GT TOKENIZAÇÃO

Guia rápido de melhores práticas para emissores

abecs

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 através do canal *e-commerce*, informações de cartões estão armazenadas em centenas de locais, e a proteção dos dados sensíveis se torna mais complexa.

Os pagamentos digitais estão se tornando uma realidade irreversível. Acompanhando esta evolução, a tecnologia de *Tokens* de Pagamento surgiu para oferecer uma alternativa digital às transações realizadas com os cartões tradicionais.

Em sua essência, *tokens* são credenciais digitais equivalentes a um cartão, com recursos de proteção e segurança adicionais ao modelo tradicional. Os *tokens* consistem em credenciais do portador, registradas em cada um dos comércios onde ele realiza transações regularmente e armazenadas nos seus dispositivos como *notebooks*, *smartphones*, relógios digitais e etc.

Os padrões de tokenização foram definidos pelo Consórcio EMV (EMVCo) e implementados pelas principais bandeiras (marcas) internacionais, se transformando num padrão mundial da indústria de pagamentos.

VERSÃO ABRIL/2022

OS PRINCIPAIS BENEFÍCIOS DO USO DOS *TOKENS*:

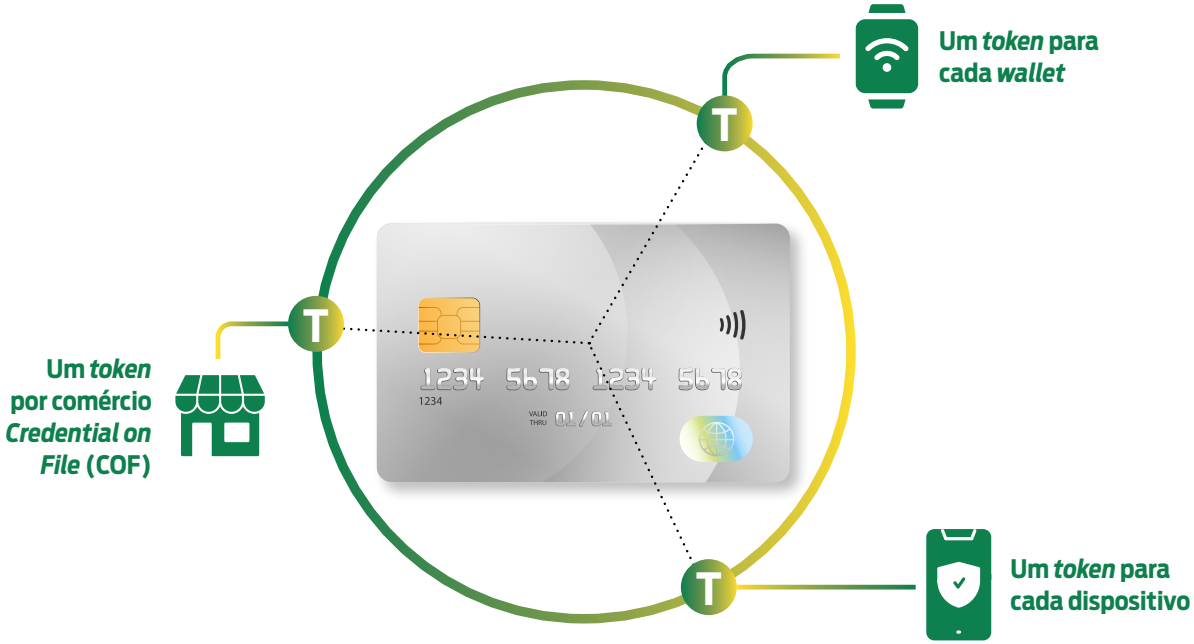
Para os emissores

- **Oferece segurança para o portador** ao embarcar toda a tecnologia de tokenização nas compras não presenciais.
- **Aumenta as taxas de autorização** graças à validação prévia dos dados pelo emissor e à atualização automática dos dados do cartão.
- **Atualiza os dados do cartão com comodidade e rapidez** para o portador, garantindo suas compras recorrentes (como assinaturas ou serviços cobrados em ciclos contínuos).

