Q&A Normativo 31/2024

Principais perguntas e respostas sobre Normativo 31/2024 da Abecs, que apresenta padrão técnico para aplicação de autenticações via 3DS 2.0 (ou versão superior).

53 anos
94 associados | +95% da indústria de meios eletrônicos de pagamento
44 emissores | +80% do segmento
25 credenciadoras | +90% do segmento
06 bandeiras (instituidores de arranjo) | +98% do segmento

1. Quais são as principais mudanças a serem introduzidas pelo Normativo 31/2024 da Abecs?

O normativo determina que deve-se responder a requisições de autenticação e autorização de pagamento baseadas no protocolo 3DS, em conformidade com as especificações da EMVCo e seguindo os parâmetros e níveis mínimos de serviço definidos para o mercado nacional, com base em práticas adotadas em diversos países.

Nesse sentido, por exemplo, o normativo estimula os emissores a expandirem o nível de cobertura de autenticações silenciosas (ou sem desafio) atualmente adotado na indústria, com base em parâmetros internacionais. Essas autenticações estarão baseadas na avaliação de risco de um determinado portador de cartão a partir de diversos dados, como o dispositivo utilizado e dados cadastrais enviados no pedido de autenticação (a exemplo do que há anos acontece com transações bancárias no internet banking).

A iniciativa representará um importante ganho para os estabelecimentos comerciais, que terão uma operação mais segura em relação a fraudes e custos menores para mitigá-las e, indiretamente, para os consumidores, com redução da possibilidade de fraudes e maior comodidade na realização de transações.

2. O normativo pretende trazer a obrigatoriedade de utilização do 3DS em todas as transações digitais? Caso contrário, qual seria o patamar mínimo por transação? Existirá diferenciação de acordo com a natureza do negócio?

Não, a obrigatoriedade de utilização do 3DS será aplicável apenas a transações acima de determinados valores mínimos (thresholds), com cartões de débito e com cartões de crédito ou pré-pago, de acordo com os segmentos econômicos (Merchant Category Code – MCC) dos estabelecimentos comerciais. Esses valores mínimos estão listados no Anexo I do normativo, incluindo os pisos para cada segmento (MCC), e foram definidos com base em uma premissa de se evitar o máximo possível de fraudes com cartões com o menor atrito possível para os consumidores (isto é, menor número de usuários de cartões afetados por um "desafio" na autenticação).

3. Haverá punições para os estabelecimentos comerciais que não adotarem o protocolo 3DS? Ou haverá um sistema de incentivos como um selo de "boas práticas"?

O normativo foi idealizado em consonância com os programas de risco e compliance das marcas (bandeiras). No entanto, conforme disposto no artigo 14 do Normativo 31, a Abecs, na sua função de indutora de boas práticas no setor de meios de pagamento, criará um selo de boas práticas (o Selo de Segurança Digital Abecs) a ser concedido aos estabelecimentos comerciais que estiverem em conformidade com as regras previstas no Normativo 31, o qual poderá ser divulgado e capitalizado por esses estabelecimentos em benefício próprio, dentro de determinados parâmetros a serem definidos pela Associação.

4. Os estabelecimentos comerciais poderão solicitar que sejam excluídos da adoção do protocolo 3DS? Se sim, em quais situações e qual seria a instância decisória?

Sim. Nos termos do artigo 6º, §2º do normativo, desde que embasados em fatos, estabelecimentos comerciais poderão submeter um pedido de reconhecimento junto às credenciadoras e PSPs (Payment Service Provider) com os quais mantenham relacionamento comercial de que não precisam adotar o 3DS.

Esse pedido será avaliado pelo Fórum de Segurança e Prevenção a Fraudes da Abecs (ou outro fórum com a mesma representatividade) e, caso insira-se em alguma das hipóteses previstas no normativo, poderá ser aprovado. Alguns exemplos de exceção que poderão ser discutidos pelo Fórum de Segurança e Prevenção a Fraudes são: não obrigatoriedade para pedidos de autenticação em cartões empresariais ou pré-pagos, transações iniciadas pelos estabelecimentos comerciais (como transações recorrentes ou de cartões em arquivo/CoF), entre outros.

5. O normativo prevê o oferecimento de alternativas à utilização do protocolo 3DS, como por exemplo a implementação do data only?

O normativo não tem por objeto o oferecimento de alternativas à utilização do protocolo 3DS, mas não impede sua adoção temporária ou contingencial pelos estabelecimentos comerciais, tampouco a migração para esse protocolo, como é o caso do data only (ou data share only, modalidade universal de troca de dados sem apresentação de um "desafio" de autenticação, prevista nas especificações da EMVCo). Utiliza-se da mesma plataforma técnica do 3DS e, por isso, pode ser considerada uma etapa intermediária entre um cenário de ausência de autenticação e outro cenário de autenticação completa com base no 3DS. Caso um estabelecimento comercial considere-se seguro quanto à conversão oferecida por um emissor, se quiser garantir a venda a partir da inversão de responsabilidade (liability shift), poderá facilmente migrar de uma estratégia de data share only para autenticações completas baseadas no protocolo 3DS.

