PRESIDÊNCIA DA REPÚBLICA
Casa Civil
Instituto Nacional de Tecnologia da Informação

PARECER – DINFRA/ITI

PROCESSO nº 00100.013033/2018-29

ASSUNTO: Resposta ao Ofício nº 1.282/2019 – COTEC/SUCOR/RFB

Em face ao despacho do Diretor-Presidente, do Instituto Nacional de Tecnologia da Informação – ITI, a este Diretor de Infraestrutura de Chaves Públicas, produz-se este Parecer que endereçam as perguntas feitas no Ofício nº 1.282/2019 – COTEC/SUCOR/RFB, de 19 de agosto de 2019.

2. Eis o Parecer.

Escopo

3. Este Parecer terá seu cerne baseado no mérito conceitual técnico e, também, descreverá os textos legislativos adotados sobre a matéria, assunto do Ofício, em outros países. Mostrar-se-á uma pesquisa sobre as legislações no mundo na área de assinatura eletrônica e digital, os relevantes conceitos técnicos e procedimentais da Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil, as explicações sobre os métodos de autenticação e identificação como usuário/senha e biometria e, para finalizar, de registros eletrônicos permanente, como *blockchain.* As proposições mencionadas alicerçarão as respostas das indagações realizadas no Ofício em lide. Os aspectos jurídicos relacionados ao assunto serão conduzidos em Parecer pela douta Procuradoria Especializada do ITI.

4. Este Parecer será dividido nas seguintes seções:

Definições

5. Para os propósitos deste Parecer, as seguintes definições são aplicadas [1, 2, 3, 4, 5, 6]:

Autoridade Certificadora: entidade credenciada a emitir certificados digitais seguindo normas específicas.

Autoridade de Registro: entidade credenciada que realiza o processo de identificação do titular de um certificado digital seguindo normas específicas.

Assinatura Digital: uma *string* de dados calculada por um elemento criptográfico, baseado em procedimentos e algoritmos estudados na matemática e na ciência da computação, que associa, com integridade, as informações de um ativo digital a uma manifestação de vontade de uma pessoa ou entidade originária.

Assinatura Eletrônica: uma *string* de dados anexada a um ativo digital gerada por um sistema, usada por um usuário signatário cadastrado no momento da assinatura eletrônica.

Ativo Digital: atos, transações, documentos, fluxos, máquinas, *softwares* disponibilizados em meios eletrônicos.

Autenticação: processo eletrônico que visa a identificação de uma pessoa, máquina, *software* ou entidade, compartilhando a informação de entrada com quem a retém e com algum dispositivo eletrônico.

Bits: menor unidade de informação eletrônica em formato binário que pode ser armazenada ou transmitida, assumindo valores 0 ou 1.

Blockchain: registro eletrônico permanente e ordenado de um ativo digital, que se ligam por processos matemáticos e de engenharia computacional e são assinados digitalmente por meio de elementos criptográficos, baseado em regras definidas de transações e registro.

Certificado Digital: documento eletrônico assinado digitalmente pela Autoridade Certificadora que o emitiu, contendo a identidade da pessoa, máquina, *software* ou entidade e a correspondente chave pública calculada.

Chave Pública: uma *string* de dados, que pode estar contida em um certificado digital, correspondente matematicamente a uma chave privada, usada para realizar operações de encriptar ou decriptar (verificar uma assinatura), neste último pelo uso exclusivo da chave

privada correspondente, dados contidos em atos, documentos ou dados eletrônicos, usando primitivas de chaves públicas.

Chave Privada: uma *string* de dados, atrelada a uma pessoa, máquina, *software* ou entidade, correspondente matematicamente a uma chave pública, usada para realizar operações de assinatura ou decriptar, neste último pelo uso exclusivo da chave pública correspondente, informações contidas em atos, documentos ou dados eletrônicos, usando primitivas de chaves públicas.

Confidencialidade: garantia de que o conteúdo de um ativo digital é acessível somente por meio de autorização.

Criptografia: em segurança da informação, é o estudo e aplicação da teoria da probabilidade, teoria da informação, teoria complexa, teoria dos números, da álgebra abstrata e de campos finitos, baseada em primitivas seguras sem chaves, de chaves simétricas ou de chaves públicas, nos quais os objetivos são possibilitar confidencialidade, integridade, autenticidade, autenticação de um dado de origem, autoria e não repúdio a uma informação.

Dados: representação da informação ou conceitos, em qualquer formato.

Documento Eletrônico: meio eletrônico em que um dado é registrado ou armazenado por um sistema computacional ou dispositivo similar que pode ser lido e percebido por uma pessoa, sistema computacional ou dispositivo similar.

Eletrônico: relacionado à tecnologia que possui capacidade elétrica, digital, magnética, sem fio, ópticas, eletromagnéticas ou similares.

Funções *Hash*: processo matemático e de engenharia computacional unidirecional que converte uma quantidade de *bits*, em um ativo eletrônico, para uma saída fixa de *bits*, em que essa saída é exclusiva para um determinado dado de origem, de modo que qualquer alteração no dado original, obrigatoriamente, resulta em uma saída (valor de *hash*) alterada.

Integridade: garantia que os dados não podem ser alterados sem autorização. Ademais é importante que os métodos implementados detectem qualquer alteração que por ventura for realizada.

Não-Repúdio: ato que previne uma entidade de negar prévia manifestação, comprometimento ou ação.

Usuário e Senha: método de autenticação em meio eletrônico.

Par de Chaves: um par de chaves são mantidos por uma pessoa, máquina, *software* ou entidade que inclui uma chave privada e uma chave pública que são matematicamente relacionadas, mas distintas umas das outras.

Prestador de Serviço de Confiança: entidade credenciada a emitir certificados digitais ou armazenar chaves criptográficas de usuários, permitindo o acesso remoto, ou fornecendo serviços de portal de assinatura seguindo normas específicas.

Primitivas de Chaves Públicas: aplicação de teoria da matemática, computacional e de engenharia utilizada para realizar operações de encriptação (confidencialidade), assinaturas digitais, troca de chaves e identificação, obrigatoriamente utilizando um par de chaves (também comumente chamado de criptografia assimétrica).

Sistema Biométrico: método de comparação estatístico de medição biológica das características físicas e comportamentais de um indivíduo.

String: um conjunto representativo de *bits* em sistemas computacionais ou similares.

Comparação descritiva entre a assinatura digital no Brasil e as legislações ao redor mundo

6. O termo assinatura digital utilizado no Brasil é, em suma, chamado de assinatura eletrônica qualificada ou avançada ou segura ao redor do mundo [7]. Destacam-se algumas legislações sobre a matéria, que também subsidiarão as respostas e esclarecimentos necessários ao Ofício nº 1.282/2019 – COTEC/SUCOR/RFB.

- *M.P. 2.200-2/01* (Brasil)

7. A Medida Provisória 2.200-2[1], de 24 de agosto de 2001, define a matéria sobre assinatura digital no Brasil [8]. Entre outros, estabelece a ICP-Brasil como uma infraestrutura hierárquica de chaves públicas, com Autoridades Certificadoras – AC – e Autoridades de Registros – AR – credenciadas por um conjunto de normas, cria o Comitê Gestor da ICP-Brasil, entidade definidora das normativas técnicas e procedimentais da ICP-Brasil, e o Instituto Nacional de Tecnologia da Informação – ITI, Autarquia Federal que tem por função operar a AC Raiz, credenciar, auditar e fiscalizar as entidades de acordo com as normas da ICP-Brasil.

[1] A MP 2.200-2, de 24 de agosto de 2001, possui força de Lei no Brasil dada a Emenda Constitucional nº 32, de 11 de setembro de 2001, que versa: Art. 2º As medidas provisórias editadas em data anterior à da publicação desta emenda continuam em vigor até que medida provisória ulterior as revogue explicitamente ou até deliberação definitiva do Congresso Nacional.

8. Instituiu, conforme transcrito abaixo, as garantias que a ICP-Brasil entrega a documentos, aplicações e transações, quando utilizados certificados digitais desta infraestrutura.

> *Art. 1o Fica instituída a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras.*

9. O ditame legal brasileiro faz uma distinção entre a presunção de veracidade gerada nos processos de certificação da ICP-Brasil e outras formas – mesmo assim, essas formas devem ser acordadas entre partes e aceito por quem for oposto o documento –. Veja-se: não nega a utilização de outras formas que por ventura possam ser válidas para as comprovações descritas, entretanto, nota-se, que a outra parte pode não aceitar e repudiar a forma oposta. Deixa claro que a presunção de veracidade, embasado em requisitos técnicos e procedimentais seguros (vide seção da ICP-Brasil), está relacionada somente ao processo de certificação da ICP-Brasil.

