Pagamentos Instantâneos

Especificações técnicas e de negócio do ecossistema de pagamentos instantâneos brasileiro

Anexo IV – Manual de Segurança

Versão 2.0

BANCO CENTRAL DO BRASIL

SUMÁRIO

Histórico de revisão

Data	Versão	Descrição das alterações
16/01/2020	1.0	Versão inicial.
24/03/2020	2.0	- Alteração do nome do Ecossistema de Pagamentos Instantâneos para PIX; - Atualização e inclusão de referências; - Alteração da seção 1.2 e subseções para incluir o processo de assinatura digital no DICT; - Detalhamento dos processos de ativação e desativação de certificados digitais do BC e dos PSPs (seções 1.3.2 a 1.3.4) - Inclusão da seção 1.3.5: Verificação da revogação de certificados digitais; - Inclusão da seção 1.4: Segurança de *QR Codes* dinâmicos.

Apresentação

Este anexo descreve os principais requisitos técnicos de segurança do ecossistema de pagamentos instantâneos (PIX), e tem como objetivo descrever como deve ser implementada a criptografia da comunicação, a autenticação, os processos de assinatura digital e de gestão dos certificados digitais utilizados no ecossistema, bem como os aspectos de segurança associados à iniciação de pagamentos por *QR Codes* dinâmicos.

Termos de Uso

Estas especificações fazem parte de um trabalho em desenvolvimento, e novos conceitos e definições serão abordados em versões futuras deste documento. Dessa maneira, nenhuma informação aqui apresentada deve ser considerada final ou apropriada para qualquer propósito específico.

Referências

Estas especificações baseiam-se, referenciam, e complementam onde aplicável, os seguintes documentos:

Referência	Origem
Especificações técnicas e de negócio do ecossistema de pagamentos instantâneos brasileiro	https://www.bcb.gov.br/estabilidadefinanceira/forumpagamentosinstantaneos - última versão disponível consta na seção à direita.
Manual de Segurança do SFN	https://www.bcb.gov.br/estabilidadefinanceira/comunicacaodados - última versão disponível consta na seção "Segurança".
Manual de Redes do SFN	https://www.bcb.gov.br/estabilidadefinanceira/comunicacaodados - última versão disponível consta na seção "Redes".
Catálogo de Mensagens do SPI	https://www.bcb.gov.br/estabilidadefinanceira/forumpagamentosinstantaneos - última versão disponível consta na seção à direita.
Padrões para Iniciação do PIX	https://www.bcb.gov.br/estabilidadefinanceira/forumpagamentosinstantaneos - última versão disponível consta na seção à direita.
ISO 20.022	https://www.iso20022.org/
XML Signature Syntax and Processing (Second Edition)	https://www.w3.org/TR/2008/REC-xmldsig-core-20080610/
ICP-Brasil	https://www.iti.gov.br/icp-brasil
Sistema de Transferência de Arquivos do Banco Central (STA)	https://sta.bcb.gov.br
Aplicação BC Correio	https://bccorreio.bcb.gov.br/bccorreio/
Padrão de assinatura digital *JSON Web Signature (JWS) – RFC* 7515	https://tools.ietf.org/html/rfc7515
DNS CAA (Certification Authority Authorization) – RFC 6844	https://tools.ietf.org/html/rfc6844
Padrão *Base64url – RFC* 4648	https://tools.ietf.org/html/rfc4648#section-5
JSON Web Key – RFC 7517	https://tools.ietf.org/html/rfc7517
Well-Known URIs – RFC 8615	https://tools.ietf.org/html/rfc8615
Web Host Metadata – RFC 6415	https://tools.ietf.org/html/rfc6415
Uniform Resource Locators (URL)	https://tools.ietf.org/html/rfc1738
Good Practices for Capability URLs	https://www.w3.org/TR/capability-urls/
Randomness Recommendations for Security – RFC 1750	https://tools.ietf.org/html/rfc1750

Sugestões, críticas ou pedidos de esclarecimento de dúvidas podem ser enviados ao BC por meio do e-mail pagamentosinstantaneos@bcb.gov.br.

1. Manual de segurança do ecossistema de pagamentos instantâneos brasileiro (PIX)

Introdução

Conforme descrito no documento "Especificações técnicas e de negócio do ecossistema de pagamentos instantâneos brasileiro"[1], é necessário implementar criptografia e autenticação mútua na comunicação entre os participantes e o PIX e as mensagens transmitidas no âmbito do sistema devem ser assinadas digitalmente. Em ambos os casos são utilizados certificados digitais ICP-Brasil[2] no padrão SPB. A iniciação de pagamentos, em especial quando ocorre por meio de *QR Codes* dinâmicos, também possui aspectos de segurança importantes que devem ser considerados.

Este documento apresenta os detalhes técnicos associados aos requisitos de segurança a serem adotados nas diferentes *API*s e tecnologias que compõem o PIX.

[1] Documento "Especificações técnicas e de negócio do ecossistema de pagamentos instantâneos brasileiro" – última versão disponível na seção à direita da página: https://www.bcb.gov.br/estabilidadefinanceira/forumpagamentosinstantaneos

[2] ICP-Brasil – Infraestrutura de Chaves Públicas Brasileira – mais informações disponíveis em: https://www.iti.gov.br/icp-brasil

1.1. Comunicação segura

A comunicação entre cada PSP e o PIX é realizada por meio da Rede do Sistema Financeiro Nacional (RSFN). A conexão do PSP com a RSFN deve observar as regras e padrões dispostos no Manual de Redes do SFN[3].

O PSP deve se conectar às *APIs* disponíveis no PIX exclusivamente por meio do protocolo *HTTP* versão 1.1 utilizando criptografia *TLS* versão 1.2 ou superior, com autenticação mútua obrigatória no estabelecimento da conexão. Deve ser suportada, no mínimo, a *Cipher Suite ECDHE-RSA-AES-128-GCM-SHA256 (0xc02f)*, ou seja, os seguintes algoritmos devem ser utilizados:

Fase/Função	Algoritmo
Troca de chaves	*ECDHE (Elliptic Curve Diffie Hellman Ephemeral)*
Autenticação	*RSA*
Criptografia simétrica	*AES* com chaves de 128 *bits* utilizando o modo *GCM*
MAC (Message Authentication Code)	*SHA* com chaves de 256 *bits*

Tabela 1: Algoritmos utilizados na criptografia TLS.

Tanto o servidor (Banco Central) como o cliente (PSP) devem utilizar certificados ICP-Brasil no padrão SPB. Mais informações sobre certificados constam na seção 1.3 deste documento.

Os clientes *HTTP* do PSP devem sempre respeitar o *TTL* (*Time To Live*) dos servidores *DNS*. A falha em respeitar o *TTL* pode causar indisponibilidade no acesso às *APIs* do PIX.

[3] Manual de Redes do SFN – última versão disponível na seção "Redes" da página: https://www.bcb.gov.br/estabilidadefinanceira/comunicacaodados.

1.2. Assinatura digital

No intuito de garantir a integridade e o não repúdio das transações no âmbito do PIX, todas as mensagens trafegadas no Sistema de Pagamentos Instantâneos (SPI)[4] devem ser assinadas digitalmente pelo emissor. No caso do Diretório de Identificadores de Contas Transacionais (DICT)[5], apenas as requisições de consulta (*GET*) não precisam ser assinadas, enquanto todas as demais requerem assinatura. Seja qual for a operação realizada, tanto no SPI como no DICT, a resposta do BC para o PSP é sempre assinada.

O padrão de assinatura digital a ser utilizado no PIX é o *XMLDSig*[6]. No SPI, as mensagens seguem o padrão *ISO* 20.022[7], portanto a assinatura digital deve constar no elemento <*Sgntr*> do *Business Application Header (BAH)*[8], conforme descrito no Catálogo de Mensagens do SPI[9]. No DICT, por sua vez, as requisições e respostas não são realizadas por meio de mensagens *ISO 20.022*, então o cabeçalho (*BAH*) não existe. Nesse caso, a assinatura (elemento <*Signature*>) deve constar na raiz do *XML*.

A tabela abaixo mostra os elementos/*tags* que devem compor a assinatura digital:

#	Elemento/*tag*	Descrição
1	<*Signature*>	Elemento raiz da assinatura *XMLDSig*, onde se define o *namespace*, que aponta para a *URI* do esquema *XML* (*XML Schema Definition – XSD*) a ser utilizado para a assinatura digital. Inclui todos os elementos descritos nas demais linhas desta tabela. No PIX, é utilizado *XMLDSig*: http://www.w3.org/2000/09/xmldsig#
1.1	<*SignedInfo*>	Contém as principais informações necessárias para a assinatura, e inclui as *tags* <*CanonicalizationMethod*>, <*SignatureMethod*> e *tags* <*Reference*>, descritas abaixo.
1.1.1	<*CanonicalizationMethod*>	Especifica o algoritmo de canonicalização a ser aplicado no elemento <*SignedInfo*>, com o objetivo de gerar a forma canônica do conteúdo a partir do qual será gerado o resumo *(digest)* para posterior assinatura digital. No PIX, deve ser utilizado o

[4] Detalhes sobre o SPI constam no documento "Especificações técnicas e de negócio do ecossistema de pagamentos instantâneos brasileiro" – última versão disponível na seção à direita da página: https://www.bcb.gov.br/estabilidadefinanceira/forumpagamentosinstantaneos

[5] A API do DICT é documentada em manual específico, cuja última versão está disponível na seção à direita da página: https://www.bcb.gov.br/estabilidadefinanceira/forumpagamentosinstantaneos.

[6] *W3C Recommendation – XML Signature Syntax and Processing (Second Edition)*, disponível em: https://www.w3.org/TR/2008/REC-xmldsig-core-20080610/

[7] Padrão *ISO* 20.022 – mais informações disponíveis em: https://www.iso20022.org/

[8] Mais detalhes sobre o *BAH* podem ser obtidos na página da ISO 20.022 (ver referência anterior).

[9] Catálogo de Mensagens do SPI – última versão disponível na seção à direita da página: https://www.bcb.gov.br/estabilidadefinanceira/forumpagamentosinstantaneos.

		algoritmo de canonicalização *XML* exclusiva: http://www.w3.org/2001/10/xml-exc-c14n#.
1.1.2	*<SignatureMethod>*	Define o algoritmo utilizado para geração e validação da assinatura digital. No PIX, utiliza-se *RSA-SHA256*: http://www.w3.org/2001/04/xmldsig-more#rsa-sha256.
1.1.3	*<Reference>*	Elemento que referencia o conteúdo a ser assinado, e inclui as *tags* *<Transforms>*, *<DigestMethod>* e *<DigestValue>*. A utilização do elemento *<Reference>* é detalhada na seção 1.2.1 a seguir.
1.1.3.1	*<Transforms>*	Inclui uma ou mais *tags* *<Transform>*, que indicam que transformações devem ser aplicadas, sempre em sequência, no conteúdo a partir do qual será gerado o resumo (*digest*). As transformações realizadas constam nas tabelas 3 e 4 da seção 1.2.1.
1.1.3.2	*<DigestMethod>*	Identifica qual algoritmo de *digest* será aplicado ao conteúdo a ser assinado. No PIX, utiliza-se *SHA-256*: http://www.w3.org/2001/04/xmlenc#sha256.
1.1.3.3	*<DigestValue>*	Elemento que contém o resumo (*digest*) codificado em *base64*.
1.2	*<KeyInfo>*	Elemento que contém os dados do certificado utilizado para assinar digitalmente o conteúdo. Inclui a *tag* *<X509Data>*, explicada abaixo.
1.2.3	*<X509Data>*	Contém os dados do certificado *X509* utilizado pelo assinador. Inclui a *tag* *<X509IssuerSerial>,* descrita abaixo.
1.2.3.1	*<X509IssuerSerial>*	Contém as *tags* *<X509IssuerName>* e *<X509SerialNumber>*, descritas abaixo.
1.2.3.1.1	*<X509IssuerName>*	Contém o nome (*Distinguished Name – DN*) da AC que gerou o certificado utilizado para assinatura digital.
1.2.3.1.2	*<X509SerialNumber>*	Contém o número de série do certificado utilizado para assinatura digital.
1.3	*<SignatureValue>*	Elemento que contém a assinatura digital propriamente dita, codificada em *base64*.

Tabela 2: Elementos que compõem a assinatura digital no PIX.

1.2.1.Informações a serem assinadas

No SPI, as informações a serem assinadas são:

- Mensagem *ISO 20.022* (elemento *<Document>*);
- Cabeçalho – *BAH* (elemento *<AppHdr>*);
- Elemento *<KeyInfo>*.

Portanto, no SPI são utilizados 3 elementos *<Reference>*, como mostra a tabela 3:

Tag	Conteúdo referenciado	Transformações a serem realizadas
<Reference URI="<unique-id-to-KeyInfo>	*<KeyInfo Id="unique-id-to-KeyInfo">* *(.....)* *</KeyInfo>*	Canonicalização *XML* Exclusiva: http://www.w3.org/2001/10/xml-exc-c14n#
<Reference URI ="">	*BAH* (excluindo os elementos da assinatura digital)*:* *<AppHdr>* *(.....)* *</AppHdr>*	*XMLDSig Enveloped Signature*: http://www.w3.org/2000/09/xmldsig#enveloped-signature e Canonicalização *XML* Exclusiva: http://www.w3.org/2001/10/xml-exc-c14n#
<Reference>	*<Document>* *(.....)* *</Document>*	Canonicalização XML Exclusiva: http://www.w3.org/2001/10/xml-exc-c14n#

Tabela 3: Elementos <Reference> utilizados no SPI, bem como as transformações realizadas.

Observação: no SPI, a tag <Reference>, sem o atributo URI, deve ser interpretada pela aplicação de forma a referenciar a mensagem ISO 20.022 propriamente dita (elemento <Document>).

Já no caso do DICT, é necessário assinar o conteúdo do elemento raiz do *XML* e do *<KeyInfo>*, o que resulta na utilização de apenas 2 *tags <Reference>*, conforme mostrado na tabela abaixo:

Tag	Conteúdo referenciado	Transformações a serem realizadas
<Reference URI="<unique-id-to-KeyInfo>	*<KeyInfo Id="unique-id-to-KeyInfo">* *(.....)* *</KeyInfo>*	Canonicalização *XML* Exclusiva: http://www.w3.org/2001/10/xml-exc-c14n#
<Reference URI ="">	*<Elemento-raiz-do-XML>* *(.....)* *</Elemento-raiz-do-XML>*	*XMLDSig Enveloped Signature*: http://www.w3.org/2000/09/xmldsig#enveloped-signature e Canonicalização *XML* Exclusiva: http://www.w3.org/2001/10/xml-exc-c14n#

Tabela 4: Elementos <Reference> utilizados no DICT, bem como as transformações realizadas.

Observação: ressalta-se que, no caso do DICT, a tag <Reference URI =""> aponta para a raiz do XML, diferentemente do que ocorre no SPI.

1.2.2.Processo de assinatura digital

No SPI, o processo de assinatura digital das mensagens inclui os passos abaixo:

1. Obter a mensagem completa a ser assinada;
2. Construir o elemento *<KeyInfo>*, incluindo as informações sobre o certificado digital utilizado na assinatura, conforme item 1.2 e subitens da tabela 2;
3. Extrair *BAH* (*tag <AppHdr>*);
4. Extrair mensagem *ISO 20.022* (*tag <Document>*);
5. No elemento *<SignedInfo>*, definir o algoritmo de canonicalização e de assinatura digital a serem utilizados, conforme itens 1.1.1 e 1.1.2 da tabela 2;
6. Criar os elementos *<Reference>*, incluindo as *tags <Transforms>* e *<Transform>* conforme tabela 3 e item 1.1.3 e subitens da tabela 2;

7. Efetuar as transformações nos conteúdos, conforme tabela 3;
8. Gerar os *digests* para os conteúdos referenciados nos itens acima, incluindo-os nos respectivos elementos <*DigestValue*>;
9. Canonicalizar o elemento <*SignedInfo*> e assiná-lo digitalmente conforme algoritmos definidos no passo 5 acima;
10. Inserir a assinatura digital gerada no passo anterior no elemento <*SignatureValue*>.

A figura a seguir ilustra o processo de assinatura no SPI:

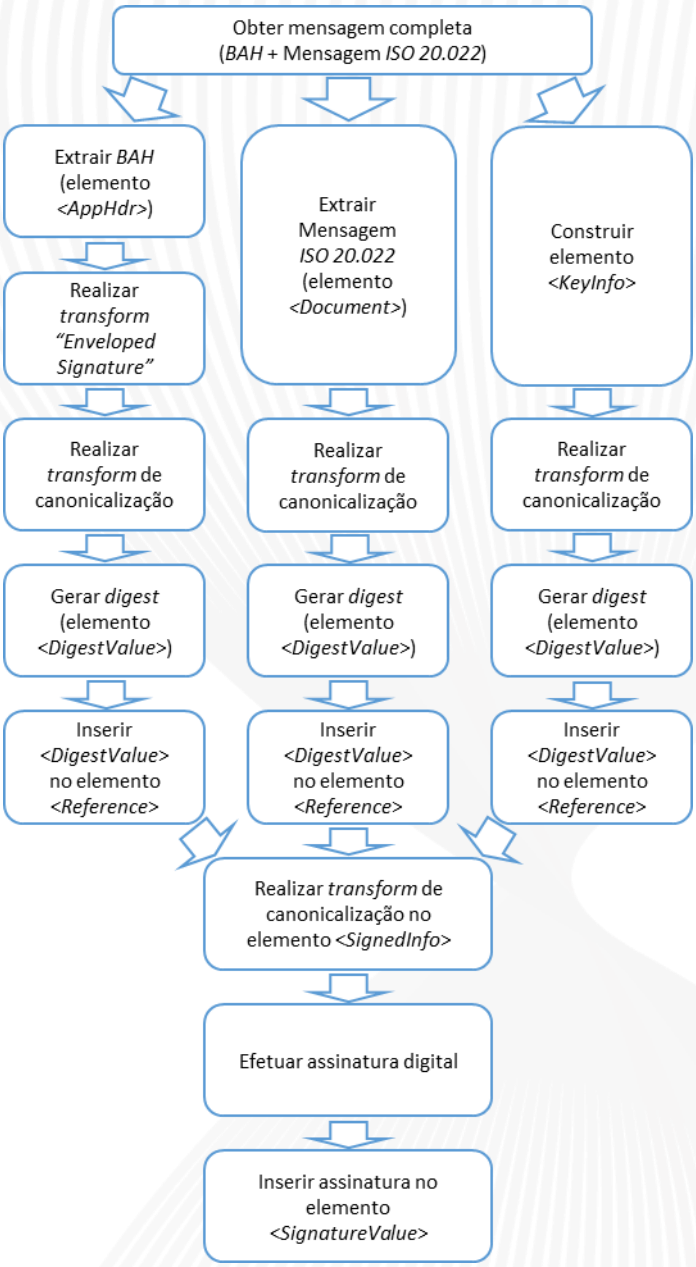

Figura 1 – Fluxo de assinatura digital da mensagem no SPI.

A seguir consta um exemplo de mensagem *pacs.008* assinada digitalmente:

```
<Envelope xmlns="pacs.008.spi.1.0.xsd">
  <AppHdr>
    (...)
    <Sgntr>
      <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
          <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
          <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
          <ds:Reference URI="#b2177f73-7685-39ac-83db-fa00ffd2b89c">
            <ds:Transforms>
              <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>

<ds:DigestValue>zqj93e6vEFVL2Pssc9nUdPweSYVxUadBaTebSuaCG0I=</ds:DigestValue>
          </ds:Reference>
          <ds:Reference URI="">
            <ds:Transforms>
              <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"/>
              <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>

<ds:DigestValue>LrZoVaudkSbJbCM8/s0QT7ejlPGNVHt0uaT/HrCoZX8=</ds:DigestValue>
          </ds:Reference>
          <ds:Reference>
            <ds:Transforms>
            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
          </ds:Transforms>
          <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>

<ds:DigestValue>xaYzMm+MbzWxgpZyRPUTa7X6mFQ6bn5EAccCtcXOOEc=</ds:DigestValue>
          </ds:Reference>
        </ds:SignedInfo>

<ds:SignatureValue>z2rH67+Rv3ofKoGkrufiUXSgLO3DxqblwuaTbR5qbyYHnVrOPB5su3wwAJoA
PNEW5Lr
Sh9pD3ECq4nrRd7UDHi9cmSalr42zKPvpwvVPZTgQkGTyvyQAFCUCnfhpj/qalU1fIfw0Ie60WTsqH
nAY/sUXn6HIBdHtJ/Vd7ZuWB8elCd09DE3MlV9gTqN7KCgEEvw+y0KvODme1SXngVKNA//udA4n
hpsUCqDQpCmNzUXDG9yWiziSL4fXE/IQ1frgoglw/IZkZ1Emc4VdNJd+q4U3HJBThHeMj1fYtucLS/
JZi+urbAIolIwpYldGgmd/sEEKe0gE9cMWryjsSVBnxg==
        </ds:SignatureValue>
        <ds:KeyInfo Id="b2177f73-7685-39ac-83db-fa00ffd2b89c">
          <ds:X509Data>
            <ds:X509IssuerSerial>
              <ds:X509IssuerName>CN=SPI - Banco Central do Brasil</ds:X509IssuerName>
                <ds:X509SerialNumber>176494203047153765 49</ds:X509SerialNumber>
              </ds:X509IssuerSerial>
            </ds:X509Data>
          </ds:KeyInfo>
        </ds:Signature>
      </Sgntr>
    </AppHdr>
  <Document>
    (...)
  </Document>
</Envelope>
```

Observação: trechos do XML não relacionados à assinatura foram cortados e estão representados com (...). Mais informações sobre o XML como um todo constam no Catálogo de Mensagens do SPI.

No DICT, por sua vez, o processo de assinatura digital inclui os passos abaixo:

1. Obter o conteúdo do elemento raiz do *XML* a ser assinado;
2. Construir o elemento <*KeyInfo*>, incluindo as informações sobre o certificado digital utilizado na assinatura, conforme item 1.2 e subitens da tabela 2;
3. No elemento <*SignedInfo*>, definir o algoritmo de canonicalização e de assinatura digital a serem utilizados, conforme itens 1.1.1 e 1.1.2 da tabela 2;
4. Criar os elementos <*Reference*>, incluindo as *tags* <*Transforms*> e <*Transform*> conforme tabela 4 e item 1.1.3 e subitens da tabela 2;
5. Efetuar as transformações nos conteúdos, conforme tabela 4;
6. Gerar os *digests* para os conteúdos referenciados nos itens acima, incluindo-os nos respectivos elementos <*DigestValue*>;
7. Canonicalizar o elemento <*SignedInfo*> e assiná-lo digitalmente conforme algoritmos definidos no passo 3 acima;
8. Inserir a assinatura digital gerada no passo anterior no elemento <*SignatureValue*>.

A figura na página a seguir ilustra o processo de assinatura no DICT:

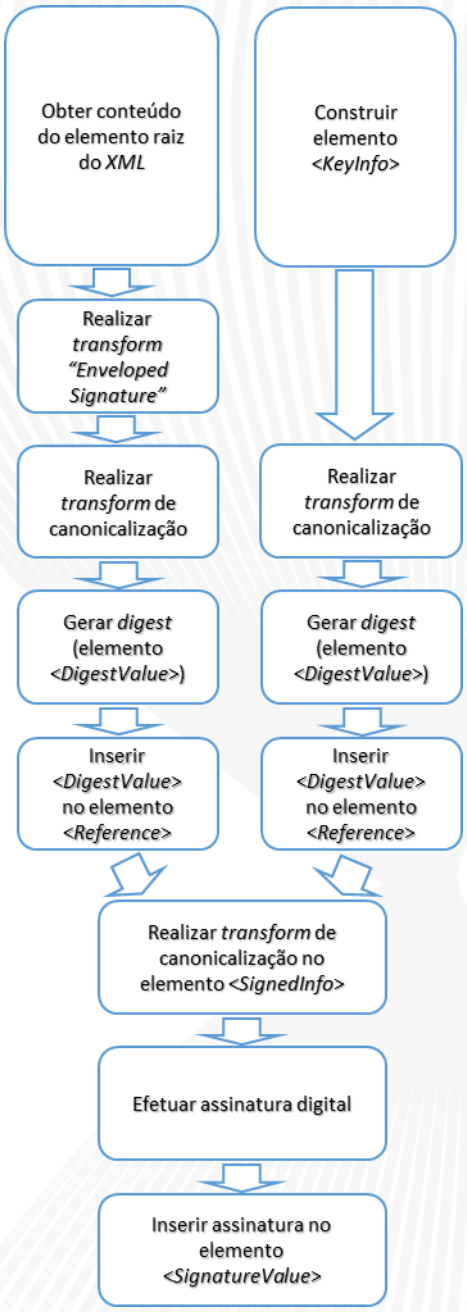

Figura 2 – Fluxo de assinatura digital no DICT.

1.2.3.Verificação da assinatura digital

No SPI, o processo de verificação da assinatura digital das mensagens inclui os passos abaixo:

1. Extrair o elemento <*KeyInfo*> da assinatura (*tag* <*Signature*>);
2. Extrair a mensagem *ISO 20.022* (*tag* <*Document*>);
3. Extrair o *BAH* (*tag* <*AppHdr*>*)* e aplicar o *transform "Enveloped Signature"*;
4. Canonicalizar o resultado dos 3 passos acima;
5. Gerar o *digest* dos 3 resultados obtidos no passo anterior;
6. Comparar os *digests* gerados com os valores dos campos <*DigestValue*> que constam nos respectivos elementos <*Reference*>;
7. Caso a verificação seja bem sucedida, proceder com os passos abaixo. Caso contrário, retornar erro.
8. Obter a assinatura digital da mensagem (elemento <*SignatureValue*>);
9. A partir das informações constantes no elemento <*KeyInfo*>, obter certificado do emissor (*);
10. Canonicalizar elemento <*SignedInfo*>;
11. Verificar a assinatura obtida no passo 8 utilizando a chave pública do certificado obtido no passo 9 acima para confirmá-la.
12. Caso a verificação seja bem sucedida, finalizar processo com status de sucesso. Caso contrário, retornar erro.

(*) Cada PSP é responsável por manter uma base atualizada com os números de série e respectivas chaves públicas dos certificados digitais do BC utilizados para assinatura digital. O BC ativará seus certificados conforme descrito na seção 1.3.3.

A figura na página a seguir ilustra o processo:

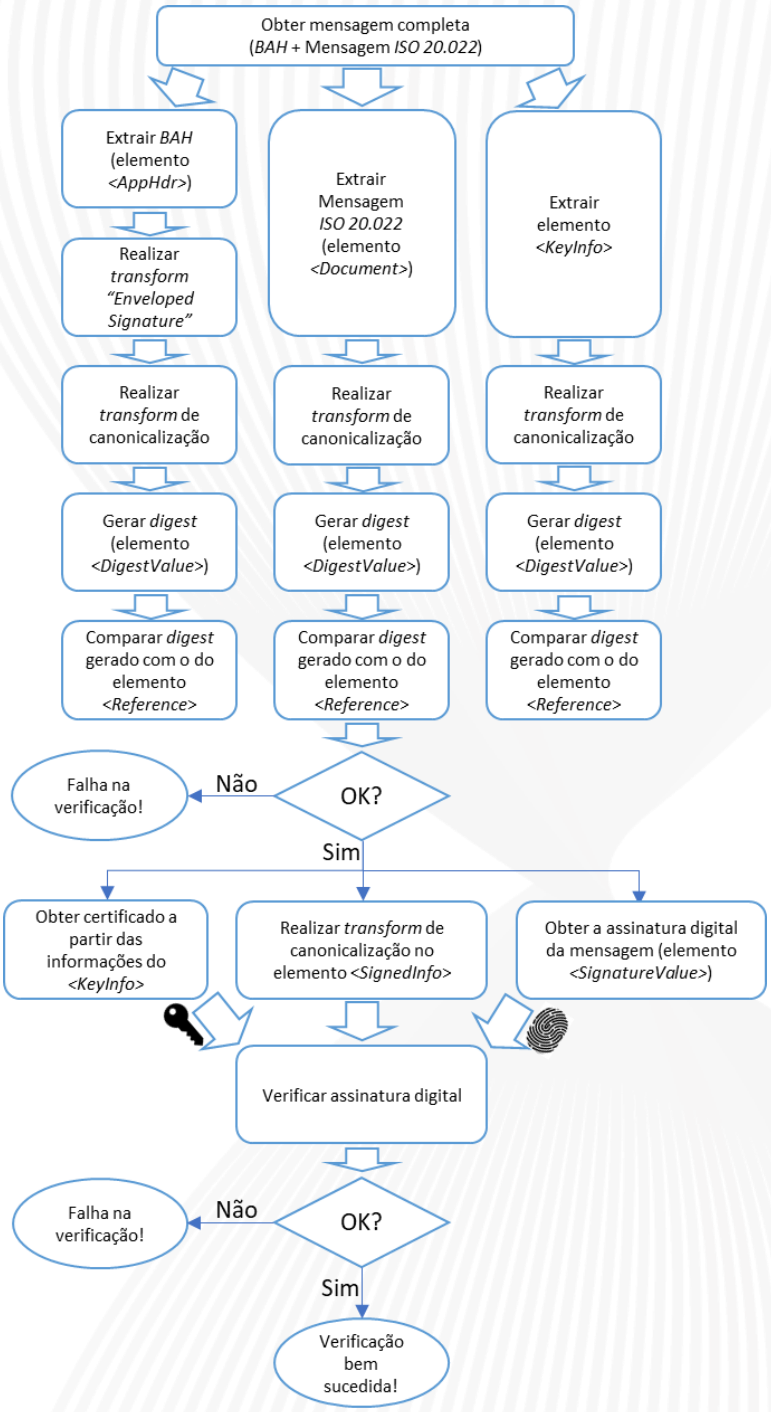

Figura 3 – Fluxo de verificação da assinatura digital da mensagem no SPI.

Já no DICT, o processo de verificação da assinatura digital consiste nos seguintes passos:

1. Obter o conteúdo do elemento raiz do *XML*;
2. Aplicar o *transform "Enveloped Signature"* no conteúdo;
3. Extrair o elemento <*KeyInfo*> da assinatura (*tag* <*Signature*>);
4. Canonicalizar o resultado dos passos 2 e 3 acima;
5. Gerar o *digest* dos 2 resultados obtidos no passo anterior;
6. Comparar os *digests* gerados com os valores dos campos <*DigestValue*> que constam nos respectivos elementos <*Reference*>;
7. Caso a verificação seja bem sucedida, proceder com os passos abaixo. Caso contrário, retornar erro.
8. Obter a assinatura digital (elemento <*SignatureValue*>);
9. A partir das informações constantes no elemento <*KeyInfo*>, obter certificado do emissor;
10. Canonicalizar elemento <*SignedInfo*>;
11. Verificar a assinatura obtida no passo 8 utilizando a chave pública do certificado obtido no passo 9 acima para confirmá-la.
12. Caso a verificação seja bem sucedida, finalizar processo com status de sucesso. Caso contrário, retornar erro.

A figura na página a seguir ilustra o processo:

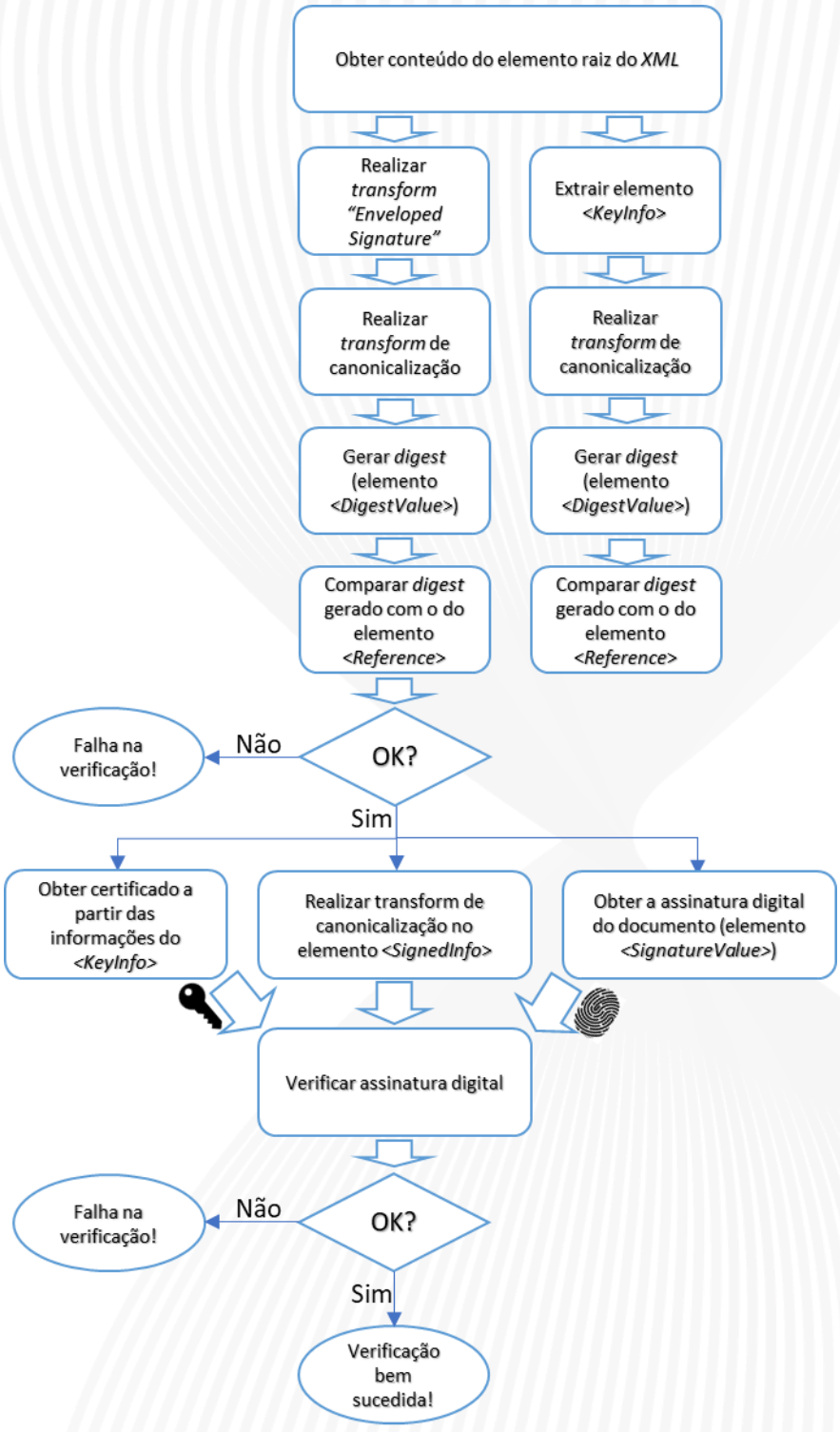

Figura 4 – Fluxo de verificação da assinatura digital no DICT.

1.3. Certificados digitais

Esta seção apresenta os detalhes a respeito dos tipos de certificados a serem utilizados e descreve o processo de ativação, desativação e de verificação da revogação de certificados.

1.3.1. Certificados digitais a serem utilizados

Tanto para autenticação e criptografia da conexão com as *APIs* do PIX como para assinatura digital das mensagens, devem ser utilizados certificados digitais ICP-Brasil no padrão SPB. As especificações para a geração desse tipo de certificado constam nas seções 4.2, 4.3 e 4.4 (subitens 4.4.1 a 4.4.5, 4.4.15 e 4.4.16) do Manual de Segurança do SFN[10]. Recomenda-se que cada instituição utilize certificados distintos, exclusivos para cada finalidade.

Nos sites que hospedam *URLs* de *QR Codes* dinâmicos gerados pelo recebedor, não será necessário que o certificado seja padrão SPB, conforme detalhado na seção 1.4 a seguir.

As instituições participantes devem possuir processos adequados de gestão (geração, guarda, ativação e revogação) dos seus certificados digitais utilizados no âmbito do PIX. Nesse contexto, recomenda-se a utilização de dispositivos de criptografia baseados em *hardware* (*HSMs*) para armazenamento das chaves privadas dos certificados.

Poderão estar ativos simultaneamente múltiplos certificados por instituição – 1 ou mais certificados para autenticação e criptografia da conexão e 1 ou mais certificados para assinatura digital. O mesmo se aplica aos certificados do BC.

1.3.2. Ativação de certificados digitais dos PSPs

Para ativar um novo certificado digital, os PSPs devem enviá-lo por meio do Sistema de Transferência de Arquivos (STA)[11], seguindo os códigos/nomes de arquivo abaixo:

Finalidade do certificado	Código do arquivo	Nome do arquivo
Autenticação da conexão	*CPIC*	*CERTPIC – Certificado Digital do PSP no SPI para conexão*
Assinatura digital	*CPIA*	*CERTPIA – Certificado Digital do PSP no SPI para assinatura*

[10] Manual de Segurança do SFN, disponível para download na seção "Segurança" da página: https://www.bcb.gov.br/estabilidadefinanceira/comunicacaodados

[11] Sistema de Transferência de Arquivos do Banco Central, disponível em: https://www.bcb.gov.br/acessoinformacao/sistematransferenciaarquivos

Após o recebimento do certificado, o BC efetua sua validação conforme padrões definidos no Manual de Segurança do SFN. Concluída a validação, o certificado será arquivado na base de dados do BC e será ativado automaticamente para utilização no PIX. Cada PSP poderá confirmar a habilitação do seu certificado no próprio registro do protocolo de envio no STA.

1.3.3.Ativação de certificados digitais do BC

A ativação de novos certificados do BC será comunicada com antecedência de, no mínimo, 7 dias, por meio de Comunicado Sisbacen. Os novos certificados serão publicados no portal da RSFN[12], juntamente com os demais certificados ativos. A ativação de novos certificados digitais por parte do BC ocorrerá conforme os processos descritos abaixo:

Certificados de assinatura digital:

- Será enviada uma mensagem específica do Catálogo de Mensagens do SPI[13] para todos os participantes contendo o novo certificado e o prazo para a sua ativação.
- Passado o prazo definido no comunicado, o BC começará a assinar mensagens com o novo certificado. A critério do BC, a transição entre o certificado anterior e o novo poderá ser escalonada, de forma que inicialmente apenas um percentual das mensagens seja assinado com o novo certificado.

Certificados de autenticação e criptografia da conexão:

Passado o prazo definido no comunicado, o BC ativará o novo certificado nos seus sites. Cada PSP deve estar preparado para aceitar mais de um certificado ativo pelo BC e deve efetuar, no mínimo, as validações abaixo:

- Certificado deve ser emitido por uma das ACs do SPB / ICP-Brasil;
- ISPB do Banco Central deve constar no *DN* (ISPB "00038166");
- CNPJ do Banco Central do Brasil deve constar no *OID* 2.16.76.1.3.3 do certificado;
- *URL* do certificado do BC deve constar no campo *SAN*, e deve corresponder à *URL* do PIX ("*.pi.rsfn.net.br");
- Certificado não pode estar expirado.

1.3.4.Desativação de certificados digitais

[12] Disponível somente para os participantes da RSFN, no endereço: http://www.rsfn.net.br
[13] Leiaute a ser definido pelo BC.

Todos os certificados – tanto do BC como dos PSPs – deverão ser automaticamente desativados às 03:00 *UTC* da sua data de expiração e, portanto, após a desativação, não deverão ser aceitos no PIX.

Caso um PSP precise desativar determinado certificado, motivadamente e com urgência, o diretor da instituição responsável pelo PIX – identificado no cadastro da instituição no ecossistema[14] – deverá enviar solicitação, com justificativa técnica, ao Departamento de Tecnologia da Informação (DEINF) do Banco Central por meio do BC Correio[15]. O referido diretor deverá constar como "transmissor" da mensagem.

Caso o BC precise desativar um de seus certificados, será enviado Comunicado Sisbacen aos participantes informando o certificado a ser desativado e a data em que ele não deverá mais ser aceito pelos participantes do ecossistema.

1.3.5.Verificação da revogação de certificados

Tanto o BC como os demais participantes do PIX deverão verificar as listas de revogação de certificados (*"Certificate Revocation Lists" – CRLs*) para confirmar que nenhum certificado utilizado no ecossistema foi revogado. Porém, considera-se tecnicamente inviável a verificação de *CRLs* de forma *online* – a cada conexão ou mensagem – por dois motivos principais:

- No PIX, os sistemas dos PSPs, PSTIs e BC estão conectados apenas à RSFN e, portanto, não possuem conectividade com a Internet. Por esse motivo, não conseguirão acessar os pontos de distribuição das *CRLs*;
- A consulta de forma *online*, a cada conexão ou mensagem, poderia impactar o tempo total de processamento das transações, resultando em uma experiência ruim para os usuários finais.

Dado o exposto acima, o Banco Central efetuará a verificação das *CRLs* por meio de processo separado e assíncrono, porém frequente. Caso o certificado de algum participante conste como revogado, o BC enviará notificação para a instituição via BC Correio e deixará de aceitar transações de/para essa instituição. É recomendado que todos os participantes do ecossistema implementem a verificação de *CRLs* de forma similar à realizada pelo BC.

