

# Eckoh

Stop card data coming into your organisation without changing your systems or processes.

## Why DataGuard?

- Requires no integration with your existing systems or processes.
- Fully PCI DSS Compliant Hosted Service.
- The tokenised data is useless to hackers.
- The format fits legacy credit card fields.
- Removes the whole contact centre from PCI DSS compliance scope.
- Allows repeat payments.
- De-couples your technology and operations from PCI compliance.

**As a merchant, you will have heard the highly publicised horror stories of companies becoming victims to cybercriminals and having millions of card details stolen.**

During a payment authorisation a card number passes through many points in the authorisation process. This increases the risk of fraud because this data can be intercepted by hackers. By using DataGuard you can prevent payment data from even reaching your network. This is the best way to ensure that sensitive cardholder data is made safe.

As part of the Secure Payments Suite, DataGuard offers a simple technology with a clear value proposition.

It uses tokens to substitute actual card data within the organisation, which cannot be used to make a transaction, rendering the numbers useless to thieves.

DataGuard uses tokenisation to isolate cardholder data from payments made over the web, mobile device apps or through file transfers. It has major advantages over other PCI DSS compliance services, such as:

- no integration requirements; and
- no capital expenditure needed to buy tokenisation servers.

Ideal for organisations taking payments over the web or mobile apps



## What is Tokenisation?

Numeric credit card data (the PAN and CV2 code) is replaced with randomly generated numbers. These tokens can transit through or be stored in your environment. This means hackers have nothing of value to steal.

Typically, the token will retain the first six and last four digits of the card as a means of accurately matching the token to the payment card number. This enables

you to operate without card data in your environment.

Tokenisation is emerging as the primary solution for organisations wanting to reduce the risk and impact of a security breach as well as reduce their PCI scope and related costs. The actual payment data is securely cached in Eckoh's PCI DSS Level One certified data centres.

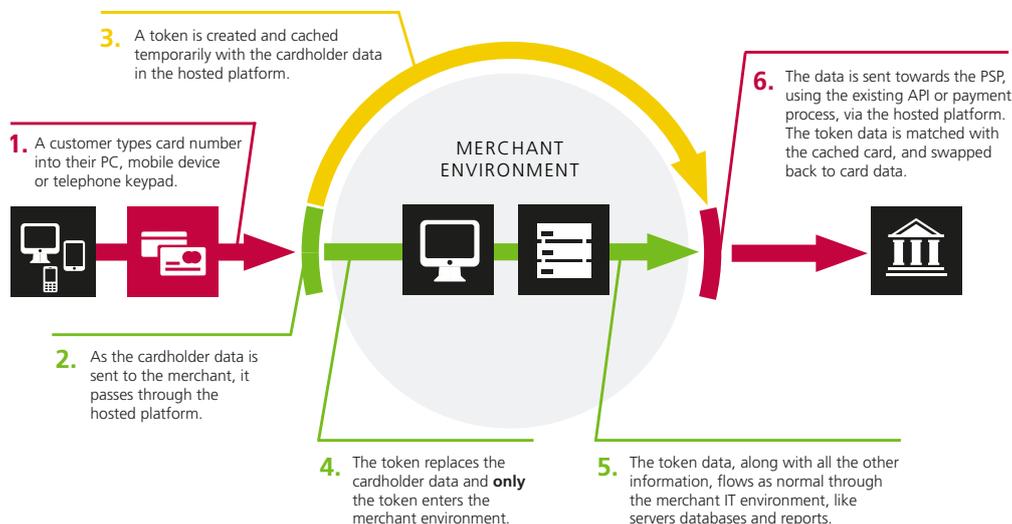
## Advantages of using DataGuard

Unlike standard tokenisation solutions, DataGuard is extremely quick to implement and does not involve complex changes to your databases, payment processes, security systems or other IT areas. It requires no integration, so you do not need to secure capital expenditure to buy tokenisation servers.

through the web or over the phone. It meets PCI DSS compliance regulation standards with fewer controls, less complexity, reduced audit scope, and fewer systems to review. You can de-couple your technology and operations from PCI compliance, allowing you to focus on running your business, rather than worrying about PCI DSS.

DataGuard provides retained, flexible options that can be used to take payments

## How DataGuard Works



# Eckoh