> *Art.10. Consideram-se documentos públicos ou particulares, para todos os fins legais, os documentos eletrônicos de que trata esta Medida Provisória.*
>
> *§ 1º As declarações constantes dos documentos em forma eletrônica produzidos com a utilização de processo de certificação disponibilizado pela ICP-Brasil presumem-se verdadeiros em relação aos signatários, na forma do art. 131 da Lei nº 3.071, de 1º de janeiro de 1916 - Código Civil.*
>
> *§ 2º O disposto nesta Medida Provisória não obsta a utilização de outro meio de comprovação da autoria e integridade de documentos em forma eletrônica, inclusive os que utilizem certificados não emitidos pela ICP-Brasil, desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento.*

10. Será demonstrado neste Parecer que somente o uso do processo de certificação da ICP-Brasil, por si só, conforme a MP. 2.200-2/01, garante presunção de autoria, integridade, autenticidade, confidencialidade (se for o caso), temporalidade (se for o caso) e não repúdio. Outras formas isoladas não garantem, tecnicamente, presunção de validade jurídica a documentos eletrônicos.

- REGULAMENTO (UE) N.º 910/2014 (União Europeia)

11. O *REGULAMENTO (UE) N.º 910/2014 DO PARLAMENTO EUROPEU E DO CONSELHO* – também chamado de eIDAS (*electronic IDentification, Authentication and trust Services*) – define a matéria para todos os países que compõem a União Europeia [9]. Substituiu a Diretiva 1999/93/EC e impôs àqueles países um novo regulamento para a agenda digital no continente. Entre os novos conceitos, estabelece uma estrutura legal para assinaturas eletrônicas, selos eletrônicos, carimbos de data e hora, documentos eletrônicos, serviços de certificação para sites, entre outros.

12. Determina critérios de uso de assinaturas eletrônicas, explicitando a necessidade da criação de uma Infraestrutura de Chaves Públicas. A seguir segue texto retirado da lei europeia.

> *(7) O Parlamento Europeu, na sua resolução de 21 de setembro de 2010 sobre a realização do mercado interno do comércio eletrónico (1), realçou a importância da segurança dos serviços eletrónicos — em especial, os de assinaturas eletrónicas — e a necessidade de criar uma infraestrutura de chave pública a nível pan-europeu e instou a Comissão a criar um portal europeu para as autoridades de validação, a fim de assegurar a interoperabilidade transfronteiriça das assinaturas eletrónicas e aumentar a segurança das transações efetuadas através da Internet.*

13. Não nega a validade que uma assinatura eletrônica comum pode ter como evidência legal, com o devido acordo e concordância do meio entre partes, entretanto distingue claramente os efeitos e as presunções da forma de uso qualificada. Nesse sentido, transcrito abaixo, deixa claro que somente as assinaturas eletrônicas qualificadas (assinatura, selo e tempo), feitas por uma infraestrutura de chaves públicas e por provedores de serviço de confiança qualificados e credenciados, com regramentos específicos, tem essas presunções.

> *Artigo 25.º*
> *2. A assinatura eletrónica qualificada tem um efeito legal equivalente ao de uma assinatura manuscrita.*
>
> *Artigo 35.º*
> *2. O selo eletrónico qualificado beneficia da presunção da integridade dos dados e da correção da origem dos dados aos quais está associado.*

> *Artigo 41.º*
> *2. O selo temporal qualificado beneficia da presunção da exatidão da data e da hora que indica e da integridade dos dados aos quais a data e a hora estão associadas.*

14. Pela leitura sistêmica da regulação eIDAS, conclui-se que essa tem seus princípios técnicos e literais muito próximos a concepção dada no Brasil.

- *PIPEDA* (Canadá)

15. O "*PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT*" – PIPEDA – define a matéria no Canadá [3]. Também é possível encontrar uma distinção entre assinaturas eletrônicas comuns, as quais deve também ser acordadas, consensualizadas e relacionadas as consequências entre as partes, e as assinaturas eletrônicas seguras providas por uma Infraestrutura de Chaves Públicas, com Autoridade Certificadoras credenciadas pelo governo Canadense [10]. Adentrando a lei, define onde o uso das assinaturas eletrônicas seguras deve ser feito, começando pelos documentos como evidências ou provas assinados por um ministro ou funcionário público.

> *Documents as evidence or proof*
> *36 A provision of a federal law that provides that a certificate or other document signed by a minister or public officer is proof of any matter or thing, or is admissible in evidence, is, subject to the federal law, satisfied by an electronic version of the certificate or other document if the electronic version is signed by the minister or public officer with that person's secure electronic signature.*

16. Além do mencionado, o Canadá impõe o uso de assinaturas eletrônicas seguras, equivalentes às assinaturas digitais no Brasil, para diversos atos, destacando o uso em documentos eletrônicos originais e às declarações de veracidade, transcritos abaixo.

> *Seal*
> *39 A requirement under a provision of a federal law for a person's seal is satisfied by a secure electronic signature that identifies the secure electronic signature as the person's seal if the federal law or the provision is listed in Schedule 2 or 3.*
>
> *Original documents*
> *42 A requirement under a provision of a federal law for a document to be in its original form is satisfied by an electronic document if*
> *(a) the federal law or the provision is listed in Schedule 2 or 3;*
> *(b) the electronic document contains a secure electronic signature that was added when the electronic document was first generated in its final form and that can be used to verify that the electronic document has not been changed since that time; and*

(c) the regulations respecting the application of this section to the provision have been complied with.

Statements made under oath
44 A statement required to be made under oath or solemn affirmation under a provision of a federal law may be made in electronic form if
(a) the person who makes the statement signs it with that person's secure electronic signature;
(b) the person before whom the statement was made, and who is authorized to take statements under oath or solemn affirmation, signs it with that person's secure electronic signature;
(c) the federal law or the provision is listed in Schedule 2 or 3; and
(d) the regulations respecting the application of this section to the provision have been complied with.

Statements declaring truth, etc.
45 A statement required to be made under a provision of a federal law declaring or certifying that any information given by a person making the statement is true, accurate or complete may be made in electronic form if
(a) the person signs it with that person's secure electronic signature;
(b) the federal law or the provision is listed in Schedule 2 or 3; and
(c) the regulations respecting the application of this section to the provision have been complied with.

- *Lei nº 19.799* (Chile)

17. A "*LEY SOBRE DOCUMENTOS ELECTRONICOS, FIRMA ELECTRONICA Y SERVICIOS DE CERTIFICACION DE DICHA FIRMA*" - define a matéria no Chile [11]. Separa, também, os conceitos de uma assinatura eletrônica e assinatura eletrônica avançada, fornecidos por Prestadores de Serviço de Certificação credenciados.

18. No Chile, todas as assinaturas eletrônicas possuem efeitos legais como uma manuscrita. Entretanto, a lei é expressa em obrigar o uso se assinaturas eletrônicas avançadas em determinados instrumentos, como faz o Canadá. Destaca-se que todos os instrumentos públicos devem ser assinados na forma avançada e também que os instrumentos particulares devem ter suas datas providas pelos prestadores credenciados, para atestar a data do documento. Segue parte do texto legal transcrito abaixo.

Artículo 4º
Los documentos electrónicos que tengan la calidad de instrumento público, deberán suscribirse mediante firma electrónica avanzada.

> *Artículo 5º*
> *Los documentos electrónicos podrán presentarse en juicio y, en el evento de que se hagan valer como medio de prueba, habrán de seguirse las reglas siguientes:*
>
> > *1.Los señalados en el artículo anterior, harán plena prueba de acuerdo con las reglas generales, y*
> > *2.Los que posean la calidad de instrumento privado, en cuanto hayan sido suscritos con firma electrónica avanzada, tendrán el mismo valor probatorio señalado en el número anterior. Sin embargo, no harán fe respecto de su fecha, a menos que ésta conste a través de un fechado electrónico otorgado por un prestador acreditado.*
>
> *Artículo 7º*
> *Los actos, contratos y documentos de los órganos del Estado, suscritos mediante firma electrónica, serán válidos de la misma manera y producirán los mismos efectos que los expedidos por escrito y en soporte de papel.*
>
> *Con todo, para que tengan la calidad de instrumento público o surtan los efectos propios de éste, deberán suscribirse mediante firma electrónica avanzada.*

- *eSIGN e UETA* (EUA)

19. Os "*ELECTRONIC SIGNATURES IN GLOBAL AND NATIONAL COMMERCE ACT*" – eSING – e "*UNIFORM ELECTRONIC TRANSACTIONS ACT*" – UETA – esclarecem a matéria nos Estados Unidos [1, 2]. Nessas legislações não há distinção entre assinaturas eletrônicas e, desde que estabelecidos acordos e consensos expressos entre partes, os documentos assinados podem ter validade independente da tecnologia usada. É importante notar que nesse país existe uma ampla cultura de livre forma para diversos atos, inclusive os que envolvem direitos e deveres, sem mesmo a necessidade de papel/contratos assinados para estabelecimento de vínculo. Segue comentário transcrito abaixo [2].

> *A. Scope of the Act and Procedural Approach.*
> *In general, there are few writing or signature requirements imposed by law on many of the "standard" transactions that had been considered for exclusion. A good example relates to trusts, where the general rule on creation of a trust imposes no formal writing requirement.*

20. Entretanto, é minimalista em relação aos efeitos legais que o próprio ditame legal pode ter em uma corte. O caso nº 16-22134-D-7, de 13 de julho de 2016, da Corte de Falência dos Estados Unidos, Distrito Leste da Califórnia [12], o juiz Robert S. Bardwil decidiu que a assinatura eletrônica "simples", i.e., somente clicar em botão assinar, gerando

o nome do suposto signatário (em uma base comparativa e compartilhada – usuário e senha), não pode ser utilizada para efeitos de preenchimento da documentação oficial relacionada com falências. No caso concreto, uma assinatura eletrônica simples não gerou presunção e efeitos legais. Segue o comentário transcrito sobre a lei americana [2].

