A Diretoria Estatutária da Abecs, com base no Estatuto Social da Associação Brasileira das Empresas de Cartões de Crédito e Serviços (Abecs) e no Código de Ética e Autorregulação, sanciona as regras abaixo, formalizando preceitos comuns a todas as signatárias da Associação no que concerne à aplicação, no mercado nacional, de autenticação para transações eletrônicas *online* através do protocolo EMV 3D-Secure (ou "3DS") e do "*Framework* de Autenticação".

NORMATIVO Nº 31

Dispõe sobre a disponibilização de documento técnico de padronização para a aplicação de autenticações via protocolo de autenticação dentro da versão 2.0 ou superior do protocolo global EMV 3DS e do "*Framework* de Autenticação" com base no índice de fraudes de um Estabelecimento Comercial e *tokens* verificados para os casos de uso aplicados.

CONSIDERANDO as finalidades institucionais da Associação Brasileira de Empresas de Cartão de Crédito e Serviços (Abecs), incluindo a autorregulação do mercado de cartões para o bom funcionamento das relações comerciais e de negócios no País;

CONSIDERANDO a Abecs como entidade representativa das empresas integrantes do sistema operacional e jurídico de meios eletrônicos de pagamento;

CONSIDERANDO a autorregulação da Abecs como um sistema de autodisciplina complementar e suplementar às normas já existentes, cujos princípios fundamentais são: (a) a transparência das relações; (b) o respeito e cumprimento à legislação vigente; (c) a expansão sustentável do número de portadores de cartões no mercado brasileiro e de Estabelecimentos Comerciais credenciados; (d) a adoção de comportamento ético e compatível com as boas práticas comerciais; (e) a liberdade de iniciativa, livre concorrência e função social; (f) a proibição de práticas que infrinjam ou estejam em desacordo com o Código de Proteção e Defesa do Consumidor e o Código de Ética e Autorregulação; e (g) o estímulo às boas práticas de mercado;

Rua Elvira Ferraz, 250, 4º andar, conj. 411
São Paulo, SP
11 3296-2750
www.abecs.org.br

CONSIDERANDO que o objetivo deste Normativo é estabelecer parâmetros e um roteiro operacional mínimo com a finalidade de aumentar a segurança contra fraudes de identidade nas transações eletrônicas *online* (sem a presença do cartão).

CONSIDERANDO a necessidade de se estabelecer índice de fraudes do Estabelecimento Comercial (por "Merchant ID") para se requerer uma autenticação através do protocolo EMV 3DS e do *Framework* de Autenticação, de modo que os comércios eletrônicos submetam à aprovação dos Emissores pedidos de autenticação de clientes em transações CNP;

CONSIDERANDO a necessidade de se criar parâmetros na forma de níveis mínimos de serviço (do ponto de vista quantitativo ou qualitativo) sob a responsabilidade de Emissores e/ou Credenciadores / PSPs, visando garantir aos Estabelecimentos Comerciais o atendimento a estes pedidos de autenticação;

CONSIDERANDO que a referida padronização de alguns procedimentos e requisitos não significa qualquer exploração conjunta de atividade econômica pelos participantes envolvidos e nem a troca de informações sensíveis para a implementação da solução no Brasil de forma interoperável entre as entidades que compõem o modelo de 4 partes;

RESOLVE a Diretoria Estatutária, com fundamento no Código de Ética e Autorregulação da Abecs, instituir o presente Normativo, que dispõe sobre a expansão de autenticação forte em transações online através do protocolo EMV 3DS e do *Framework* de Autenticação no mercado nacional, como forma de mitigar as perdas de fraude e reversões (*chargebacks*), além de aumentar a conversão geral no ambiente virtual a partir de autenticações diretas e individuais.

Art. 1 Para efeitos deste Normativo, tem-se as seguintes definições:

§1º . Autenticação Forte do Cliente (ou SCA, sigla em inglês): é uma condição que estabelece a satisfação de pelo menos 2 (dois) de 3 (três) fatores em uma autenticação – quais sejam: o que um portador conhece (ex. seus dados demográficos), o que possui (ex. dispositivo) e o

Rua Elvira Ferraz, 250, 4º andar, conj. 411
São Paulo, SP
11 3296-2750
www.abecs.org.br

que é (ex. dados biométricos) – condição reforçada por diretivas internacionais exigidas em pagamentos eletrônicos através de autenticação multifator;

§2º . Autenticação 3D-Secure: método de autenticação padronizado internacionalmente que habilita recursos para executar a autenticação de compradores online com reduzido nível de atrito e atendendo ao requisito de SCA;

§3º . Índice de Fraude: indicador matemático que expressa a razão entre o valor de transações reportadas com fraude e o valor total de transações faturadas, no âmbito de cada arranjo de pagamento, em determinado período (sendo 1 ponto-base equivalente a 0,01%);

§4º . Cartão Não Presente – CNP (*Card Not Present*): a sigla indica a realização de uma transação a partir da transcrição dos dados de um cartão, sem sua leitura física;

§5º . EMVCo: consórcio que estabelece padrões e regulamentos em escala global para transações eletrônicas realizadas com cartões de débito, crédito ou pré-pago;

§6º . Autenticação Silenciosa: Em inglês, "*frictionless authentication*" ou autenticação sem atrito – em que, com base em dados como comportamento do cliente, dispositivo utilizado, dados cadastrais compartilhados pelo Estabelecimento Comercial, tipo e valor de compra, entre outras informações, respaldam a análise de risco do Emissor, liberando o portador do cartão de intervir na transação – como ser solicitado a apresentar uma resposta a um "desafio" (por exemplo, a digitação de código disponibilizado pelo seu Emissor);

