GT TOKENIZAÇÃO

Guia rápido de melhores práticas para credenciadoras e gateways

abecs

Credenciadoras e gateways de pagamento exercem um papel extremamente importante no sistema de pagamentos, oferecendo aos comércios, além da captura das transações e sua liquidação junto às marcas (bandeiras), serviços adicionais como operação dos checkouts, autenticação de portadores nas compras online, proteção contra fraudes e outros serviços importantes para o processo de pagamentos.

A proteção dos dados de cartões tem sido um dos maiores desafios da indústria de pagamentos ao longo dos anos. Com o rápido crescimento das transações não presenciais e as compras por meio do canal e-commerce, informações de cartões estão armazenadas em centenas de locais e a proteção dos dados sensíveis se torna mais complexa. A tecnologia de Tokens de Pagamento foi desenvolvida para oferecer uma alternativa digital às transações realizadas com os cartões tradicionais.

Além de oferecer mais segurança, os tokens têm um índice de aprovação maior, pois possuem menor risco para os emissores.

Com a implantação da tecnologia de tokenização, credenciadoras e gateways têm a oportunidade de oferecer um serviço de alto valor agregado aos comércios associados, operando o provisionamento e a gestão do ciclo de vida dos tokens para os seus clientes.

A importância dos tokens para os comércios

Um dos fatos marcantes dos sistemas de pagamento nos últimos anos foi o crescimento vertiginoso das compras online, impulsionado pela necessidade de isolamento social imposta pela pandemia de COVID-19.

Na mesma escala, foi visível o aumento das tentativas de fraude, utilizando os mais diversos métodos. As compras não presenciais têm sido alvo privilegiado das transações fraudulentas, utilizando dados de cartões roubados.

VERSÃO AGOSTO/22

BONS MOTIVOS PARA A IMPLANTAÇÃO DE TOKENS DE PAGAMENTO:

Oferece segurança dos pagamentos
Tokens de pagamento protegem os dados dos clientes e reduzem os riscos de violação de dados.

Amplia a confiança do cliente
Informe ao cliente que as informações sobre suas preferências de pagamento estão seguras pelas mais modernas tecnologias oferecidas pelas bandeiras, reduzindo os riscos de fraudes das transações de cartão não presente (CNP).

Aumenta as taxas de conversão
Os tokens de pagamento são mais seguros, em particular para transações recorrentes, permitindo maiores índices de aprovação.

Cria experiências inovadoras para os clientes
A jornada de compras do cliente se torna mais simples e segura e está em linha com a evolução dos pagamentos, como compras inApp, usando dispositivos wereable e IoT (Internet das Coisas).

Reduz os requisitos de PCI
Os dados dos tokens não são considerados dados sensíveis de um cartão, o que simplifica a aplicação dos recursos de segurança da indústria de pagamentos.

Alavanca o uso de "Credenciais de Pagamento"
O futuro do sistema de pagamentos está baseado no uso de credenciais seguras de pagamento por compradores e vendedores. A adoção dos tokens de pagamento para os clientes é o primeiro passo nessa direção.

TOKENIZAÇÃO E PCI

Os tokens substituem os números de cartão armazenados nos cadastros dos clientes, oferecendo proteção contra roubos, invasões e sequestros de dados. Ao eliminar esses dados sensíveis, o comércio simplifica os requisitos de segurança, em conformidade com as diretrizes do PCI e da LGPD[1].

Tokens de pagamento não são considerados dados sensíveis de cartão e estão associados a condições de uso que reduzem as possibilidades de fraudes (associados a uma wallet, a um dispositivo, provisionados para um determinado comércio etc.).

Dessa forma, a adoção da tokenização reduz o escopo da certificação PCI e elimina a necessidade de uso de cofres de segurança para armazenar dados de cartões.

		Elemento de dados	Armazenamento permitido	Converter dados armazenados ilegíveis conforme Requisito 3.4
Dados contábeis	Dados do titular do cartão	O número da conta principal (PAN)	Sim	Sim
		Nome do titular do cartão	Sim	Não
		Código de serviço	Sim	Não
		Data de vencimento	Sim	Não
	Dados de autenticação confidenciais	Dados de rastreamento completo	Não	Não armazenável conforme Requisito 3.2
		CAV2/CVC2/CVV2/CID	Não	Não armazenável conforme Requisito 3.2
		PIN/Bloco de PIN	Não	Não armazenável conforme Requisito 3.2

Os requisitos 3.3 e 3.4 do PCI DSS aplicam-se apenas ao PAN. Se o PAN for armazenado com outros elementos dos dados do titular do cartão, somente o PAN deverá ser convertido como ilegível de acordo com o Requisito 3.4 do PCI DSS.

Dados de autenticação confidenciais não devem ser armazenados após a autorização, mesmo se forem criptografados. Isso se aplica mesmo onde não há PAN no ambiente. As organizações devem entrar em contato diretamente com seu adquirente ou empresa de pagamento para saber se é permitido armazenar o SAD (Sensitive Authentication Data, ou dados de autenticação sensíveis) antes da autorização, por quanto tempo quaisquer que sejam os requisitos de proteção e utilização.

