PRESIDÊNCIA DA REPÚBLICA - CASA CIVIL
SCN, Quadra 02 Bloco E - CEP 70712-905 - Brasília/DF
Telefone: (61) 3424-3850 - https://www.iti.gov.br

Nota Técnica

1. Introdução

O Instituto Nacional de Tecnologia da Informação – ITI, autarquia federal vinculada à Casa Civil da Presidência da República do Brasil, encaminha esta Nota Técnica sobre as perspectivas, diretrizes, objetivos e cenários técnicos no âmbito de atuação e conhecimento do corpo técnico do ITI e da Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil, correlacionadas às tecnologias criptográficas e de identificação digital, para o ano de 2020. O ITI está à disposição dos usuários de serviços digitais, gestores de aplicações e agentes públicos do Brasil, assim como das entidades credenciadas da ICP-Brasil, para esclarecer todos os assuntos elencados neste documento.

A. Organização:

Esta Nota Técnica está organizada nas seguintes seções:

– Na seção 2, é comentada a criptografia pós-quântica.

– Na seção 3, são abordados os esquemas de assinatura em *hash*.

– Na seção 4, é destacado o assunto das redes *blockchain*.

– Na seção 5, é feito um compilado de assuntos que envolvem a segurança em redes 5G, *Internet of Things* – IoT – e Cidades Inteligentes.

– Na seção 6, são comentadas as identidades digitais.

– Na seção 7, é comentada a Lei Geral de Proteção de Dados – LGPD.

– Na seção 8, é abordada a ICP-Brasil.

– Na seção 9, traz a conclusão desta Nota Técnica.

2. Criptografia Pós-Quântica

O Instituto Nacional de Padrões e Tecnologia do Governo Americano – NIST (acrônimo em inglês) – iniciou ao final do ano de 2016 uma competição mundial de novos algoritmos de chaves públicas para cifra e estabelecimento de chaves, assim como para as assinaturas digitais [1-3]. Essa competição mundial indicará uma mudança criptográfica dos algoritmos de chaves públicas mais usados no mundo digital [4-10], inclusive todos os usados na ICP-Brasil [11]. Esta mudança é consequência do fato que os atuais e mais conhecidos algoritmos para, *e.g.*, assinaturas digitais e encriptação usando chaves públicas poderão estar inseguros nos próximos anos devido os já conhecidos processos matemáticos, que permitem fatorar grandes números inteiros e calcular logaritmos discretos em tempo polinomial [12, 13], não mais representarem desafios computacionais inviáveis, em tempo de execução. Um computador quântico [14-17] operacional e eficiente, com alguns milhares de *qubits* lógicos, caso for construído, estará apto a quebrar os mais conhecidos algoritmos usados para essas funções criptográficas. Esses avanços tecnológicos impõem, também, o uso adequado de tamanhos, em *bits*, de chaves e saídas em algoritmos de cifras de blocos e funções *hash* [18]. Entre os anos de 2022 e 2024 estão previstos os primeiros *drafts* destes novos algoritmos de chaves públicas. Para mais detalhes sobre essa competição, por favor refira-se ao Anexo I deste documento.

O ITI, em sua missão institucional [19], acompanhará ao longo do ano de 2020 as discussões técnicas, criptoanálises e eventos (inclusive com a proposta de um curso de capacitação e palestras no Brasil) desses novos algoritmos. Ademais, será discutido, com a participação da indústria e academia, um desenho de projetos, bibliotecas e formas de implementações de alguns desses conceitos matemáticos. Não se sabe quando esses computadores quânticos, com essa capacidade, estarão operacionais e eficientes, mas reconhece-se, conforme demonstrado, que é obrigatório o planejamento de um novo *parquet* criptográfico para a segurança do mundo digital, protegendo as aplicações digitais nas próximas décadas, pelo menos de ataques atualmente conhecidos. **Entretanto, a Medida Provisória 2.200-2 – MP 2.200-2 – de 24 de agosto de 2001 [20], ditame legal que cria a ICP-Brasil, da forma como está escrita, não recepciona e admite parte desse futuro tecnológico que se aproxima. O ITI alerta que é necessária a tempestiva alteração desta lei para que o Brasil esteja tecnicamente em acordo com o futuro de uma infraestrutura de chaves públicas**.

3. Esquemas de assinatura baseada em *hash* (*Merkle-Tree*)

Assinatura baseada em *hash* (*hash-based signatures*) é um esquema para cálculos de uma assinatura digital, no qual o fundamento matemático foi inicialmente proposto por Lamport [21] e redefinido por Merkle [22]. Anos após as primeiras propostas, redefinições e aprimoramentos, existem dois esquemas que estão formalmente definidos em *Request For Comments* – RFC [23, 24]. Ademais, dentre os nove algoritmos restantes para esquemas de assinaturas digitais na competição comentada do NIST [3], também está classificado o algoritmo de chave pública baseado em *hash* chamado de Sphincs$^+$ [25, 26][1]. Entretanto, pela alta complexidade de avaliação e padronização destes algoritmos nesta competição, comentada na Seção 2, até o próprio NIST considera que o resultado final pode, ainda, demorar algum tempo.

Por isso, no dia 13/12/2019, o NIST convidou toda comunidade criptográfica a comentar o "*Draft NIST Special Publication (SP) 800-208. Recommendation for Stateful Hash-Based Signature Schemes"* [27]. A equipe técnica do ITI transcreve, em inglês, o convite, com grifo nosso.

"NIST invites comments on Draft NIST Special Publication (SP) 800-208, Recommendation for Stateful Hash-Based Signature Schemes. ***All of the digital signature schemes specified in Federal Information Processing Standards Publication (FIPS) 186-4 will be broken if large-scale quantum computers are ever built****. NIST is in the process of developing standards for post-quantum secure digital signature schemes that can be used as replacements for the schemes that are specified in FIPS 186-4. However, this standardization process will not be complete for several years.*

In this draft recommendation, NIST is proposing to supplement FIPS 186 by approving the use of two stateful hash-based signature schemes: the eXtended Merkle Signature Scheme (XMSS) and the Leighton-Micali Signature system (LMS) as specified in Requests for Comments (RFC) 8391 and 8554, respectively*. Stateful hash-based signature schemes are not suitable for general use since they require careful state management in order to ensure their security. However, their use may be appropriate for applications in which use of the private key may be carefully controlled and where there is a need to transition to a post-quantum secure digital signature scheme before the post-quantum cryptography standardization process has completed.*

Draft SP 800-208 profiles LMS, XMSS, and their multi-tree variants. This profile approves the use of some but not all of the parameter sets defined in RFCs 8391 and 8554. The approved parameter sets use either SHA-256 or SHAKE256 with 192- or 256-bit outputs. This profile also requires that key and signature generation be performed in hardware cryptographic modules that do not allow secret keying material to be exported."

[1] O algoritmo Picnic, também classificado entre os nove, é um novo desenvolvimento, também baseado em funções *hash*, com cifra de blocos e provas de zero conhecimento.

A proposta do NIST é construir, imediatamente, padrões para esquemas de assinaturas em *hash*. Estes dois algoritmos de assinaturas apresentados, que não servem para aplicações de uso geral, XMSS [23, 28] e LMS [24, 29], segundo o NIST, possuem uso apropriado em "aplicativos em que o uso da chave privada pode ser cuidadosamente controlado e onde é necessário fazer a transição para um esquema de assinatura digital segura pós-quântico antes que o processo de padronização da criptografia pós-quântico seja concluído".

Nesses algoritmos, as chamadas "chaves públicas", ou chaves de verificação, são atualizadas (*state*) à medida que uma assinatura é feita com uma chave criptográfica (cada chave deve ser usada para assinar somente uma mensagem). Todo conceito matemático para assinatura e verificação se altera, comparado com os atuais da ICP-Brasil. Nessas infraestruturas em *hash*, deixam de existir os conhecidos certificados digitais atualmente comercializados na ICP-Brasil e nas PKI (acrônimo em inglês para ICP) pelo mundo. Tecnicamente, estas plataformas de assinatura conviverão com as plataformas de assinaturas baseadas em chaves públicas, atuais e futuras. É disso que trata o chamado do NIST. As assinaturas em *hash* possuem conceitos matemáticos amplamente estudados e atualmente seguros [30][2] e já estão sendo usadas em plataformas de governo, em conjunto com redes Blockchain, como na Estônia [31-33]. Para mais detalhes sobre as assinaturas em *hash*, por favor refira-se ao Anexo II deste documento.

O ITI, em sua missão institucional, acompanhará as discussões técnicas e proporá ao NIST, ao longo do ano de 2020, adendos para o *Draft NIST Special Publication (SP) 800-208*. **Entretanto, mais uma vez, a MP 2.200-2 não recepciona e admite esse marco tecnológico que se aproxima. O Brasil ainda não possui marco legislativo amparando esses tipos de assinaturas. O ITI alerta que é necessária a tempestiva formação de uma lei para que o Brasil esteja tecnicamente em acordo com o futuro das assinaturas digitais. Outras infraestruturas de assinaturas poderão surgir, em conjunto com as novas e com diferentes propósitos de uso infraestruturas de chaves públicas. O Brasil deve estar pronto legislativamente e tecnicamente para a recepção e utilização de diferentes tecnologias e propósitos de assinatura para as mais diversas aplicações, públicas e privadas**.

[2] Como toda infraestrutura de assinatura, além do conceito matemático seguro, é necessário que as implementações e procedimentos de geração e uso de uma chave sejam, também, seguros.

4. Blockchain

Em 2020, o ITI pretende apresentar um projeto com a solução integrada de *blockchain* para o governo brasileiro, aprimorando ideias concebidas [33-48], incluindo novas, normatizando um barramento entre as entidades públicas. Também, ao longo do ano, será apresentado um projeto para algumas aplicações internas das entidades credenciadas na ICP-Brasil. Acredita-se que tecnicamente, e do ponto de vista do cidadão, os projetos de órgãos e entidades na esfera do governo federal não deveriam ser segregados em redes e protocolos diferentes e, ademais, é necessário atenção aos algoritmos e os procedimentos que são utilizados em alguns desses protocolos [49-55]. Nesse ponto comenta-se que alguns desses protocolos em redes *blockchain* conhecidos já estão em processo de estudo para alteração de seus algoritmos criptográficos [56, 57], preparando-as para a mudança pós-quântica que se aproxima.

É importante esclarecer e chamar a atenção para algumas questões sobre as tão comentadas redes *blockchain*, cuja consecução está baseada em assinaturas digitais e ligações criptográficas dos ativos digitais. Toda rede *blockchain* possui uma plataforma para emissão de chaves criptográficas de assinatura e verificação; não há conflito entre *blockchain* e assinaturas com chaves públicas[3]. O fato a se observar, porém, é que várias soluções em *blockchain* não possuem o devido processo de identificação de seus usuários, não tem interoperabilidade entre diferentes protocolos (cada usuário terá que ter sua *wallet* para as diferentes redes), muitas vezes sem o devido critério de confiança temporal, usando, *e.g.*, somente o tempo do bloco na rede, e sem a mínima segurança do ciclo de vida das chaves, dos algoritmos usados ao controle, requisição e emissão do par de chaves. Então, consequentemente, não há como, do ponto de vista técnico pericial, presumir veracidade e eficácia probatória enquanto esses processos inexistirem. É possível, entretanto, modificar esse cenário sobre redes *blockchain* e aperfeiçoá-los. A Estônia, *e.g.*, já fez algumas das adequações necessárias [33]. Para mais detalhes sobre redes *blockchain*, por favor refira-se ao Anexo III deste documento.

O ITI acompanhará, portanto, as discussões em 2020 sobre redes *blockchain* implementadas, principalmente as governamentais e legislações sobre o tema. O ITI, conforme colocado, possui soluções para uma rede *blockchain* no governo federal. **Ressalta-se, mais uma vez, que a MP 2.200-2 não está pronta para esse marco tecnológico existente. O ITI alerta que é necessária a tempestiva alteração desta lei, que trata de criptografia, para a recepção desta e de outras tecnologias**.

[3] O fato é que a maioria dos protocolos em *blockchain* não aceitam ou seriam capazes de verificar a assinatura digital realizada com certificados ou chaves externos a sua concepção.