Para os comércios

- **Diminui o impacto de vazamento de dados.** Em essência, o *token* é formado a partir da criptografia de dados e possui parametrizações que inibem o uso em possíveis vazamentos.
- **Aumenta as taxas de conversão de vendas** graças à validação prévia dos dados pelo emissor e à atualização automática dos dados do cartão.
- **Aumenta os índices de fidelização**, pois o cartão é atualizado automaticamente, ao ser armazenado no cadastro do *e-commerce*.

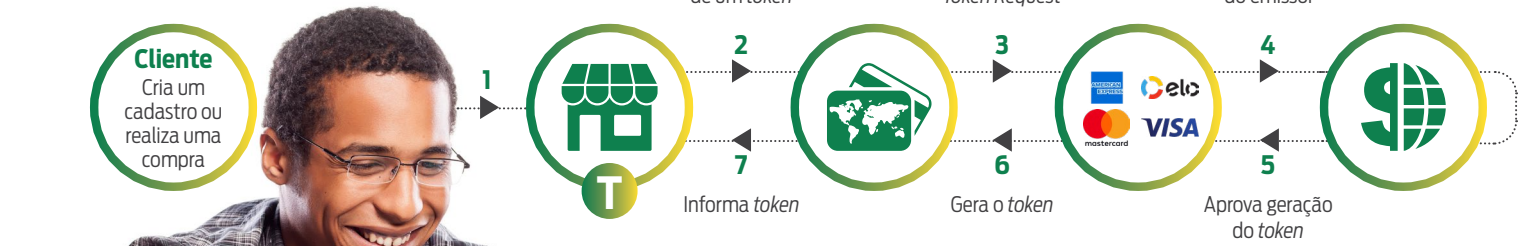
Podem ser gerados inúmeros *tokens* associados a um mesmo cartão, destinados às carteiras digitais, dispositivos IoT (como *smart watches*) e para cadastramento nos comércios, como mostra a figura a seguir:



Este documento se dedicará a apresentar dicas de melhores práticas para os *tokens* dedicados aos comércios.

REQUISIÇÃO DE *TOKENS* PELOS COMÉRCIOS

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.

RECOMENDAÇÕES PARA OS EMISSORES

A seguir, apresentamos algumas recomendações de boas práticas para os emissores, com base nas definições das bandeiras:

- O **provisionamento** de *tokens* para os comércios pode ser **simplificado** em relação a *wallets*. Desta forma, os emissores incentivam os comércios a substituir os números de cartão armazenados em seus cadastros por *tokens* (credenciais), reduzindo riscos de vazamento de dados sensíveis e invasão de bases cadastrais.

- É recomendável que se provisione um novo *token* sempre que possível, independentemente do saldo da conta, **desde que a conta esteja habilitada para realizar transações**.

- Sempre deve ser considerado que **a presença do Código de Segurança é opcional**. Por isso, o provisionamento de um *token* não deve ser negado unicamente pela ausência do Código de Segurança. Se ele estiver presente, execute sua validação e, caso esteja incorreto, negue o provisionamento.

TRANSAÇÕES REALIZADAS COM *TOKENS*

As solicitações de autorização de transações utilizando *tokens* podem ser iniciadas pelos próprios portadores do cartão (transação do tipo "CIT", ou *Consumer Initiated Transaction* em inglês), ou pelo comércio ("MIT" – *Merchant Initiated Transaction*).

A presença de um criptograma de *token* numa transação de *e-commerce* garante que houve um processo válido de autenticação do cliente e que a bandeira assegura a validade do *token*.

Nas transações iniciadas pelo comércio (MIT), o emissor deve analisar os dados que identificam a transação e considerar estes valores em sua lógica de decisão.