[1] *As demais informações confidenciais do cliente continuam exigindo do comércio as medidas de proteção adequadas, de acordo com a LGPD.*

TOKENIZAÇÃO É PRIORIDADE PARA AS BANDEIRAS

Todas as bandeiras que operam no Brasil estabeleceram a tokenização como sua prioridade, com o objetivo de ampliar a segurança nas transações digitais, oferecer maior comodidade aos usuários e preparar a infraestrutura de pagamentos para o futuro digital, utilizando os recursos de velocidade e capacidade das redes (5G) e integração invisível (Internet das Coisas – IoT), Open Finance, entre outros recursos. Mais que uma forma de proteção para o momento atual, a tokenização, aliada a outras tecnologias como a autenticação, são preparativos para o futuro dos pagamentos.

A partir deste ano, AMEX, ELO, MASTERCARD e VISA estão acelerando seus programas de implantação da tecnologia e incentivando a adesão dos participantes do sistema de pagamentos. As bandeiras oferecem aos participantes do sistema ampla documentação técnica e ferramentas de integração que aceleram a implantação das novas tecnologias.

A OPORTUNIDADE DE AMPLIAÇÃO DO PORTFÓLIO DE SERVIÇOS

Pequenos e médios lojistas encontram dificuldades para desenvolver, implantar e operar um sistema de gestão de tokens, em função dos requisitos técnicos, custos envolvidos, certificações e escala operacional. Ao mesmo tempo, a oferta de serviços de tokenização por provedores independentes certificados ainda é muito pequena. Dessa forma, credenciadoras e gateways podem ser agentes estratégicos para a disseminação do uso de tokens.

Pesquisas por amostra realizadas pela ABECS junto a comerciantes, credenciadoras e gateways definiram o seguinte cenário:

- 65% dos comércios que responderam à pesquisa já implementaram serviços de tokenização.
- 60% desses comércios usam serviços oferecidos por credenciadoras, gateways e provedores independentes.
- 55% das credenciadoras e gateways que responderam à pesquisa ainda não oferecem tokenização aos seus clientes e a maioria ainda não iniciou projeto de implantação dos serviços.

É importante destacar que essas amostras compreendem ainda um segmento bastante restrito dos participantes do sistema, o que significa que existe um amplo espaço para crescimento no futuro e que a janela de oportunidades é bastante relevante.

Disseminar o uso de tokens significa **ampliar o volume de conversão de transações** online e ao mesmo tempo **criar maiores barreiras às fraudes,** nas transações com cartão não presente (CNP), transações recorrentes e prestação de serviços online.

ESTIMULANDO O COMÉRCIO A ADOTAR A TOKENIZAÇÃO

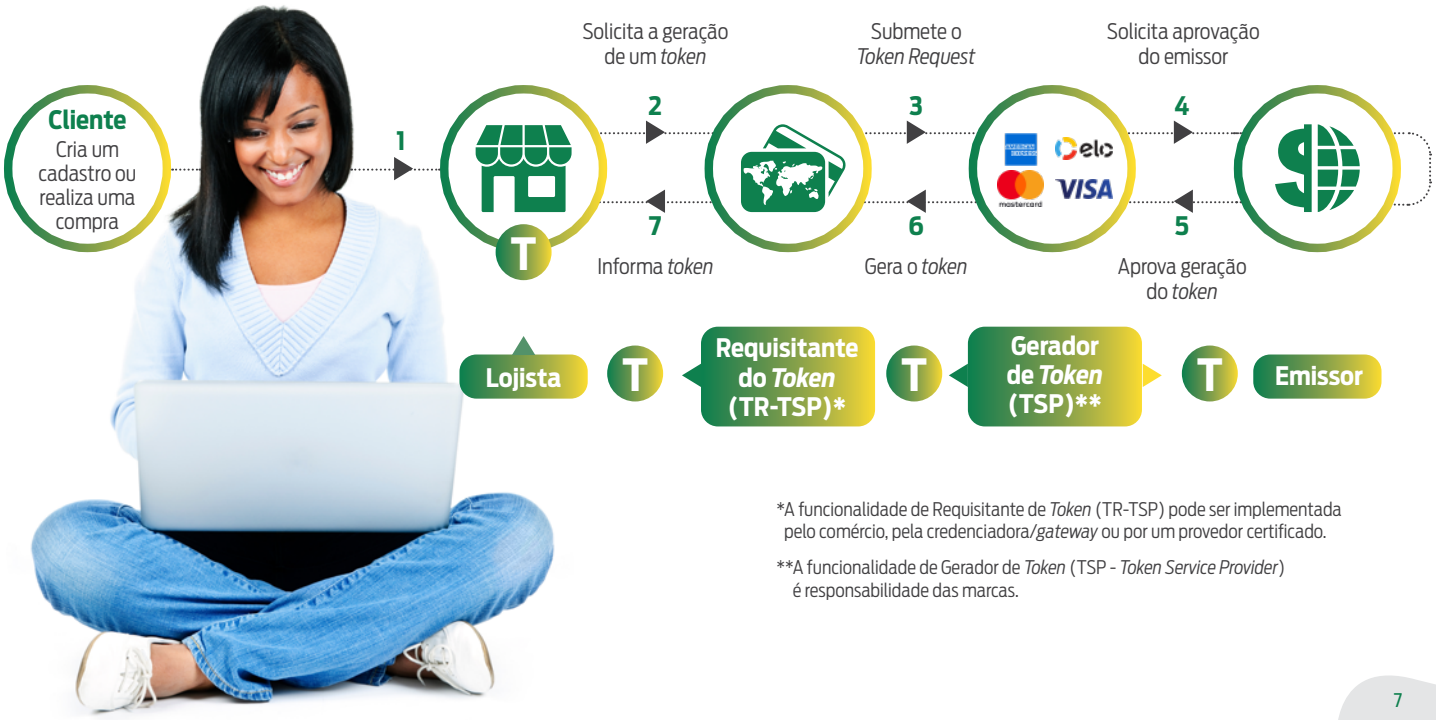
Algumas credenciadoras e gateways de pagamento estão utilizando programas de comunicação com o comércio para incentivar a adoção de tokens. Além de páginas explicativas em seus sites, materiais específicos como infográficos, folders e outros recursos levam ao comércio as informações mais relevantes sobre a importância de aderir à tokenização.