> *B. Procedural Approach.*
> *The Act's treatment of records and signatures demonstrates best the minimalist approach that has been adopted. Whether a record is attributed to a person is left to law outside this Act. Whether an electronic signature has any effect is left to the surrounding circumstances and other law.*

21. Não obstante, diversos órgãos de segurança dos Estados Unidos, como a *National Security Agency* – NSA – [13] e o *Committee on National Security Systems* – CNSS – [14], impõe uma série de requisitos para sistemas, comunicações, entre outros, com o uso de tecnologias baseadas em primitivas de chaves públicas seguras.

22. Pelas dificuldades de interoperabilidade e formato independente federativo dos Estados Unidos, inclusive na formação de um padrão ICP, em 2017, na Comissão de Comércio, Ciência e Transporte, do Senado Americano, a ICP-Brasil foi citada como referência mundial em relação às assinaturas eletrônicas e identidades dinâmicas [15].

- *Act nº 5792* (Coreia do Sul – lei traduzida)

23. A "*DIGITAL SIGNATURE ACT*" define a matéria na Coreia do Sul [16]. Assim como a grande maioria das leis ao redor do mundo, como também versa a brasileira, não nega validade para outras formas de assinaturas eletrônicas, desde que acordadas e consentidas entre partes. Entretanto, é, também, clara em fazer uma distinção de presunção de validade quando usado certificados digitais para assinaturas digitais (na Coreia, assim como no Brasil, se usa o termo assinatura digital feita por um certificado digital), nos modelos de chaves públicas emitidas por entidades credenciadas junto ao governo. Abaixo, transcreve-se parte da lei Coreana, de forma traduzida ao inglês, retirado de [16].

> *Article 3 (Effect, etc. of Digital Signature)*
> *(1) In cases where a signature, signature and seal, or name and seal is, under other Acts and subordinate statutes, required to be affixed on a paper-based document or letter, it shall be deemed that such requirements are satisfied if there is a certified digital signature affixed on an electronic message. <Amended by Act No. 6585, Dec. 31, 2001>*
> *(2) In cases where a certified digital signature is affixed on an electronic message, it shall be presumed that such a digital signature is the signature, signature and seal, or name and seal of the signer of the electronic message concerned and that there has been no alteration in the contents of such message since it was*

signed digitally. <Amended by Act No. 6585, Dec. 31, 2001> (3) A digital signature other than a certified digital signature shall have such an effect of a signature, signature and seal, or name and seal, as is agreed between the parties concerned. <Newly Inserted by Act No. 6585, Dec. 31, 2001>

Article 4 (Designation of Licensed Certification Authority)
(1) The Minister of Public Administration and Security may designate as a licensed certification authority an entity that is deemed to be capable of performing authorized certification work (hereinafter referred to as "certification work") in a secure and reliable manner. <Amended by Act No. 6585, Dec. 31, 2001; Act No. 8852, Feb. 29, 2008>
(2) The entity that can be designated as a licensed certification authority shall be limited to State agencies, local governments and corporations.
(3) The entity that desires to be designated as a licensed certification authority shall meet such requirements as technical and financial capabilities, facilities and equipment, and other required matters as provided by Presidential Decree.
(4) Where the Minister of Public Administration and Security designates a licensed certification authority under paragraph (1), he/she may designate it, for a sound development, etc. of the authorized certification market, by dividing the domain of certification work under the establishment purpose in cases of State agencies, local governments, non-profit corporations or corporations established by special Acts. <Newly Inserted by Act No. 7813, Dec. 30, 2005; Act No. 8852, Feb. 29, 2008>
(5) Procedures for designation of a licensed certification authority and other necessary matters shall be determined by Presidential Decree.

24. Diversos outros países [17] possuem leis que distinguem e dão presunção de validade (alguns com os efeitos legais de assinaturas manuscritas), como o Brasil, para as assinaturas eletrônicas qualificadas, seguras ou avançadas ou assinaturas digitais. Alguns desses países são: Rússia, Indonésia, Peru, Singapura, África do Sul, Suíça, Turquia, México, Israel, China, Filipinas.

25. Países como Austrália, Nova Zelândia e Uruguai seguem a linha minimalista adotada pelos Estados Unidos.

26. Embora não seja o contexto das perguntas elencadas no Ofício assunto deste Parecer, todas as leis citadas ao longo dos anos progrediram com emendas para que o texto reflita o cenário atual de tecnologias e procedimentos. O Brasil também precisa realizar uma atualização em seu marco legal sobre assinaturas digitais, principalmente relacionados a incorporação de novas tecnologias, algoritmos e os processos que os cercam.

ICP-Brasil: aspectos técnicos e procedimentais

27. Descrita pela Medida Provisória 2.200-2/01, a ICP-Brasil possui seu ditame legal calcado, obrigatoriamente, em pressupostos técnicos – de segurança física e lógica –, matemáticos, computacionais, procedimentais, de auditoria e de fiscalizações mínimos. A ICP-Brasil é a única plataforma em funcionamento no Brasil que garante aos documentos, transações e atos eletrônicos concomitantemente autoria, integridade, confidencialidade, autenticidade, temporalidade, não repúdio, e, por consequência, presunção de validade jurídica, nas autenticações e assinaturas digitais em meio eletrônico. Repisa-se, os normativos da ICP-Brasil compõem um *parquet* tecnológico e procedimental mínimo para que a eficácia probatória dos documentos eletrônicos possa ser garantida. Não há como, do ponto de vista técnico, discorrer sobre normas e leis tentando garantir presunção de validade (autoria, integridade, temporalidade, não repúdio) a documentos eletrônicos caso, no mínimo, esses requisitos não sejam cumpridos.

28. Outro ponto relevante de como funciona a ICP-Brasil é que qualquer entidade, pública ou privada, que cumpra os requisitos legais e infralegais pode ser credenciada na ICP-Brasil. A infraestrutura não é um monopólio. O ITI, como Autarquia Federal e AC Raiz, não emite certificados digitais para usuários finais, não participa ou regula a parte comercial da ICP-Brasil.

29. Um princípio capital da ICP-Brasil é ser uma plataforma segura de requisição, geração, emissão, armazenamento e revogação de elementos criptográficos. São, para a ICP-Brasil, denominados de chaves públicas e privadas. Um conjunto de procedimentos seguros [18] e determinados por um Comitê Gestor autônomo, outros pilares da ICP-Brasil (que se somam a segurança na manifestação de vontade de um titular de uma chave), atrelam indivíduos, entidades, aplicações, códigos e máquinas a esses elementos. A entidade que gera as chaves (AC) não é a mesma que determina as regras (Comitê-Gestor); e uma terceira entidade (ITI) audita e fiscaliza se as normas estão sendo cumpridas. Esse funcionamento é determinante para a presunção de validade legal das assinaturas digitais realizadas com as chaves da ICP-Brasil.

30. Os elementos criptográficos da ICP-Brasil possuem diversas características, auditadas e fiscalizadas em conceitos extremamente conhecidos, públicos e seguros. São gerados baseados em teorias matemáticas, da ciência da computação, da proteção do módulo criptográfico, da engenharia de *software* e *hardware*, entre outros. Percorrem da geração de números verdadeiramente aleatórios a dificuldade, em qualquer nível de computação e ataques conhecidos atualmente, em fatorar números primos grandes ou em resolver o problema do logaritmo discreto.

31. Essa ação matemática/criptográfica para assinaturas digitais na ICP-Brasil funciona assim, derivado de [4]:

32. Uma assinatura digital e sua verificação segura, em um esquema de primitivas de chaves públicas, deve ter a seguinte característica de reversibilidade:
i. $Dd(Ee(m)) = Ee(Dd(m)) = m$, em que *Ee* é a operação de encriptação ou verificação usando uma chave pública, *Dd* é a operação de assinatura ou decriptar usando uma chave privada, correspondente a *Ee*, e m é a mensagem pertencente ao espaço *M* para o esquema de assinatura, que pode ser apresentada em uma função *hash* ou em texto claro;
ii. A assinatura de uma mensagem m é $s = Dd(m)$, para toda $m \in M$;
ii. A verificação, *Va*, de uma assinatura é feita assim: $Va(m,s) =$ {verdadeiro, se $Ee(s) = m$; falso, em outros casos}.

33. A assinatura digital pode ser facilmente calculada pelo "assinador" titular, com um elemento seguro criptográfico/matemático, e verificada por qualquer um, com outro elemento seguro criptográfico/matemático distinto do usado na assinatura. Deve ser computacionalmente segura em relação a não ser forjada.

34. Dois tipos de algoritmos, descritos em RFC[2] (*Request for Comments*), são utilizados e amplamente reconhecidos no mundo pela sua força, se bem implementado, em repelir ataques conhecidos e possíveis de serem aplicados. Esses são o RSA (Rivest, Shamir, Adleman) e DSA (*Digital Signature Algorithm*). O entendimento matemático e procedimental é um dos argumentos mínimos para que um documento eletrônico seja autocontido (íntegro e interoperável), explicado adiante, garantido a presunção de validade jurídica.