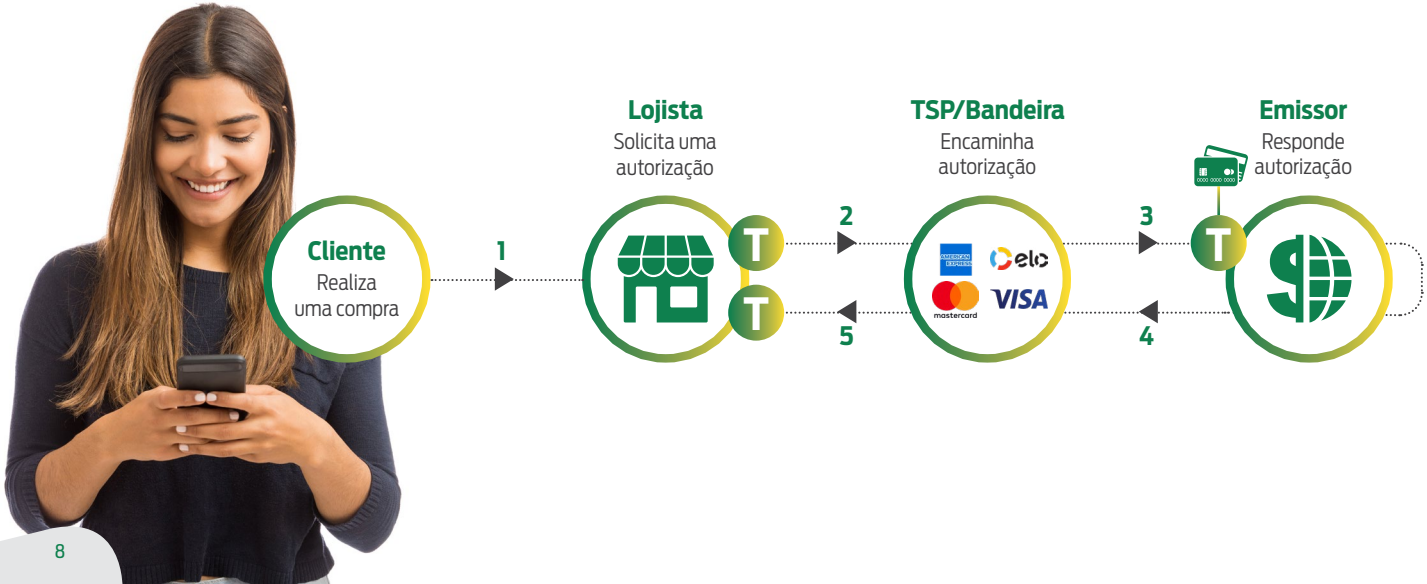
RECOMENDAÇÕES PARA OS REQUISITANTES (TR-TSPs)

Ao obter um *token* junto ao emissor, repasse aos estabelecimentos comerciais a referência dos 4 últimos números do cartão associados a este *token* e um código de identificação do *token*, para que os estabelecimentos possam eliminar de seus cadastros os dados sensíveis dos cartões.

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 PAN, enviando para o emissor as duas informações (PAN e credencial associada utilizada na autorização).



RECOMENDAÇÕES PARA OS EMISSORES

A prática tem demonstrado a necessidade de implementar **regras específicas de autorização** para transações que usam *tokens*, de forma a aproveitar ao máximo os recursos de segurança, oferecer mais flexibilidade para o processo e melhorar os índices de conversão de vendas.

Alguns casos de regras específicas reportados por emissores participantes do Grupo de Trabalho de Tokenização da ABECS demonstraram aumento do índice de aprovação de transações de maneira segura. Alguns exemplos de utilização em regras de negócio:

- Validade do *token.*
- Associação do *token* ao portador ou ao comércio que submeteu a autorização.
- Dados da mensagem de autorização associadas ao uso de *tokens* para transações CNP (cartão não presente), transações recorrentes etc.