§7º . *Key Performance Indicators* – KPIs (indicadores-chave de desempenho): medem os níveis de desempenho obtido em comparação às metas estabelecidas;

§8º . Autenticação Multifator (MFA, sigla em inglês): é um processo de login de conta com mais de uma etapa, que obriga o usuário a inserir informações que vão além de uma simples senha, como por exemplo um código enviado por e-mail ou SMS;

§9º . *Framework* de Autenticação: conjunto estruturado de métodos, protocolos e tecnologias que são utilizados para verificar a autenticidade de usuários com base em credenciais digitais

Rua Elvira Ferraz, 250, 4º andar, conj. 411
São Paulo, SP
11 3296-2750
www.abecs.org.br

(ou tokens) verificados pelo emissor e/ou um serviço de autenticação para validar a identidade do portador em diferentes pontos de interação.

§10º . *Payment Passkey*: método de autenticação de pagamentos baseado no padrão internacional FIDO (*Fast Identity Online*), consistente em chave de autenticação digital que substitui a necessidade de senhas tradicionais e utiliza métodos biométricos (como reconhecimento facial, impressão digital ou PIN) para autenticar usuários de forma segura e rápida, conforme descrito no anexo I.

§11º . Verificação de token: processo de Identificação e Verificação (ID&V) que utiliza, na estrutura do *Framework* de Autenticação, métodos específicos de verificação de *tokens*, como a autenticação multifator (MFA) e padrões estabelecidos por entidades como a EMVCo, permitindo que os *tokens* vinculem-se a um dispositivo utilizando chaves, *cookies* ou aplicativos móveis.

§12º . FIDO Alliance (*Fast Identity Online*): aliança aberta da indústria que tem por objetivo reduzir a dependência mundial de senhas, promovendo o desenvolvimento, uso e conformidade com padrões de autenticação, programas de certificação e adoção de mercado.

§13º . *Authentication Requestors*: são todos os provedores de soluções de autenticação aceitas, integrados e homologados junto às IAPs.

Art. 2 Para o desenvolvimento do protocolo de autenticação EMV 3DS, as Associadas terão por base os padrões técnicos descritos nas especificações técnicas disponibilizadas pela EMVCo, bem como para o *Framework* de Autenticação, com base nos padrões descritos nas especificações técnicas disponibilizadas pela FIDO Alliance, sendo objeto deste Normativo a definição do índice de fraudes mínimo, conforme padrões internacionais e a partir de indicadores locais.

Rua Elvira Ferraz, 250, 4º andar, conj. 411
São Paulo, SP
11 3296-2750
www.abecs.org.br

Da Elegibilidade do Protocolo:

Art. 3 Independentemente do tipo ou categoria, qualquer comércio eletrônico em território nacional que realize transações virtuais com cartões de crédito, débito ou pré-pago estará automaticamente elegível à aplicação de métodos de autenticação forte em todas as transações enquanto o índice máximo de fraudes definido tiver sido atingido por um Estabelecimento Comercial, sendo, portanto, uma faculdade do Estabelecimento Comercial enviar pedidos de autenticação de acordo com o Protocolo 3DS ou o "*Framework* de Autenticação" se estiver abaixo deste índice.

§1º . Os Estabelecimentos Comerciais não-conformes que devem adotar o protocolo 3DS e/ou o *Framework* de Autenticação serão levados por Credenciadores / PSPs e/ou Emissores e analisados pelo grupo de trabalho de autenticação e tokenização e/ou do Fórum de Segurança e Prevenção a Fraudes da Abecs.

Art. 4 Os requisitos mínimos para elegibilidade do protocolo são:

I - Ser um cartão de crédito, débito ou pré-pago emitido no Brasil;

II - O Credenciador ou PSP deve ser licenciado no Brasil e o Estabelecimento Comercial deve estar localizado no Brasil;

III - Ter valores de patamar mínimo de conversão, de autenticações silenciosas e de disponibilidade de serviço (BINs ativos no programa), de acordo com metas de desempenho estabelecidas no art. 9º, §4ºdeste Normativo.

Da aderência às normas estabelecidas:

Art. 5 Ficam estabelecidos a Comissão de Arranjos Abertos e o Fórum de Segurança e Prevenção a Fraudes da Abecs compostos por representantes com conhecimento do protocolo, em conjunto com os Instituidores do Arranjo de Pagamentos – IAPs (Bandeiras) para acompanhar os indicadores-chave de desempenho (KPIs) na aplicação do *Framework* de Autenticação e/ou de autenticações 3D-Secure.

Rua Elvira Ferraz, 250, 4º andar, conj. 411
São Paulo, SP
11 3296-2750
www.abecs.org.br

§1º . Os Fóruns estabelecidos no *caput* poderão ser alterados, desde que suportem o mesmo escopo/representatividade;

§2º . Para análise do progresso, serão considerados como índices iniciais os resultados obtidos após 90 (noventa) dias da publicação deste Normativo, e, as medições de frequência mínima serão realizadas trimestralmente após a apuração inicial. A coleta dos resultados será estabelecida em instrumento padronizado paralelo e validado pelos Credenciadores / PSPs;

§3º . O Emissor será responsável por garantir que o patamar mínimo de resposta às requisições dos Estabelecimentos Comerciais seja atingido, cumprindo os requisitos de tempo de resposta esperados e atendendo aos indicadores de conversão e de autenticações silenciosas estabelecidos neste Normativo. Casos pontuais de ataques crônicos de fraude poderão ser tratados separadamente;

§4º . O Credenciador / PSP será responsável por assegurar que os Estabelecimentos Comerciais observem um nível de fraude dentro do tolerável e do permitido, de acordo com os critérios estabelecidos por cada IAP em suas regras usuais, assim como as notificações e contato com os Estabelecimentos Comerciais participantes do sistema.