6. Será necessário realizar a autenticação com base no protocolo 3DS no caso de cartões tokenizados? E no caso de combinar tokenização com data only?

Quanto à combinação de tokenização com data only, desde que os índices de fraude estejam num patamar razoável, se o comércio tiver menor aversão a risco poderá adotar essa combinação.

7. Como o normativo tratará o caso da utilização do 3DS no modelo card on file? Haverá regras específicas? As transações Zero Auth também terão de usar o protocolo 3DS obrigatoriamente?

No caso de modelos de negócio de estabelecimentos comerciais baseados no conceito de card on file ou recorrência, é recomendável a realização de autenticação pelo protocolo 3DS no momento do cadastramento do cartão em uma conta de pagamento ou em uma carteira digital ou na primeira compra com o cartão. Em transações subsequentes com o cartão, a tokenização já assegurará a segurança do processo e, consequentemente, novas autenticações não serão mais necessárias (exceto em casos nos quais o emissor identifique um risco excessivo, como transações concentradas ou consecutivas).

8. No caso de transações recorrentes, de que forma está sendo proposta a autenticação? Há modelos de assinaturas digitais em que o primeiro mês é gratuito e só se cobra após um determinado período, de forma assíncrona. Como está prevista a implementação nesse cenário?

A versão do protocolo 3DS utilizada hoje pelo mercado (2.2) já estabelece que transações iniciadas pelo estabelecimento comercial (chamadas MIT) podem ser autenticadas sem a presença do cliente, desde que haja a referência de uma primeira transação autenticada que iniciou essa série. E, conforme descrito anteriormente, isso pode ser combinado com uma tokenização de pagamentos (network token), o que garante a fluidez e segurança ao longo de toda a recorrência, sem necessidade de o cliente se autenticar a cada lançamento (a não ser que políticas de KYC estabeleçam essa necessidade).

9. No caso de estabelecimentos comerciais com um índice de fraude controlado, há abertura para estabelecer exceções à obrigatoriedade de uso do 3DS?

Conforme abordado na questão 4, as exceções precisam ser justificadas por fatos e validadas pelo Fórum de Segurança e Prevenção a Fraudes da Abecs. Mas, mesmo que cada modelo de negócio contenha suas especificidades, é importante avaliar antes quais alternativas estão disponíveis e que façam uso extensivo de protocolos de segurança oferecidos pelas bandeiras (autenticação e tokenização, entre outros).

10. Há previsão de obrigações aos emissores para que melhorem a comunicação com os seus clientes para aumentar o conhecimento e a confiança sobre esse modelo de autenticação?

Não. A Abecs considera que os emissores são responsáveis pela comunicação junto a seus clientes. Paralelamente, a Abecs poderá produzir peças de esclarecimento para os usuários finais acerca dos ganhos resultantes do uso da autenticação baseada no protocolo 3DS frente aos métodos de autenticação que são usados atualmente pelos principais agentes de mercado (como o push no app e uso de biometria para resolução de uma autenticação).

11. Qual é o calendário previsto para adoção do normativo pelas bandeiras e posterior adaptação dos participantes dos arranjos de pagamento?

O Normativo 31/2024 foi publicado em 21/08/24 e está disponível no seguinte endereço eletrônico: www.abecs.org.br/normas.

A maioria dos emissores e credenciadoras já está habilitada a trabalhar com o protocolo 3DS.

Quanto aos solicitantes de autenticação (estabelecimentos comerciais), espera-se que, nos próximos meses, as credenciadoras apoiem seus clientes na adoção do 3DS, tanto no aspecto técnico para inicialização (set-up) do ecossistema do 3DS e ajustes no fluxo, quanto na otimização do uso desse protocolo no caso de estabelecimentos comerciais que tenham aderido a ele. Na visão da Abecs, esse é um processo que vai requerer um esforço coletivo de toda a indústria, a fim de se garantir o objetivo principal da iniciativa em questão: elevar a segurança dos estabelecimentos comerciais em relação a fraudes e reduzir os custos para mitigá-las.

12. No caso de transações via marketplaces, quando o normativo prevê a implementação do 3DS por MCC, é considerado o MCC do marketplace ou o MCC de cada um dos sellers do marketplace?

Dada a diversidade de perfis dos estabelecimentos comerciais que operam em um marketplace, o MCC deve ser o do seller. Isso inclusive evitará distorções na análise de risco que os emissores fazem com base no produto/serviço (de acordo com o setor de atividade).