35. O algoritmo RSA foi proposto pelos eméritos professores Ron Rivest, Adi Shamir e Leonard Adleman [19].

36. O RSA é baseado no problema da fatoração em que qualquer número natural diferente de 1 pode ser escrito de forma única – desconsiderando a ordem – como um produto de números primos, chamados de fatores primos, de um número inteiro – Teoria Fundamental da Aritmética –, ou seja, um número *n* pode ser fatorado em $n = p_1^{e1} * p_2^{e2} * \ldots * p_k^{ek}$, em que p_i são primos distintos emparelhados e $e_i \geq 1$.

37. De acordo com a *RSA Laboratories* e o desafio proposto de fatoração [20, 21, 22], se tem registro que o RSA-768 *bits*, um número decimal representativo de 232 dígitos (i.e., $2^{768} = 10^n$; 768 log(2) = n log(10); n = 768 log(2) = 231,19), utilizando centenas de computadores e técnicas demorou 3 anos para ser fatorado. Estimou-se que RSA-1024 *bits* demoraria mais de 3000 anos, utilizando as mesmas técnicas. Atualmente a

[2] Documentos formais da *Internet Engineering Task Force* (IETF) que, em sua versão final, tornam-se padrões da Internet.

ICP-Brasil utiliza RSA-2048 *bits* (um número decimal representativo de 617 dígitos) e RSA-4096 *bits* (um número decimal representativo de 1234 dígitos) para seus usuários finais e RSA-4096 *bits* para suas Autoridades Certificadoras. Em relação a força computacional e de técnicas existentes, a estimativa necessária para quebrar/fatorar esses é de centenas de milhares de anos, o que torna a segurança do processo ainda inquebrável em tempo operacional (O) polinomial ($2^{O(\log n)}$).

38. O algoritmo RSA funciona assim:

i. gera-se dois grandes primos aleatórios distintos p e q, com aproximadamente o mesmo tamanho – fundamental que existam processos seguros, testados e auditados para essa geração;
ii. calcula-se $n = pq$ e $\Phi = (p - 1)(q - 1)$;
iii. seleciona-se de forma aleatória um inteiro e, $1 < e < \Phi$, de tal modo que mdc(e, Φ) = 1;
iv. usa-se o algoritmo de Euclides estendido [23, 24] para computar o único inteiro d, $1 < d < \Phi$, de tal modo que $ed \equiv 1 \pmod{\Phi}$, ou seja, d é o inverso multiplicativo de e em mod $\Phi(n)$;
v. a chave pública é (n, e) e a chave privada é d;
vi. a assinatura RSA é: $s = m^d \bmod n$;
vii. para verificar assinatura em RSA é: $m = s^e \bmod n$;
viii. formatos PKCS#1 (somente das chaves) [25] e PKCS#7 (envelopes/certificados) [26] podem ser utilizados.

39. O algoritmo DSA foi proposto pelo *National Institute for Science and Technology* – NIST, tornando-se um padrão por meio da *Federal Information Processing Standard* – FIPS [27]. As variantes mais utilizadas no mundo é o DSA baseado em curvas elípticas ECDSA [28] e, mais recente, EdDSA [29].

40. O DSA (ECDSA e EdDSA) é baseado no problema do logaritmo discreto. A solução de uma equação $a^x = b$ é $\log_a(b)$. Para um grupo cíclico Z_p {1,...,p-1}, deseja-se encontrar a k-ésima potência de um dos números desse grupo. Para tanto, deve-se calcular o resto da divisão por p (GDLP – *Generalized Discrete Logarithm Problem*[3]). Um exemplo: $3^k \bmod 17 = 12$; resolvendo o logaritmo: k = 29. Outro exemplo: $654325^k \bmod 25678932032712177 = 2999871234567$; k = ?. Não é uma equação fácil de ser resolvida. Quando amplia-se para os algoritmos DSA bem implementados, essa solução não é viável usando a força computacional existente atualmente.

41. O algoritmo ECDSA, ou EdDSA, funciona assim:

[3] Dado um grupo cíclico finito G de ordem n, um gerador α de G e um elemento β ϵ G, ache um inteiro x, $0 \leq x \leq n - 1$, tal que $\alpha^x = \beta$ [4].

i. seleciona-se um grupo abeliano finito (que possui propriedades associativa, neutra, inversa, comutativa) *E* sobre uma curva elíptica Z_p (ou Z_2^m);
ii. seleciona-se um ponto (x, y) G, gerador do grupo finito $E(Z_p)$ de ordem n (cardinalidade);
iii. seleciona-se uma chave privada d, entre 1 e n – 1; fundamental que existam processos seguros, testados e auditados para essa seleção;
iv. calcula-se a chave pública: Q = d G;
v. também são públicos: *E*, n e G;
vi. assinar em ECDSA/EdDSA: selecione k entre 1 e n – 1; calcule $(x_1, y_1) = k\ G$ e $r = x_1$. volte à escolha de k enquanto r = 0; a seleção de k é fundamental para segurança do processo;
vii. calcule $s = k^{-1}[h(m) + d\ r] \bmod n$; volte à escolha de k enquanto s = 0, h é a função hash;
viii. o par (r, s) é a assinatura digital de m;
ix. verificar em ECDSA/EdDSA: calcule $w = s^{-1} \bmod n$; calcule $u_1 = h(m)w \bmod n$ e $u_2 = rw \bmod n$; calcule $u_1G + u_2Q = (x_2, y_2)$, $v = x_2 \bmod n$; se v = r, então (r, s); se v = r assinatura válida.

42. Atualmente a ICP-Brasil utiliza os algoritmos em curvas elípticas brainpoolP512r1, ed448 e E-521 para as Autoridades Certificadoras e brainpoolP256r1, brainpoolP512r1, ed25519, ed448 e E-521 para usuários finais. Para registro, as curvas Edwards (EdDSA) possuem o polinômio $x^2 + y^2 = 1 + dx^2y^2$; e as curvas de Montgomery possuem o polinômio $by^2 = x^3 + ax^2 + x$.

43. Como se pode notar em ambos algoritmos, derivam-se desses processos dois elementos (uma chave pública e privada) matematicamente ligados a fazerem operações aritméticas nos *bits* do documento eletrônico (ou no *hash* desse), mas distintos um do outro. Essa característica é fundamental na preservação de qualquer assinatura (manifestação de vontade) no meio eletrônico – garante integridade dos dados assinados e não há compartilhamento do elemento de assinatura. Um é privado, de controle exclusivo e ligado a um titular, e outro público, podendo ser enviado para realizar operações diversas como a verificação de uma assinatura da chave privada ou encriptação de um ativo digital. Garante que tal operação feita com um dos elementos no ato eletrônico somente, e exclusivamente, pode ter vindo do outro.

44. É notório que reluzem das assertivas anteriores uma alta dependência da proteção do ciclo dessas chaves, para que a presunção de validade dos atos eletrônicos advindos desses elementos criptográficos seja garantida. Os algoritmos, os ambientes, as auditorias e os procedimentos dessa requisição, geração, emissão e armazenamento obrigatoriamente precisam ser, rigorosamente, seguros e conhecidos [18]. O uso de regras mundialmente conhecidas, em dispositivos testados e homologados, como os *Hardware*

Security Module - HSM, e ambientes e redes/conexões seguros e controlados, auditados por métodos transparentes e conhecidos, se faz obrigatoriamente necessários.

45. Outro princípio basilar da ICP-Brasil é a interoperabilidade. Um documento eletrônico assinado com ICP-Brasil, além de poder ser verificado em qualquer outro meio eletrônico, é autocontido, i.e., não depende de um sistema exclusivo para ser verificado/autenticado. A "vida" (garantia de eficácia da prova/verificação) do documento eletrônico, assim como em uma assinatura manuscrita em um documento físico, deve ser independente de um sistema. Essa é uma grande diferença das assinaturas digitais da ICP-Brasil, que são independentes e autocontidas, para outros mecanismos de assinatura e registro eletrônico.

46. A ICP-Brasil também endereça algo importante nos dias atuais. Além dos termos legislativos e técnicos da MP 2.200-2/01 e seus atos infralegais, que tratam e garantem presunção de validade jurídica às autenticações e assinaturas digitais, é importante a segurança e confidencialidade que a ICP-Brasil pode prover aos dados eletrônicos, a luz da Constituição Brasileira, como direito ao sigilo fiscal, bancário e telemático, e de marcos legais como a Lei Geral de Proteção de Dados – LGPD [30]. No mundo das comunicações de dados eletrônicas, cujo princípio vital é a troca informações em benefício de facilitar o provimento de serviços aos cidadãos (por isso é tão difícil ajustar normas no rol de proteção de dados nas redes computacionais), surgem leis ao redor do mundo para impelir que abusos e vazamentos sejam feitos com dados eletrônicos de cidadãos e empresas [31].