Além dos aspectos de segurança, os tokens oferecem uma vantagem adicional para os comércios que operam com transações recorrentes e cartões em arquivo: os tokens são atualizados automaticamente nas bandeiras, quando o cartão é renovado ou substituído por perda, roubo ou extravio. No momento da atualização dos tokens na bandeira, os comércios terão à sua disposição os 4 últimos dígitos do novo cartão associado ao seu token, para mostrar ao cliente que nenhuma ação de atualização cadastral é necessária para que ele continue usufruindo o relacionamento com o estabelecimento comercial.

REQUISIÇÃO DE TOKENS PELOS COMÉRCIOS

A requisição de tokens (função de Token Requestor-TSP) em nome dos comércios é uma atividade de valor agregado para aumentar a proteção das transações contra fraudes, oferecer maior comodidade aos clientes e melhorar a conversão de transações, principalmente para as compras de e-commerce e transações recorrentes.

A figura a seguir apresenta o fluxo de requisição de tokens por um estabelecimento comercial:



*A funcionalidade de Requisitante de *Token* (TR-TSP) pode ser implementada pelo comércio, pela credenciadora/*gateway* ou por um provedor certificado.

**A funcionalidade de Gerador de *Token* (TSP - *Token Service Provider*) é responsabilidade das marcas.

ONBOARDING DA TOKENIZAÇÃO

Existem alguns modelos de implementação da tokenização que representam estratégias distintas de negócio, mas atendem ao objetivo central de eliminar os dados sensíveis dos cartões, em particular o PAN, dos cadastros dos comércios, reduzindo os riscos de fraudes.

Dentre os modelos de implementação, temos:

1- Através de um provedor independente(TR-TSP)

a. Atualmente há dois modelos básicos de prestação de serviços de gestão de tokens.
   i. Tokens criados em nome da Credenciadora ou Gateway – Neste caso, os tokens ficam hospedados no prestador, que oferece ao comércio uma chave de identificação que associa o token ao cliente da loja.
   ii. Tokens criados em nome do Comércio – Neste caso, após a geração do token, este é enviado à loja para que seja incluído no cadastro do cliente.

b. Toda a gestão e controle dos tokens ficam a cargo do provedor.

c. Implementação pronta para o comércio, se seu Adquirente/Gateway já for TR-TSP.

2- Licenciar uma plataforma já desenvolvida e homologada

3- Desenvolver a solução in-house

a. Abrir um projeto com cada bandeira.

b. Desenvolver e testar o processo de tokenização via APIs.

c. Certificação com cada bandeira.

d. Prazo de implementação de cerca de 6 meses, dependendo. dos tempos de desenvolvimento e testes integrados.

Para mais informações, os interessados devem procurar os contatos de relacionamento de cada bandeira.

PROVISIONANDO TOKENS PARA OS COMÉRCIOS

Atuando em nome dos comércios, credenciadoras, gateways de pagamentos e outros provedores de serviços podem solicitar a geração (provisionamento) de um token em nome do seu cliente, receber as mensagens enviadas pelas bandeiras e comandar as atualizações correspondentes, em cada caso do ciclo de vida dos tokens:

- Requisitar tokens
- Registrar a ativação do token
- Registrar a suspensão/reativação do token
- Registrar o cancelamento do token
- Processar a alteração dos 4 últimos dígitos do cartão, associados ao token
- Processar a alteração da arte do cartão

A solicitação de um token pode ser iniciada em momentos como:

- O cadastramento de um novo cliente – No momento em que o cliente cria ou altera dados do seu cadastro e informa dados do cartão, é iniciado o procedimento de solicitação do token. Caso a solicitação seja executada com sucesso, as informações sobre o token recebidas da bandeira devem ser registradas e os dados originais do cartão podem ser descartados.
- A realização de uma transação – No checkout, antes do fechamento da transação, os dados do cartão são utilizados para solicitar o provisionamento de um token. Caso o processo seja bem-sucedido, os dados do token podem substituir os dados originais do cartão, que podem ser descartados. Caso o provisionamento seja negado, os motivos de negativa podem ser avaliados para definir os próximos passos (confirmação dos dados com o cliente, substituição do cartão ou nova tentativa).