Ao negar um pedido de autorização que utilizou um *token*, é recomendável que se procure utilizar códigos de retorno adequados para identificar a causa raiz da negativa de autorização. O uso excessivo de códigos genéricos (como o "05 = *do not honor*") deve ser evitado.

Considerando que **a presença do Código de Segurança é opcional**, não se devem negar as autorizações realizadas com um *token* unicamente pela ausência do Código de Segurança. Se ele estiver presente, é indicado que se execute sua validação antes e que se negue uma autorização apenas no caso do Código de Segurança estar incorreto.

É importante que os emissores realizem análises comparativas de performance de autorização, considerando os índices de aprovação com PAN e com *token*.

Exemplos de relatório

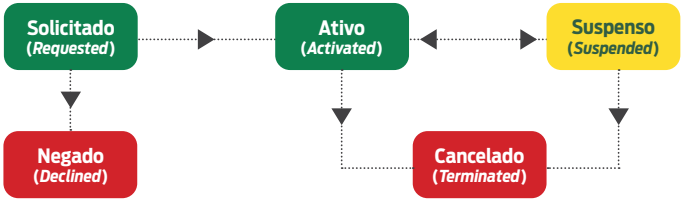
AUTORIZAÇÕES PROCESSADAS											
Janeiro		Fevereiro		Março		Abril		Maio		Junho	
% *Token*	% PAN	% *Token*	% PAN	% *Token*	% PAN	% *Token*	% PAN	% *Token*	% PAN	% *Token*	% PAN
4,8%	95,2%	4,9%	95,1%	4,8%	95,2%	8,2%	91,8%	8,4%	91,6%	8,3%	91,7%

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%

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

CICLO DE VIDA DOS *TOKENS*

Os *tokens* seguem um ciclo de vida independente de um cartão ativo, conforme a imagem apresentada a seguir:



Portanto, cada *token* criado pode ser gerenciado individualmente, oferecendo maior flexibilidade e segurança para os pagamentos.

As ações de manutenção no cadastro de cartões tokenizados devem ser comunicadas às bandeiras, de forma a permitir a atualização automática de todos os *tokens* associados, evitando negativas de autorização desnecessárias e ações do portador do cartão para atualizar seus cadastros nos comércios.

Importante lembrar que é necessário atualizar os dados das bandeiras quando:

- O número do cartão mudar, momento em que se deve informar o novo final de número do cartão.
- A arte (ou *layout*) do cartão mudar, para que a nova arte seja apresentada ao consumidor, sempre que isso for possível e necessário (nas *wallets*, por exemplo).

A gestão do ciclo de vida dos *tokens* pode ser feita a partir da utilização de mensagens ISO 8583. Porém, as APIs são instrumentos mais eficientes para se fazer o gerenciamento do ciclo de vida dos *tokens*, uma vez que se adicionam funcionalidades inexistentes no modelo ISO. Por isso, sua implementação é altamente recomendável para garantir maior flexibilidade no futuro.

RECOMENDAÇÃO PARA TRATAMENTO DE *TOKENS* EM RENOVAÇÃO DE PLÁSTICOS

Quando um novo plástico é personalizado para substituir um cartão próximo ao seu vencimento, todos os *tokens* ativos devem ser atualizados com os dados do novo número do cartão criado, utilizando o serviço de "*PAN UPDATE*" oferecidos via API ou ISO 8583 pelas bandeiras. Assim, **não é necessário cancelar os *tokens* já criados**, evitando negativas de autorização desnecessárias e requisições de novos *tokens* pelos comércios.

RECOMENDAÇÃO PARA TRATAMENTO DE *TOKENS* EM REPOSIÇÃO POR PERDA/ROUBO OU EXTRAVIO

Quando um novo plástico é personalizado para substituir um cartão perdido/roubado ou extraviado, todos os *tokens* ativos podem ser atualizados com os dados do novo número do cartão criado, utilizando o serviço de '*PAN UPDATE*' via API ou ISO 8583. Da mesma forma, **não é necessário cancelar os *tokens* já criados**, evitando assim negativas de autorização desnecessárias e requisições de novos *tokens* pelos comércios.