5. 5G, IoT e Cidades Inteligentes

O ITI observará as regulamentações e implantações da rede 5G no Brasil e no mundo, assim como projetos em IoT e Cidades Inteligentes. O foco será na parte de segurança criptográfica dos dispositivos nas redes 5G [58], amplamente implementada em comparação às redes *Long-Term Evolution* – LTE, e na segurança, quanto ao propósito de uso, e na comunicação segura dos dispositivos com capacidade de interação de dados.

No contexto das redes 5G [58-60], existem três classes de usos distintos, em alto nível e para propósitos de simplificação do escopo para cada aplicação:

i. banda larga móvel aprimorada – eMBB (acrônimo em inglês), em relação ao usuário, é o primeiro serviço já normatizado e propriamente aproveitado das redes 5G permitindo volumes de dados maiores e uma experiência aprimorada do usuário, *e.g.*, ao suportar altas taxas de dados para as aplicações dos usuários finais.

ii. comunicação massiva de tipo de máquina – mMTC (acrônimo em inglês), corresponderá a classe de uso caracterizada por um elevado número de dispositivos, *e.g.*, sensores e monitores dos dispositivos. Os principais requisitos para esses serviços incluem a mitigação do consumo de energia e um custo muito baixo do dispositivo, permitindo um aumento da vida útil muito longa da bateria do dispositivo. Cada dispositivo consome e gera apenas uma quantidade relativamente pequena de dados, ou seja, o suporte a altas taxas de dados é de menor importância. É importante deixar claro que essa classificação está em alto nível, *e.g.*, pode haver casos de uso que exijam dispositivos de custo muito baixo, mas onde a possibilidade de uma vida útil da bateria muito longa não é tão importante.

iii. comunicação ultra confiável e de baixa latência – URLLC (acrônimo em inglês), classe de serviços que exige baixa latência e confiabilidade extremamente alta. Dispositivos cada vez mais relacionados a implementação de inteligência artificial, *machine learning* como carros automáticos, segurança no trânsito, controle automático e automação de fábrica, cidades inteligentes farão parte dessa classe de serviços. É importante deixar claro que essa classificação está em alto nível, *e.g.*, pode haver serviços que exigem confiabilidade muito alta, mas para os quais os requisitos de latência não são tão críticos.

Fica claro que a evolução do 5G habilitará que dispositivos estejam interconectados formando uma rede IoT. O ITI ressalta que é importante, para que uma rede 5G/IoT seja confiável, que se mantenha a segurança dos dispositivos e da

comunicação entre os mesmos. É possível realizar ataques em redes 5G/IoT mal implementadas [61], sem contar todos os possíveis ataques nos dispositivos. Ao longo dos últimos anos o ITI aproximou-se dessas classes de uso para dispositivos com a proposta de criação dos certificados A CF-e-SAT e OM-BR para a ICP-Brasil [62]. Esses projetos visam dotar os equipamentos de cupom fiscal e de metrologia, no âmbito do INMETRO, de uma chave criptográfica para aumentar a segurança dos resultados advindos desses dispositivos, combatendo massivamente a fraude e ampliando a proteção de dados transacionados.

Sobre cidades inteligentes e aplicações aos usuários, o ITI acompanhará e promoverá debates ao longo de 2020. Alguns projetos e perspectivas que acompanharemos, estritamente focados nas tecnologias criptográficas, de *machine learning* e inteligência artificial, de escopo geral, para ilustração, em 2020 são: Uber *Air flying taxi service* [63], projetos de automação e eletricidade em prédios e carros, com os *hubs* de mobilidade e zonas livres de carros, e questões envolvendo privacidade e segurança dos dados e do próprio cidadão, com o aumento do fluxo de dados entre aplicações.

Ressalta-se, mais uma vez, que a MP 2.200-2 não considerou esses avanços tecnológicos existentes. A razão é que dispositivos móveis com alta capacidade de processamento, armazenamento e interação por meio de aplicativos, inclusive com uso de biometrias, 5G-IoT/*Device-to-Device*, uso massivo de Inteligência Artificial e *Machine Learning*, entre outros, não existiam ou eram incipientes em 2001. A ICP-Brasil, com preços amplamente acessíveis, agilidade, modernidade e menos burocracia, deveria contribuir com esses avanços, propondo plataformas criptográficas para todas essas aplicações.

6. Identificações Digitais

O ITI tem interesse nos projetos do Governo Federal e dos Estados em relação às identidades digitais. Alguns Estados e entes do Governo Federal já estão provendo aos cidadãos soluções em identidade digital, algumas delas providas por aplicativos em dispositivos móveis. Outro projeto que o ITI observará é o Documento Nacional de Identificação – DNI [64]. O ITI repisa que é fundamental para qualquer aplicação, inclusive as criptográficas, que o Brasil tenha um sistema de identificação do seu cidadão robusto, baseado em identificação biométrica segura.

É também importante esclarecer que processos tecnológicos de autenticação de uma pessoa em um sistema, como usuário/senha e biometria, não realizam, com a devida presunção de veracidade, assinaturas digitais em documentos eletrônicos. Essas

assinaturas eletrônicas simples não possuem concomitantemente os pressupostos fáticos e jurídicos de presunção de veracidade, autoria, integridade, autenticidade, confidencialidade, temporalidade e, por consequência, não repúdio. Para tal presunção, ainda são necessários o estabelecimento e geração de dispositivos criptográficos, com implementações e plataformas seguras, seguidas de procedimentos de identificações robustos. Somente dessa forma é possível atribuir esses pressupostos a um documento eletrônico.

Ressalta-se que o ITI possui a expertise necessária para propor soluções robustas para esse tipo de identificação digital do cidadão, inclusive com a promoção de padrões de interoperabilidade para que, assim como um documento de viagem, possa ser lido e validado em qualquer país do mundo. Inclui-se nessas soluções, a construção de bases para uma rede biométrica on-line, como a devida definição de fluxos, tratamento de exceções, disponibilidade, segurança e proteção dos dados e da privacidade do cidadão.

7. LGPD

A Lei Geral de Proteção de Dados Pessoais – LGPD [65] – traz desafios e oportunidades, seja no âmbito público, seja no privado. Com vigência a se iniciar em agosto deste ano de 2020, toda entidade, quanto ao tratamento de dados pessoais que utiliza em suas atividades internas ou na prestação de serviços ao cidadão brasileiro, deverá revisar e ajustar sua política de governança de dados e respectivos sistemas de gestão de segurança da informação e comunicação, de modo a estar em conformidade com a lei. O desafio está na complexidade envolvida, dado que as exigências legais são muitas, ao garantir ao cidadão a titularidade e o domínio de seus dados pessoais mesmo quando sob custódia de terceiros. A oportunidade se materializa numa governança e gestão de dados mais séria, profissional, tecnológica, de modo a proporcionar serviços com mais qualidade e segurança.

Tecnologias criptográficas, a exemplo de chaves criptográficas, certificados digitais, assinaturas digitais, são fundamentais para se garantir autenticações seguras no acesso a dados pessoais e assinaturas de consentimentos de coleta, uso, compartilhamento e demais tratamentos de dados pessoais. A criptografia é essencial para a boa governança de dados pessoais e a garantia de entrega dos direitos do cidadão.

O ITI participará ao longo do corrente ano de atividades que endereçam o tema da LGPD, seja proferindo palestras em eventos e reuniões temáticas sobre soluções criptográficas para o tratamento de dados pessoais, seja apoiando atividades regulatórias e orientadoras acerca do tema. Neste item, em especial, o ITI integra o Comitê Central de Governança de Dados – CCGD (Decreto 10.046, de 9 de outubro de 2019), representando

a Casa Civil da Presidência da República, e colabora, no âmbito do subcomitê LGPD, na elaboração de um guia de orientação à Administração Pública quanto à preparação e adequação à LGPD.

8. ICP-Brasil

A. Resoluções.

O ITI[4] acompanhará atentamente a evolução das Resoluções nº 151 e 155 [66], aprovadas pelo Comitê Gestor da ICP-Brasil – CG-ICP-Brasil – em 2019. Essas trouxeram substanciais mudanças para a ICP-Brasil quanto a simplificação de processos, com redução de custos para as entidades credenciadas, ampliação dos requisitos de segurança lógicos e sobre a confirmação de cadastro do usuário já realizado presencialmente por uma Autoridade de Registro – AR. Em mais de 18 anos, com pouco mais de 8 milhões de certificados digitais ativos, a maioria emitidos para pessoas jurídicas, e menos de 3% da população brasileira alcançada, o ITI espera que o ambiente criado possa reduzir os preços de um certificado digital ICP-Brasil, simplificar os processos de emissão com adoção de mais processos lógicos, facilitar a inclusão de novos usuários e o uso de um certificado digital e desburocratizar o atendimento, mantendo a já conhecida segurança da ICP-Brasil. Ademais, a equipe técnica do ITI, cumprindo sua missão institucional, continuará estudando e propondo soluções técnicas e procedimentais para que a ICP-Brasil se torne ainda mais dinâmica, acessível, de fácil uso, transparente e segura para todos os seus usuários.

Observação: em relação às aplicações e certificados da ICP-Brasil, o ITI não recomenda mais o uso de SHA1 para as assinaturas em qualquer documento devido às fragilidades encontradas no processo [67].

B. WebTrust SSL.

O ITI aguarda, para o mês de Fevereiro de 2020, a publicação pelo governo americano (NIST) do selo [68] para os equipamentos da Autoridade Certificadora Raiz do Brasil – AC-Raiz. Em fase final de acreditação, a publicação do selo por parte do NIST dará início a auditoria WebTrust SSL da ICP-Brasil. O ITI, enquanto AC-Raiz, e as ACs subsequentes estão preparados para as respectivas auditorias [69]. A consecução das auditorias permitirá, posteriormente e para alguns navegadores ainda no primeiro semestre de 2020, que os certificados da ICP-Brasil possam ser incorporados automaticamente nos repositórios confiáveis dos sistemas operacionais, terminando com

[4] É importante lembrar, pelo descrito na MP-2.200-2, que o ITI não controla os preços dos certificados digitais emitidos na ICP-Brasil, assim como não emite certificados digitais ao usuário final.

a sinalização de erro aos usuários.

C. Acordos Internacionais.

No contexto internacional, ITI e Ministério das Relações Exteriores – MRE – darão continuidade aos trâmites necessários à internalização do Acordo de Reconhecimento Mútuo de Certificados de Assinatura Digital do Mercosul, assinado em 05 de dezembro de 2019, durante a Cúpula do Vale dos Vinhedos em Bento Gonçalves/RS. O acordo seguirá para aprovação do Congresso Nacional, o que se dará por meio de decreto legislativo e, posteriormente, deverá ser promulgado pelo Senhor Presidente da República mediante decreto presidencial. Após isto, então, o acordo passará a vincular e obrigar no plano do direito positivo interno brasileiro. Durante esse mesmo período, reuniões técnicas entre os Estados Partes (Argentina, Brasil, Paraguai e Uruguai), representados por suas Autoridades Certificadoras Raízes, discutiram e definiram os procedimentos operacionais a serem adotados na validação de certificados e assinaturas digitais provenientes de cada um dos países.

Noutra frente internacional, dando continuidade às conversações iniciadas durante o 11º Diálogo de Economia Digital União Europeia – Brasil, realizado em 26 de novembro de 2019 em Bruxelas/Bélgica, ITI e UE estão construindo uma agenda de cooperação técnica para o ano de 2020 com o intuito principal de lograr a assinatura de um Acordo de Reconhecimento Mútuo de Assinaturas Eletrônicas entre a UE e o Brasil.

Ao longo das atividades estabelecidas na agenda, outros temas serão também objeto de troca de conhecimento e experiências, a exemplo de Blockchain, algoritmos criptográficos híbridos e pós-quânticos e Internet das Coisas (IoT). Visitas técnicas estão previstas como, a participação brasileira na *Blockchain Expo Europe 2020* e a participação europeia durante o CertForum 2020, que contará com um painel específico sobre o eIDAS[5] (*Electronic Identification, Authentication and Trust Services*) e também com o 1º Encontro Internacional sobre Assinaturas Eletrônicas.