47. Não está no escopo deste Parecer, mas, resumidamente, é fundamental notificar que a ICP-Brasil entrega a cidadãos e empresas o devido poder de decidir quais dados devem ser protegidos a consultas e quando liberá-los. As informações eletrônicas dos cidadãos podem ser protegidas por um elemento criptográfico de controle exclusivo do titular, ou às entidades e os órgãos os quais as leis no país impõem certas atividades que necessitam desses dados. Trata-se de, a claridade versada na Constituição brasileira, prover a garantia da segurança dos dados eletrônicos dos seus cidadãos e de qualquer comando em lei ordinária ou complementar para esses. A ICP-Brasil provê rastreabilidade dos atos usados sob sua plataforma, estabelecendo ampla segurança, técnica e jurídica, das informações e, caso necessário, a processos periciais por alguma inconformidade ou ilegalidade no uso ou vazamento dos dados eletrônicos.

- Nota:

48. Descreve-se, neste instante, algo orgânico na abordagem da ICP-Brasil, quando da utilização de outros certificados fora desta infraestrutura. Estabeleceu-se um importante marco de entendimento jurídico para a ICP-Brasil. O Mandado de Segurança nº

2007.72.00.002903-9/SC, impetrado pelo ITI contra o município de Florianópolis, pela edição do Decreto Municipal, 4.446/2006 foi julgado pelo Juiz Gustavo Dias de Barcellos [32]. Abaixo transcreve-se trechos da sentença:

> *O Decreto Municipal nº 4446/06, questionado nesta ação, introduz intenção de conferir presunção de veracidade aos documentos fiscais gerados e emitidos em forma eletrônica (art. 15). O referido Diploma, na condição de mero regulamento administrativo, não tem força de Lei, não podendo alterar a norma legal expressa acima destacada.*
>
> *Outra ponderação relevante destacada na inicial é a necessária garantia da interoperabilidade entre os diversos Sistemas, todos integrados, de forma hierárquica, ao Instituto Nacional de Tecnologia da Informação - ITI, o qual figura como Autoridade Certificadora Raiz e constitui uma raiz única. Tal garantia de interoperabilidade permitirá, no futuro, intercâmbio e gerenciamento de informações entre as entidades públicas que venham a operar com a tecnologia em questão, por exemplo: Receita Federal (já integrante), secretarias de fazenda estaduais e municipais.*
>
> *Nesse quadro, a existência de um sistema fechado, exclusivo de um município e seus contribuintes, tornaria difícil essa interoperabilidade.*
>
> *No mesmo sentido, aponto o trecho da decisão proferida no Agravo nº 2007.0400009343-4 (fl. 87), ao tratar do Sistema Nacional de Certificação Digital: Tal regramento encontra perfeita sintonia com o disposto no parágrafo único do art. 154, da Lei Adjetiva, ao dar tratamento unificado nacionalmente. Ora, não se diga que a matéria tratada no Decreto Municipal objurgado (n. 4.446/06), seria de índole eminentemente tributária - instituiu o Sistema de Autorização de Documentos Fiscais Eletrônicos - AEDE, criando-se uma autoridade de Registro (AR) própria da Secretaria Municipal da Receita -. Com isso, praticamente, estabeleceu um sistema de Infra-Estrutura de Chaves Públicas Municipal, paralelo, ao sistema nacional antes referido, de sorte que, acaso legitimada tal conduta, importaria em irrogar-se a todos os municípios do Brasil tal possibilidade, cujas conseqüências seriam desastrosas para o sistema.*
>
> *A mesma decisão considerou consistente a alegação de que a ICP-BRASIL objetiva constituir uma cadeia de confiança, cujo objetivo fundamental é o de permitir, nacionalmente, a comprovação da autenticidade e da integridade das manifestações de vontade das pessoas físicas e jurídicas.*
>
> *ANTE O EXPOSTO, acolhendo integralmente a fundamentação e o pedido do impetrante, e reportando-me aos termos da decisão já proferida no Agravo (fls. 87), concedo a segurança para declarar*

> *a ilegalidade do Decreto Municipal nº 4.446/2006, editado pelo Prefeito Municipal de Florianópolis/SC, afastando seus efeitos, nos termos da fundamentação.*

49. Tal decisão foi confirmada pelo Tribunal Regional Federal da 4ª Região, relatada pelo Desembargador Edgard Antônio Lipmann Júnior, publicada no Diário Eletrônico de Justiça em 26/11/2007.

***Explicação sobre outras tecnologias, como: usuário/senha (login/senha), sistema biométrico e blockchain* em relação a autoria e integridade de dados.**

- *Usuário e Senha*

50. O emprego de usuário e senha não garante, em absoluto, nem a presunção de autoria, nem muito menos a integridade de documentos eletrônicos.

51. Explica-se.

52. Usuário e senha, por si só, quando ampliado a realizar processos de assinatura eletrônica, é um sistema desprovido de segurança. É, usualmente, um segredo compartilhado: a senha, teoricamente sigilosa, é armazenada em um servidor do depositário – dessa forma, não apenas o seu proprietário tem acesso e a manipula. Quando usado para autenticação, usualmente a referida senha trafega abertamente na rede, estando suscetível a ataques, violações ou cópias mal-intencionadas de toda espécie. Ora, nada mais frágil sob a ótica da segurança da informação, visto que o elemento que "assina" é compartilhado, ou seja, com usuário e senha "assina-se" e verifica-se eletronicamente com o mesmo elemento. É comum notícias de furtos a senhas pelo mundo, utilizando, as vezes, técnicas simples de ataques [33].

53. Ainda que se exija alguma senha mais robusta, tais como a utilização de letras e números, *hashing* passwords, selos, a adoção da tecla *Caps Lock*, entre outros, o *login* não perderá a sua fragilidade [34, 35, 36].

54. A consequência de assinar eletronicamente com usuário e senha, em termos mais explícitos, é que basta a negativa (repúdio) de quem a utiliza para carrear o ônus da prova à outra parte [36].

55. Adentra-se a obscura tentativa de dar comprovação de integridade ao documento eletrônico por outras vias, como usuário e senha [36]. É impossível nos dias atuais, tecnicamente, garantir, por si só, integridade a um documento eletrônico sem a utilização de um elemento criptográfico, como em uma assinatura digital. Integridade de um documento eletrônico deve ser feita utilizando regras matemáticas/computacionais que

incidem diretamente na *string* de *bits* que compõem um documento eletrônico (ou no *hash* desse). É feito um cálculo criptográfico nesses *bits*, de modo a integralizá-los com a chave de assinatura de controle exclusivo do titular e tornar viável sua conferência por outro elemento distinto criptográfico, preservando fielmente o conteúdo da mensagem. Usuário e senha não possui processos seguros que incidem matematicamente nos *bits* de um documento eletrônico. São somente anexados a composição do documento, podendo ser facilmente manipulados. Ou seja, não se garante integridade de um documento eletrônico utilizando somente uma técnica de autenticação chamada de usuário e senha.

56. Admitisse, no limite, a utilização de usuário e senha apenas para fins de autenticação, isto é, para o (simples) acesso a sistemas informacionais, mas jamais, para se assinar com o reconhecimento de presunção de autoria ou integridade a qualquer documento eletrônico. Entretanto, até para autenticação, é recomendável o uso de outro método conjugado. Existe uma forte tendência ao desuso do método usuário e senha inclusive para as autenticações [37, 38].

57. Assim, a autenticação por usuário e senha, por si só, não garante nem a autoria (não se tem como saber se aquela pessoa é efetivamente quem afirma o ser), nem tampouco o conteúdo da mensagem (que pode sofrer alterações no caminho entre o emissor e o destinatário). Qualquer disposição legal ou normativa, ao prever a comprovação de tais elementos por meio de usuário e senha, encontra-se completamente incongruente sob a ótica técnica, implicando, inevitavelmente, em insegurança técnica/jurídica.

58. Ademais, um documento eletrônico que possui anexado uma autenticação de usuário e senha não é autocontido. Significa que esse documento eletrônico só pode ser verificado dentro do próprio sistema que criou o usuário e senha. Sem o sistema, o documento eletrônico não tem "vida", que é totalmente oposto a um documento assinado de forma manuscrita em papel ou assinado digitalmente. Um documento eletrônico precisa ter independência e interoperabilidade de sistemas para que esse possa ser autêntico.

59. Em um litígio judicial, ou simplesmente o repúdio por parte de alguém, não é possível periciar, por si só, o documento eletrônico e aferir prova de autoria e integridade. Isso significa que as partes (oficial e particular) devem ter acesso ao sistema para, talvez, encontrar outros indícios de autoria. Para sistemas públicos e de segurança isso pode se tornar um incidente muito grave.

60. Usar esse método simples de autenticação como uma garantia de presunção de autoria e integridade é, do ponto de vista técnico, o anonimato virtual de pessoas e das aplicações, sem rastreabilidade e sem a segurança dos dados. Por óbvio, usuário e senha, entre outros, não são métodos que se utilizam dos padrões, da segurança, da gestão de identidade e de sistemas criptográficos como a ICP-Brasil, conforme explicado.

- *Sistema Biométrico*

61. Um sistema biométrico é um método automatizado que busca garantir a identificação por meio da comparação estatística de uma medida perene biológica de um indivíduo. Existem vários sistemas civis e criminais que se utilizam de biometrias físicas (e.g., impressão digital, face, íris, entre outros) e comportamentais (e.g., assinatura manuscrita e voz). Para que tal método garanta a identificação de um indivíduo são necessárias a consecução de diversos procedimentos que visam proteger a coleta da biometria e a base a qual essa será comparada [18, 39, 40].