Da Responsabilidade dos Participantes:

Art. 6 São padrões mínimos esperados dos Estabelecimentos Comerciais (*'Authentication Requestors'*), os quais devem ser fiscalizados pelos Credenciadores / PSPs:

§1º . Executar procedimentos de autenticação multifator para seus clientes;

§2º . Identificar e reportar ao Credenciador / PSP possíveis exclusões à necessidade de autenticação, que, por sua vez, devem ser avaliadas e ratificadas pelo Fórum de Segurança e Prevenção a Fraudes – como por exemplo, mas não se limitando a:
(a) transações iniciadas pelo Estabelecimento Comercial em que a presença do portador não seja requerida – como em transações recorrentes, em arquivo ou digitadas;

Rua Elvira Ferraz, 250, 4º andar, conj. 411
São Paulo, SP
11 3296-2750
www.abecs.org.br

(b) transações de cartões pré-pagos anônimos;
(c) transações com cartões corporativos (exceção feita aos profissionais liberais que atuem de forma autônoma ou no regime de empresa individual);
(d) listas de exceção definidas entre Emissores e Estabelecimentos Comerciais (ex.: elegíveis ao programa do DSS - Débito Online);
(e) outras exceções discutidas e validadas pelo Fórum de Segurança e Prevenção a Fraudes.

§3º . Avaliar o risco de transações e, sempre que possível, sinalizar ao Emissor a classificação de risco no pedido de autenticação, utilizando-se das funcionalidades disponibilizadas pelo protocolo e/ou pelo *Framework* de Autenticação;

§4º . Compartilhar com Emissores todos os dados obrigatórios e recomendados – como, por exemplo (e não se restringindo a): a opção do portador pelo pagamento na função débito ou crédito, a identificação do dispositivo utilizado no pedido de autenticação, informações transacionais do comércio, informações do dispositivo e do portador do cartão – bem como envidar esforços para, em benefício próprio (isto é, aumentar a probabilidade de sucesso na autenticação, inclusive de forma transparente ou silenciosa), complementar com informações corretas e válidas, constantes também na autorização, que estejam disponíveis e que permitam aos Emissores uma análise de risco mais precisa, conforme funcionalidades disponibilizadas pelo protocolo e/ou pelo *Framework* de Autenticação e de acordo com os parâmetros mínimos constantes no "Anexo II", ou mesmo a partir de orientações técnicas das IAPs e fornecedores de serviços de autenticação;

§5º . Não selecionar transações apenas por nível de risco ao submeter pedidos de autenticação completa, utilizando seleção randômica ou todos os atributos do protocolo 3DS na sua integralidade – não apenas baseando-se no risco da transação, mas sim adotando o modelo de compartilhamento de dados previsto pela EMVCo (`*data share only*) para todas as transações em que não se justifique o pedido de uma autenticação completa.

Rua Elvira Ferraz, 250, 4º andar, conj. 411
São Paulo, SP
11 3296-2750
www.abecs.org.br

Art. 7 São responsabilidades dos Credenciadores e Gateways que fornecem serviço de PSP *("Authentication Requestors")*:

§1º . Apoiar os Estabelecimentos Comerciais na implantação e otimização do protocolo EMV 3DS e/ou do *Framework* de Autenticação;

§2º . Ter KPIs dinâmicos por canal e Estabelecimento Comercial, nas etapas de autenticação e autorização, para avaliação da conversão final nas etapas de autenticação e autorização, exceto quando os insumos sejam externos à organização, conforme exemplos no Anexo III;

§3º . Acompanhar a presença e acurácia de dados do portador do cartão que se configurem relevantes para a análise de risco do Emissor, como, por exemplo, e-mail ou celular do comprador, CEP de entrega ou de faturamento etc.;

§4º . Apoiar os Estabelecimentos Comerciais na correção de erros e tomar ações mitigatórias com participantes reincidentes;

Art. 8 São responsabilidades de Emissores e provedores de autenticação para Emissores (ACS ou, em inglês, Servidor de Controle de Acesso e/ou *Token Requestors*):

§1º . Receber, executar e responder às requisições de autenticação e autorização nos intervalos de tempo definidos como padrão pela EMVCo em suas publicações EMV® 3-D Secure (EMV 3DS), Tokenização de Pagamento EMV e FIDO Alliance (*Payment Passkey*);

§2º . Adotar recursos de autenticação silenciosa em casos de exceção em transações de baixo risco, principalmente as baseadas nas informações relativas ao dispositivo utilizado *(device ID* ou *device fingerprint)*;

§3º . Enviar aos Estabelecimentos Comerciais códigos de retorno adequados aos resultados da análise, facilitando o entendimento sobre eventuais negativas, de acordo com o padrão especificado pelas regras da EMVCo e Normativo nº 21 da Abecs;

Rua Elvira Ferraz, 250, 4º andar, conj. 411
São Paulo, SP
11 3296-2750
www.abecs.org.br

§4º . Prover informações que proporcionem um diagnóstico preciso das intercorrências reportadas pelos Estabelecimentos Comerciais e seus provedores de serviço;

Art. 9 Os elementos técnicos disponibilizados nos artigos 3º a 8º não abordam a totalidade do desenvolvimento da solução, sendo que cada Associado é responsável por desenvolver e disseminar o Protocolo 3DS e/ou o *Framework* de Autenticação dentro dos seguintes parâmetros:

§1º . O protocolo 3DS utilizará o padrão técnico definido pelo Consórcio EMVCo, adotado e implementado pelas IAPs.