O uso crescente de transações eletrônicas no mundo, nas relações G2G, B2B, B2C, especialmente em matéria de comércio eletrônico, comércio exterior, dentre outras, demandam que os países se adequem e promovam a inclusão digital de seus cidadãos, por meio de medidas que garantam segurança e confiança aos documentos, processos e transações eletrônicas. Nesse sentido, percebe-se um maior interesse e o surgimento de oportunidades para a construção de outros acordos de reconhecimento mútuo de assinaturas eletrônicas, a exemplo do celebrado no Mercosul e do em construção com a UE. Aliança do Pacífico, Comunidade dos Países de Língua Portuguesa, Portugal, Moçambique, Catar, Emirados Árabes Unidos, BRICS, representam outras frentes possíveis de desenvolvimento de trabalho ao longo de 2020.

[5] É esperada uma nova versão do eIDAS para 2020.

D. Protocolo de Tempo.

A Entidade de Auditoria do Tempo – EAT – da ICP-Brasil possui uma solução denominada Sistema de Auditoria e Sincronismo – SAS – que tem como objetivos 3 funções na rede de carimbo de tempo:

i. estabelecer uma conexão segura entre o SAS e os Sistemas de Carimbo de Tempo – SCT – das Autoridades de Carimbo de Tempo – ACTs;

ii. verificar a hora correta nos SCTs, comparar com a hora da escala de tempo de nossa infraestrutura e ajustar a frequência do SCT para sincronizar com os osciladores de césio da EAT (Sincronismo);

iii. uma vez estabelecido o sincronismo, emitir um alvará de funcionamento (*hash*) temporário para o SCT, de forma a atestar que o SCT está sincronizado com a escala de tempo da EAT, garantindo assim que os carimbos de tempo emitidos pela ACT durante o período de validade do alvará possuem exatidão em relação a hora correta (Auditoria).

O ITI apresentará um projeto de desenvolvimento de um novo protocolo de carimbo do tempo para a EAT. O objetivo é garantir a interoperabilidade entre um novo SAS a ser desenvolvido para o ITI e os equipamentos utilizados pelas ACTs, utilizando-se um protocolo de comunicação e sincronismo de tempo que seja aberto (*open source*), sem as limitações de propriedade intelectual inerentes as soluções existentes no mercado atualmente e que esteja de acordo com os padrões adotados pela ICP-Brasil na EAT. Desta forma, busca-se concentrar em uma única solução SAS a comunicação com todas as ACTs independente do fabricante dos equipamentos adotados pela ACT, que poderá desenvolver ou contratar sua própria solução SCT, aumentando assim a competitividade entre as empresas fornecedoras, a confiabilidade da solução, a continuidade do negócio e contribuindo assim com o avanço tecnológico da ICP-Brasil.

E. Auditoria.

A área de auditoria do ITI não poderia estar de fora das mudanças previstas. Afinal, todas estas tecnologias disruptivas colocam a Auditoria tradicional em cheque. Somos uma organização que está calcada em tecnologia. Sendo assim, temos também a obrigação de ter um olhar para o futuro no sentido de buscar aplicabilidade e, acima de tudo, ampliação de uso das tecnologias emergentes para a melhoria do nosso trabalho como um todo. É isto que vai garantir a solidez e perenidade dos mecanismos de segurança que produzimos hoje, na ICP-Brasil.

A missão da auditoria é prestar avaliação objetiva confiável sobre a adequação e eficácia dos controles, processos e estruturas implementadas na busca de melhorar a percepção e transmissão de confiança à comunidade de usuários de um sistema. Além da independência estrutural, a objetividade da auditoria é possibilitada por ter e aplicar uma mentalidade objetiva, aderindo a um processo rigoroso e sistemático alinhando-se às normas e padrões amplamente aceitos, contudo o papel do auditor não substitui a obrigação da organização (entidades da ICP Brasil) de monitorar riscos e adotar mecanismo de *compliance*.

O modelo tradicional de trabalho precisa ser revisto. Isto é fato.

A lista das tecnologias disruptivas é grande e não vai parar de crescer porque, simplesmente, o surgimento de novas descobertas não dependem de um único fator, mas da combinação deles fundamentados por novos estudos e pesquisas.

Seguindo esta tendência de mudança a Auditoria também deve remodelar-se para acompanhar os movimentos em torno de uma nova forma de trabalho. Não se trata de ter mais trabalho, mas de trabalhar melhor a partir da conexão entre infraestrutura, plataformas de soluções, recursos e pessoas capacitadas. Não podemos esquecer também as novas legislações como a LGPD que impactará nas auditorias.

O sucesso da aplicação dessas tecnologias está na escolha de quais podem ser utilizadas e, se será isoladamente ou em conjunto. O desafio será descobrir a forma correta (encontrar talentos com expertise, *know-how*) de implementar todos esses novos componentes com efetividade e segurança.

A Auditoria passará por mudança apoiada em conceitos como o de analytics para apoiar o trabalho dos auditores, o que permitirá amostragens qualificadas das informações a serem analisadas. Sistemas de apoio com relatórios padronizados, recursos de *business intelligence* (BI) e IA podem proporcionar agilidade ao trabalho do auditor e auxiliar na prevenção de fraudes. São ferramentas empregadas em várias áreas e que podem também ser empregadas em prol da auditoria.

Os 5 (cinco) pilares [70] que norteiam a auditoria são representados por:

- *Intelligent* (inteligente) - A utilização de ferramentas e tecnologias elevam o patamar da auditoria.
- *Intuitive* (intuitivo) - Acessar dados em tempo real torna o processo intuitivo e transparente.
- *Informed* (informado) - A execução passa a exigir conhecimentos sobre riscos e regulações.

- *Integrated* (integrado) - O resultado exige maior interação e um olhar para o ambiente global.
- *Insightful* (esclarecedor) – Fomenta a confiança e transparência e beneficia a tomada de decisões.

Os *drivers* dessa revolução são a qualidade, que impulsiona um trabalho de confiança, e a inovação, como agente transformador da mudança.

Os instrumentos para a transformação serão: tecnologia e capacitação.

As novas tecnologias são uma oportunidade e não uma ameaça. É com esse olhar para o futuro, vislumbrando a ampliação de seu escopo de atuação, para que como autoridade competente, que nós do ITI estamos conduzindo nossas ações tanto com foco nas estratégias internas como externas.

O ITI acredita que a inovação é o oxigênio fundamental para a manutenção dos negócios.

8. Conclusão

Por fim, o ITI esclarece aos usuários de serviços digitais, aos gestores de aplicações e aos agentes públicos desse país que o ITI tem as alternativas de soluções para assinaturas e identificações digitais atual e futura, contemplando diversas aplicações que abrangem a segurança da comunicação no mundo digital, incluindo IoT e cidades inteligentes. O ITI continuará trabalhando para tornar a ICP-Brasil mais segura, moderna, ágil, acessível e em condições de ofertar preços menores. É fundamental tecnicamente evoluir a atual legislação da ICP-Brasil, promulgada em 2001, a qual, além de não contemplar diversas evoluções tecnológicas dos últimos 19 anos, não vai mais proteger o país em um futuro próximo. **É necessário que o Brasil tenha uma lei que permita recepcionar as mais diversas tecnologias, aplicações e propósitos de uso na esfera de segurança e criptografia**. Cada cidadão brasileiro deve ter o direito de ter sob seu controle uma chave criptográfica para sua manifestação de vontade e proteção de dados no mundo digital. O ITI, em seu compromisso institucional, possui o conhecimento e as soluções, assim como continuará estudando e promovendo ações para que as atuais e novas plataformas eletrônicas de assinaturas sejam de fato usufruídas por toda sociedade brasileira.

Referências

[1] NIST. *Post-quantum cryptography: NIST's plan for the future*, 2016, disponibilizado em http://csrc.nist.gov/groups/ST/post-quantum-crypto/documents/pqcrypto-2016-presentation.pdf. (visto em 03/03/2020).

[2] NIST. *Post-Quantum Cryptography*, disponibilizado em https://csrc.nist.gov/projects/post-quantum-cryptography. (visto em 03/03/2020).

[3] NIST. *Round 2 Submissions*, disponibilizado em https://csrc.nist.gov/Projects/post-quantum-cryptography/round-2-submissions. (visto em 03/03/2020).

[4] Rivest, R. L., Shamir, A., and Adleman L., *A method for obtaining digital signatures and public-key cryptosystems*. Commun. ACM 21, 2 (February 1978), 120-126. DOI=http://dx.doi.org/10.1145/359340.359342, 1978.

[5] FIPS 186, *Digital Signature Standard*, Federal Information Processing Standards Publication 186, U.S. Department of Commerce/N.I.S.T., National Institute Information Service, Springfield, Virginia, 1994.

[6] RFC 2315, *PKCS #7: Cryptographic Message Syntax*, Version 1.5. Internet Request for Comments 2315, B. Kaliski, Mar. 1998.

[7] RFC 6090, *Fundamental Elliptic Curve Cryptography Algorithms*, Internet Request for Comments 6979, T. Pornin, Aug. 2013.

[8] RFC 6979, *Deterministic Usage of the Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm (ECDSA)*, Internet Request for Comments 6979, T. Pornin, Aug. 2013.

[9] RFC 8017, *PKCS #1: RSA Cryptography Specifications*, Version 2.2. Internet Request for Comments 8017, K. Moriarty, B. Kaliski, J. Jonsson, and A. Rusch, Nov. 2016.

[10] RFC 8032, *Edwards-Curve Digital Signature Algorithm (EdDSA)*, Internet Request for Comments 8032, S. Josefsson and I. Liusvaara, Jan. 2017.

[11] *Padrões e Algoritmos Criptográficos da ICP-Brasil*, disponibilizado em https://www.iti.gov.br/images/repositorio/legislacao/documentos-principais/01.1/DOC-ICP-01.01_-_v.4.2_PADROES_E_ALGORITMOS_CRIPTOGRAFICOS_DA_ICP-BRASIL_copy.pdf. (visto em 03/01/2020).

[12] Shor, P. W., *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*. SIAM J. Comput. 26, 5 (October 1997), 1484-1509. DOI=http://dx.doi.org/10.1137/S0097539795293172, 1997.

[13] Watrous, J., *Quantum algorithms for solvable groups*. In STOC '01, pages 60–67. ACM Press, DOI:10.1145/380752.380759, 2001.

[14] Nielsen M., and Chuang I., *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[15] Arute, F., Arya, K., Babbush, R. et al., *Quantum supremacy using a programmable superconducting processor*. Nature 574, 505–510, doi:10.1038/s41586-019-1666-5, 2019.

[16] *IBM Q*, disponibilizado em https://www.ibm.com/quantum-computing/. (visto em 03/03/2020).

[17] *Microsoft Quantum*, disponibilizado em https://www.microsoft.com/en-us/quantum. (visto em 03/03/2020).

[18] Grover, L. K., *A fast quantum mechanical algorithm for database search*. In Annual ACM Symposium on Theory of Computing, pages 212–219. ACM, 1996.

[19] ITI. *Plenajamento Estratégico 2019-2022*, disponibilizado em https://www.iti.gov.br/images/repositorio/institucional/planejamentoestrategico/pe2019-2022.pdf. (visto em 16/01/2020).

[20] *Medida Provisória nº 2.200-2, de 24 de Agosto de 2001*, disponibilizado em http://www.planalto.gov.br/ccivil_03/mpv/antigas_2001/2200-2.htm. (visto em 03/01/2020).

[21] Lamport, L., *Constructing digital signatures from a one way function*. Technical Report SRI-CSL-98. SRI International Computer Science Laboratory, 1979.

[22] Merkle, R., *A Certified Digital Signature*. In Advances in Cryptology – CRYPTO '89 (LNCS), Gilles Brassard (Ed.), Vol.435. Springer, 218–238, 1990.

[23] RFC8391, *XMSS: eXtended Merkle Signature Scheme*. https: //doi.org/10.17487/https://rfc-editor.org/rfc/rfc8391.txt, A. Hülsing, D. Butin, S.-L.Gazdag, J. Rijneveld, and A. Mohaisen, 2018.

[24] RFC8554, *Leighton-Micali Hash Based Signatures.* https://doi.org/10.17487/RFC8554, D. McGrew, M. Curcio, and S. Fluhrer. 2019.