62. É importante notar que a identificação de um indivíduo só pode ser aferida por sistemas biométricos se, de ponta a ponta, os processos forem seguros e auditáveis. Não há como garantir identificação se, por exemplo, a coleta ou verificação da biometria não tiver processos rígidos de controle e qualidade da biometria, de verificação de vida, de envio da biometria pela rede, assim como a base de comparação não proporcionar a comparação técnica adequada, além de ser segura contra vazamentos de dados.

63. A correta implementação de sistemas biométricos é fundamental, visto que vazamentos podem ocorrer e causar graves prejuízos, como ocorreu com a base da Índia [41]. Quando um dado biométrico vaza, significa que uma informação sensível e perene do indivíduo poderá ser ilegalmente usada para sempre. Não há como trocar a biometria de indivíduo, quando estritamente compara-se a outros métodos.

64. Isto posto, adentra-se a análise do uso estendido da biometria para assinar documentos eletrônicos. O uso de um sistema biométrico, por si só, também não garante concomitantemente a um documento eletrônico autoria e integridade.

65. Explica-se.

66. Um sistema biométrico é, normalmente, assim como usuário e senha, o uso de um segredo compartilhado: o dado biométrico, teoricamente sigiloso, é armazenado em um servidor do depositário – dessa forma, não apenas o seu proprietário tem acesso e o manipula. Quando usado para identificação, é necessário garantir, de ponta a ponta (dispositivo de coleta e base de dados) e na comunicação entre dispositivos, que tais processos são seguros. Quando usado de forma estendida para assinar eletronicamente, o elemento que "assina" é compartilhado, ou seja, também com biometria "assina-se" e verifica-se eletronicamente com o mesmo elemento, ou melhor, com a mesma representação vetorial da biometria.

67. Da mesma forma apontada nos métodos de usuário e senha, adentra-se a obscura tentativa de dar comprovação de integridade ao documento eletrônico por uso de um sistema biométrico. Conforme já explicado, e toda matemática e ciência computacional envolvida, é impossível nos dias atuais, tecnicamente, garantir, por si só, integridade a um documento eletrônico sem a utilização de um elemento criptográfico, como em uma assinatura digital. Um sistema biométrico não possui processos seguros que incidem matematicamente nos *bits* de um documento eletrônico. São somente anexados a composição do documento, podendo ser facilmente manipulados. Ou seja, não se garante integridade de um documento eletrônico utilizando somente uma técnica de identificação.

68. Entende-se como adequada a utilização de biometria, quando bem implementada e com uso de outros métodos auxiliares, apenas para fins de identificação em sistemas, mas jamais, para se assinar com o reconhecimento de presunção de autoria ou integridade a qualquer documento eletrônico.

69. Assim, a identificação por sistemas biométricos, por si só, não pode garantir a autoria, nem muito menos a integridade do conteúdo da mensagem eletrônica. As mesmas consequências comparadas ao método usuário e senha, quando do mau uso estendido de biometria para assinaturas eletrônicas, podem acontecer.

- *Blockchain*

70. Outro mecanismo muito discursado ultimamente são as redes baseadas em *blockchain*. Apesar de o assunto não estar relacionado diretamente as perguntas elencadas no Ofício nº 1.282/2019 – COTEC/SUCOR/RFB, é importante para o entendimento do uso de chaves fora de uma infraestrutura legal normativa.

71. As redes baseadas em *blockchain* tornaram-se conhecidas por meio do protocolo Bitcoin [42]. 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* [43] é utilizado.

72. *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.

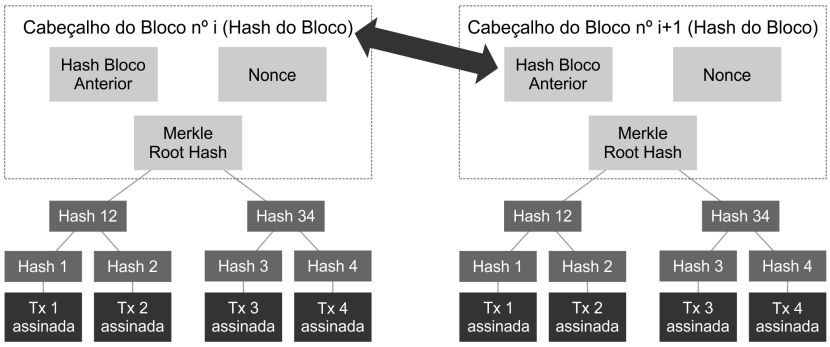

Fig. 1 – Transações em Bitcoin, adaptado de [42]

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

74. 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* [44], *Proof of Authority* [45]. 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) [46] e *Hashgraph* [47]. Tudo depende de como uma aplicação em uma rede deve ser executada.

75. 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.

76. 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.

77. Não será explicado neste Parecer, mas 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.

78. Para este Parecer, 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;
v. re-assinatura.

79. Em que pese existam esforços para identificar uma pessoa por meio de uma rede *blockchain* [48], 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. Eu suma, não há identificação primária segura de pessoas em redes *blockchain* sem o apoio de outras infraestruturas de identificação.

80. 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 inerentes 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.

81. O ciclo de vida das chaves em redes *blockchain* pode ser outro problema das implementações. Sem um processo que vise dar segurança e auditabilidade as chaves criptográficas requisitadas, geradas, enviadas e armazenadas, com os devidos processos

normativos, autônomos e independentes de atuação (vide seção "ICP-Brasil" deste Parecer), não há como garantir presunção de validade às transações geradas sob um protocolo *blockchain*. Qualquer texto legal ou normativo que tente inserir essa presunção, recai nos mesmos problemas dos métodos de usuário e senha e biometria. 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.

82. São necessários processos seguros, fiscalizados e auditáveis nesse sentido. Caso não haja, não há como garantir a ligação entre uma pessoa e sua chave (manifestação de vontade) e nem que a chave de assinatura não possa ser extraviada ou duplicada.

83. 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) [49, 50], 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*.

84. Paul Kocher, no painel dos criptógrafos, da Conferência RSA em 2019, disse em relação a redes *blockchain*, transcrito de [51]:

> *" ...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."*

85. 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.

86. 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.

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

88. 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 [52, 53, 54, 55]. Uma ressalva: o protocolo HyperLedger iniciou estudos para implementação de algoritmos, em teoria, resistentes a ataques quânticos [56].

89. A não garantia que tais curvas são seguras, geram a uma incerteza sobre as assinaturas. Ora, não há o que se falar em presunção de validade das transações em redes *blockchain* que, além de não preservarem o ciclo de vida das chaves, usam algoritmos suspeitos.

90. Uma parte importante é que redes *blockchain*, por si só, não endereçam garantia de temporalidade, mas somente de ordenamento das transações. 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/mundias deve ser usada.

91. Outro ponto é 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 autentico dentro de um sistema específico, o que é um erro.

92. Uma questão com a segurança do processo envolve o fato dos protocolos conhecidos não permitirem re-assinatura do ativo digital registrado. Isso significa que toda a segurança do processo, em relação a integridade dos dados, estará relacionada à função *hash* utilizada [57]. É importante notar que existem avanços em relação a quebra dos algoritmos criptográficos usados nos protocolos *blockchain* [58, 59, 60, 61]. Em documentos que necessitam sua validação a longo prazo (20, 25, 30 anos), é possível confiar na segurança do processo nas funções *hash* atualmente utilizadas? Ao longo dos anos, funções *hash* foram quebradas e colisões achadas em operações de tempo polinomial factíveis de serem implementadas [62, 63]. É fundamental que os documentos eletrônicos nessas redes sejam autocontidos, podendo ser reassinados.

93. 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 sejam feitas 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?

94. O ITI, estudando e melhorando as mais modernas implementações de governos [5, 64, 65], 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 às redes *blockchain*.

95. Portanto, a garantia de autoria, integridade, autenticidade e não repúdio de documentos eletrônicos assinados devem ter no mínimo as características impostas às chaves e processos da ICP-Brasil. Não há outro caminho ou alternativa. Os documentos que se inserem dentro de uma rede *blockchain* devem ser autênticos e íntegros, se não, haverá um documento possivelmente imutável, entretanto, fraudado dentro da rede.

Respostas ao Ofício nº 1.282/2019 – COTEC/SUCOR/RFB

a) o Decreto nº3.996, de 2001, informa em seu art. 2º §1º, que os serviços de certificação digital na Administração Pública Federal devem ser providos pela ICP-Brasil. Com base nesse disposto, é correto o entendimento de que os serviços digitais de governo na internet devem utilizar, exclusivamente, certificados ICP-Brasil?

96. A resposta será dada no Parecer Jurídico da douta Procuradoria Especializada do ITI.

b) O Decreto nº 8.539, de 2015, informa em seu art. 6º, § 1º, que não se obsta a utilização de outro meio de comprovação de autoria e integridade de documentos em forma eletrônica, inclusive os que utilizem identificação por meio de usuário e senha. Com base nesse dispositivo, é correto o entendimento de que os serviços digitais de governo na internet podem utilizar certificados fora da Infraestrutura da ICP-Brasil?