TOKENIZANDO O LEGADO DE CARTÕES ARMAZENADOS NOS CADASTROS DOS COMÉRCIOS

O comércio possui uma grande quantidade de números de cartão (PAN) armazenados em arquivos e sujeitos a vazamentos e invasões. Auxiliar os comércios a substituir rapidamente os números de cartões por tokens é uma ação importante para aumentar a proteção contra as fraudes.

É importante desenvolver, juntamente com os comércios, as estratégias para que a tokenização do legado de cartões seja eficaz. Algumas sugestões que podem tornar a operação mais produtiva:

- Fazer a pré-seleção dos cartões candidatos, priorizando aqueles que realizam mais transações.
- Descartar os cartões vencidos que não realizaram transações em período recente.
- Solicitar tokens para os cartões que estiverem com data de expiração próxima.

Existem dois métodos possíveis para executar um processo rápido de migração do legado de cartões:

- Utilizando um processo batch – As bandeiras disponibilizam processos para submeter lotes de cartões (Bulk File) para a geração de tokens. Cada bandeira disponibiliza a documentação de suporte para o desenvolvimento dessas rotinas.
- Utilizando um processo online – Neste caso, as requisições de tokens podem ser submetidas em ciclos, a partir da leitura de uma lista de cartões a tokenizar, emulando uma atividade online.

Seguem algumas recomendações para comércios, credenciadoras e gateways de pagamento que decidam realizar a migração rápida para os tokens.

1. Informar à bandeira a programação de execução da atividade. Dessa forma, a bandeira poderá avisar aos emissores, para evitar que essa migração seja entendida como uma tentativa de fraude.

2. Não enviar requisições para apenas um BIN ou conjunto de BINs do mesmo emissor, para evitar a sobrecarga dos processos do Emissor.

3. Estabelecer critérios de prioridade de migração dos cartões, procurando tokenizar os cartões que mais realizam transações em primeiro lugar. Se possível, executar uma atividade de limpeza do cadastro, eliminando cartões que estão inativos em um período elevado.

4. Processar a log de execução das requisições de tokens para medir a eficiência do processo e identificar as maiores incidências de negativas de provisionamento dos tokens, com seus respectivos códigos de resposta. O Subgrupo de Processos da ABECS, assim como os representantes técnicos das bandeiras, poderão auxiliar no contato com os emissores, para solucionar eventuais volumes elevados de negativas.

RECOMENDAÇÕES PARA OS PRESTADORES DE SERVIÇOS DE TOKENIZAÇÃO

A implantação dos tokens de pagamento no Brasil ainda está em fase de amadurecimento e o grande desafio para todos os participantes é equalizar o conhecimento sobre a tokenização e aplicar as melhores práticas no uso dos tokens, aproveitando assim todo o potencial que a tecnologia oferece.

Os grupos de trabalho de Tokenização da ABECS acompanham o uso da tecnologia junto a todos os participantes do sistema e registrou em seus estudos alguns aspectos, que devem ser considerados:

Bandeiras

- O grau de avanço na implantação da tokenização ainda é diferenciado entre as bandeiras e ainda não existe entre elas um plano comum, em relação às datas-limite de implantação da tecnologia.
- A quantidade de transações tokenizadas ainda é pequena, em relação ao total de transações realizadas, mas tende a crescer drasticamente no próximo ano.

Emissores

- O grau de maturidade da tecnologia entre os emissores ainda é heterogêneo, considerando as bandeiras suportadas, os tipos de cartão (débito e crédito) e os métodos de comunicação (mensagens ISO 8583 ou APIs).
- Ainda no universo dos emissores, existem significativas diferenças no nível de implementação da gestão do ciclo de vida dos tokens, do processo de requisição até a substituição de cartões vencidos e cancelamento de tokens. Nem todos seguem todo o ciclo aplicando as melhores práticas sugeridas pelo “standard”.

Comércios, Credenciadoras e Gateways

- Em vários casos identificados, a geração de tokens não resultou na eliminação dos dados sensíveis do cartão dos cadastros, o que significa que os riscos de segurança persistem.
- Nos casos nos quais o número do cartão não foi eliminado, foram identificadas situações em que o PAN não está protegido de acordo com os padrões do PCI. Proteger o PAN nessas condições é um requisito de segurança indispensável.

CICLO DE PROVISIONAMENTO DE TOKENS POR BANDEIRA

As bandeiras incentivam os emissores a implantar e manter processos de provisionamento de tokens específicos para os comércios nessa etapa de transição, como forma de acelerar a adoção da tecnologia. Todas oferecem APIs de integração que permitem a rápida implantação de solicitações de provisionamento de tokens, em fluxos simplificados.

As respostas a uma solicitação de provisionamento de token para os comércios se resumem às opções de aprovado e negado. Nessa etapa da implantação, as bandeiras não estão exigindo dos comércios uma etapa adicional de autenticação (ID&V – Identificação e Verificação), o que poderá ser utilizado no futuro como forma de aumentar o grau de confiança em um token.

