *indexes* possuírem uma função muito bem definida, existem alguns que estão disponíveis para que uma aplicação ou sistema operacional utilize da forma que melhor atenda a alguma necessidade específica. Com isso, é viável estabelecer políticas sobre o que deve ser medido em determinados PCRs e incluí-los na lista que será usada durante a geração do *quote*, ampliando a flexibilidade da solução proposta para os mais diversos cenários.

5. Conclusão

Este trabalho propôs um sistema de autenticação e atestação que vincula um usuário a um dispositivo utilizando TPM. A contribuição central desta solução para ambientes urbanos e teletrabalho reside na oferta de um método eficaz para reforçar a segurança digital sem sacrificar a usabilidade cotidiana dos usuários. Ao vincular rigidamente cada usuário ao seu dispositivo específico, e ao verificar continuamente a integridade do equipamento por meio do TPM, a proposta reduz significativamente o risco de acesso não autorizado em contextos nos quais os dispositivos podem estar frequentemente expostos a redes não confiáveis e ambientes inseguros. Essa característica é especialmente crítica no teletrabalho, onde funcionários acessam remotamente dados sensíveis das empresas a partir de diferentes locais e redes.

Os resultados obtidos demonstraram que a abordagem implementada fortalece significativamente a segurança do processo de autenticação, dificultando ataques baseados em roubo de credenciais ou comprometimento do ambiente do usuário. Adicionalmente, ao bloquear ataques comuns, como roubo ou vazamento de credenciais, *phishing* e

adulteração indevida do equipamento, a solução permite que as empresas e organizações operem com maior confiança e segurança na continuidade dos seus serviços.

Como próximos passos, pretendemos investigar técnicas para reduzir o tempo de autenticação sem comprometer a segurança, por meio de otimizações no processo atual e/ou da utilização de algoritmos alternativos de chave, como a Elliptic Curve Cryptography, ou Criptografia de Curva Elíptica (ECC) [Ramsdell 2010]. Uma possibilidade de otimização é armazenar a chave EK em uma área de memória não volátil do TPM, evitando sua recriação a cada autenticação. Outra proposta é modificar o processo de verificação para que, em caso de senha incorreta, não haja necessidade de interação com o TPM, o que pode reduzir o tempo de execução e, simultaneamente, mitigar ataques de força bruta ao dispositivo. Além disso, pretendemos ampliar a aplicação da solução para diferentes contextos, como controle de acesso físico, assinatura digital de documentos ou autenticação em sistemas embarcados. Por fim, planeja-se realizar análises de segurança mais aprofundadas, incluindo testes contra ataques mais sofisticados que visem comprometer o *firmware* do TPM.

6. Agradecimentos

Os autores agradecem ao Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) (N^o 303877/2021-9 e N^o 405976/2022-4) pelo apoio financeiro e a Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001.

Referências

Angafor, G. N., Yevseyeva, I., and Maglaras, L. (2024). Securing the remote office: reducing cyber risks to remote working through regular security awareness education campaigns. *International Journal of Information Security*, 23(3):1679–1693.

Ferreira, M. C., Ribeiro, S. E., Nobre, F. V., Linhares, M. L., Araújo, T. P., and Gomes, R. L. (2024). Mitigating measurement failures in throughput performance forecasting. In *2024 20th International Conference on Network and Service Management (CNSM)*. IFIP.

Fiolhais, L. and Sousa, L. (2023). Qr tpm in programmable low-power devices.

Gomes, R., Junior, W., Cerqueira, E., and Abelem, A. (2010). A qoe fuzzy routing protocol for wireless mesh networks. In Zeadally, S., Cerqueira, E., Curado, M., and Leszczuk, M., editors, *Future Multimedia Networking*, pages 1–12, Berlin, Heidelberg. Springer Berlin Heidelberg.

Pinheiro, B., Nascimento, V., Gomes, R., Cerqueira, E., and Abelem, A. (2011). A multimedia-based fuzzy queue-aware routing approach for wireless mesh networks. In *2011 Proceedings of 20th International Conference on Computer Communications and Networks (ICCCN)*, pages 1–7.

Portela, A., Linhares, M. M., Nobre, F. V. J., Menezes, R., Mesquita, M., and Gomes, R. L. (2024a). The role of tcp congestion control in the throughput forecasting. In *Proceedings of the 13th Latin-American Symposium on Dependable and Secure Computing*, LADC '24, page 196–199, New York, NY, USA. Association for Computing Machinery.

Portela, A. L., Menezes, R. A., Costa, W. L., Silveira, M. M., Bittecnourt, L. F., and Gomes, R. L. (2023). Detection of iot devices and network anomalies based on anonymized network traffic. In *NOMS 2023-2023 IEEE/IFIP Network Operations and Management Symposium*, pages 1–6.

Portela, A. L. C., Ribeiro, S. E. S. B., Menezes, R. A., de Araujo, T., and Gomes, R. L. (2024b). T-for: An adaptable forecasting model for throughput performance. *IEEE Transactions on Network and Service Management*, pages 1–1.

Ramsdell, B. (2010). RFC 5753: Use of Elliptic Curve Cryptography (ECC) Algorithms in Cryptographic Message Syntax (CMS). Request for Comments 5753.

Rekha, K. S., Sivagami, V., Usharani, R., Amutha, T., and Pushparani, S. (2024). Implementing multi-factor authentication in cloud services for enhanced security. In *2024 International Conference on Recent Advances in Science and Engineering Technology (ICRASET)*, pages 1–5. IEEE.

Silva, M., Ribeiro, S., Carvalho, V., Cardoso, F., and Gomes, R. L. (2023). Scalable detection of sql injection in cyber physical systems. In *Proceedings of the 12th Latin-American Symposium on Dependable and Secure Computing*, LADC '23, page 220–225, New York, NY, USA. Association for Computing Machinery.

Silveira, M. M., Portela, A. L., Menezes, R. A., Souza, M. S., Silva, D. S., Mesquita, M. C., and Gomes, R. L. (2023). Data protection based on searchable encryption and anonymization techniques. In *NOMS 2023-2023 IEEE/IFIP Network Operations and Management Symposium*, pages 1–5.

Souza, M. S., Ribeiro, S. E. S. B., Lima, V. C., Cardoso, F. J., and Gomes, R. L. (2024). Combining regular expressions and machine learning for sql injection detection in urban computing. *Journal of Internet Services and Applications*, 15(1):103–111.

Trusted Computing Group (2019a). Tcg trusted attestation protocol (tap) information model. Technical report, Trusted Computing Group.

Trusted Computing Group (2019b). Tpm 2.0 library specification, part 1: Architecture, revision 1.59. Technical report, Trusted Computing Group.

Trusted Computing Group (2021). Tpm 2.0 keys for device identity and attestation, version 1.12. Technical report, Trusted Computing Group.

Trusted Computing Group (2024). Tcg ek credential profile for tpm family 2.0; level 0, version 2.6. Technical report, Trusted Computing Group.

Wang, X., Yan, Z., Zhang, R., and Zhang, P. (2021). Attacks and defenses in user authentication systems: A survey. *Journal of Network and Computer Applications*, 188:103080.

Xavier, H. B., de Barros Sampaio, S. C., Falcão Sobral, M. F., and Cormican, K. (2024). From the table to the sofa: The remote work revolution in a context of crises and its consequences on work attitudes and behaviors. *Education and Information Technologies*, pages 1–40.