[25] Bernstein, D. J., Dobraunig, C., Eichlseder, M., Fluhrer, S., Gazdag, S.L., Hülsing, A., Kampanakis, P., Kölbl, S., Lange, T., Lauridsen, M. M., Mendel, F., Niederhagen, R., Rechberger, C., Rijneveld, J., and Schwabe, P., *SPHINCS*$^{+}$. *Submission to NIST's postquantum crypto standardization project*, https://sphincs.org, 2017.

[26] Bernstein, D. J., Hülsing, A., Kölbl, S., Niederhagen, R., Rijneveld, J., and Schwabe, P., *The SPHINCS*$^{+}$ *Signature Framework*, https://sphincs.org/data/sphincs+-paper.pdf, 2019.

[27] *Recommendation for Stateful Hash-Based Signature Schemes*, disponibilizado em https://csrc.nist.gov/publications/detail/sp/800-208/draft. (visto em 07/01/2020)

[28] Buchmann, J., Dahmen, E., Hülsing, A. (2011), *XMSS - A Practical Forward Secure Signature Scheme Based on Minimal Security Assumptions*. In: Yang BY. (eds) Post-Quantum Cryptography. PQCrypto 2011. Lecture Notes in Computer Science, vol 7071. Springer, Berlin, Heidelberg, 2011.

[29] Leighton, F., Micali, S., *Large provably fast and secure digital signature schemes based on secure hash functions*, https://www.google.com/patents/ US5432852, US Patent 5,432,852, Jul 1995.

[30] Song, F., *A Note on Quantum Security for Post-Quantum Cryptography*. In: Mosca, M. (ed.) PQCrypto 2014. LNCS, vol. 8772, pp. 246–265. Springer, Heidelberg, 2014.

[31] Buldas, A., Kroonmaa, A., Laanoja, R., *Keyless Signatures' Infrastructure: How to Build Global Distributed Hash-Trees*. In: Riis Nielson H., Gollmann D. (eds) Secure IT Systems. NordSec 2013. Lecture Notes in Computer Science, vol 8208. Springer, Berlin, Heidelberg, 2013.

[32] Buldas, A., Laanoja, R., Truu, A., *Efficient Implementation of Keyless Signatures with Hash Sequence Authentication*, Cryptology ePrint Archive, Report 2014/689, https://eprint.iacr.org/2014/689, 2014.

[33] *e-Estonia, Security and Safety*, disponibilizado em https://e-estonia.com/solutions/security-and-safety/. (visto em 07/03/2020).

[34] Cheng, S., Daub, M., Domeyer, A., and Lundqvist M., *Using blockchain to improve data management in the public sector*, disponibilizado em https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/using-blockchain-to-improve-data-management-in-the-public-sector, 2017. (visto em 07/03/2020).

[35] *Distributed Ledger Technology: Beyond Block Chain*, UK Government Chief Scientific Adviser, London: Crown Copyright, disponibilizado em https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf. (visto em 07/03/2020).

[36] Allessie, D., Sobolewski, M., Vaccari, L., *Blockchain for digital government, An assessment of pioneering implementations in public services*, disponibilizado em https://publications.jrc.ec.europa.eu/repository/bitstream/JRC115049/blockchain_for_digital_government_online.pdf. (visto em 07/03/2020).

[37] Mark, G., Melinda, N., Lisa, P., Bell, G., Downing, J., Rahbari, K., Kilani M., Woods, K., Curtis T., Everette J., Enforcement, Scott S., Varrone, A., *Blockchain and its Suitability for Government Applications*, disponibilizado em https://www.dhs.gov/sites/default/files/publications/2018_AEP_Blockchain_and_Suitability_for_Government_Applications.pdf. (visto em 07/03/2020)

[38] *Blockchain Playbook for the U.S. Federal Government*, April 2, 2018, American Council for Technology Industry Advisory Council (ACT-IAC), https://www.actiac.org/act-iac-white-paper-blockchain-playbookus-federal-government, (visto em 07/03/2020).

[39] D'Cunha, S., *Dubai Sets Its Sights On Becoming The World's First Blockchain-Powered Government*, Forbes, December 28, 2017. [Online]. Available: https://www.forbes.com/sites/suparnadutt/2017/12/18/dubai-setssights-on-becoming-the-worlds-first-blockchain-powered-government/#2b9298e7454b. (visto em 07/03/2020).

[40] *2018 China's Blockchain Industry White Paper*, Ministry of Industry and Information Technology, Qifeng Financial Blockchain Institute, May 2018. [Online]. Available: http://www.miit.gov.cn/n1146290/n1146402/n1146445/c6180238/part/6180297.pdf. (visto em 07/03/2020).

[41] Mearian, L., *IBM sees blockchain as ready for government use*, Computer World, February 14, 2018. [Online]. Available: https://www.computerworld.com/article/3254202/blockchain/ibm-sees-blockchain-as-ready-forgovernment-use.html. (visto em 07/03/2020).

[42] *Sovrin Foundation*, disponibilizado em https://sovrin.org/. (visto em 07/03/2020).

[43] Nakamoto, S., *Bitcoin: A peer-to-peer electronic cash system*, 2008.

[44] Back, A., *Hashcash – a denial of service counter-measure*. Technical report, 2002.

[45] Nguyen, C. T., Hoang, D. T., Nguyen, D. N., Niyato, D., Nguyen, H. T. and Dutkiewicz, E., *Proof-of-Stake Consensus Mechanisms for Future Blockchain Networks: Fundamentals, Applications and Opportunities*, in IEEE Access, vol. 7, pp. 85727-85745, doi: 10.1109/ACCESS.2019.2925010, 2019.

[46] De Angelis, S., Aniello, L., Baldoni, R., Lombardi, F., Margheri, A., and Sassone, V., *PBFT vs proof-of-authority: applying the CAP theorem to permissioned blockchain*. Italian Conference on Cyber Security. 11 pp, 2018.

[47] Gorczyca, A. and Decker, A., *Distributed Ledger Witness Selection in Bounded Width Directed Acyclic Graphs*, 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Seoul, Korea (South), 2019, pp. 124-127. doi: 10.1109/BLOC.2019.8751447, 2019.

[48] Baird, L., *The swirlds hashgraph consensus algorithm: Fair, fast, byzantine fault tolerance*. Swirlds Tech Reports SWIRLDS-TR-2016-01, Tech. Rep., 2016.

[49] *Ethercombing: Finding Secrets in Popular Places* disponibilizado em https://www.securityevaluators.com/casestudies/ethercombing/. (visto em 07/03/2020).

[50] Kleina, N., *Hackers levam 7 mil bitcoins da corretora Binance em roubo superelaborado*, 2019, disponibilizado em https://www.tecmundo.com.br/mercado/141055-hackers-levam-7-mil-bitcoins-corretora-binance-roubo-superelaborado.htm. (visto em 07/03/2020).

[51] *The Cryptographers' Panel*, RSA Conference USA 2019, disponibilizado em https://www.rsaconference.com/industry-topics/presentation/the-cryptographers-panel. (visto em 07/03/2020).

[52] Bernstein, D. J., and Lange T., *SafeCurves: choosing safe curves for elliptic-curve cryptography,* 2014, disponibilizado em https://safecurves.cr.yp.to. (visto em 07/03/2020).

[53] Bernstein, D. J., and Lange T., *Non-uniform cracks in the concrete: The power of free precomputation*. In K. Sako and P. Sarkar, editors, Advances in Cryptology – ASIACRYPT, pages 321–340, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg, 2013.

[54] Bernstein, D. J., and Lange T., *Failures in NIST ECC standars*, disponibilizado em https://cr.yp.to/newelliptic/nistecc-20160106.pdf, 2016. (visto em 07/03/2020).

[55] Shumow, D., and Ferguson, N., *On the possibility of Back Door in NIST SP 800-90 Dual Ec PRNG*, Microsoft, 2012.

[56] Campbell, Sr. R. E., *Transitioning to a Hyperledger Fabric Hybrid Quantum Resistant-Classical Public Key Infrastructure*, Capitol Technology University, Laurel, USA, ISSN Online: 2516-3957 ISSN Print: 2516-3949 https://doi.org/10.31585/jbba-2-2-(4)2019, 2019.

[57] Chalkias, K., Brown, J., Hearn, M., Lillehagen, Nitto, T., I. and Schroeter, T., *Blockchained Post-Quantum Signatures*, 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 2018, pp. 1196-1203. doi: 10.1109/Cybermatics_2018.2018.00213, 2018.

[58] 3GPP, *Security Architecture and Procedures for 5G System (Release 15)*, 3rd Generation Partnership Project (3GPP), Technical Specification (TS) 33.501, 09 2019, version 15.6.0. [Online], disponibilizado em https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3169. (visto em 13/01/2020).

[59] Ghosh, A., Mäder, A., Baker, M., and Chandramouli, D., *5G Evolution: A View on 5G Cellular Technology Beyond 3GPP Release 15*, IEEE Access, vol. PP, pp. 1–1, 09 2019.

[60] Ji, X., Huang, K., Jin, L., Tang, H., Liu, C., Zhong, Z., You, W., Xu, X., Zhao, H., Wu, J., and Yi, M., *Overview of 5G Security Technology*, Science China Information Sciences, vol. 61, 08 2018.

[61] Piqueras Jover, R., and Marojevic, V., *Security and Protocol Exploit Analysis of the 5G Specifications*, IEEE Access, vol. 7, pp. 24 956– 24 963, 2019.

[62] *Requisitos Mínimos para as Declarações de Práticas de Certificação das Autoridades Certificadoras da ICP-Brasil,* disponibilizado em https://www.iti.gov.br/images/repositorio/legislacao/documentos-principais/05/DOC-ICP-05_-_v.5.3_REQ_MIN_PARA_AS_DPC.pdf. (visto em 10/03/2020).

[63] *Are flying cars close? Leaders say yes, but doubts linger*, disponibilizado em https://www.smartcitiesdive.com/news/are-flying-cars-close-leaders-say-yes-but-doubts-linger/567764/. (visto em 10/03/2020).

[64] *Lei nº 13.444, de 11 de maio de 2017*, disponibilizado em http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/L13444.htm. (visto em 10/03/2020).

[65] *Lei nº 13.709, de 14 de agosto de 2018*, disponibilizado em http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm. (visto em 10/03/2020).

[66] *Resoluções*, disponibilizado em https://www.iti.gov.br/legislacao/61-legislacao/501-resolucoes. (visto em 03/01/2020).

[67] Leurent, G., and Peyrin, T., *SHA-1 is a Shambles - First Chosen-Prefix Collision on SHA-1 and Application to the PGP Web of Trust*, 2020, Cryptology ePrint Archive, Report 2020/014, disponibilizado em https://eprint.iacr.org/2020/014. (visto em 16/01/2020).

[68] *Modules In Process List* (2020), disponibilizado em https://csrc.nist.gov/Projects/cryptographic-module-validation-program/Modules-In-Process/Modules-In-Process-List. (visto em 03/01/2020).

[69] *ICP-Brasil avança para recebimento do selo Webtrust* (2019), disponibilizado em https://www.iti.gov.br/component/content/article?id=4071. (visto em 03/01/2020).

[70] *A auditoria do futuro. As transformações que impactam o exercício dessa função*, disponibilizado em https://www2.deloitte.com/br/pt/pages/audit/articles/auditoria-do-futuro.html. (visto em 16/03/2020).

Brasília, 20 de janeiro de 2020.