Em caso de negativa, as bandeiras enviam aos solicitantes informações adicionais como:

- Cartão inválido
- Data de expiração inválida
- Código de segurança inválido (quando presente)
- Erro de processamento no emissor

Nos três primeiros casos, o Solicitante do Token deve decidir se solicita que o portador confirme as informações digitadas ou se pede que ele registre um cartão diferente. Quando ocorrer um erro no processo, o Solicitante deve planejar o envio de nova solicitação, considerando as vantagens e desvantagens de fazê-lo imediatamente ou em um momento posterior.

Os diagramas a seguir mostram como cada Marca (bandeira) trata os códigos de retorno para o provisionamento dos tokens.
A recomendação é que os processos de solicitação de provisionamento de tokens sejam realizados sempre por API.

A AMEX permite que os comércios requisitem tokens utilizando mensagens ISO ou APIs.

Nas mensagens ISO, o comércio poderá receber os seguintes códigos de retorno no Elemento de Dados (DE) 39 (ou "Bit 39"):

- 000 = Aprovado
- 001 = Aprovado com identificação
- 100 = Recusado
- 101 = Cartão expirado / data de validade inválida
- 107 = Por favor, entre em contato com o emissor
- 109 = Estabelecimento inválido
- 111 = Conta inválida

Códigos de Resposta (Response Codes)		
Status Code	**Mensagem de Status (Status Message)**	**HTTP Status Code**
4211	Invalid Field Lenght (comprimento de campo inválido)	400
4212	Account Number Invalid (número de conta inválido)	404
8999	Internal Server Error (erro interno do servidor)	500
0000	Success (sucesso)	200

Campo	Formato	Obrigatoriedade	Descrição
sk_score	String (1)	Sim	Indica o score de risco (risk score). - G (green) - Aprovado - Y (yellow) - Autenticação adicional requerida. Exemplo: One-time Password (OTP) - R (red) - Negado Obs.: para tokenização de Card-on-File , a resposta do Issuer é "R" (red) ou "G" (green).
risk_reason	String (3)	Condicional	Indica a razão para o score. Este campo trará o motivo real quando o score for "R". Se o emissor for capaz de avaliar o risco para o cartão (risk assessment), deve retornar '0000' com a cor recomendada. Se a cor for "R", deve, conforme mencionado, fornecer o reason code no campo de risk_reason. Os possíveis valores incluem: * 001 - CID incorreto e data de validade. * 203 - o cartão não pode ser provisionado devido a um status inválido ou outras razões. * 204 - suspeita de fraude no cartão. * 206 - o cliente excedeu o limite máximo de cartões (tokens). * 207 - muitos tokens associados ao mesmo dispositivo. * 209 - o cliente excedeu o número máximo de dispositivos. * 'Em branco' são scores do tipo red devido a outras razões de fraude.
status_code	String (4)	Sim	Indicador do status de resposta (response status).

Na VISA, o provisionamento de tokens pelos comércios deverá ser realizado sempre por API. Não existe rotina de provisionamento de tokens nos comércios, utilizando mensagens ISO.

A API de solicitação de provisionamento retornará os campos actionCode e reason:

Campo	Descrição
actionCode	**Códigos de Status de Ação** **Formato: é um dos seguintes valores:** 00 - Aprovação incondicional (provisionar e ativar imediatamente para pagamentos). 85 - Aprovação condicional (provisionar, mas não ativar até que uma verificação adicional do cliente seja realizada). Qualquer código de rejeição presente diferente de 00 ou 85 vai impedir o provisionamento do dispositivo. **Negativa de aprovação devido a uma das seguintes razões:** N7 - falha no CVV2 14 - PAN inválido 54 - data de expiração inválida 05 - recusa genérica 96 – erro interno de sistema no emissor

Códigos de erro (Response Codes)

Se aparecer um erro de processo, se assume que nenhum erro padrão foi detectado no pedido via API. Os códigos de razão relativos a erros de processo no domínio específico do VTS são os seguintes:

Error Code Field (campo do código de erro)	Error Code Description (descrição do código de erro)
ISS_ERROR_REQUIRED_DATA_MISSING	Dados requeridos faltantes
ISS_ERROR_INVALID_FIELD_LENGHT	Comprimento de campo inválido
ISS_ERROR_INVALID_FIELD_TYPE	Tipo de campo inválido
ISS_ERROR_CRYPTOGRAPHY_ERROR	Erro de criptografia
ISS_ERROR_INVALID_FIELD_VALUE	Valor de campo inválido
ISS_ERROR_PAN_INELEGIBLE	Pan inelegível
ISS_ERROR_INVALID_EXPIRATION_DATE	Data de expiração inválida
ISS_ERROR_INTERNAL_SYSTEM_ERROR	Erro interno de sistema
ISS_ERROR_CVV2_FAILURE	Falha no CVV2

A Visa permite a utilização de processo adicional de autenticação (ID&V), utilizando uma API específica para essa finalidade, como parte do programa denominado DAF – Digital Authentication Framework.

