

32 – Maio de 2001

SPB: três letras e muitos desafios

Surge mais um acrônimo para exigir de nossa memória, desta vez relacionado ao segmento financeiro e não diretamente à informática – como de costume. O SPB ou Sistema de Pagamentos Brasileiro passa a ser o assunto de pauta de todos os mais de 170 bancos brasileiros e câmaras de compensação e liquidação, e nasce pelas mãos do Banco Central do Brasil.

Inovação, tecnologia e a conseqüente ebulição provocada pelas novidades e constantes mudanças não são novidade para o segmento, pois em função do perfil de nosso mercado – há muito marcado pelo efeito inflacionário – passamos a ter um dos sistemas financeiros mais ágeis, automatizados e informatizados do mundo, além de revelar-se como o setor da economia que mais aplica tecnologia ao negócio. Tais características são hoje percebidas por todos os demais, como benéficos, afinal, adquiriram maior dinamismo e adaptabilidade para suportar as próximas e certas mudanças que estão por vir.

A iniciativa SPB propõe a utilização de uma infra-estrutura de comunicação de dados para o monitoramento do fluxo monetário relacionado aos depósitos e fundos de reserva dos bancos junto ao Banco Central.

Didaticamente falando, a idéia ganha vida através de uma rede de comunicação de dados, capaz de colocar todos os bancos e clearing houses (câmaras de compensação e liquidação) em um canal comum único para troca de mensagens criptografadas assinadas digitalmente em tempo real. Mas ainda existem detalhes operacionais, pois como pensado originalmente, apenas as transferências de valores acima de um limite pré-estabelecido, estarão sujeitos à via expressa do SPB automaticamente. Importâncias inferiores terão de sinalizar o interesse em trafegar pela infovia do sistema.

As mudanças propostas são ainda mais profundas, pois o modelo sugere diversos padrões para comunicação eletrônica, como o formato da mensageria, índices de confidencialidade, integridade, disponibilidade e autenticidade através de regras de segurança ligadas à criptografia, certificado digital e padrões de segurança física e lógica.

Mas os desafios não terminam por aí. Apesar de toda a vantagem inerente ao ganho de velocidade financeira e transferência de riscos do Banco Central para os bancos e câmaras de compensação e liquidação, tornando o sistema financeiro mais coeso e fortalecido, ainda restam os obstáculos técnicos e temporais, afinal, o prazo para a operacionalidade do sistema foi estipulado para janeiro próximo.

Para que todas as instituições envolvidas estejam preparadas à tempo, torna-se coerente dividimos agora o problema em pedaços a fim de auxiliar a análise, entendimento e a elucidação da solução.

Aplicação SPB

Por se tratar de uma aplicação nova, deve ser desenvolvida especificamente para suportar a operação definida pelo Banco Central. Terá o papel de servir de interface entre o anel da rede SPB e os sistemas legados da instituição financeira. Em função da curta janela de tempo entre a especificação definitiva e a data limite para operação e produção, não há grande oportunidade para testes homologatórios, por isso, a necessidade de uma metodologia de desenvolvimento de software capaz de garantir sua qualidade e conformidade aos padrões de documentação e manutenção.

Camada de Segurança

Como previsto originalmente, a aplicação SPB deve possuir uma camada de software específica e em conformidade com as especificações do Banco Central, apta a aplicar os mecanismos de criptografia e certificado digital a fim de proteger a confidencialidade e autenticidade das mensagens por intermédio da assinatura eletrônica. Por trás deste modelo há um processo rebuscado de emissão dos certificados digitais por entidades previamente certificadas e autorizadas pelo Banco Central.

Certificado Digital

O momento de maior risco no processo é aquele em que a chave privada é empregada na assinatura e criptografia das mensagens, pois se utilizada e copiada indevidamente, permitirá a emissão de mensagens fraudulentas que comprometerão a integridade do sistema. Pensando nisso, soluções que oferecem índices reduzidos de risco já adotam equipamentos (hardware) específicos para a armazenagem e principalmente para a manipulação da chave privada. Além disso, proporcionam performance incomparável, redundância operacional, balanceamento de carga e altos índices de disponibilidade.

Contingência Operacional

Outro aspecto que deve ser considerado é a contingência operacional proporcionada pela redundância de equipamentos, e também a redundância de certificados digitais. Afinal, a lei de Murph diz que se algo pode dar errado, ele dará. Então, por que não se antecipar à possibilidade de ter o certificado primário revogado erradamente, ter sua privacidade questionada ou a integridade atingida?

Para isso, recomenda-se utilizar três certificados, onde um é exclusivamente empregado no período de testes homologatórios, o segundo como instrumento oficial de assinatura e o terceiro e último como backup.

Perímetro SPB

Por mais que queiramos restringir os desafios de segurança encurralando apenas a aplicação SPB, não podemos esquecer do bem mais precioso: a informação. Esta não estará somente exposta enquanto manuseada, armazenada, transportada e descartada pela aplicação, mas também estará suscetível à tentativas de quebra de segurança explorando-se os aspectos físicos, tecnológicos e humanos. Por isso, será necessário tomar ações de segurança que implementem controles, reduzindo os riscos inerentes as ameaças: naturais (incêndio, inundação, falta de energia elétrica etc), físicas (rede elétrica não estabilizada,

controle de acesso à sala do servidor inadequado, cabeamento de rede impróprio etc), tecnológicas (defeitos de software, vulnerabilidades do sistema operacional, queda dos links de comunicação etc) e humanas (erro humano, sabotagem, engenharia social etc).

Assim, recomenda-se realizar a Análise de Segurança da Aplicação à procura de brechas, códigos ocultos e falhas de desenvolvimento; Teste de Invasão a fim de por à prova os mecanismos de segurança do perímetro; Plano de Continuidade específico para o ambiente, objetivando a disponibilidade operacional mesmo em situações de desastre; e ainda assegurar que o novo processo seja posto em funcionamento sem sobressaltos com o auxílio de uma equipe de emergência preparada para responder com velocidade diante de uma situação imprevisível.

Sistemas Legados

Não equacionamos todo o problema, pois ainda restam os sistemas legados, afinal estes devem interagir diretamente com a nova aplicação SPB, e agora estarão igualmente expostos. Deve-se considerar os novos índices de riscos a que as informações institucionais estarão suscetíveis, e a partir de uma análise de segurança, identificar os melhores mecanismos de controle para evitar que os benefícios nítidos proporcionados pelo Sistema de Pagamentos Brasileiro não venham comprometer a segurança do seu negócio.

De forma conclusiva, mas buscando estimular a reflexão, pergunto: o novo Sistema de Pagamentos Brasileiro reduz os riscos operacionais do mercado financeiro, mas será que faz o inverso com as informações das instituições financeiros ligadas a ele?!

Tranquilizando...independentemente da resposta, uma certeza. Empenhe-se em administrar os novos riscos... e bons negócios!

Marcos Sêmola é MBA em Tecnologia Aplicada, Bacharel em Ciência da Computação, Professor da cadeira de Segurança da Informação da FGV – Fundação Getúlio Vargas, Gerente de Produto e Consultor de Segurança da Módulo Security Solutions S.A.

msemola@modulo.com.br