§2º . *Payment Passkey*: o produto utilizará o padrão técnico definido pelo Protocolo 3DS e/ou do *Framework* de Autenticação (conforme definições de cada IAP) e uma *Payment Passkey* (baseada em autenticação biométrica) adotada e implementada pelas IAPs.

§3º . Extensão: qualquer Estabelecimento Comercial identificado pelo "MID" ou *Merchant ID* afiliado a PSPs dos arranjos de pagamento estará elegível às condições estabelecidas por este Normativo, devendo ser estimulado, apoiado e monitorado pelo Credenciador / PSP *("Authentication Requestor")* a solicitar, na máxima extensão possível, autenticações sempre que se encontrar acima do índice de fraude estabelecido – e quando:

I – estiver como objeto de qualquer programa de risco e segurança das IAPs , como os programas de *chargeback excessivo*, de compliance por alta incidência de fraude

II – em programas de qualidade de dados das IAPs que estabelecem níveis mínimos de desempenho nas transações processadas; ou

III – aos Estabelecimentos Comerciais enquadrados nos casos dos incisos I e II, sugere-se o pedido de autenticação para qualquer valor ou perfil de transação, como forma de mitigar fraudes, conforme diagrama de decisão constante no Anexo IV.

Rua Elvira Ferraz, 250, 4º andar, conj. 411
São Paulo, SP
11 3296-2750
www.abecs.org.br

§4º . Nível de serviço: a observância dos níveis mínimos de desempenho por parte dos demais componentes da tríade de autenticação (Emissor, *"Authentication Requestors"* e IAPs) deverá seguir os parâmetros discutidos e condensados no Fórum de Segurança e Prevenção à Fraudes da Abecs ou outros fóruns com a mesma representatividade, como um processo de melhoria continuada da oferta aos Estabelecimentos Comerciais que adotam o presente Normativo.

Art. 10 A Taxa de Conversão plena às requisições de autenticação EMV 3DS com sucesso, caracterizada pela aprovação mínima na autorização de transações autenticadas sobre total de pedidos de autenticação recebidos, bem como a disponibilidade de BINs ativos nos programas para Emissores é de:

I – Para 2025: 85%;

II – A partir de 2026: 90%;

III – BINS não ativos: não ultrapassar 3% do total de autenticações.

Art. 11 O Índice Mínimo de Autenticações Silenciosas bem-sucedidas via EMV 3DS para Emissores é de:

I – Para 2025: 30%;

II – A partir de 2026: 40%.

§ 1º . Nível de autenticação silenciosa (sem desafio): para este KPI, nas transações EMV 3DS deve-se considerar apenas as transações finalizadas com *Transaction Status* = "Y" sobre o total de pedidos de autenticação – isto é, transações sem requisição de desafio na AReq (Emissor). Não devem ser consideradas neste indicador outras decisões como rejeições antes de se iniciar uma autenticação (TransStatus "N" ou "R"), nem autenticações concedidas pelas IAPs em nome do Emissor (TransStatus "A"). Para transações de baixo risco e baixo valor realizadas via SRC (*Secure Remote Commerce*) , deve-se considerar apenas transações que cheguem na autorização com nível de segurança de uma transação tokenizada e autenticada.

Rua Elvira Ferraz, 250, 4º andar, conj. 411
São Paulo, SP
11 3296-2750
www.abecs.org.br

§2º . Os novos entrantes deverão se atentar ao Anexo IV (diagrama de decisão para Estabelecimentos Comerciais), até que estejam capacitados para aplicar o protocolo EMV 3DS ou soluções que compõem o *Framework* de Autenticação em sua integralidade.

Art. 12 Caso um Emissor não atinja os parâmetros acima estabelecidos por 2 (dois) trimestres consecutivos, o episódio será levado ao Fórum de Segurança e Prevenção a Fraudes da Abecs, após discussões, estas serão levadas ao conhecimento das IAPs que poderão tomar medidas, de acordo com seus regulamentos e as suas respectivas políticas internas, contra reincidências.

Art. 13 Se porventura os Estabelecimentos Comerciais não atenderem ao propósito deste Normativo – qual seja, não pedirem autenticação para todas as compras enquanto estiverem acima do nível mínimo (índice) de fraude sem uma justificativa válida (como a apresentação de uma exceção respaldada pelo Fórum de Segurança e Prevenção a Fraudes da ABECS), cabe às IAPs e Credenciadores / PSPs:

§1º . Investigar o motivo de não cumprimento do Estabelecimento Comercial e definir planos de ação para a adesão do protocolo ou ao *Framework* de Autenticação, com o devido respaldo de indicadores de desempenho e/ou apresentação de casos de sucesso;

§2º . Estimular o referido Estabelecimento Comercial a aderir ao protocolo ou ao *Framework* de Autenticação no menor prazo possível, municiando-o com indicadores comparativos de performance entre transações autenticadas e transações CNP, levando em conta uma composição de custos associados ao tratamento de fraudes e *chargebacks*;

§3º . Apresentar as evoluções junto ao Fórum de Segurança e Prevenção a Fraudes como forma de compartilhamento de melhores práticas.

Art. 14 Criar-se-á o "Selo de Segurança", que poderá ser obtido pelo Estabelecimento Comercial ao seguir as diretrizes do referido Normativo, com a inclusão de boas práticas, sendo que o Fórum de Segurança e Prevenção a Fraudes da Abecs ou equivalente definirá as regras e mecanismos para a obtenção do selo, bem como sua operacionalização (incluindo tempo de

Rua Elvira Ferraz, 250, 4º andar, conj. 411
São Paulo, SP
11 3296-2750
www.abecs.org.br

vigência para que os Estabelecimentos Comerciais possam capitalizar sobre o reconhecimento de que cuidam da segurança de transações *online)*.