EDUARDO MAGALHAES DE LACERDA FILHO

Assinado de forma digital por EDUARDO MAGALHAES DE LACERDA FILHO
Dados: 2020.01.20 11:07:43 -03'00'

EDUARDO MAGALHÃES DE LACERDA FILHO
Diretor de Infraestrutura de Chaves Públicas Brasileira

ANGELA MARIA DE OLIVEIRA

Assinado de forma digital por ANGELA MARIA DE OLIVEIRA
Dados: 2020.01.20 11:40:58 -03'00'

ÂNGELA MARIA DE OLIVEIRA
Diretora de Auditoria, Fiscalização e Normalização

ANDRE MACHADO CARICATTI:26734818187

Digitally signed by ANDRE MACHADO CARICATTI:26734818187
Date: 2020.01.20 10:13:32 -08'00'

ANDRÉ MACHADO CARICATTI
Coordenador-Geral de Operações

JOSE RODRIGUES GONCALVES JUNIOR

Assinado de forma digital por JOSE RODRIGUES GONCALVES JUNIOR
Dados: 2020.01.20 11:28:28 -03'00'

JOSÉ RODRIGUES GONÇALVES JÚNIOR
Coordenador-Geral de Infraestrutura e Segurança da Informação

WILSON ROBERTO HIRATA

Assinado de forma digital por WILSON ROBERTO HIRATA
Dados: 2020.01.20 11:11:17 -03'00'

WILSON ROBERTO HIRATA
Coordenador-Geral de Normalização e Pesquisa

PEDRO PINHEIRO CARDOSO:38664267120

Assinado de forma digital por PEDRO PINHEIRO CARDOSO:38664267120
Dados: 2020.01.20 11:51:15 -03'00'

PEDRO PINHEIRO CARDOSO
Coordenador-Geral de Auditoria e Fiscalização

Mauricio Augusto Coelho:1285163

Assinado de forma digital por Mauricio Augusto Coelho:1285163
Dados: 2020.01.20 12:59:22 -03'00'

MAURÍCIO AUGUSTO COELHO
Assessor Especial da Presidência

ANDRE SERPA

Assinado de forma digital por ANDRE SERPA
Dados: 2020.01.20 11:29:51 -03'00'

ANDRÉ SERPA
Assessor Especial da Presidencia

ALINE SOZA DE MELO

Assinado de forma digital por ALINE SOZA DE MELO
Dados: 2020.01.20 11:25:13 -03'00'

ALINE SOZA DE MELO
Chefe de Gabinete

RICARDO FERRI CONZATTI

Assinado de forma digital por RICARDO FERRI CONZATTI
Dados: 2020.01.20 11:24:09 -03'00'

RICARDO FERRI CONZATTI
Coordenador-Geral de Planejamento, Orçamento e Administração

LUIS CARLOS DE OLIVEIRA PORTO

Assinado de forma digital por LUIS CARLOS DE OLIVEIRA PORTO
Dados: 2020.01.20 11:15:47 -03'00'

LUÍS CARLOS DE OLIVEIRA PORTO
Coordenador de Operações da AC Raiz

GERALDO CLAY DE SOUZA MACIEL

Assinado de forma digital por GERALDO CLAY DE SOUZA MACIEL
Dados: 2020.01.20 11:14:39 -03'00'

GERALDO GLAY DE SOUZA MACIEL
Coordenador de Segurança da Informação

WELLINGTON DE JESUS NOUGA
Coordenador de Infraestrutura Tecnológica

FELIPE BIMBATO RODRIGUES

Assinado de forma digital por FELIPE BIMBATO RODRIGUES
Dados: 2020.01.20 11:19:45 -03'00'

FELIPE BIMBATO RODRIGUES
Coordenador de Tecnologia da Informação e Comunicações

JORGE CARVALHO DE OLIVEIRA

Assinado de forma digital por JORGE CARVALHO DE OLIVEIRA
Dados: 2020.01.20 11:12:43 -03'00'

JORGE CARVALHO DE OLIVEIRA
Coordenador Substituto de Normalização e Pesquisa

LEONARDO FELICIANO CLEMENTE

Assinado de forma digital por LEONARDO FELICIANO CLEMENTE
Dados: 2020.01.20 15:52:47 -03'00'

LEONARDO FELICIANO CLEMENTE
Auditor

ERICA COSTA MELLO

Assinado de forma digital por ERICA COSTA MELLO
Dados: 2020.01.20 15:36:48 -03'00'

ÉRICA COSTA MELLO DE MORAES
Auditora

LUCAS ROCHA RIBEIRO

Assinado de forma digital por LUCAS ROCHA RIBEIRO
Dados: 2020.01.20 11:18:40 -03'00'

LUCAS ROCHA RIBEIRO
Assistente Técnico

JOSE ANTONIO ALVES MOREIRA

Assinado de forma digital por JOSE ANTONIO ALVES MOREIRA
Dados: 2020.01.20 11:17:35 -03'00'

JOSÉ ANTÔNIO ALVES MOREIRA
Analista de Sistemas

ANA LÍLIA BISPO DE FREITAS
Analista Técnico

LUCIANA CRISTINA CORREA DE SIQUEIRA

Assinado de forma digital por LUCIANA CRISTINA CORREA DE SIQUEIRA
Dados: 2020.01.20 11:20:52 -03'00'

LUCIANA CRISTINA CORREA DE SIQUEIRA
Assistente Técnico

GIORDANNO AZEVEDO COSTA MARTINS

Assinado de forma digital por GIORDANNO AZEVEDO COSTA MARTINS
Dados: 2020.01.20 12:29:07 -03'00'

GIORDANNO AZEVEDO COSTA MARTINS
Coordenador Substituto de Tecnologia da Informação e Comunicações

LUIZ CLAUDIO FRANCA LIMA:87541971715

Assinado de forma digital por LUIZ CLAUDIO FRANCA LIMA:87541971715
Dados: 2020.01.20 11:09:37 -03'00'

LUIZ CLÁUDIO FRANÇA LIMA
Auditor

HENRIQUE LUIS HELEODORO DA SILVA

Assinado de forma digital por HENRIQUE LUIS HELEODORO DA SILVA
Dados: 2020.01.20 11:38:13 -03'00'

HENRIQUE LUÍS HELEODORO DA SILVA
Analista em Tecnologia da Informação

MARCO ANTÔNIO BENEDETI
Analista em Tecnologia da Informação

RONEY CARVALHO DOS SANTOS

Assinado de forma digital por RONEY CARVALHO DOS SANTOS
Dados: 2020.01.20 14:43:15 -03'00'

RONEY CARVALHO DOS SANTOS
Analista em Tecnologia da Informação

ROBERTO WAGNER DE CARVALHO ARAUJO:99495015120

Assinado de forma digital por ROBERTO WAGNER DE CARVALHO ARAUJO:99495015120
Dados: 2020.01.20 14:49:56 -03'00'

ROBERTO DE ARAÚJO
Analista em Tecnologia da Informação

Aprovo,

MARCELO AMARO BUZ

Assinado de forma digital por MARCELO AMARO BUZ
Dados: 2020.01.20 11:45:17 -03'00'

MARCELO AMARO BUZ
Diretor-Presidente do ITI

ANEXO I

Algoritmos Criptográficos Pós-Quânticos[6]

A competição do NIST para definição de novos algoritmos de chaves públicas impôs aos participantes alguns requisitos técnicos. De maneira resumida, segundo o documento e apresentações do NIST, destacaremos os mais importantes:

A. Escopo

Novos algoritmos para assinatura digital (FIPS 186) e encriptação de chaves públicas/encapsulamento de chaves (SP 800-56A e SP 800-56B).

B. Resultados esperados

Padronização de diferentes algoritmos.

C. Funcionalidades / Definições de segurança

i. Assinatura Digital

• *Existential Unforgeability under Chosen Message Attack* – EUF-CMA – até 2^{64} requisições de assinatura.

ii. *Public Key Encryption*/*Key Encapsulation Mechanisms* – PKE/KEM (primeira opção)

• *Indistinguishability Chosen Ciphertext Attack* – IND-CCA – até 2^{64} requisições de decifrar/desencapsular.

• Necessário em situações que exige reutilização de chave.

iii. PKE / KEM (segunda opção)

• *Indistinguishability Chosen Plaintext Attack* – IND-CPA.

• Necessário restrições de uso para impedir a reutilização de chaves.

Observação: O NIST descreve que pode valer a pena padronizar além dos esquemas IND-CCA, se houver benefícios significativos de desempenho.

D. Critérios de avaliação

i. Segurança (contra os ataques clássicos e quânticos)

• I – pelo menos tão difícil de quebrar quanto o AES-128 (busca exaustiva por

[6] Para mais detalhes por favor refiram-se a [1-3]

chaves).

• II – pelo menos tão difícil de quebrar quanto o SHA-256 (pesquisa por colisão).

• III – pelo menos tão difícil de quebrar quanto o AES-192 (busca exaustiva por chaves).

• IV – pelo menos tão difícil de quebrar quanto o SHA-384 (pesquisa por colisão).

• V – pelo menos tão difícil de quebrar quanto o AES-256 (pesquisa exaustiva por chaves).

Observação: O NIST solicitou aos remetentes que se concentrassem nos níveis 1, 2 e 3. (os níveis 4 e 5 são de alta segurança).

ii. Desempenho – medição realizada por meio de plataformas clássicas.

iii. Outras propriedades: substituições *drop-in*, sigilo direto perfeito, resistência a ataques de *side-channels*, simplicidade e flexibilidade, resistência a uso indevido, entre outros.

Na primeira rodada, foram 82 submissões recebidas e 69 aceitas como completas e apropriadas. Ao longo dos anos, muitas submissões foram fundidas, outras retiradas e algumas foram descobertos algum tipo de ataque ou insegurança. Em 2019, o NIST classificou para a segunda rodada 26 algoritmos, sendo 17 para PKE/KEM e 9 para assinaturas digitais.

Apresentamos uma tabela com o resumo do número de algoritmos pós-quânticos baseado na dificuldade do problema matemático e que foram classificados para a segunda rodada da competição do NIST.

Tabela I: Resumo dos algoritmos classificados, com a quantidade de cada, para a segunda rodada da competição do NIST.

Algoritmo PQC (conceito)	Segurança (dificuldade do problema)	Assinatura (*signatures based*)	PKE/KEM
Látice	Achar/detectar SVP e CVP[7] em um espaço látice finito com *n*-dimensões	3	9
Códigos (*Rank*)	Decodificar um código linear aleatório	0	7

[7] *Shortest vector problem* e *Closest vector problem*

Quadráticos Multivariados	Resolver equações quadráticas multivariadas sobre campos finitos	4	0
Simétrico (*hash*)	Resistir à segunda pré-imagem	2	0
Isogenia	Achar um mapa isogênico entre curvas elípticas com o mesmo número de pontos.	0	1

ANEXO II

Esquemas de assinatura baseado em *hash*[8]

As funções de sentido único utilizadas para assinaturas digitais (*hash-based signature* - *Merkle-tree*) são, em conceito comum, algoritmos que partem de esquemas *one-time-signature* (OTS) proposto por Lamport, estendidos para os esquemas de autenticação de Merkle. Para um k inteiro positivo, a função *hash* com um domínio e um codomínio $\mathfrak{H}:\{0,1\}^* \rightarrow \{0, 1\}^k$ endereça uma entrada arbitrária de tamanho $m \in \{0, 1\}^*$ para uma saída fixa $y \in \{0, 1\}^k$, chamada de resumo da mensagem. Resumidamente, introduziremos os conceitos matemáticos utilizados nos algoritmos XMSS, LMS, esses dois podem ser vistos com mais detalhes nas RFCs, e Sphincs$^+$. Também abordaremos o BLT, algoritmo usado pelo governo da Estônia em sua rede *Keyless Signature Infrastructure Blockchain* – KSI.

O conceito matemático de assinatura em *hash* inicia-se com OTS. Essa é realizada escolhendo uma chave aleatória $X = ((x_{k-1}[0], x_{k-1}[1]), ..., (x_0[0], x_0[1])) \in_R \{0, 1\}^{(k,2k)}$. A chave de verificação $Y(y)$ contém o mesmo número de elementos de $X(x)$ sendo que $y_i[j] = \mathfrak{H}(x_i[j])$, $0 \leq i \leq k\text{-}1$, $j = (0, 1)$. Para assinar uma mensagem M, faz-se $\mathfrak{H}(M) \rightarrow m$, tal que $m = (m_{k-1}, ..., m_0)$, então a assinatura será $S = (x_{k-1}[m_{k-1}], ..., x_1[m_1], x_0[m_0] \in \{0, 1\}^{(k,k)}$. Caso o i-ésimo *bit* de m for 0, o elemento de X usado será $x_i[0]$; caso seja 1, $x_i[1]$. Para verificar a assinatura S de M basta checar $(\mathfrak{H}(S_{k-1}), ..., \mathfrak{H}(S_0)) = (y_{k-1}[m_{k-1}], ..., y_0[m_0])$.

