Playbook

Convego® Service Broker and Token Cockpit
GIVE BACK THE PAYMENT #CX TO THE CUSTOMER

Introduction
How can customers have control over who has access to their payments data? What if someone gets hold of card numbers and CVV codes, and misuses the information?

Recent reports show that phishing scams are on the rise, targeting consumers primarily through email, secondarily through text messages but also thru reach out via direct phone calls.

Actually, as many as 27% of consumers have been hit with pandemic-themed phishing scams, according to a survey done by TransUnion.

But there is a solution! With Convego® Service Broker and its Token Cockpit, G+D provides a token management tool integrated for example in the mobile banking app, fully controlled by the end-customer itself. In this cockpit, the customer has a full overview of where the payment credentials are tokenized, and can also enable and revoke tokenized cards, for total control. This empowers customers to deploy the mobile phone as a remote controller of payment cards for all digital channels. Then the Token Cockpit provides same enablers to Issuing banks in terms of web-UI, for customer support purposes.

What is Convego® Service Broker and its Token Cockpit?
Service Broker is a cloud-based solution that acts as an aggregator of tokenization services. We do the work of integrating with a multitude of token service providers and token requestors, including managing the ongoing adherence to certifications, legislation and regulations. Financial institutions, issuers and fintechs can connect to Service Broker via a simplified API set, without having to worry about the detailed inner workings of the payment networks' and token requestors' connectivity requirements. This means that issuers and other financial institutions can easily keep up with the changes in the payment ecosystem without the need to continually invest time and money in upgrading their own systems.

Simply put, push provisioning done in this way is very user friendly and convenient for your customers. Instead of always having to enter their card credentials into a third party's wallet or a merchant's online shop, the end-user just selects the wallet or merchant in your banking app, providing a simple and trusted payment lifecycle management tool.

Why Token Cockpit?
For issuers, banks and fintechs to offer a complete security solution, allowing the customers to have a transparent and fully control of their payments data, the Token Cockpit is a sophisticated way to bypass fraudsters in getting hold of and misuse card details: The customers can easily monitor where the tokenized credentials are afoot, and in a jiffy revoke or momentarily disable the same if wanted.

This eliminates the risks of costly security breaches, the customers feel confident in how their payments are in use, and the customer relationship is strengthened. And the right merchants receive payments at the checkout. A win-win for everyone!

TOP 3 challenges for e-commerce
Cybersecurity, competition and order fullfillment

27% of consumers have been hit with phishing scams in 2020

95% of e-commerce payments will be tokenized in 2022

Digital banking enabling customer control of payment credentials, prevents churn

Benefits in a nutshell:

- ✓ Puts your brand in front of the customers when it comes to safeguard their payment credentials
- ✓ Service Broker supports multiple payment networks such as Mastercard, Visa and eftpos
- ✓ It supports a growing list of digital device and issuer wallets, and X-Pays
- ✓ Card-on-file merchant tokenization is supported, allowing card issuers to meet network mandates
- ✓ Service Broker supports push provisioning, which enables the user to trigger payment capability to any channel from one app
- ✓ Token Cockpit, a feature enabled by Service Broker, allows the your customers to see all available tokens and manage any of them instantly
- ✓ Enables loyalty and stickiness as a transparent payment lifecycle management tool is given to the customers
- ✓ Issuers, banks and fintechs only need to perform one integration to enable tokenization across multiple payment networks, wallets, merchants and any other token requestor

Giesecke+Devrient

Giesecke+Devrient Mobile Security GmbH
Prinzregentenstrasse 159
81677 Munich
Germany

www.gi-de.com
mobilesecurity@gi-de.com

Follow us on: