Estudo Técnico Preliminar 107/2023

1. Informações Básicas

Número do processo: 230536

2. Descrição da necessidade

O ambiente PIX e alguns sistemas críticos do Bacen possuem requisitos de segurança que exigem a confidencialidade, integridade, autenticidade e não-repúdio das informações trocadas entre o Bacen e outras instituições.

Para atingir os objetivos descritos, o Deinf utiliza-se de criptografia com certificação digital baseado na Infraestrutura de chaves públicas da ICB-Brasil. Para otimização das operações criptográficas, os sistemas em plataforma distribuída e no ambiente PIX repassam a execução dessas operações a módulos de segurança criptográfica de rede, que armazenam hermeticamente as chaves privadas do Banco Central.

Os HSM’s são módulos de rede especializados na realização de operações criptográficas com alto desempenho e implementando cofres extremamente herméticos para, quando necessário, guardar de forma inexpugnável as chaves privadas essenciais para garantir a força e sigilo dos algoritmos de criptografia assimétrica.

É importante destacar a impressionante aceitação do PIX pela população brasileira que duplicou o número de transações de 2.021 para 2.022 se tornando o meio de pagamento mais utilizado no Brasil. Cabe lembrar que ano passado o BC percebeu a necessidade de expandir a capacidade a solução quando a monitoração do PIX verificou que o uso das CPU’s dos HSM’s chegou a cerca de 60% na Sede e 40% na UNIBC, com picos na casa dos 70% na Sede e 60% na UniBC em 05/agosto/22, quando se batia um recorde de transações PIX. Desde então recordes estão sendo batidos frequentemente. Na sexta-feira, 07/julho/2023, por exemplo, o recorde era batido novamente se chegando-se a 134,8 milhões superando o anterior, de 129,4 milhões de transações alcançado um dia antes, na quinta-feira, 06/julho/2023.

3. Área requisitante

Área Requisitante	Responsável
Departamento de Informática (DEINF) - Banco Central do Brasil	Caio Moreira Fernandes

4. Necessidades de Negócio

Módulo de segurança criptográfico (HSM)

O ambiente PIX e alguns sistemas críticos do Bacen possuem requisitos de segurança que exigem a confidencialidade, integridade, autenticidade e não-repúdio das informações trocadas entre o Bacen e outras instituições.

Para atingir os objetivos descritos, o Deinf utiliza-se de criptografia com certificação digital baseado na Infraestrutura de chaves públicas da ICB-Brasil. Para otimização das operações criptográficas, os sistemas em plataforma distribuída e no ambiente PIX repassam a execução dessas operações a módulos de segurança criptográfica de rede, que armazenam hermeticamente as chaves privadas do Banco Central.

Além disso, as operações criptográficas são executadas em hardware, o que acelera e otimiza a execução dessas operações.

5. Necessidades Tecnológicas

Os módulos atuais foram adquiridos através dos Contratos BCB/Deinf 51064/2019 e BCB/Deinf 50194/2020, celebrado com a Dínamo Networks, vencedora do Pregão Eletrônico Demap nº 98/2019 e da Ata de Registro de Preços 26/2019. A solução teve seu aceite de instalação em 10/12/2019, e sua garantia vale por 48 meses (encerrando em 10/12/2023). Faz-se necessário preparar nova contratação para implantação até a data de vencimento da solução atual.

Dessa forma, propomos a realização de licitação para nova contratação de módulos de segurança criptográfica. Os novos módulos de segurança criptográfica deverão ser capazes de processar, no mínimo, 7000 operações por segundo, utilizando chaves RSA de 2048 bits. Os atuais módulos terão sua garantia e suporte renovados.

6. Demais requisitos necessários e suficientes à escolha da solução de TIC

Atualmente os ambientes tecnológicos do Banco Central possuem 14 módulos de segurança criptográfica perfeitamente operacionais. Eventual troca de fabricante dos módulos acarretaria um grande risco de interrupção através de todos os ambientes em que esses módulos são utilizados (PIX/SPB, homologação/produção). Os atuais sistemas clientes dessa tecnologia precisariam ter seus códigos e APIs alterados para nova integração com equipamentos de outros fabricantes, além de demandar capacitação de inúmeras equipes de desenvolvimento e suporte à infraestrutura. Assegurando que o custo de aquisição de alguns módulos e renovação da garantia e suporte dos atuais seja consideravelmente inferior à troca de todos os módulos por

equivalentes de outro fabricante, a equipe técnica do DEINF optou pela renovação da garantia e suporte do atuais e aquisição de novos módulos complementares a atual infraestrutura.

7. Estimativa da demanda - quantidade de bens e serviços

Será necessário realizar um processo licitatório em substituição aos Contratos BCB /Deinf 51064/2019 e BCB/Deinf 50194/2020 para aquisição de 6 módulos de segurança criptográfica, com garantia e suporte por 36 meses, e contratação de garantia e suporte por 36 meses dos outros 14 módulos, já em operação no ambiente do Banco Central.

8. Levantamento de soluções

A estabilidade da solução é essencial para que o nível de serviço esperado pelos sistemas críticos que dependem de criptografia de alta performance no ambiente do Banco Central.

O desenvolvimento de uma solução no Bacen exigiria conhecimento especializado, e caso haja insucesso no desenvolvimento, a estabilidade dos sistemas estaria comprometida.

Como já esclarecido anteriormente, devido ao alto risco de interrupção dos serviços críticos envolvidos nesse tipo de equipamento, inclusive risco de interrupção no ambiente 24/7 PIX, a equipe técnica considerou a manutenção da fornecedora atual.

Como já estão instalados 14 módulos plenamente operacionais, a equipe técnica optou por realizar a renovação da garantia e suporte desses módulos e adquirir outros 6 módulos da atual fabricante, a fim de permitir a estabilidade do ambiente PIX e expansão sua capacidade.

Após pesquisas de mercado mostrarem a compatibilidade da proposta da atual Contratada, Dínamo Networks, com os preços praticados no mercado, a equipe técnica do Banco Central optou pela manutenção e expansão da atual arquitetura.

9. Análise comparativa de soluções

Embora haja outros fabricantes de HSM, optou-se pela manutenção do atual, visto que o custo da proposta enviada pela Contratada compete favoravelmente com os preços praticados no mercado.

Por se tratar de um componente crítico e imprescindível para o funcionamento do PIX, com sistemas adaptados às suas APIs e equipes treinadas e especializadas na atual solução, a equipe técnica recomendou a renovação da atual estrutura e ainda

aquisição de outros seis equipamentos, a fim de suportar a planejada expansão do ambiente, necessária devido à grande demanda de uso do PIX.

Requisito	Solução	Sim	Não	Não se Aplica
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	Solução 1	X		
A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	Solução 1			X
A Solução é composta por software livre ou software público? (quando se tratar de software)	Solução 1			X
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Solução 1	X		
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Solução 1	X		
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)	Solução 1			X

10. Registro de soluções consideradas inviáveis

Pelos motivos retratados anteriormente, as soluções avaliadas de outros fabricantes (Thales, Kryptus) foram consideradas inviáveis ou de risco inaceitável ao ambiente crítico do Banco Central (PIX, SPB e Swift), seja por demandar reprogramação e adaptação de sistemas, redefinição de arquitetura do ambiente, novos treinamentos, perda da inteligência adquirida ou capacidade insuficiente, seja pelo alto custo da solução.

11. Análise comparativa de custos (TCO)

O mapa comparativo dos cálculos totais de propriedades (TCO) está contido no campo "Mapa TCO".

12. Descrição da solução de TIC a ser contratada

Inicialmente, a equipe de planejamento da contratação fez pesquisa de mercado para aquisição de 24 módulos de segurança criptográfica de rede novos. Devido ao alto custo dos dispositivos, ajustes foram feitos no projeto para abarcar 20 módulos, sendo que 14 dos quais já em operação no ambiente do Banco Central, cuja garantia e suporte serão renovados por 36 meses, e aquisição de 6 módulos novos.

13. Estimativa de custo total da contratação

[Conteúdo Sigiloso | Justificativa: É praxe, no Bacen, não divulgar o orçamento detalhado e suas planilhas de custo usados para a escolha e estimativa de custo da solução.]

14. Justificativa técnica da escolha da solução

O ambiente PIX e alguns sistemas críticos do Bacen possuem requisitos de segurança que exigem a confidencialidade, integridade, autenticidade e não-repúdio das informações trocadas entre o Bacen e outras instituições.

Para atingir os objetivos descritos, o Deinf utiliza-se de criptografia com certificação digital baseado na Infraestrutura de chaves públicas da ICB-Brasil. Para otimização das operações criptográficas, os sistemas em plataforma distribuída e no ambiente PIX repassam a execução dessas operações a módulos de segurança criptográfica de rede, que armazenam hermeticamente as chaves privadas do Banco Central. Além disso, as operações criptográficas são executadas em hardware, o que acelera e otimiza a execução dessas operações.

Por se tratar de um componente crítico e imprescindível para o funcionamento do PIX, com sistemas adaptados às suas APIs e equipes treinadas e especializadas na atual solução, a equipe técnica recomendou a renovação da atual estrutura e ainda aquisição de outros seis equipamentos, a fim de suportar a planejada expansão do ambiente, necessária devido à grande demanda de uso do PIX.

15. Justificativa econômica da escolha da solução

Como é possível verificar no conjunto das propostas sintetizadas nas tabelas do campo 17, os preços indicados da atual fornecedora são mais vantajosos do que os praticados no mercado quando comparados com os contratos celebrados por outras entidades. A consulta ao Painel de Preços do Ministério da Economia não retornou compra com objeto similar ao desta contratação.

Foi realizada também uma pesquisa de contratos celebrados com a administração pública, descrita em tabela disponível no campo 17, adaptando os valores para a duração do contrato (36 meses), capacidade e quantidade de módulos assim como suas respectivas garantias

16. Mapa TCO

[Conteúdo Sigiloso | Justificativa: É praxe, no Bacen, não divulgar o orçamento detalhado e suas planilhas de custo usados para a escolha e estimativa de custo da solução.]

17. Estimativa de custo - tabelas

[Conteúdo Sigiloso | Justificativa: É praxe, no Bacen, não divulgar o orçamento detalhado e suas planilhas de custo usados para a escolha e estimativa de custo da solução.]

18. Benefícios a serem alcançados com a contratação

As renovações e aquisições objetos dessa licitação possibilitarão a projetada expansão da capacidade do ambiente PIX e de outros sistemas ativos no Banco Central.

19. Providências a serem Adotadas

Não há necessidade de adequações no ambiente do Banco Central para viabilizar a execução contratual.

Já existem módulos de segurança criptográfica em operação no ambiente do Banco Central.

20. Declaração de Viabilidade

Esta equipe de planejamento declara **viável** esta contratação.

20.1. Justificativa da Viabilidade

Levando em consideração os estudos realizados na análise comparativa de soluções, aspectos econômicos e qualitativos, registrados ao longo do Estudo Técnico

Preliminar, a equipe de planejamento considera viável a contratação.
As soluções alternativas pesquisadas não foram favoráveis financeiramente, a atual fabricante deteve o melhor preço pesquisado.

A troca de fabricante da atual solução foi considerada pela equipe técnica de elevado risco para a estabilidade e disponibilidade dos ambientes afetados. As equipes já se encontram treinadas e os sistemas integrados à solução. O esforço e o risco dessa mudança de fabricante não estão amparados economicamente, de acordo com a pesquisa de preços feita pela equipe de planejamento da contratação, onde pde-se verificar que a manutenção da atual fabricante não é apenas mais segura e eficiente como também é a opção financeiramente mais vantajosa.

21. Responsáveis

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

FABIO CESAR MIRANDA DE ARAUJO
Analista

MARCOS JOSE CANDIDO EUZEBIO
Coordenador

CAIO MOREIRA FERNANDES
Chefe Adjunto

MARCIO RODRIGUES ALVES DOS SANTOS
Chefe de Subunidade