97. A resposta será dada no Parecer Jurídico da douta Procuradoria Especializada do ITI.

98. Ressalta-se que, conforme exposto neste Parecer (vide subseção "Usuário e Senha"), não há como, por si só, estabelecer garantias de autoria e muito menos de integridade a documentos em forma eletrônica por meio do uso de usuário e senha. Os documentos eletrônicos requerem tratamentos especiais para garantia de tais atributos. Além da insegurança na forma, o § 1º, do artigo 6º, decreto nº 8.539, de 2015 é uma anomalia, sem qualquer respaldo do ponto de vista técnico, além de expor os documentos e usuários a ataques e vazamentos de dados.

99. A utilização de certificados fora da ICP-Brasil, ou sem os requisitos mínimos técnicos e procedimentais, transgride, fortemente, a segurança de qualquer aplicação (vide a seção "ICP-Brasil"). Por isso, diversos países no mundo fazem a distinção de instrumentos e procedimentos comuns de assinatura eletrônica, para os efeitos legais e de procedimentos (e, também, como e em que usar) de uma assinatura digital (ou assinatura eletrônica avançada, segura, qualificada). A má implementação de sistemas criptográficos, usando qualquer primitiva, conforme mostrado neste Parecer (vide subseção "*Blockchain*"), também causa problemas irreversíveis quanto a segurança de uma assinatura digital e de qualquer documento eletrônico.

c) A MP 2.200-2, de 2001, regula em seu art. 10, §2º, que não se obsta a utilização de outro meio de comprovação da autoria e integridade de documentos em forma eletrônica, inclusive os que utilizem certificados não emitidos pela ICP-Brasil, desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento. Com base nesse dispositivo, é correto afirmar que o disposto no art. 6º, §1º, do Decreto 8.539, de 2015, depende de prévia manifestação de concordância entre as partes para utilização de certificados fora da ICP-Brasil?

100. A resposta será dada no Parecer Jurídico da douta Procuradoria Especializada do ITI.

101. Repisa-se que a lei brasileira se coaduna com o que a maioria dos países versam em termos de aceitar uma assinatura eletrônica comum, desde que acordado e consensualizado entre as partes, e a presunção de validade das assinaturas digitais usando a plataforma da ICP-Brasil (vide seção "Comparação descritiva entre a assinatura digital no

Brasil e as legislações ao redor mundo”). Conforme demonstrado ao longo deste Parecer, é imprescindível que requisitos mínimos sejam estabelecidos para a devida presunção de autoria e integridade aos documentos eletrônicos. É fundamental a segurança, rastreabilidade e confidencialidade que a ICP-Brasil (vide seção “ICP-Brasil”) pode prover aos dados eletrônicos, a luz da Constituição Brasileira, como direito ao sigilo fiscal, bancário e telemático, e de marcos legais como a Lei Geral de Proteção de Dados – LGPD. Outras formas, não garantem, por si só, a segurança desses dados. A ICP-Brasil é a plataforma oficial do Estado Brasileiro para assinatura (manifestação de vontade) em documentos eletrônicos.

d) Se o Gov.br enviar as credenciais do usuário autenticado, para os serviços digitais de governo que o utilize, mediante assinatura com a ICP-Brasil, a garantia de autenticidade e não repudio (art. 10, §1º da MP 2.200-2, de 2001) restringe-se a comunicação entre o Gov.br e o serviço digital, ou abrange, inclusive, a autenticação do usuário realizada pelo Gov.br, independente do certificado digital utilizado para comunicação com o cidadão?

101. Restringe-se somente a comunicação entre o Gov.br para os serviços digitais, se utilizado um certificado digital ICP-Brasil. Caso não seja utilizado um certificado ICP-Brasil, conforme explicado neste Parecer, não há garantia nem na comunicação entre Gov.br e os serviços digitais.

102. Não abrange a autenticação realizada pelo usuário no portal Gov.br. Essa, se feita com dispositivos inseguros, não atesta, por si só, do ponto de vista técnico, qualquer garantia de autoria, integridade de dados, autenticidade e, por tanto, não há o que se falar em não-repúdio. Ao contrário, sistemas baseados dispositivos inseguros (e.g., usuário e senha), e que também amplia erroneamente esse método para assinatura eletrônica ou preservação dos dados na forma eletrônica, imputa a todos os dados o repúdio e as vulnerabilidades quanto aos possíveis vazamentos ou comprometimento da informação.

e) Se a resposta do item “d” for de que abrange a autenticação do usuário, é correto o entendimento de que com base no disposto no art. 6º, §1º, do Decreto 8.539, de 2015, há comprovação de autoria e integridade para logins realizados por meio de usuário e senha no âmbito do Gov.br?

103. Conforme explicado neste Parecer, o §1º, no art. 6º do Decreto 8.539, de 2015, é uma aberração do ponto de vista técnico. Não há como, por si só, comprovar autoria e muito menos integridade de dados para *logins* realizados por usuário e senha. Trata-se de um comando normativo sem qualquer respaldo técnico.

104. A autenticação (simples) por usuário e senha, por ser um segredo compartilhado e vulnerável, pode ser amplamente repudiada. A insegurança desse tipo de método e os ataques que podem ser realizados possuem ampla publicidade e literatura

técnica. Mais obscuro é a letra sem sentido do decreto quando versa que esse método garante, por si só, integridade dos dados. Não há como um processo de assinatura eletrônica simples garantir, por si só, integridade dos dados anexando, sem qualquer esforço matemático/computacional, o usuário e senha de um cidadão. A insegurança técnica desses sistemas quando ampliados seu escopo a realizarem algo que não é possível, como comprovação de autoria e integridade a um documento eletrônico, além dos nefastos problemas de ordem de vazamento e manipulação de dados, podem trazer efeitos irreparáveis a população (vide subseção "Usuário e Senha").

105. Outro problema grave desse tipo de método é sua verificação/interoperabilidade. O documento não é autocontido. Obrigatoriamente para que possivelmente se verifique a autenticidade somente do usuário e senha anexado ao documento eletrônico, é necessário que o sistema que o criou esteja funcional. Sem o sistema, essa possível autenticidade do usuário e senha não pode ser checada por outros meios.

106. Como os documentos, atos e transações eletrônicos "assinados" eletronicamente por usuário e senha (ou outros métodos de assinatura eletrônica não segura) não são autocontidos, é necessário, em caso de litígio (por qualquer razão/repúdio de uma parte), a verificação do sistema pela busca da verdade pericial. Essa perícia tentará descobrir outros indícios sobre a contenda, que não podem ser atestados somente pelo documento eletrônico. Entretanto, necessariamente significa dizer que o sistema poderá, a luz dos processos judiciários brasileiros, ser periciado pelas partes. Peritos oficiais e contratados pelas partes podem requerer ou obter acesso aos sistemas de dados para tentar achar indícios que tenha alguma eficácia probatória. Implica, em muitos casos, como provavelmente são os serviços, e.g., da Receita Federal do Brasil, em abrir sistemas sensíveis a perícias/verificações externas. Isso pode trazer graves consequências e riscos aos serviços digitais da administração pública.

Brasília, 16 de setembro de 2019

EDUARDO MAGALHAES DE LACERDA FILHO

Assinado de forma digital por EDUARDO MAGALHAES DE LACERDA FILHO
Dados: 2019.09.16 14:57:07 -03'00'

EDUARDO MAGALHÃES DE LACERDA FILHO

Diretor de Infraestrutura de Chaves Públicas

Instituto Nacional de Tecnologia da Informação

Referências

[1] *Electronic Signatures in Global and National Commerce Act* (eSIGN) (2000), disponibilizado em https://www.govinfo.gov/content/pkg/PLAW-106publ229/pdf/PLAW-106publ229.pdf. (visto em 28/08/2019).

[2] *Uniform Electronic Transactions Act* (UETA) (1999), disponibilizado em http://euro.ecom.cmu.edu/program/law/08-732/Transactions/ueta.pdf. (visto em 28/08/2019).

[3] *Personal Information Protection and Electronic Documents Act* (PIPEDA) (2000 – last amended on April, 2019), disponibilizado em https://laws-lois.justice.gc.ca/PDF/P-8.6.pdf. (visto em 28/08/2019).

[4] Menezes, A. J., Vanstone, S. A., and Oorschot, P. C. V., *Handbook of Applied Cryptography*. CRC Press, Inc., Boca Raton, FL, USA, 1st edition, 1996.

[5] Lacerda Filho, E. M., *The second era of the internet, digital signature infrastructures and trusted entities KSI, PKI and Permissioned Blockchain*. Cryptoid. Internet, 2018.

[6] American National Standard for Information Systems, ANSI/NIST-ITL 1-2011 Update:2015, *Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information*, National Institute of Standards and Technology Special Publication 500-290e3, 2015.

[7] Mason, S., *World electronic signature legislation. Digital Evidence and Electronic Signature Law Review*. 15. 10.14296/deeslr.v15i0.4917, 2018

[8] *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 04/09/2019).