Art. 15 As IAPs poderão ajustar suas regras de arranjo, caso entendam necessário, a fim de integrar a aplicação de autenticações fortes às suas normas, bem como envidar os esforços necessários para fazer valer a integridade da proposição de ampliação de autenticações com o objetivo de mitigar fraudes e garantir um serviço de valor aos portadores de cartões.

Art. 16 Os Emissores se comprometem a atingir o patamar mínimo de resposta às requisições de autenticação EMV 3DS e de aumento gradativo dos índices de autenticação silenciosa (*frictionless autentication*), conforme os artigos 10 e 11.

Art. 17 Os Credenciadores e PSPs se comprometem a auxiliar os Estabelecimentos Comerciais associados a atingir os patamares mínimos de solicitação de autenticação previstos nos artigos 10 e 11, enviando as informações técnicas (EMV e "Planilha Abecs de Revisão de Campos 3DS", disponibilizado no site da Abecs) de forma a assegurar a melhor análise de risco possível pelos Emissores e IAPs.

Art. 18 Este Normativo entra em vigor a partir da data de sua publicação, com implementação efetiva 120 (cento e vinte) dias após a data da publicação, sendo, a partir da publicação, parte integrante do Código de Ética e Autorregulação da ABECS para todos os fins específicos.

Publicação:
1ª edição: 21 de agosto de 2024.
2ª edição: 17 de novembro de 2025.

Rua Elvira Ferraz, 250, 4º andar, conj. 411
São Paulo, SP
11 3296-2750
www.abecs.org.br

ANEXO I

FRAMEWORK DE AUTENTICAÇÃO

O que é:

O *Framework* de Autenticação é um conjunto estruturado de métodos, protocolos e tecnologias que serve para verificar a identidade de usuários em ambientes digitais, garantindo que apenas indivíduos autorizados possam acessar determinados recursos ou realizar certas ações. Para tal, pode se utilizar de *tokens* verificados por meio de um fator de autenticação, biometria, autenticação baseada em risco (RBA) e fluxos via 3DS.

Tokens são validados através de desafio gerado pelo emissor via serviço de tokenização de IAPs *("network token")* ou via protocolo EMV 3DS, com base em fatores como: dispositivo, localização e comportamento. Para se garantir a inversão de responsabilidade, devem cumprir todos os requisitos do programa de cada IAP.

O objetivo é garantir a segurança na autenticação sem comprometer a usabilidade, melhorando a experiência do usuário ao potencialmente eliminar a necessidade de inserir manualmente informações sensíveis, permitindo validações invisíveis ou invasivas em caráter mínimo.

Principais vantagens:

O diferencial do framework é a implementação da autenticação via *Payment Passkey,* baseada no padrão FIDO2/WebAuthn.

As *passkeys* são credenciais criptográficas armazenadas localmente em dispositivos confiáveis, protegidas por autenticação biométrica ou PIN. São resistentes a ataques de *phishing*, além de eliminarem a dependência de senhas.

Passkeys são totalmente compatíveis com plataformas modernas (Android, iOS, navegadores e carteiras digitais), permitindo autenticação forte em múltiplos canais, com uma experiência do usuário (UX) unificada.

Rua Elvira Ferraz, 250, 4º andar, conj. 411
São Paulo, SP
11 3296-2750
www.abecs.org.br

Componentes do *Framework*:

1. *Tokens*: protegem as credenciais do cliente ao substituir o número real do cartão por um código seguro, reduzindo o riso de fraudes.
2. Identificação e Verificação de Tokens (ID&V): processo que identifica o portador na criação do *token* ou confirma automaticamente se o *token* ainda é válido no momento da compra ou nas ações em que é requisitado.
3. Autenticação: suporta autenticação via banco emissor (EMV 3DS) ou através de recursos biométricos *(Payment Passkeys)*.
4. Integração com sistemas: conectividade com diferentes plataformas provendo APIs (para integração com sistemas legados), SDKs (para aplicativos de celular), entre outros, proporcionando uma autenticação unificada.
5. Suporte para carteiras digitais globais (chamadas *digital wallets)*: *framework* preparado para aceitação de *tokens* e autenticação via carteiras digitais na modalidade *pass-through*.

Benefícios do *Framework* de Autenticação:

Segurança: Reduz a exposição de dados sensíveis ao utilizar *tokens* dinâmicos e autenticação biométrica, FIDO2 e 3DS.

Facilidade de Uso: Elimina etapas manuais com validações silenciosas ou por dispositivos confiáveis, reduzindo abandono.

Escalabilidade: Suporta picos de vendas (como Black Friday ou datas sazonais), sem provocar falhas sistêmicas.

Flexibilidade: APIs compatíveis com diferentes sistemas (ERPs, *gateways*, apps, plataformas de *wallets*), vários tipos de *checkout* (por exemplo, o SRC – *Secure Remote Commerce*) e capacidade de serem embutidas no *front-end* do comércio.

Principal vantagem na aplicação do *Framework*:

Utilização de autenticação via *Payment Passkey* (autenticação biométrica) em todos os canais ou tipos de *checkout* (*Guest checkout*, *Card on file* e *Click to Pay*).

Payment Passkeys são credenciais de autenticação criptográficas baseadas nos padrões FIDO (*Fast Identity Online*) que permitem que os usuários façam login e pagamentos em aplicativos e sites utilizando o mesmo processo que usam para desbloquear seus dispositivos, como biometria ou PIN. A autenticação via *Passkey* é projetada para ser resistente a *phishing* e oferece uma experiência de autenticação segura e sem senhas.