O esquema de WOTS (Winternitz OTS) assina simultaneamente vários *bits* da mensagem com uma sequência da chave OTS. Define-se um parâmetro $w > 1$, referente ao número de *bits* que serão assinados concomitantemente, sendo $L = l_1 + l_2$, com $l_1 = \lceil k/w \rceil$; $l_2 = \lceil (\lfloor log_2\, l_1 \rfloor + 1 + w) \,/\, w \rceil$. A criação da chave (semente) é feita aleatoriamente, tal que, $X = (x_{L-1}, ..., x_0) \in_R \{0, 1\}^{(k,\, L)}$. A chave de verificação $Y(y)$ contém o mesmo número de elementos de $X(x)$, sendo que $y_i = \mathfrak{H}^{(2\hat{}w)-1}(x_i)$, $0 \leq i \leq L\text{-}1$. Para assinar uma mensagem M, faz-se $\mathfrak{H}(M) \rightarrow m$, tal que $m = (m_{k-1}, ..., m_0)$. Um *padding* de zeros é feito, se necessário, em m para que o tamanho de m seja divisível por w, e concatena-se, $m = b_{L-1}||...||b_{L-l_1}$. Os blocos de b_i são representados como inteiros na base $w\{0, 1, ..., 2^w\text{-}1\}$. O *checksum* c é calculado $c = \sum_{i=L-l_1}^{L-1} (2^w - b_i)$.

Sendo $c \leq l_1 2^w$, o tamanho da representação binária de c é menor que $\lfloor log_2\, l_1 2^w \rfloor + 1$. Dividem-se os blocos c de tamanho w em $c = b_{l_2-1}||, ..., b_0$ e, se necessário, *padding* de zeros em c deve ser feito para que tamanho da *string* de *bits* seja divisível por w. Então a assinatura é computada $S = (\mathfrak{H}^{b_{L-1}}(x_{L-1}),..., \mathfrak{H}^{b_1}(x_1), \mathfrak{H}^{b_0}(x_0)$. Para verificar S calcula-se $b = b_{L-1},...,b_0$ de tamanho w e verifica se $(\mathfrak{H}^{(2\hat{}w)-1-b_{L-1}}(S_{L-1}), ..., \mathfrak{H}^{(2\hat{}w)-1}(S_0)) = (y_{k-1}, ..., y_0)$. Se a

[8] Para mais detalhes por favor refira-se a [21-32]. Os parâmetros apresentados neste anexo foram retirados dessas referências.

assinatura tiver validade, então, $S_i = \mathfrak{H}^{b_i}(x_i)$ e $\mathfrak{H}^{(2^{\wedge}w)-1-b_i}(S_i) = \mathfrak{H}^{(2^{\wedge}w)-1}(x_i) = y_i$.

Exemplo: dado $k = 4$, $w = 3$ e $\mathfrak{H}(x_i) \rightarrow (x + 1)$ *mod* 16 e $m = (1, 1, 0, 0)$. Calcula-se $l_1 = 2$, $l_2 = 3$, com $L = 5$. A semente aleatória $X(x) = (1011)^{(4,5)} \rightarrow Y(y) = (0010)^{(4,5)}$. *Padding* de dois 0 em $m = 001||100$. Calcula-se $c = (8\text{-}5)+(8\text{-}1) \rightarrow 1010$, *padding* de dois 0, c = 00||10||10. S = (1100, 0000, 1011, 1101, 1101). Para verificar: S_4 calcula-se $\mathfrak{H}^6(1100) = Y_4 = 0010$, ..., S_0 calcula-se $\mathfrak{H}^5(1101) = Y_0 = 0010$, *i.e.*, assinatura válida. Em OTS o tamanho da assinatura é de k^2 enquanto em WOTS é de Lk.

Outro fundamento importante é a assinatura de Merkle (MSS), apresentado na Figura 1, permitindo que se guarde um caminho (chave pública) para verificar as assinaturas realizadas com S_u. Escolhe-se aleatoriamente X_j, empregando um algoritmo *PRNG* (*pseudo randon number generator*), tal que uma única semente é armazenada $\text{Seed}_{\text{OTS0}}(X_0)$ e calcula-se $(\text{Seed}_{\text{OTSj}}, \text{Seed}_{j+1}) = PRNG(\text{Seed}_j)$, $0 \leq j < 2^H$.

Gera-se $Y_j = \mathfrak{H}(Xj)$, $0 \leq j \leq 2^H$. As primeiras folhas são os resultados de uma função *hash* $G(Y_j)$: G: $\{0, 1\}^* \rightarrow \{0, 1\}^n$. Os resultados $G(Y_j)$ das folhas são concatenados dois a dois (esquerda e direita) para um nó interno da árvore sequencialmente acima, até se chegar na raiz (invertida) da árvore, que é a chave pública da MSS, $n_h[j] = g(n_{h-1}[2j]||n_{h-1}[2j+1])$, $1 \leq h \leq H$, $0 \leq j \leq 2^{H-h}$. Não há nós (folhas) a direita, um h é reduzido; Normalmente, somente H nós são armazenados. A Figura 1 resume MSS, com sua sequência.

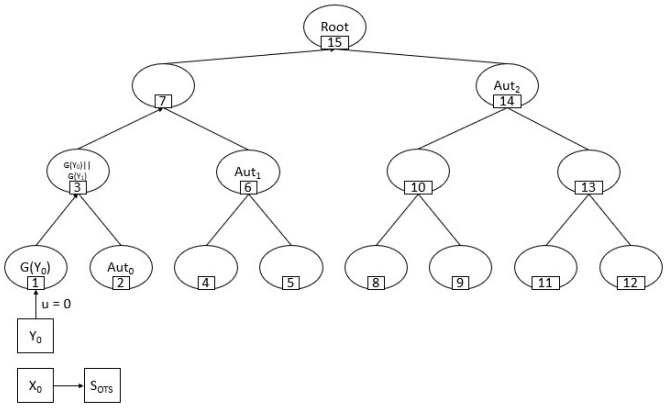

Fig. 1 – Árvore de Merkle. $H = 3$.

A assinatura em MSS é feita utilizando qualquer esquema de OTS, mais um índice u e um caminho de autenticação, tal que, $Aut_u = (a_0, ..., a_{H-1})$, permitindo a verificação de $G(Y_u)$ até a chave pública da MSS. $a_h = n_h[u/2^h - 1]$, se $\lfloor u/2^h \rfloor \equiv 1$ *mod* 2 ou $a_h = \{n_h[u/2^h + 1]\}$, se $\lfloor u/2^h \rfloor \equiv 0$ *mod* 2, para $h = (0, ..., H\text{-}1)$. A assinatura é $S_u = \{u, S_{OTS},$

Y_u, Aut_u}. A verificação consiste em dois passos: (i) utiliza-se o processo de verificação da Y_u pelo algoritmo de OTS escolhido e (ii) verifica a validade de Y_u construindo o caminho reverso $p = (p_0, ..., p_H)$, tal que $p_h = G_h(a_{h-1}||p_{h-1})$, se $\lfloor u/2^{h-1} \rfloor \equiv 1 \ mod \ 2$ ou $p_h = G_h(p_{h-1}||a_{h-1})$, se $\lfloor u/2^{h-1} \rfloor \equiv 0 \ mod \ 2$, para $h = (1, ..., H\text{-}1)$ e $p_0 = G(Y_u)$. Se p_H = chave pública da MSS, o caminho é válido.

Finalmente, antes da teoria sobre os algoritmos, é importante entender o esquema ampliado de W-OTS$^+$. Esse possui uma alteração na função família F e por consequência na assinatura e verificação $(sk, pk) \leftarrow K_g(1^n)$. Cria-se uma função de encadeamento $c_k^i(x, r)$, $x \in \{0, 1\}^n$, i (*counter*) $\in N$, $k \in K$ (*keyspace*) e elementos aleatórios $r = (r_1, ..., r_j) \in \{0, 1\}^{n,j}$. Com $j \geq i$, no caso de $i = 0$, $c = x$. Para $i > 0$, $c_k^i(x, r) = f_k(c_{ki-1}(x, r) \oplus r_i)$. A chave de verificação $(pk_0, ..., pk_L) = ((r, k), c_k^{w-1}(sk_1, r), ..., c_k^{w-1}(sk_L, r)$. A assinatura $S = (sk_1, ..., sk_L) = (c_k^{b_1}(sk_1, r), ..., c_k^{b_L}(sk_L, r))$, $b = (b_1, ..., b_L) = M||C$, feito em WOTS.

O primeiro algoritmo que descreveremos é o esquema *stateful* XMSS. Inicialmente, usa-se uma função família $F_n = \{f_k : \{0, 1\}^n \rightarrow \{0, 1\}^n | K \in \{0, 1\}^n\}$ e uma função *hash* família $G_n = \{g_k : \{0, 1\}^{2n} \rightarrow \{0, 1\}^n | K \in \{0, 1\}^n\}$. Define-se o parâmetro de segurança $n \in N$, $w > 1 \in N$, tamanho da mensagem $m \in N$, da árvore $h \in N$ e as chaves OTS $x \in \{0, 1\}^n$, escolhidas de forma pseudo-aleatórias e pelo servidor da aplicação da infraestrutura. As OTS x são usadas para construir as chaves de verificação pk aplicando $F_n \rightarrow f_k(x) = G(Pad(K)||Pad(x))$, K e $x \in \{0, 1\}^n$, com $Pad(z) = (z||10^{b-|z|-1})$, para $|z| < b$, em que b é o tamanho do bloco da função *hash*.

Para K e $x \in \{0, 1\}^n$, $e \in N$ e $f_k \in F_n$, a função família se comporta com $f_k^e(x)$: $f_k^0(x) = K$. Para $e > 0, f_k^e(x) = f_k'(x)$: $K' = f_k^{e-1}(x)$. O esquema de $L = l_1 + l_2$, permanece em relação a WOTS. A chave de verificação é $pk_i = f_{ski}^{w-1}(x)$, $i = [1, ..., L]$, com sk_i escolhida aleatoriamente. A assinatura S, depois dos cômputos do *checksum* e montagem de B_i, semelhante a WOTS, é: $S = (s_1, ..., s_L) = (f_{ski}^{b_1}(x), ..., f_{ski}^{b_L}(x))$. Para verificar, $(pk_1, ..., pk_L) = (f_{s_1}^{w-1-b_1}(x), ..., f_{s_1}^{w-1-b_L}(x))$.

A árvore binária, com tamanho H, tem H+1 de níveis e usa a função g_k e a *bitmask* $(b_{l,j}||b_{r,j}) \in \{0, 1\}^{2n}$, escolhidos aleatoriamente. Usando uma máscara XOR nos nós filhos, tal que $NODE_{i,j} = g_k((NODE_{2i,j-1} \oplus b_{l,j})||(NODE_{2i,j-1} \oplus b_{r,j})\}$. Para gerar as folhas, uma nova árvore XMSS é criada, chamada de L_{tree}. As primeiras L folhas da *L-tree* são $(pk_0, ..., pk_L)$ da chave de verificação. Como L pode não ser potência de 2, um nó que não tem irmão a direita é levantado para um nível acima. Os processos de autenticação dos caminhos mostrados em MSS são calculados pela XOR - *bitmask* $(b_{l,j}||b_{r,j})$.

O algoritmo LMS é muito similar ao esquema XMSS descrito. Uma diferença importante é que enquanto o LMS possui entradas com alterações previsíveis, o XMSS fornece à função *hash* entradas independentes aleatórias para cada cálculo de *hash*. O

LMS possui dois parâmetros: i. a altura da árvore, H, que é o número de níveis na árvore menos um. O sistema de assinatura suporta cinco valores deste parâmetro, *i.e.*, $H = 5; 10; 15; 20;$ e 25. Existem 2^H folhas em uma árvore; ii. o número de *bytes* emitidos pela função hash, m, é a quantidade de dados associados a cada nó na árvore. A RFC 8554 suporta somente SHA-256 com $m = 32$ (número de *bytes*).

Os coeficientes de Winternitz suportados para cada assinatura OTS são, $w = 1; 2; 4; 8$. Os algoritmos de geração de chaves, assinatura e verificação de LM-OTS tomam como parâmetros de entrada I e q. O parâmetro I é uma cadeia de 16 *bytes* que indica com qual árvore Merkle este LM-OTS é usado. O parâmetro q é um número inteiro de 32 *bits* que indica a folha da árvore de Merkle em que a chave pública do OTS aparece.