[9] *REGULAMENTO (UE) N. o 910/2014 DO PARLAMENTO EUROPEU E DO CONSELHO de 23 de julho de 2014 relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno e que revoga a Diretiva 1999/93/CE*, disponibilizado em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32014R0910&from=PT. (visto em 28/08/2019).

[10] *Secure Electronic Signature Regulations*, SOR/2005-30 (2005 – last amended on April, 2011), disponibilizado em https://laws-lois.justice.gc.ca/PDF/SOR-2005-30.pdf (visto em 28/08/2019).

[11] *Ley Sobre Documentos Electronicos, Firma Electronica y Servicios de Certificacion de Dicha Firma*, disponibilizado em https://www.leychile.cl/Navegar?idNorma=196640&buscar=19.799. (visto em 28/08/2019).

[12] *Case nº 16-22134-D-7*, United States Bankruptcy Court, Eastern District of California, Date: July 13, 2016, disponibilizado em http://www.caeb.uscourts.gov/documents/Judges/Opinions/Local/Mayfield-ForWebsite.pdf?dt=202716160. (visto em 30/08/2019).

[13] *Commercial National Security Algorithm Suite and Quantum Computing FAQ*, Information Assurance Directorate, National Security Agency/Central Security Service (2016), disponibilizado em https://apps.nsa.gov/iaarchive/library/ia-guidance/ia-solutions-for-classified/algorithm-guidance/cnsa-suite-and-quantum-computing-faq.cfm. (visto em 28/08/2019).

[14] *Policies*, Committee on National Security Systems (2016), disponibilizado em http://www.cnss.gov/CNSS/issuances/Policies.cfm. (visto em 28/08/2019).

[15] *Written Testimony of Todd Wilkinson*, *President and Ceo, Entrust Datacard*, Hearing on Protecting Consumers in the Era of Major Data Breaches, Before the U.S. Senate Committee on Commerce, Science, and Transportation, November 8, 2017.

[16] *Republic of Korea Digital Signature Act* (2009), disponibilizado em http://moleg.go.kr/english/korLawEng?pstSeq=52667. (visto em 02/09/2019).

[17] Adobe Systems Incorporated. *Global Guide to Electronic Signature Law: Country by country summaries of law and enforceability*, 2017, disponibilizado em https://acrobat.adobe.com/content/dam/doc-cloud/en/pdfs/document-cloud-global-guide-electronic-signature-law-ue.pdf. (visto em 02/09/2019).

[18] Instituto Nacional de Tecnologia da Informação, *Documentos Principais*, 2019, disponibilizado em https://www.iti.gov.br/legislacao/61-legislacao/504-documentos-principais. (visto em 02/09/2019).

[19] 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.

[20] Lenstra, A. K. and Verheul, E. R. *Selecting Cryptographic Key Sizes,* in Public Key Cryptography. Third International Workshop on Practice and Theory in PublicKey

Cryptosystems, PKC, 2000 (Ed. H. Imai and Y. Zheng). Berlin: Springer-Verlag, 446-465, 2000.

[21] Kleinjung, T., Aoki, K., Jens Franke, Lenstra, A. K., Thomé, E., Bos, J. W., Gaudry, P., Kruppa A., Montgomery, P. L., Osvik, D. A., Riele H. T., Timofeev A., and Zimmermann, P., *Factorization of a 768-bit RSA modulus*. In Proceedings of the 30th annual conference on Advances in cryptology (CRYPTO'10), Tal Rabin (Ed.). Springer-Verlag, Berlin, Heidelberg, 333-350, 2010.

[22] Kaliski B., *RSA factoring challenge*. In: van Tilborg H.C.A. (eds) Encyclopedia of Cryptography and Security. Springer, Boston, MA, 2005.

[23] Rotman, J., *A First Course in Abstract Algebra: With Applications*. Pearson Prentice Hall, 2006.

[24] Cormen, T. H., Leiserson, C. E., Rivest, R. L., and Stein, C., *Introduction to Algorithms*, Second Edition. MIT Press and McGraw-Hill. ISBN 0-262-03293-7. Pages 859–861 of section 31.2: Greatest common divisor, 2001.

[25] 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.

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

[27] 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.

[28] 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.

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

[30] *Lei nº 13.709*, de 14 de agosto de 2018, Lei Geral de Proteção de Dados (LGPD), disponibilizada em http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. (visto em 02/09/2019).

[31] *Regulation (eu) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*, disponibilizada em https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en. (visto em 02/09/2019).

[32] *Mandado de Segurança nº 2007.72.00.002903-9/SC*, disponibilizado em https://www2.trf4.jus.br/trf4/processos/visualizar_documento_gedpro.php?local=jfsc&documento=1344975&DocComposto=&Sequencia=&hash=059f973f55f7fe5aea6e8eb8899252d2. (visto em 03/09/2019).

[33] *Pwned websites*, disponibilizado em https://haveibeenpwned.com/PwnedWebsites#Adobe. (visto em 03/09/2019).

[34] Bošnjak, L., Sreš J., and Brumen B., *Brute-force and dictionary attack on hashed real-world passwords*, 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, 2018, pp. 1161-1166. doi: 10.23919/MIPRO.2018.8400211, 2018.

[35] Bernstein, D. J., Hülsing, A., Lange, T., Niederhagen, R., *Bad Directions in Cryptographic Hash Functions*. In: Foo E., Stebila D. (eds) Information Security and Privacy. ACISP 2015. Lecture Notes in Computer Science, vol 9144. Springer, Cham, 2015.

[36] Garcia, A. P., *Curso de Direito da Certificação Digital*. Brasília: Ed. do Autor, 2016.

[37] Tung, L., *Microsoft: Here's why we're declaring end of password era*, 2018, disponibilizado em https://www.zdnet.com/article/microsoft-heres-why-were-declaring-end-of-password-era/. (visto em 02/09/2019).

[38] Hern, A., *Google aims to kill passwords by the end of this year*, 2016, disponibilizado em https://www.theguardian.com/technology/2016/may/24/google-passwords-android. (visto em 03/09/2019).

[39] *Commission Implementing Decision (EU) 2019/329 of 25 February 2019 laying down the specifications for the quality, resolution and use of fingerprints and facial image for biometric verification and identification in the Entry/Exit System (EES)*, disponbilizado em https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019D0329&from=EN. (visto em 03/09/2019).

[40] NIST Special Publication 800-76-2, *Biometric Specifications for Personal Identity Verification*, Grother, P., Salamon, W., Chandramouli, R., 2013.

[41] *Aadhaar Data Of 6.7 Mn LPG Brand Indane Users Leaked, Reveals French Cybersecurity Expert*, disponibilizado em https://inc42.com/buzz/aadhaar-data-of-6-7-mn-lpg-brand-indane-users-leaked-reveals-french-cybersecurity-expert/. (visto 05/09/2019).

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

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

[44] C. T. Nguyen, D. T. Hoang, D. N. Nguyen, D. Niyato, H. T. Nguyen and E. Dutkiewicz, *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.

[45] 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.

[46] 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.

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

[48] *Sovrin Foundation*, disponibilizado em https://sovrin.org/. (visto em 03/09/2019).

[49] *Ethercombing: Finding Secrets in Popular Places* disponibilizado em https://www.securityevaluators.com/casestudies/ethercombing/. (visto em 05/09/2019).

[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 05/09/2019).

[51] *The Cryptographers' Panel*, RSA Conference USA 2019, disponibilizado em https://www.rsaconference.com/industry-topics/presentation/the-cryptographers-panel. (visto em 03/09/2019).

[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 02/09/2019).

[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 02/09/2019).

[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] FIPS Pub. 180-4, *Secure Hash Standard (SHS)*, Mar. 2015, National Institute of Standards and Technology. Federal Information Processing Standards Publication. https://doi.org/http://dx.doi.org/10.6028/NIST. FIPS.180-4.

[58] Grover, L. K., *A fast quantum mechanical algorithm for database search*. In ANNUAL ACM SYMPOSIUM ON THEORY OF COMPUTING, pages 212–219. ACM, 1996.

[59] 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.

[60] Bernstein, D. J., Buchmann, J., and Dahmen, E., *Post Quantum Cryptography*. Springer Publishing Company, Incorporated, 1st edition, 2009.

[61] *Post-Quantum Cryptography Standardization*, NIST, Computer Security Resource Center, disponibilizado em https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post-Quantum-Cryptography-Standardization. (visto em 04/09/2019).

[62] Wang, X., and Yu, H., *How to break MD5 and other hash functions,* In Proceedings of the 24th annual international conference on Theory and Applications of Cryptographic Techniques (EUROCRYPT'05), Ronald Cramer (Ed.). Springer-Verlag, Berlin, Heidelberg, 19-35. DOI=http://dx.doi.org/10.1007/11426639_2, 2005.

[63] Stevens, M., Karpman, P., and Peyrin, T., *Freestart Collision for Full SHA-1*. In Proceedings, Part I, of the 35th Annual International Conference on Advances in Cryptology --- EUROCRYPT 2016 - Volume 9665, Marc Fischlin and Jean-Sébastien

Coron (Eds.), Vol. 9665. Springer-Verlag, Berlin, Heidelberg, 459-483. DOI: https://doi.org/10.1007/978-3-662-49890-3_18, 2016.

[64] 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.

[65] 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 03/09/2019).