Rua Elvira Ferraz, 250, 4º andar, conj. 411
São Paulo, SP
11 3296-2750
www.abecs.org.br

Casos de uso:

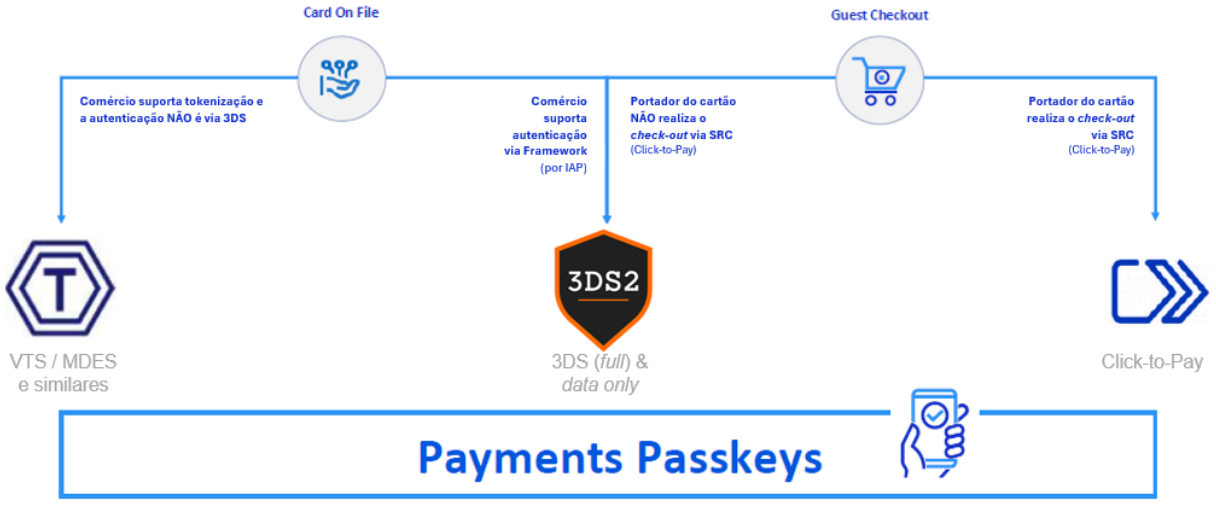
1. Assinaturas e Pagamentos Recorrentes (MIT, ou transações iniciadas pelo Estabelecimento Comercial)
2. *Card on File* + 1ª transação (CIT, ou transações iniciadas pelo cliente)
3. *Guest checkout* (CIT, ou transações iniciadas pelo cliente)
4. Transações não tokenizadas (CIT, ou transações iniciadas pelo cliente)

Quadro-resumo:

TIPO DE *CHECKOUT*	TIPO DE TRANSAÇÃO	TECNOLOGIA EMPREGADA
ASSINATURAS E PAGAMENTOS RECORRENTES	MIT (TRANSAÇÃO INICIADA PELO EC)	VERIFICAÇÃO DE *TOKEN* (ID&V)
***CARD ON FILE* + 1ª TRANSAÇÃO**	CIT (TRANSAÇÃO INICIADA PELO CLIENTE)	*PAYMENT PASSKEYS*
GUEST CHEKOUT	CIT (TRANSAÇÃO INICIADA PELO CLIENTE)	*PAYMENT PASSKEYS* E AUTENTICAÇÃO PASSIVA
TRANSAÇÕES NÃO TOKENIZADAS	COF, SRC E MIT (TRANSAÇÕES INICIADAS PELO CLIENTE)	3DS

COMO AS SOLUÇÕES SE COMBINAM

O *Framework* de Autenticação permite a combinação estratégica de diferentes tecnologias para otimizar a segurança e a experiência do usuário em diversos fluxos de pagamento.



Rua Elvira Ferraz, 250, 4º andar, conj. 411
São Paulo, SP
11 3296-2750
www.abecs.org.br

ANEXO II

Critérios para elegibilidade para aplicação do *Framework* de Autenticação

- **Índice de Fraude >= 20 pontos base ("*basis points*") em algum das IAPs em 3 meses consecutivos.**

$$\text{Índice de Fraude} = \frac{Valor\ Total\ de\ Transações\ Reportadas\ como\ Fraude}{\text{Valor Total de Transações Aprovadas}} \times 10.000\ (em\ pontos\ base)$$

Rua Elvira Ferraz, 250, 4º andar, conj. 411
São Paulo, SP
11 3296-2750
www.abecs.org.br