Veja um resumo destas dicas práticas:

DISPOSITIVO VINCULADO	CREDENCIAL EM ARQUIVO – *TOKEN E-COMMERCE*
• Mantenha o *token*. O dispositivo continua seguro[1].	• Se o *token* foi provisionado antes do evento de perda ou roubo, mantenha o *token*. • Se o *token* foi provisionado após o evento de perda ou roubo, suspenda o *token* e confirme a atividade com o portador do cartão.

[1]Presume-se que qualquer tentativa de provisionamento será mal sucedida devido aos parâmetros de risco e requisitos de autenticação.

Para mais informações, consulte a documentação técnica de cada bandeira e conheça os recursos disponíveis para o provisionamento, ativação, suspensão e cancelamento de *tokens*.

PREVENÇÃO CONTRA FRAUDES

Regras específicas de autorização para *tokens* permitem a implementação de ações baseadas em métodos de prevenção dedicados, que por sua vez proporcionam maior controle sobre as autorizações, redução dos índices de fraudes e maior eficiência nas conversões de transações.

É importante lembrar que, na ocorrência de uma **evidência de fraude** em um *token*, **não é necessário tomar ação com os demais *tokens* existentes**. A ação pode ser dirigida apenas ao *token* em questão, promovendo sua suspensão ou cancelamento. Comunicadas sobre esta ação, as bandeiras informarão o solicitante da credencial em tempo real para que, a partir do incidente, tome qualquer providência que achar necessária.

Também é importante lembrar que, na ocorrência de uma evidência de **fraude num PAN tokenizado, não é necessário cancelar os *tokens* gerados antes do evento**. A melhor ação é gerar um novo cartão substituindo o PAN comprometido e fazer um '*PAN UPDATE*' com o novo número de cartão, associando-o a esses *tokens*.

O que fazer quando o dispositivo é perdido ou roubado

DISPOSITIVO VINCULADO	CREDENCIAL EM ARQUIVO – *TOKEN E-COMMERCE*
• Delete os *tokens* vinculados ao dispositivo.	• Confirmar com o titular do cartão qual atividade de pagamento ocorreu (com estes *tokens*) no dispositivo antigo. • Excluir os *tokens* em que o titular do cartão não pôde impedir o acesso do dispositivo antigo.

Tratamento de transações suspeitas de fraude

DISPOSITIVO VINCULADO	CREDENCIAL EM ARQUIVO – *TOKEN E-COMMERCE*
• Se a transação não foi realizada pelo *token* do dispositivo, mantenha o *token* do dispositivo. • Se a transação foi realizada pelo *token* do dispositivo, confirme a atividade com o portador. • Se for confirmada uma atividade suspeita com o *token*, envie comando de delete para o *token*.	• Se a transação suspeita aconteceu antes da data de provisionamento, mantenha o *token*. • Se a transação suspeita aconteceu após a data de provisionamento, suspenda o *token* e confirme a atividade com o titular do cartão. • Se for confirmada uma atividade suspeita com o *token*, envie comando de delete para o *token*.

CREDENCIAIS EXPOSTAS A INVASÕES E VAZAMENTOS DE DADOS

Para *tokens* provisionados antes da data de identificação do incidente, **mantenha os *tokens*** (um '*PAN UPDATE*' deverá ser enviado para cada *token* comprometido).

Para os *tokens* provisionados depois da data de identificação do incidente, confirme o provisionamento e as atividades do *token* com o portador do cartão. Se forem identificadas atividades suspeitas com o *token*, **delete o *token***.

Saiba mais:

AMEX | ELO | EMVCo | MASTERCARD | VISA*

abecs

abecs.org.br

*Após login, acessar: Products > Digital Solutions > Visa Token Service > Resources