A API de solicitação de provisionamento retornará os seguintes códigos:

- 00 – Green Path – Appove
- 05 – Red Path – Decline

Por enquanto, a API utilizada pelos comércios não retorna o código 85 – Yellow Path, utilizado para solicitar um fator adicional de autenticação (ID&V). Seu uso está previsto para o futuro e permitirá que o comércio obtenha um nível de segurança superior no provisionamento dos tokens.

A ELO não implementou códigos específicos de retorno para o provisionamento de tokens. Existe um conjunto de códigos de retorno para os mais variados tipos de erro que podem acontecer, incluindo erros na aplicação.
Os códigos de erro associados de maneira mais comum ao provisionamento são:

- **404:** Falha nos dados enviados para a requisição (alguma informação enviada pela API não foi encontrada na plataforma de tokenização a dados devem ser revistos).
- **412:** Dados não preenchidos na requisição ou inválidos a dados devem ser revistos e preenchidos adequadamente.
- **422:** Falhas técnicas ou internas na aplicação de tokenização a contatar a bandeira para entendimento e avaliação.
- **108:** "Product not able to tokenize card". Isso ocorre quando o BIN que se deseja tokenizar não está apto para esse tipo de transação. Nesse caso, o lojista deve solicitar que se tente outro cartão, pois com esse não será possível prosseguir.

Tratamento dos Códigos de Segurança

Segundo as diretrizes do EMVCo, implementadas pelas bandeiras, a presença do Código de Segurança **não é obrigatória no provisionamento, mas, se ele for informado, deve estar correto.**

MONITORAÇÃO DA PERFORMANCE DE REQUISIÇÃO DE TOKENS

A implantação de consultas, relatórios e alertas que permita avaliar a performance dos serviços de tokenização ainda não chegou ao nível de granularidade ideal, que permita medir resultados por:

- Bandeira
- Emissor
- Tipo de cartão (débito ou crédito)

A maior granularidade da análise permitirá o endereçamento mais eficaz das soluções junto às bandeiras e emissores e a identificação de erros e não conformidades com maior facilidade.

O GT recomenda que comércios, credenciadoras e gateways implementem controles que permitam identificar em detalhes onde o uso encontra bons resultados e onde ainda persistem problemas operacionais que impedem a performance esperada.

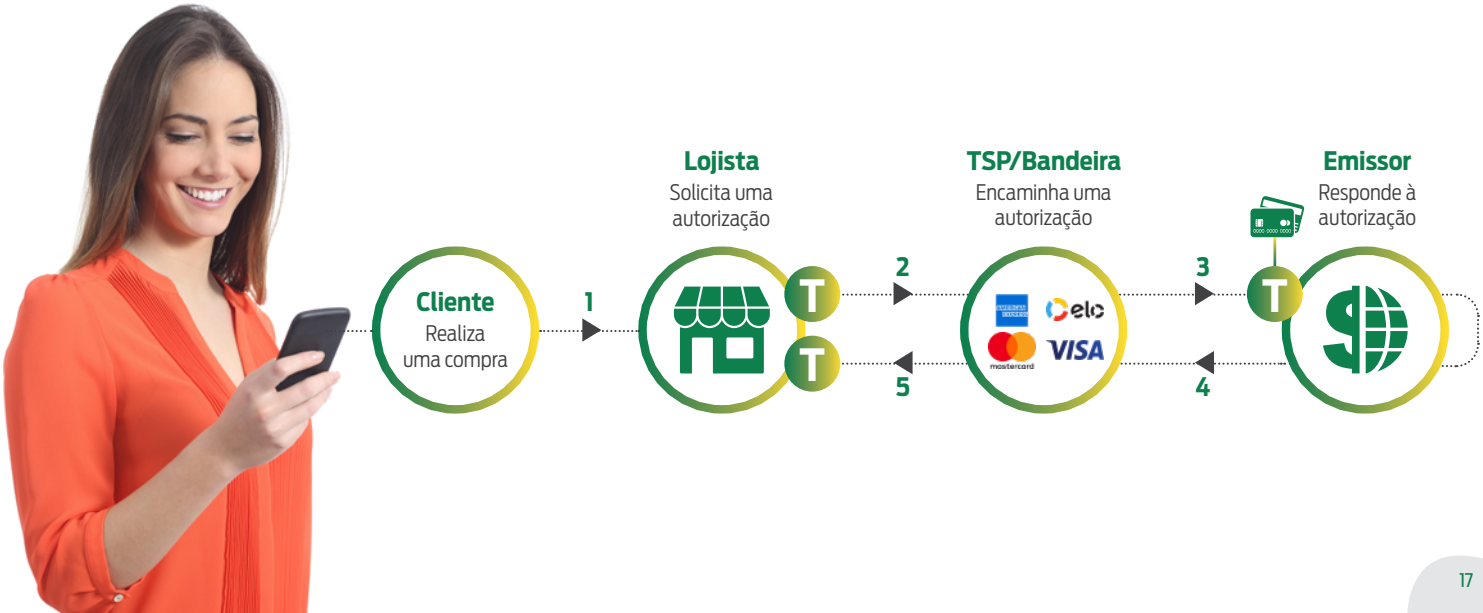
A seguir, apresentamos um exemplo de relatório de controle para o provisionamento de tokens:

Resultado	Janeiro		Fevereiro		Março		Abril		Maio		Junho	
	Qtde	% sobre o total	Qtde	% sobre o total	Qtde	% sobre o total	Qtde	% sobre o total	Qtde	% sobre o total	Qtde	% sobre o total
Aprovadas												
Informações adicionais												
Negadas												
Total de requisições												

AUTORIZAÇÕES COM *TOKENS*

Nas mensagens de autorização utilizando tokens, lojistas, gateways de pagamento e credenciadoras não utilizam o PAN, mas a credencial armazenada em seus cadastros, obtida durante o processo de provisionamento.

