3D Secure 2.0

cashless 3.0

Gerencie a autenticação do portador do cartão durante a realização de compras no e- & m-commerce

tas group
an owl company

A solução Access Control Server (ACS) implementa o novo Protocolo de autenticação EMVCo 3-D Secure 2.0, de acordo com os requisitos PSD2. O protocolo estende o seu escopo do e-commerce para o m-commerce, o qual foi projetado para fornecer uma experiência de usuário segura e amigável ao cliente durante o processo de compra. Os Emissores podem verificar a identidade do portador do cartão durante as compras on-line, com recursos completos para:

- Controlar o cadastramento do portador do cartão
- Determinar se um determinado PAN está cadastrado no Programa VbV / Identity Check
- Estabelecer a autenticação do portador de cartão
- Calcular o CAVV / AAV e enviar uma mensagem de autenticação à loja virtual

Administração completa baseada em parâmetros e relatórios de gestão, podendo ser facilmente integrado a qualquer Sistema Processamento de Cartões, sendo totalmente aderente e compatível com PCI-3DS.

Características

O cl 3D Secure 2.0 é um módulo da plataforma **cashless 3.0** que conta com uma estrutura modular, permitindo aos emissores e processadores operar processos de autenticação baseados nas especificações 3-D Secure 2.0 e altamente configurável.

Módulo de Cadastramento

- Verifica a identidade do portador do cartão (com base na informação de pré-cadastramento)
- Permite ao portador do cartão estabelecer um método de autenticação
- Utilização de diferentes métodos de cadastramento, incluindo:
  - Cadastramento no Web Site do Emissor
  - O portador de cartão acessa a página Web de cadastramento do Emissor, fornece os dados de seu cartão, informações pessoais e cria uma mensagem segurança e senha

cl 3D Segurança dos dados

- Criptografa o PAN antes de armazená-lo em uma base de dados segregada, retornando o valor de um token; O PAN é exibido em formato mascarado
- O mesmo "tratamento do token" é usado para os dados pessoais do portador do cartão
- Fornece os recursos de autenticação segura
- Fornece informações de trilha de auditoria para os eventos de segurança
- A arquitetura prevê que os dados do portador do cartão não estejam armazenados dentro da zona desmilitarizada (DMZ)
- Infraestrutura em conformidade com o PCI-3DS

Módulo de Relatórios

- Geração de relatórios das atividades de cadastramento e das transações de autenticação, facilitando o monitoramento operacional e gereciamento de disputa.
  Os relatórios podem incluir:
  - Estatísticas das transações autenticadas com sucesso, falha na autenticação, número de tentativas de cadastramento, cadastramentos bem-sucedidos e malsucedidos
  - Dados individuais das transações de autenticação tanto das bem-sucedidas como das malsucedidasl

Módulo de Autenticação

- Permite ao Emissor verificar a identidade do portador do cartão ao finalizar a compra on-line
- Suporta Autenticação Forte do Cliente (SCA: Stronger Customer Authentication) e o SCA Exemption, promovendo um sistema sem fricção no processo de checkout
- Possui a autenticação segura através de IDs dos usuários e autenticação de multifator (MFA) tanto para o acesso administrativo como para autenticação do portador do cartão durante o processo de checkout
- Opções de SCA incluindo:
  - Autenticação biométrica – a melhor maneira de autenticar o titular do cartão
  - OTP via SMS – o método mais comum em caso de falhas da autenticação biométrica
  - OTP Token (baseado em tempo) – isso requer um dispositivo ou gerador de token
  - OTP CAP / DPA – isso requer um PCR (leitor de cartão pessoal) e uma aplicação no chip EMV
  - OTP via IVR - isso requer que o cliente tenha um número de telefone ou celular; permite ao Banco cadastrar seus clientes desde que já tenha as credenciais do Home Banking
- Gerencia as chaves AAV / CAVV fornecendo evidência dos resultados da autenticação de uma transação de pagamento durante uma compra on-line

Console Administrativa

- Permite facilmente o gerenciamento da configuração paramétrica
- Permite a configuração e manutenção dos portadores de cartão, emissores, servidores de interoperabilidade
- O controle do acesso é realizado por meio de uma função de gerenciamento

SDK para Aplicativos Móveis

- Adequado para os dispositivos iOS e Android

As funcionalidades cl 3D-Secure também estão disponíveis como SaaS a partir dos Data Centres de TAS Group.