ANEXO III

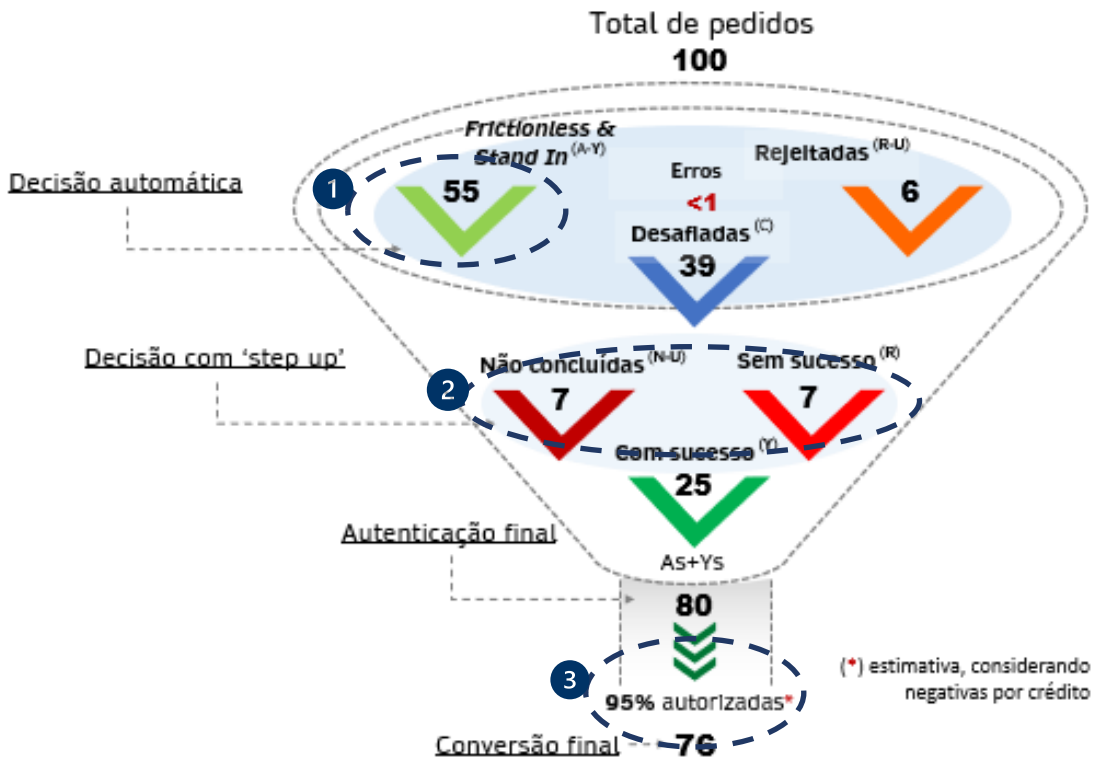
INDICADORES-CHAVE PARA MONITORAMENTO DE DESEMPENHO DE ESTABLECIMENTOS COMERCIAIS PELOS CREDENCIADORES / PSPs:

Indicadores de Conversão EMV 3DS

Objetivos primários:

(A) sugerir melhorias para os Estabelecimentos Comerciais através dos PSPs *("3DS Servers")*; (B) avaliar performance por Emissor (do ponto de vista do Estabelecimento Comercial) em termos de: (1) nível de autenticação silenciosa, (2) nível de falhas no desafio (autenticação sem sucesso) e (3) autorização das autenticações com sucesso.

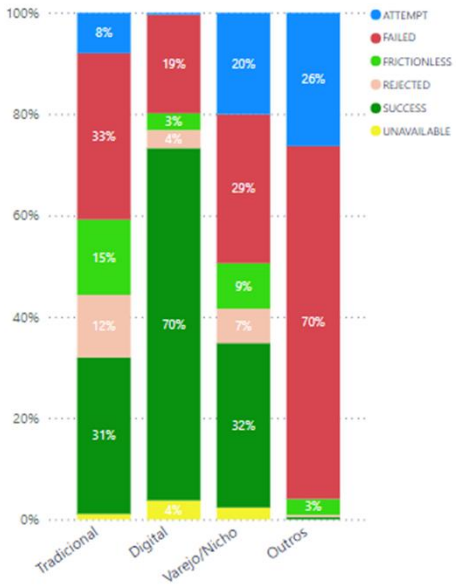
Exemplo:



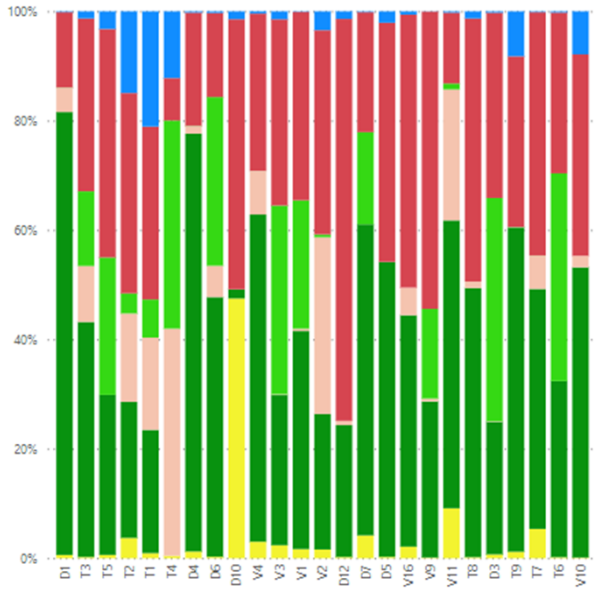
Rua Elvira Ferraz, 250, 4º andar, conj. 411
São Paulo, SP
11 3296-2750
www.abecs.org.br

Exemplos de KPIs dinâmicos (por níveis) para gestão de performance no 3DS:

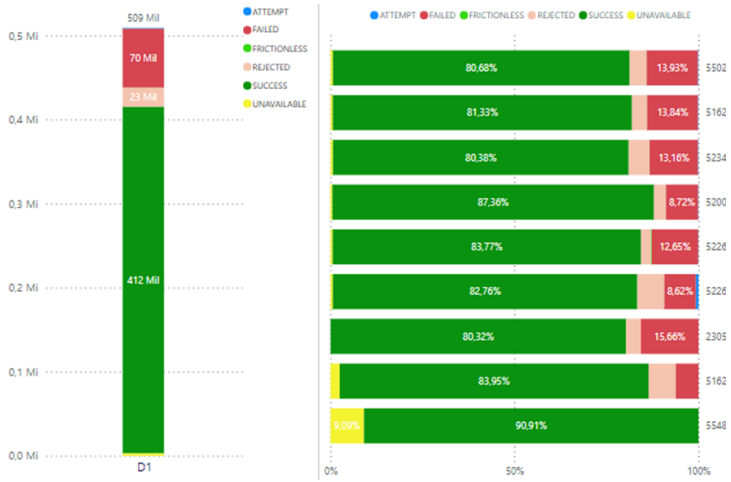
POR GRUPO



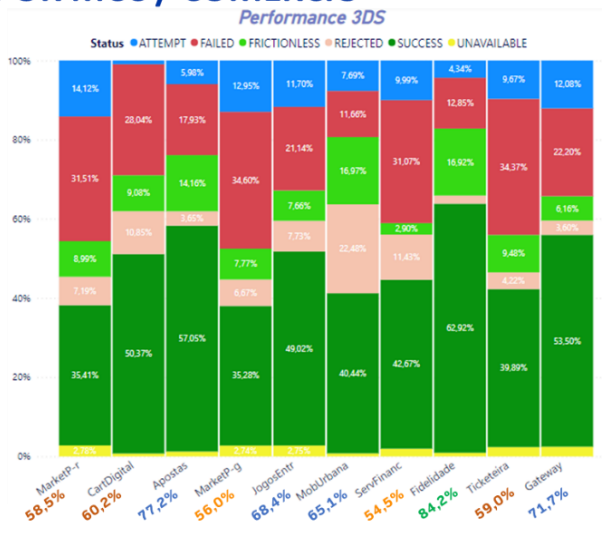
POR EMISSOR



POR PRODUTO / BIN



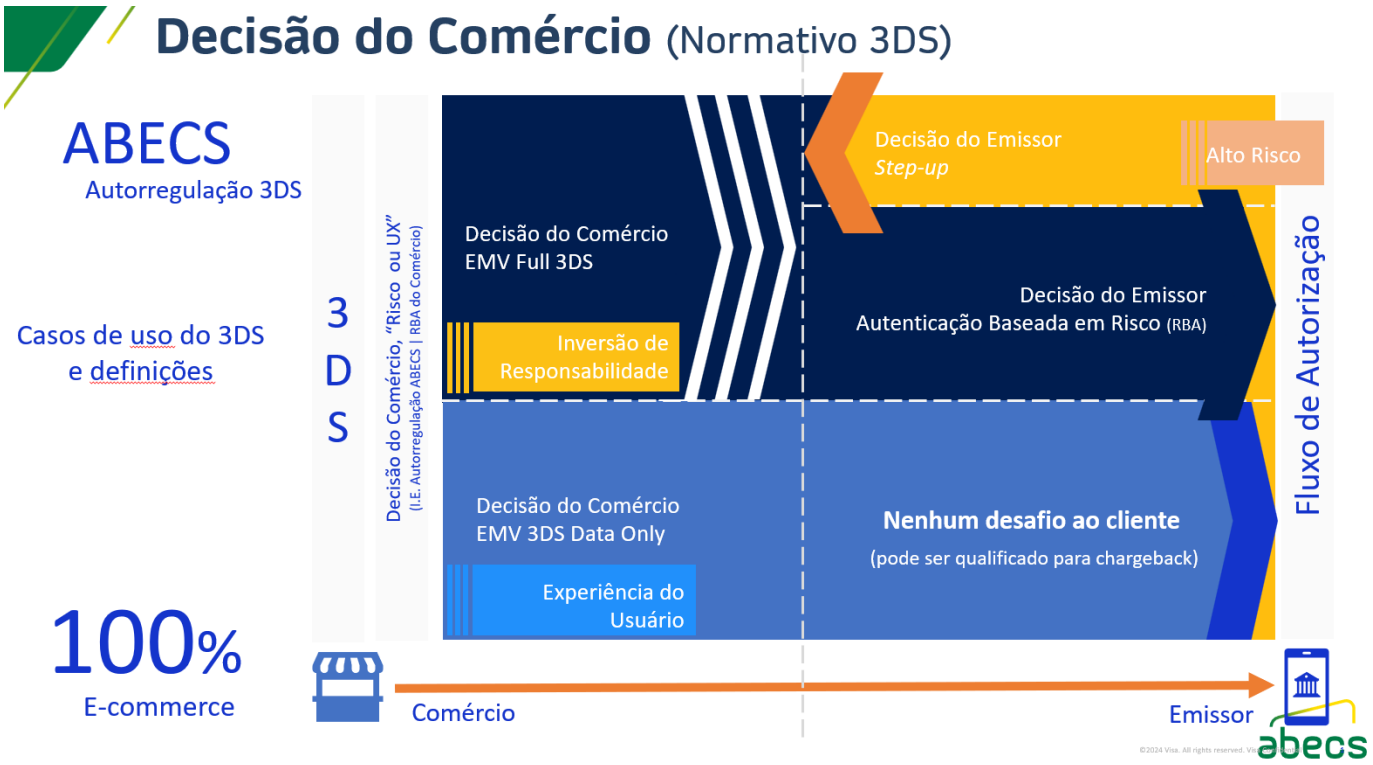
POR MCC / COMÉRCIO



Rua Elvira Ferraz, 250, 4º andar, conj. 411
São Paulo, SP
11 3296-2750
www.abecs.org.br

ANEXO IV

DIAGRAMA-REFERÊNCIA DE DECISÃO PARA ESTABELECIMENTOS COMERCIAIS:



Rua Elvira Ferraz, 250, 4º andar, conj. 411
São Paulo, SP
11 3296-2750
www.abecs.org.br