Caberá à bandeira estabelecer a correlação entre token e o número do cartão (PAN), enviando para o emissor as duas informações (PAN e credencial associada utilizada na autorização).



É necessário atentar para a existência dos campos e domínios específicos para as transações realizadas com tokens, para que não sejam recusadas pelas bandeiras.

Vale lembrar também que a implantação da tokenização implica na certificação das atividades de requisição de tokens, autorização e gestão do ciclo de vida junto às bandeiras com as quais a entidade opera.

DESEMPENHO DA AUTORIZAÇÃO

Pesquisas realizadas em localidades onde a tokenização já está em estágio mais avançado mostram que os números referentes à conversão de transações, redução de abandono de carrinhos e proteção contra fraudes tendem a ser melhores com o uso de tokens. As principais razões são o aumento da confiança entre os participantes do sistema (consumidores, comércio e emissores) e a redução do interesse dos fraudadores sobre portfólios tokenizados.

No Brasil, o acompanhamento mensal de indicadores, realizado pelo GT Token da ABECS, já demonstra a elevação dos níveis de conversão de transações nos comércios e portfólios de cartões que implantaram processos bem ajustados de tokenização.

Se for possível fazer um paralelo com a implantação do Chip, é provável que em um futuro breve se observe a fraude migrando para os portfólios e comércios não protegidos.

É importante que a migração para a tokenização seja acompanhada e monitorada em todas as etapas, incluindo a autorização. O acompanhamento dos indicadores de transações realizadas e aprovadas com tokens, versus as transações realizadas e aprovadas com PAN, permitirá controlar o ritmo da evolução e melhorar os processos ao longo do percurso.

No tratamento dos motivos de negativa de autorização com tokens é importante selecionar apenas aqueles motivos efetivamente associados ao uso do token.

Outros motivos, como saldo insuficiente ou conta cancelada, devem ser desconsiderados. A explicação é que, no caso da transação, essa seria negada mesmo que fosse realizada usando um cartão físico.

Por outro lado, é importante considerar motivos típicos de negativas associadas ao uso de tokens:

- Mau funcionamento ou indisponibilidade do sistema.
- Código de Segurança Inválido. Lembrar sempre que a presença do Código de Segurança é opcional, mas, quando presente na transação, precisa estar correto.

Apresentamos a seguir um exemplo de relatório que pode auxiliar na monitoração da performance da autorização das transações, utilizando tokens:

Exemplos de relatório

AUTORIZAÇÕES PROCESSADAS											
Janeiro		Fevereiro		Março		Abril		Maio		Junho	
% *Token*	% PAN	% *Token*	% PAN	% *Token*	% PAN	% *Token*	% PAN	% *Token*	% PAN	% *Token*	% PAN
4,8%	95,2%	4,9%	95,1%	4,8%	95,2%	8,2%	91,8%	8,4%	91,6%	8,3%	91,7%

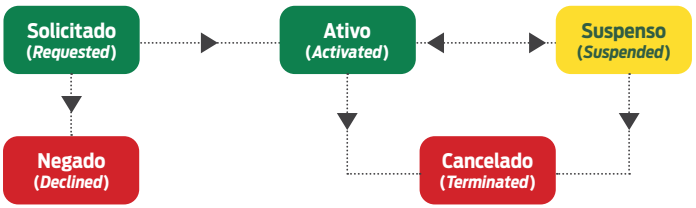
AUTORIZAÇÕES APROVADAS											
Janeiro		Fevereiro		Março		Abril		Maio		Junho	
% *Token*	% PAN	% *Token*	% PAN	% *Token*	% PAN	% *Token*	% PAN	% *Token*	% PAN	% *Token*	% PAN
4,8%	95,2%	4,9%	95,1%	4,8%	95,2%	8,2%	91,8%	8,4%	91,6%	8,3%	91,7%

Dessa forma, será possível identificar oportunidades para melhorar a conversão de autorizações, com base no uso de *tokens*.

CICLO DE VIDA DOS *TOKENS*

Tokens, assim como os cartões físicos e outras entidades em nosso sistema de pagamentos, possuem um ciclo de vida que precisa ser gerenciado pelos participantes, cada qual cuidando das etapas sob sua responsabilidade.

A figura abaixo mostra os estados (status) que um token pode receber, ao longo do seu Ciclo de Vida.



Estes estados são alterados por ações comandadas pelos Emissores, pelos Comércios e pelas bandeiras e o controle da situação de um token é responsabilidade das bandeiras, que enviam mensagens de atualização para os participantes.