A chave privada é gerada da seguinte forma. OTS $x \in \{0, 1\}^n$, escolhidas aleatoriamente, com I e q. A chave privada é a concatenação do valor do tipo de algoritmo escolhido, l, o valor do algoritmo escolhido aplicado em q e x_i. A chave pública é gerada da chave privada aplicando interativamente uma função *hash* para cada elemento de x, para $2^w - 1$ interações, com os valores resultantes - y_i. Depois de escolher o tipo de algoritmo, é configurado n, p e w de acordo com a tabela da RFC 8554. Determina-se x, l e q da chave privada. A chave pública é o valor concatenado do tipo de algoritmo escolhido, l, o valor do algoritmo escolhido aplicado a q e uma *string* K, calculada por meio da função *hash* da concatenação de l, do valor resultante do tipo de algoritmo escolhido, do valor resultante do algoritmo escolhido D_PBLC = 0x8080 (em hexa) e y_i. O *checksum*, a assinatura e a verificação podem ser vistas da RFC 8554.

O algoritmo Sphincs$^+$ torna o esquema *stateless*, *i.e.*, um par de chaves para várias assinaturas e verificações em vez de se gerar uma atualização da chave a cada assinatura. É derivado de Sphincs e construído por uma super-árvore h, com d níveis de altura h/d, que proporciona assinar até 2^{64} requisições por par de chaves, mas a assinatura tem tamanho de ~30KB. Importante destacar, pelos resultados publicados, que o Sphincs$^+$ tem tamanhos e velocidades de assinaturas e verificações muito superiores aos atuais esquemas RSA e ECDSA, o que é uma desvantagem. A nova formulação, em 2019, do Sphincs$^+$ permite uma permutação dos parâmetros, flexibilizando (*trade-off*) entre a assinatura e segurança, incluindo uso de memória e *hardware*.

Sphincs$^+$, assim como o desenvolvimento do XMSS^{MT}, usa o conceito de uma super-árvore, ligadas por meio de OTS, em que os nós das folhas são selecionados aleatoriamente. Sphincs$^+$ introduz, para permitir árvores menores, um esquema de *few-time-signatures* (FTS) chamado de FORS (*Forest Of Random Subsets*). Para permitir escolhas de parâmetros menores e mitigar ataques de segunda pré imagem, Sphincs$^+$ usa uma seleção de índice publicamente verificável nos nós das folhas escolhidos. Possui

dois esquemas de assinatura e verificação já apresentados, o WOTS^{+} e a Sphincs^{+} *hypertree*, baseada nos conceitos de XMSS^{MT}, somados a *FORS*. A Figura 2 apresenta uma super-árvore do esquema criado em Sphincs^{+}.

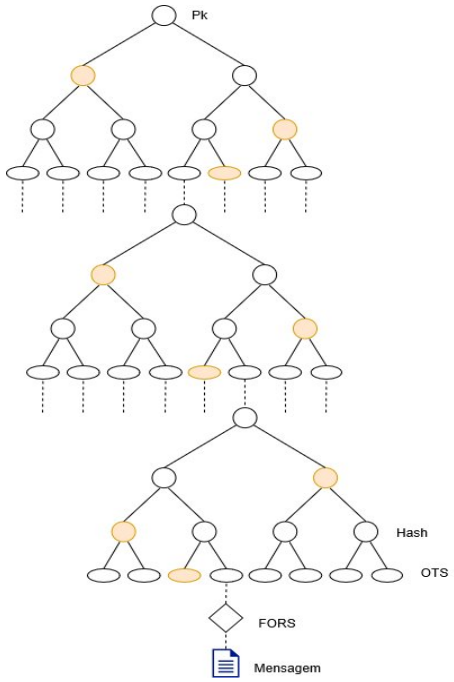

Fig. 2 – Super-árvore de Sphincs^{+}, com o caminho de verificação hachurado. h = 9; d = 3. Adaptado de [26].

Um dos conceitos novos de Sphincs^{+} é um ajuste na função *hash*. Seja $n, \alpha \in \mathbb{N}$, em que se mapeie α-bit (ln) de uma mensagem M para um valor de *hash MD* de *n-bit*, usando parâmetros de uma função pública $P \in P$ e $T \in T$, tal que $Th_l : P\{0, 1\}^n \times T\{0, 1\}^{256} \times \{0, 1\}^{ln} \rightarrow \{0, 1\}^n$, $Th(P, T, M) \rightarrow MD$. Então, $F = Th_1$ e $H = Th_2$. Usa-se como parâmetro público uma semente pública *Pk.seed*, que é parte da chave pública do Sphincs^{+}. Para identificar a posição da chamada da função *hash*, definida por um par de chaves, utiliza-se como ajuste um endereço de função *hash*, *ADRS* (*Hash Function Address Scheme*).

A função pseudo-aleatória $PRF : \{0, 1\}^n \times \{0, 1\}^{256} \rightarrow \{0, 1\}^n$ é usada para a (pseudo-aleatória) geração das chaves, e outra função pseudo-aleatória $PRFmsg : \{0, 1\}^n \times \{0, 1\}^n \times \{0, 1\}^* \rightarrow \{0, 1\}^n$ para gerar aleatoriedade para a compressão da mensagem. Uma chave adicional $Hmsg : \{0, 1\}^n \times \{0, 1\}^n \times \{0, 1\}^n \times \{0, 1\}^* \rightarrow \{0, 1\}^m$ é incluída

para processar mensagens de tamanho aleatório.

O primeiro esquema de assinatura do Sphincs$^+$ é baseado em WOTS$^+$, com uma pequena diferença no cálculo da função de encadeamento, $c = \sum_{i=1}^{l_i}(w - 1 - m_i)$. Possui dois parâmetros *n*, que é tamanho da mensagem, do elemento da chave privada e pública, e *w* que é o coeficiente de Winternitz (w = 4, 16 ou 256). A chave privada de WOTS$^+$ é derivada de uma semente secreta S*k.seed* que será parte da chave privada do Sphincs$^+$, e do endereço do par de chaves WOTS$^+$ dentro da super-árvore, usando *PRF*. Para a chave privada, cada *string* de *bits* em WOTS$^+$ é derivado de uma semente secreta de uma função pseudo-aleatória (e farão parte da chave secreta Sphincs$^+$ e de ADRS). A chave pública é calculada pela iteração *w* vezes da função *F* para cada entrada de *n-bytes* da chave privada. *F* é parametrizado pelo endereço do par de chaves WOTS$^+$ e a semente pública de *Pk.seed*, que fará parte da chave pública do Sphincs$^+$.

A *hypertree* binária de tamanho *h* possui 2^h nós de folhas cada uma, com *n bit string* L_i, $i \in [2^h - 1]$. Cada nó $N_{i,j}$, $0 < j \leq h$, $0 \leq i < 2^{h-j}$, armazena *n-bit*, com *bitmask* $Q_j \in \{0, 1\}^{2n}$. Os valores dos nós internos são $N_{i,j} = H((N_{2i,j-1} || N_{2i+1,j-1}) \oplus Q_j)$. Segundo o descrito na implementação do Sphincs$^+$, os nós das folhas WOTS$^+$ das super-árvores na camada inferior são usados para assinar as "chaves públicas" da FTS, enquanto os nós de folha das árvores em todas as outras camadas são usados para assinar os nós raiz das árvores abaixo (veja Figura 2). As assinaturas WOTS$^+$ e os caminhos de autenticação de uma folha na parte inferior da *hypertree* até a raiz da árvore mais alta constituem no caminho de autenticação. Todos os nós das folhas de todas as árvores intermediárias são chaves públicas WOTS$^+$ geradas deterministicamente independente das árvores abaixo. Durante a geração da chave, apenas a sub-árvore mais acima é calculada para derivar a chave pública.

O esquema modificado de FTS, chamado de FORS, é usado para assinar as mensagens de tamanho *m* e possui os parâmetros *k* e $t = 2^a$, $m = ka$. A chave privada de FORS consiste em valores de *n-bit* aleatórios de *kt*, agrupados em conjuntos *k* de valores *t,* deterministicamente derivada de *Sk.seed* usando *PRF* e o endereço da chave na *hypertree*. A chave pública de FORS é construída determinando as *k* árvores de *hash* sobre os conjuntos de chave privada. O valor *t* é usado com nó da folha, resultando em *k* árvore de altura *a*. Usa-se a função *H*, produzida usando a localização do par de chaves FORS na super-árvore e a posição exclusiva da chamada da função *hash* dentro das árvores FORS. Os nós raiz são calculados usando uma chamada Th_k, resultando na chave pública de FORS, com *n-bit*.

Dado uma mensagem de *ka bits*, extraindo *k string* de *a bits*, cada uma dessas *strings* é um índice um nó na folha da *k* árvore FORS. A assinatura FORS é constituída

desses nós e dos respectivos caminhos de autenticação. A verificação reconstrói cada nó raiz usando o caminho de autenticação e usa Th_k para reconstruir a chave pública.

Então, a chave pública do Sphincs$^+$ consiste em dois valores de *n-bit*: i. o nó raiz do topo da super-árvore; e ii. a semente pública aleatória *Pk.seed*. A chave privada de Sphincs$^+$ consiste em, também, dois valores de semente aleatória com *n-bit*: i. *Sk.seed*, para gerar as chaves secretas de WOTS$^+$ e FORS e; ii. $Sk._{PRF}$. A assinatura Sphincs$^+$ consiste na assinatura FORS em *m*, a assinatura WOTS$^+$ na chave pública FORS correspondente, nos caminhos de autenticação e assinaturas WOTS$^+$ para autenticar as chaves públicas WOTS$^+$. A verificação consiste na reconstrução das chaves públicas e nós raiz até o nó raiz no topo da super-árvore. É importante destacar que para os cálculos do resumo da mensagem a ser assinada e a escolha do nó da folha da árvore FORS que assinará as *strings k*, usa-se uma função pseudo-aleatória *R.* Esta é baseada na mensagem *m* e em $Sk._{PRF,}$ feita, *e.g.*, de forma não determinística adicionando um parâmetro aleatório *Rnd*. $R = PRF\ (Sk._{PRF}, Rnd, M)$, derivando qual folha será usada e o resumo da mensagem é dado por $(MD||idx) = Hmsg\ (R, Pk.seed, Pk.root, M)$.

Por fim, descreveremos o algoritmo BLT (Buldas, Laanoja, Truu) utilizado pelo governo da Estônia. O dispositivo do lado cliente gera uma semente aleatória *zs*. Para cada unidade de tempo *t*, a aplicação cliente gera uma senha (*one-time-password)*. As senhas são calculadas usando $z_i\text{-}1 = f(z_i)$, para todo $i = s,\ldots, 1$, em que *f* é a uma função de *hash*, construindo uma cadeia de chaves de *hash*: $z_0 \leftarrow z_1 \leftarrow z_2 \leftarrow \ldots \leftarrow z_s$.

O lado cliente também calcula o *hash* raiz *r* da *merkle-tree*, conforme ilustrado na Figura 3:

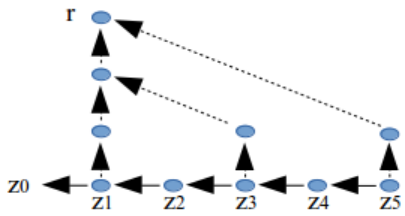

Fig. 3 – Cálculo de *r* em BLT. Adaptado de [31].

A chave pública será dada por (z_0 e r) e enviada ao servidor de assinatura. O servidor só conhecerá $z_{i\text{-}1}$ quando a aplicação cliente a utilizar, mas como o servidor conhece z_0, a senha pode ser verificada pela relação $z_{i\text{-}1} = f(z_i)$.

O "certificado" da chave pública enviado ao servidor de assinatura será: (ID_c, z_0, *r*, t_0, ID_s), em que ID_c é o identificador do lado cliente, t_0 é a unidade de tempo que o cer-

tificado tornou-se válido, ID_s é o identificador do servidor de assinatura autorizado. Para a revogação, basta o envio de uma mensagem de revogação ao servidor de assinatura deste certificado.