[14] Conforme art. 2º da Carta Circular nº 4006, de 20 de fevereiro de 2020.
[15] Aplicação BC Correio, disponível em: https://bccorreio.bcb.gov.br/bccorreio/.

1.4. Segurança de *QR Codes* dinâmicos

Esta seção apresenta as especificações de segurança de *QR Codes* dinâmicos gerados pelo recebedor.

Conforme especificado no documento "Padrões para Iniciação do PIX"[16], o *QR Code* dinâmico gerado pelo recebedor contém, dentre outras informações, uma *URL* que é acessada de forma criptografada no momento de sua leitura. O conteúdo acessado consiste em uma estrutura *JWS (JSON Web Signature)*[17] cujo *payload*, assinado digitalmente, contém informações da transação. Os detalhes a respeito da segurança no acesso às *URLs*, certificados e processo de assinatura digital constam a seguir.

1.4.1. Segurança no acesso às *URLs*

A *URL* acessada ao se efetuar a leitura de um *QR Code* dinâmico deve ser provida pelo PSP recebedor em site que implemente o protocolo *HTTPS* com criptografia *TLS* versão 1.2 ou superior. O PSP recebedor deve ser proprietário do site/domínio – ou, caso contrate provedor de serviços para essa finalidade, o PSP deve se responsabilizar pela segurança e disponibilidade do site. O certificado *SSL* utilizado no site deve:

- Ser emitido por AC amplamente conhecida pelos diferentes navegadores e clientes de mercado;
- Ser do tipo *EV* ("*Extended Validation*" – Validação Estendida);
- Conter o(s) site(s)/domínios associado(s) aos *QR Codes* dinâmicos no campo *CN* (*"Common Name"*) ou *SAN* (*"Subject Alternative Name"*);
- Ser ativado no PIX conforme especificado na seção a seguir.

Como medida adicional de segurança, além dos requisitos obrigatórios acima, recomenda-se que cada PSP crie e mantenha registros *CAA ("Certification Authority Authorization")*[18] no *DNS* do domínio que hospeda os sites relacionados a *QR Codes* dinâmicos.

A *URL* presente no *QR code* dinâmico não deve incluir prefixo de protocolo, uma vez que este deve ser sempre *HTTPS*, conforme já especificado no início desta seção.

[16] Documento "Padrões para Iniciação do PIX" – última versão disponível na seção à direita da página: https://www.bcb.gov.br/estabilidadefinanceira/forumpagamentosinstantaneos.
[17] Padrão de assinatura digital JSON Web Signature (JWS), definido pela *RFC* 7515, disponível em https://tools.ietf.org/html/rfc7515.
[18] DNS CAA (Certificate Authority Authorization, disponível em https://tools.ietf.org/html/rfc6844.

Respeitadas as regras de formação de *URL*[19] e as definições do Manual do BR Code[20], os seguintes componentes devem estar presentes:

fqdnPspRecebedor/spiEndpoint/spiUrlAccessToken/

O tamanho máximo da *URL* completa (sem o prefixo de protocolo) deve ser 77 caracteres e o domínio do recebedor na *URL* deve ser completamente qualificado (*FQDN*). O *endpoint*/aplicação do recebedor é opcional, mas, se presente, deve ser respeitado.

O *spiUrlAccessToken* evita varreduras de "força bruta" por outros agentes que não tenham acesso ao *QR Code*, viabilizando a leitura dos detalhes de pagamento (*payload JSON*) apenas para o pagador[21]. O *spiUrlAccessToken* deve respeitar as seguintes restrições:

- Tamanho mínimo de 20 *bytes* (160 *bits*) aleatórios;
- Tamanho máximo conforme disponível, considerando os demais componentes da *URL*;
- Não deve ser possível deduzir seu valor, exceto pela leitura do *QR Code*, conforme detalhado abaixo.

Para impedir a dedução do *spiUrlAccessToken* por terceiros, o PSP recebedor deve criá-lo conforme as recomendações do documento do *W3C* intitulado "*Good Practices for Capability URLs*"[22], considerando também aspectos que aumentem o seu grau de entropia e de aleatoriedade[23] e, portanto, agreguem segurança.

O pagador não efetua validações no *spiUrlAccessToken*, sendo responsabilidade do PSP recebedor garantir suas propriedades mínimas de segurança.

1.4.2. Ativação de certificados *SSL* para sites de *QR Codes* dinâmicos

De forma similar ao processo de ativação de certificados para autenticação/criptografia da conexão e para assinatura digital de mensagens, detalhado na seção 1.3.2, também é necessário ativar os certificados *SSL* associados aos sites que hospedam *URLs* dos *QR Codes* dinâmicos. Para tanto, cada PSP deve

[19] A sintaxe, a semântica e outros aspectos a respeito de *URLs* são definidas pela *RFC* 1738, disponível em https://tools.ietf.org/html/rfc1738.
[20] Conforme estabelecido pela Carta Circular 4.014/2020, disponível em https://www.bcb.gov.br/estabilidadefinanceira/arranjosintegrantesspb.
[21] A *URL* estará exposta a qualquer agente que tenha acesso ao *QR Code* gerado.
[22] *W3C – "Good Practices for Capability URLs",* disponível em https://www.w3.org/TR/capability-urls/.
[23] A *RFC* 1750 (*Randomness Recommendations for Security*), disponível em https://tools.ietf.org/html/rfc1750, apresenta os desafios e soluções para geração de dados aleatórios.

enviar previamente seu(s) certificado(s) *SSL* por meio do Sistema de Transferência de Arquivos (STA), com o código/nome de arquivo abaixo:

Finalidade do certificado	Código do arquivo	Nome do arquivo
Certificado *digital* para sites de *QR Codes* Dinâmicos	*CQRC*	*Documento CERTQRC – Certificado Digital para sites de QR Codes Dinâmicos*

A instituição poderá confirmar a habilitação do seu certificado no próprio registro do protocolo de envio no STA. Após o recebimento do certificado, o BC efetua sua validação e inclusão na base de dados do BC. Essa base poderá ser verificada periodicamente por meio de consulta à ICOM[24].

Os registros da base incluirão, no mínimo as seguintes informações do certificado:

- Emissor (*issuer*);
- *Distinguished Name* (*DN*);
- Número de série;
- *Thumbprint*;
- *Site*(s)/Domínios associado(s) – de acordo com o campo *CN* ou *SAN*.

Com essas informações, cada PSP terá meios de implementar em seus aplicativos a validação, tanto do site como do certificado associado, no momento da leitura de um *QR Code* dinâmico, conforme descrito na seção 1.4.4 deste documento.

Cada PSP poderá ativar múltiplos certificados e sites/domínios associados. Dessa forma, é possível evitar eventuais indisponibilidades devido à expiração de determinado certificado ativo.