Casos em que o comércio ou seu representante deve utilizar os comandos do ciclo de vida dos tokens:

- Receber os 4 últimos dígitos do número do cartão e a nova data de expiração, quando o plástico for renovado e o token atualizado pelo emissor (PAN Update comandado pelo emissor e mensagem recebida pelo comércio).
- Comandar o cancelamento do token. Situações:
  - Conta encerrada
  - Vazamento ou invasão de contas
  - Identificação de evento de fraude
  - Comandar a suspensão de um token – suspeita de fraude em análise

APIs PARA A GESTÃO DO CICLO DE VIDA DOS TOKENS

As bandeiras oferecem APIs de integração que permitem o gerenciamento do ciclo de vida dos tokens, permitindo que os comércios administrem os tokens provisionados para o seu uso. Elas facilitam a implantação dessas tarefas e sua integração com outras atividades de gestão dos estabelecimentos.

PREVENÇÃO CONTRA FRAUDES

O principal benefício oferecido pela tokenização é a eliminação dos riscos de apropriação indevida dos dados sensíveis do cartão, armazenados nos cadastros dos comércios e checkouts de pagamento.

Os tokens são gerados com parâmetros específicos e, por esse motivo, o seu uso fora das condições definidas (por exemplo, para o estabelecimento comercial para o qual ele foi provisionado) implicarão na negativa da autorização da transação.

CREDENCIAIS EXPOSTAS A INVASÕES E VAZAMENTOS DE DADOS

A utilização de tokens não vai impedir que aconteçam invasões ou vazamentos de dados, mas reduzirá significativamente os impactos financeiros de um evento dessa natureza. Vale lembrar que uma invasão ou vazamento pode expor o Comércio ou a Credenciadora/Gateway às consequências do não cumprimento da LGPD (exposição indevida de dados pessoais), mas evitará que fraudadores utilizem cartões obtidos nessa ação para provocar fraudes em massa em curto período.

Porém é importante que os comércios, credenciadoras, gateways de pagamento e outros provedores colaborem com a segurança e integridade do sistema, executando ações de proteção, quando um evento dessa natureza for identificado e confirmado.

Ações sugeridas:

- Comunicar a ocorrência imediatamente.
- Executar rotinas de solicitação de cancelamento ou suspensão de tokens gerados a seu pedido.
- Restaurar as condições de segurança do seu ambiente, antes de solicitar o provisionamento de novos tokens, para substituir os tokens comprometidos.

REFORÇANDO A SEGURANÇA DAS TRANSAÇÕES

A utilização conjunta dos protocolos de autenticação 3D Secure, principalmente nas suas novas versões (2.1, 2.2 e caminhando para a 2.3), com a tokenização oferece um alto nível de segurança contra compras não reconhecidas e uso indevido dos dados do cartão, além de garantir a inversão de responsabilidade da transação, em caso de não reconhecimento pelo portador.

É importante reafirmar que 3D Secure e Tokenização são tecnologias complementares:

3D Secure

Implementa a Autenticação Forte do Cliente (SCA)

Eu sei

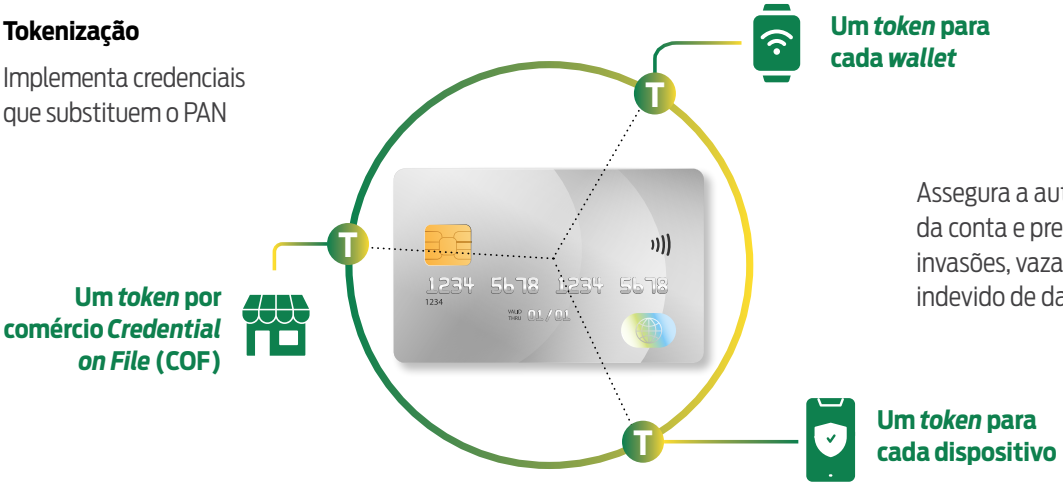
Eu tenho

Eu sou

Assegura a autenticidade do comprador e previne contra contestações por compra não reconhecida

Tokenização

Implementa credenciais que substituem o PAN



Assegura a autenticidade da conta e previne contra invasões, vazamentos e uso indevido de dados do cartão

Saiba mais:

AMEX | ELO* | EMVCo | MASTERCARD | VISA

abecs

abecs.org.br

**Manual de certificação ainda não disponível*