Para assinar uma mensagem m (calcular o *hash* de m), em que $t > t_0$: o cliente calcula $x = h(m, z_i)$ e envia x junto com o ID_c. O servidor de assinatura verifica se o certificado do cliente não foi revogado e cria um carimbo de tempo baseado em uma árvore de *hash* $S_t = (x, ID_c)$ e envia de volta ao cliente. A assinatura da mensagem m é (ID_c, i, z_i, c_i, S_t), em que c_i é a comprovação que z_i está na posição i da cadeia de chaves de *hash*. Para verificar uma assinatura (ID_c, i, z_i, c_i, S_t) de uma mensagem m o identificador do cliente deve ser o mesmo do certificado; com a chave z_i e a cadeia de *hash* c_i deve ser possível montar r. S_t é um carimbo de tempo válido em ($h(m, z_i)$, ID_c). O tempo t de S_t satisfaz $t = t_0 + i$. O identificador do servidor de assinatura em S_t e no certificado são os mesmos.

ANEXO III
Blockchain[9]

As redes baseadas em *blockchain* tornaram-se conhecidas por meio do protocolo Bitcoin. Cria-se um sistema não permissionado e público para transacionar uma moeda eletrônica de lastro finito em redes ponto a ponto, sem a necessidade de uma terceira parte confiável para o registro e validação dessas transações. Essa moeda eletrônica é uma cadeia de assinaturas digitais e funções *hash* que ligam as transações umas às outras. Essas transações são concatenadas dentro de um bloco, no qual um consenso de validação e ordenamento temporal baseado em *Proof-of-work* é utilizado.

Proof-of-work (prova de trabalho) é a verificação de um valor, por meio de cálculos de *hash* (no caso concreto em SHA-256) feitos por um ponto dessa rede chamado de minerador, até que o bloco, com as transações, tenha um *hash* em que as primeiras posições iniciais sejam zeros. Para tal, implementa-se, na prova de trabalho, um *nonce* no bloco até que se encontre um valor que forneça ao *hash* do bloco os zeros *bits* iniciais necessários. Com o esforço gasto por um minerador para satisfazer a prova de trabalho, o bloco não pode ser alterado sem refazer todo o trabalho. Como os blocos posteriores são encadeados por meio do uso do *hash* do bloco anterior, o trabalho para alterar um bloco incluiria refazer todos os blocos publicados na rede, o que torna a rede íntegra para as transações registradas (quanto mais blocos publicados, mais difícil se torna alterar maliciosamente as transações). Importante notar que essa forma denota integridade a partir do registro no bloco e não na origem da transação.

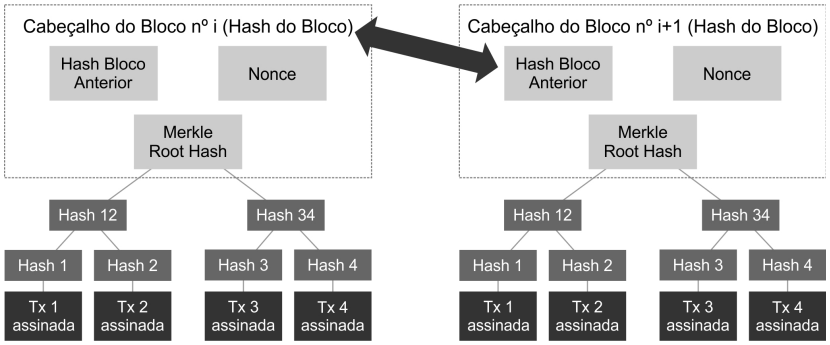

Fig. 4 – Transações em Bitcoin. Adaptado de [43].

Como o consumo de energia computacional é grande para realizar essa mineração das transações, recompensa-se o minerador de acordo com uma regra estabelecida de decaimento de pagamentos na própria moeda eletrônica e de taxas advindas das transações. Essa é uma rede tipicamente pública e não permissionada, para transações

[9] Para mais detalhes por favor refira-se a [33-50].

ponto a ponto sem a interveniência de uma terceira parte confiável.

Para ilustrar somente, existem diversos outros métodos de verificação das transações e blocos, e estabelecimento dos consensos em redes *blockchain*. Alguns exemplos são: *Proof of Stake*, *Proof of Authority*. Há também outras redes, que muitos pesquisadores não abordam como *blockchain*, que são baseadas em um outro conceito de verificação que são *Directed Acyclic Graph* (DAG) e *Hashgraph*. Tudo depende de como uma aplicação em uma rede deve ser executada.

Criou-se, então, um engenhoso procedimento tecnológico para armazenamento de dados eletrônicos que envolve um protocolo de confiança e de consenso sobre uma rede, baseado na comunicação e autenticação de registros distribuídos ponto a ponto, comumente chamado de *Distributed Ledger Technology* (DLT). Fato é que para além das moedas eletrônicas, *blockchain* pode ser aplicado para diversos outros sistemas e segmentos, como: registro de *logs* computacionais, controle de fluxo, registro de dados do cidadão/empresa, comércio, armazenamento em nuvem, entre outros.

Entretanto, por si só, também não garante, ao mesmo tempo, autoria, integridade, autenticidade das chaves e temporalidade dos documentos eletrônicos. Esse, apesar de usarem dispositivos criptográficos, como blocos eletrônicos ordenados e ligados por funções *hash* e assinaturas digitais, usando par de chaves pública e privada, não consegue atestar autoria e temporalidade das transações.

É importante registrar que existem diversos ataques que podem surgir para cada uma dessas implementações. Alguns exemplos são: *eclipse attack*, s*ybil attack*, *selfish mining attack*, *mining malware*, *51% attack*, *timejack attack*, *finney attack*, *race attack*, *DAO attack* (*smart contracts*) e *parity multisig wallet attack* (*wallets*). Existe ampla literatura técnica sobre assumir o controle da rede, quanto a ataques por má implementações de sistemas, *softwares*, entre outros.

No escopo do uso de assinaturas digitais e outros dispositivos, será comentado o que *blockchain*, por si só, não resolve. Tratar-se-á sobre:

i. identificação primária;
ii. ciclo de vida das chaves de assinatura;
iii. temporalidade;
iv. interoperabilidade;

Em que pese existam esforços para identificar uma pessoa por meio de uma rede *blockchain*, não há como essa identificação primária ocorrer sem uma infraestrutura segura e externa aos protocolos. Na grande maioria das redes *blockchain*, a atribuição da

chave privada a seu titular que assina as transações é feita somente por sistema simples (cadastro), sem qualquer controle. As redes que exigem biometria, por exemplo, na autenticação também não se apoiam em processos de verificação higienizada da mesma. Em suma, não há identificação primária segura de pessoas em redes *blockchain* sem o apoio de outras infraestruturas de identificação.

Avançando, a entrega da chave privada ao titular pode ser totalmente desprotegida. Além dos problemas inerentes ao ciclo de vida das chaves, que serão comentados a posterior, significa que um indivíduo pode receber indevidamente uma chave, se passar por outro, e por consequência realizar transações não autorizadas em nome de terceiros. É o anonimato, algumas vezes inerente ao protocolo, como no Bitcoin, das pessoas transacionando ativos digitais. Tal fato não se coaduna com a legislação vigente brasileira em que se exige para meios de prova que um documento, no caso eletrônico, tenha autoria e integridade.

O ciclo de vida das chaves em redes *blockchain* pode ser outro problema das implementações. Sem um processo que vise dar segurança e auditabilidade às chaves criptográficas requisitadas, geradas, enviadas e armazenadas, com os devidos processos normativos, autônomos e independentes de atuação, não há como garantir presunção de veracidade às transações geradas sob um protocolo *blockchain*. Todo protocolo *blockchain* conhecido se utiliza da geração de chaves criptográficas e as entrega para indivíduos. Sem a proteção desse ambiente, conforme já explicado, não há garantias sobre as assinaturas, ou seja, se as transações assinadas são íntegras e autênticas.

Ademais, por usarem uma assinatura baseada em par de chaves, é necessário manter a segurança da geração, emissão e armazenamento desse par (processos físicos e lógicos), ter um algoritmo seguro, que impute corretamente (e sem *backdoor*) as relações matemáticas, que seja interoperável em qualquer dispositivo e que o documento eletrônico tenha validade também fora da rede *blockchain*.

Paul Kocher, no painel dos criptógrafos, da Conferência RSA em 2019, disse em relação a redes *blockchain*, transcrito de:

> *“ …and I think part of the point is also that the criptographic often is the one piece that works. But it seats on top of all these other things: operation systems, processors, application code, firmware, microcode, all these sort of things that we don´t like to think about, because they are not as sexy, but if those don´t work perfectly, then the stuff that does work well “ends up failing under knees”.”*

Não há como usar corretamente, no sentido de se obter validade pericial probatória para as transações eletrônicas inseridas, uma rede *blockchain* sem que haja uma infraestrutura corretamente bem implementada.

Outro possível problema que surge para os mais conhecidos protocolos em *blockchain* é o uso de algoritmos considerados, no mínimo, suspeitos. Elenca-se abaixo os algoritmos de chaves públicas utilizados para alguns protocolos:

i. Bitcoin – secp256k1;
ii. Ethereum – secp256k1;
iii. Hyperledger – prime256v1; secp384r1; secp521r1;
iv. Chain – ed25519;
v. Monero – ed25519;
vi. Libra – ed25519.

Cada um desses protocolos usam métodos de uso da chave pública distintos.

A despeito do já mencionado em relação a segurança na requisição, geração, emissão e armazenamento das chaves criptográficas, os protocolos elencados em i, ii, iii usam curvas NIST para realizar as assinaturas digitais de suas transações. O fato é que existem várias suspeitas em relação as algumas curvas NIST (ECDSA), que vão desde o polinômio/parâmetros que as curvas foram escritas até a geração de números aleatórios realizados por essas. Uma ressalva: o protocolo HyperLedger iniciou estudos para implementação de algoritmos, em teoria, resistentes a ataques quânticos. A não garantia que tais curvas são seguras, gera uma incerteza sobre as assinaturas.

Uma parte importante é que redes *blockchain*, por si só, não endereçam garantia de temporalidade, mas somente de ordenamento das transações, com o tempo formado de cada bloco. Pela forma com que os protocolos atuam, sabe-se que uma transação veio antes/depois de outra, entretanto sem uma infraestrutura de tempo, não há garantia sobre data/hora da assinatura realizada na transação. Se existe a necessidade de garantir corretamente o horário em que tal transação foi gerada/assinada, uma infraestrutura confiável de tempo e sincronizada em relação a referências nacionais/mundiais deve ser usada.

Outro ponto que *blockchain* não endereça é a interoperabilidade entre sistemas. Protocolos em *blockchain* não interoperam seus ativos digitais uns com outros. Um usuário em uma rede, com suas transações, só pode usar sua carteira (*wallet*) naquela rede específica. As transações inseridas em uma *ledger* também só podem ser rastreadas e íntegras naquele protocolo específico criado. Recai-se sobre o problema de um documento só poder ser verificado dentro de um sistema específico, ou seja, o documento

não ser autocontido.

Algumas perguntas devem ser respondidas antes da implementação de uma rede *blockchain*:

i. Como garantir que um indivíduo é quem diz ser?
ii. Como garantir que uma chave pertence e é de controle exclusivo de um indivíduo?
iii. Como garantir que uma chave não pode ser gerada para outro indivíduo?
iv. Como garantir que uma chave não seja gerada em duplicidade?
v. Como garantir que as chaves não sejam extraviadas?
vi. Como garantir a autenticidade de uma chave?
vii. Como garantir a segurança da geração de números aleatórios?
viii. Como garantir que os algoritmos tenham a segurança necessária?
ix. Como garantir que a emissão das chaves seja feita de forma correta?
x. Como garantir que a implementação da rede, evitando ataques conhecidos, esteja correta?
xi. Como garantir o correto horário de uma transação assinada?
xii. Como garantir que os ativos digitais "vivam" íntegros e autênticos fora da rede que usam protocolos/métodos específicos?
xiii. Como garantir que os ativos digitais possam ser reassinados em caso de comprometimento do algoritmo criptográfico?

O ITI, estudando e melhorando as mais modernas implementações de governos e privadas, possui a concepção e expertise de solução que endereça de forma correta e segura uma rede *blockchain*. Essa infraestrutura normativa em redes de registros permanentes, presumirá, com a técnica e procedimentos necessários, a devida segurança e presunção de validade jurídica aos ativos digitais em redes *blockchain*. Para o relacionamento com governo, os documentos que se inserem dentro de uma rede *blockchain* devem ter autoria, autenticidade e integridade, senão, haverá um documento possivelmente imutável, entretanto, fraudado dentro da rede.