1.4.3.Definições do padrão *JWS*

Conforme já mencionado, ao se efetuar a leitura de um *QR Code* dinâmico gerado pelo recebedor, será acessada uma *URL* cujo conteúdo consiste em uma estrutura *JWS* em que o *payload* é assinado digitalmente pelo PSP recebedor, para garantir a integridade e não-repúdio das informações da transação. A estrutura *JWS* inclui:

- Cabeçalho (*JSON Object Signing and Encryption – JOSE Header*), onde se define o algoritmo utilizado e inclui informações sobre a chave pública ou certificado que podem ser utilizadas para validar a assinatura;
- *Payload* (*JWS Payload*): conteúdo propriamente dito;

[24] Mais informações sobre a Interface de Comunicação (ICOM) estão disponíveis no Manual das Interfaces de Comunicação, cuja última versão disponível consta na seção à direita da página: https://www.bcb.gov.br/estabilidadefinanceira/forumpagamentosinstantaneos.

- Assinatura digital (*JWS Signature*): assinatura digital, realizada conforme parâmetros do cabeçalho.

Cada elemento acima deve ser codificado utilizando o padrão *Base64url*[25] e, feito isso, os elementos devem ser concatenados com *"."* (método *JWS Compact Serialization*, conforme definido na *RFC* 7515).

No contexto do PIX, o cabeçalho (*JOSE Header*) deve incluir no mínimo os parâmetros abaixo:

- *alg (Algorithm)*:
  Define o algoritmo de assinatura digital utilizado.
  - Valores proibidos: *HS* (*relacionados a *HMAC)* e *none*.
  - Valores permitidos: *RS256* ou superior e *ES256* ou superior.
  - Valores recomendados: *PS256* ou *PS512*.
- *x5t (X.509 Certificate SHA-1 Thumbprint)*:
  Consiste no *thumbprint*, codificado em *Base64url*, do certificado que corresponde à chave privada utilizada para assinatura do *JWS*.
- *jku (JWK Set URL)*:
  Define a *URL* onde consta um conjunto de chaves no formato *JSON (JWK Set*[26]*).*
  - A *URL* deve estar hospedada no mesmo site/domínio associado ao certificado *CERTPIQ* ativado conforme descrito na seção 1.4.2.
- *kid (Key ID)*:
  Identificador da chave a ser utilizada para validar a assinatura digital, dentre as chaves presentes no *JWK Set* acessado por meio da *URL* definida no parâmetro *jku*.

O *JWK Set* disponível na *URL* acima deve incluir o parâmetro *keys*, cujo valor consiste em uma ou mais chaves no padrão *JWK*, conforme definido na *RFC* 7517. A estrutura *JWK*, por sua vez, deve incluir no mínimo os parâmetros abaixo:

- *kty (Key Type)*:
  Define o algoritmo criptográfico da chave.
  - Deve ser *RSA* ou *EC*.
- *key_ops (Key Operations)*:
  Identifica a operação para a qual a chave deve ser utilizada.
  - Deve ser sempre *verify*, pois a chave será usada para verificar a assinatura digital do *JWS*.
- *kid (Key ID)*:
  Identificador único da chave no *JWK Se*t.

[25] As definições sobre o padrão Base64url constam na seção 5 da *RFC* 4648, disponível em https://tools.ietf.org/html/rfc4648#section-5.
[26] A estrutura *JSON Web Key* é definida pela *RFC* 7517, disponível em https://tools.ietf.org/html/rfc7517.

- *x5t (X.509 Certificate SHA-1 Thumbprint)*:
  Consiste no *thumbprint*, codificado em *Base64url*, do certificado que corresponde à chave privada utilizada para assinatura do *JWS*.
- *x5c (X.509 Certificate Chain*):
  Especifica o certificado digital *X.509* – incluindo a chave pública que corresponde à chave privada utilizada na assinatura digital – e sua respectiva cadeia.
  - Deve-se utilizar um *array JSON* com os certificados, começando com o certificado cuja chave privada correspondente foi utilizada na assinatura, seguido pelo certificados adicionais da cadeia, onde cada certificado subsequente tenha sido utilizado para emissão do certificado anterior, conforme exemplo do *Appendix B* da *RFC* 7515.
  - Assim como no caso do certificado associado ao site que hospeda a estrutura *JWS*, o certificado neste caso deve ser válido e emitido por AC amplamente conhecida.

Os parâmetros *x5t* e *kid* definidos no *JWK Set* devem corresponder aos parâmetros de mesmo nome que constam no cabeçalho *JWS*, permitindo que a aplicação cliente consiga identificar de maneira inequívoca o certificado e a chave pública a ser utilizada para verificar a assinatura digital do *JWS*.

1.4.4.Validações a serem feitas pelos aplicativos

Após efetuar a leitura de um *QR Code* dinâmico, os aplicativos de cada PSP devem seguir os passos abaixo:

- Verificar se a *URL* que consta no *QR Code* é hospedada em site com criptografia *TLS* versão 1.2 ou superior, conforme seção 1.4.1;
- Verificar se o certificado associado ao site está ativo no PIX, conforme seção 1.4.2;
- Verificar se o site consta no campo *CN* (*"Common Name"*) ou *SAN* (*"Subject Alternative Name"*) do certificado;
- Obter chave pública conforme informações do cabeçalho *JWS* e *JWK Set*;
- Validar a assinatura digital (*JWSSignature*) com a chave pública obtida no passo anterior.
- Se e somente se a assinatura estiver válida, realizar a transação conforme informações do *payload JWS*.

Cabe aos PSPs implementarem mecanismos em seus aplicativos para otimizar o processo de verificação da assinatura digital do *JWS*. Por exemplo, é possível que o aplicativo armazene previamente um conjunto de *thumbprints* de certificados e suas respectivas chaves públicas de forma que, ao ler o parâmetro *x5t* do *JWS*, o aplicativo já consiga saber qual chave utilizar para validar a assinatura digital, sem precisar acessar a *URL* definida no parâmetro *jku*.

Recomenda-se que, para facilitar esse processo de "carga prévia" de *thumbprints* e chaves públicas nos aplicativos, cada PSP mantenha um diretório "*/.well-known/*"[27] no seu site associado a *QR Codes* dinâmicos. Tal diretório pode conter, por exemplo, um documento *host-meta*[28] que especifique as *URLs* dos seus *JWK Sets* (parâmetro *jku* do *JWS*). Assim, os demais PSPs conseguirão programar seus aplicativos para carregar previamente os *JWK Sets* de determinado PSP, de forma a agilizar o processamento de transações via *QR Codes* dinâmicos quando o recebedor for aquele PSP.

Por fim, para garantir o não-repúdio das transações efetuadas por meio de *QR Codes* dinâmicos, recomenda-se que os PSPs mantenham registros históricos das transações efetuadas, incluindo as respectivas estruturas *JWS*, certificados e chaves públicas relacionados a cada transação.

[27] A definição do recurso denominado *Well-Known URIs* é feita pela RFC 8615, disponível em: https://tools.ietf.org/html/rfc8615.
[28] O formato do documento *host-meta* é definido pela RFC 6415, disponível em: https://tools.ietf.org/html/rfc6415.