

Payment Security Risk



Steve Wilson

VP, Payment System Risk

Visa Europe



Agenda



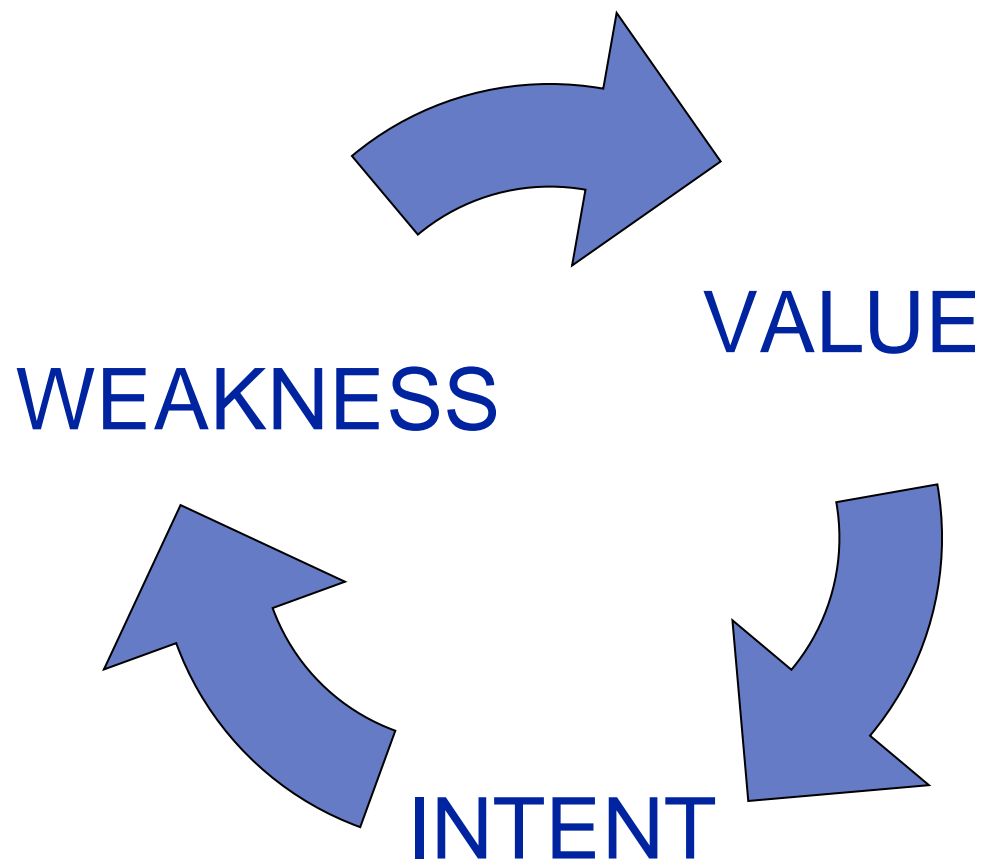
- The risk to the payment environment
- Payment Security Risk: getting the simple things right
- Reducing the effort to be secure



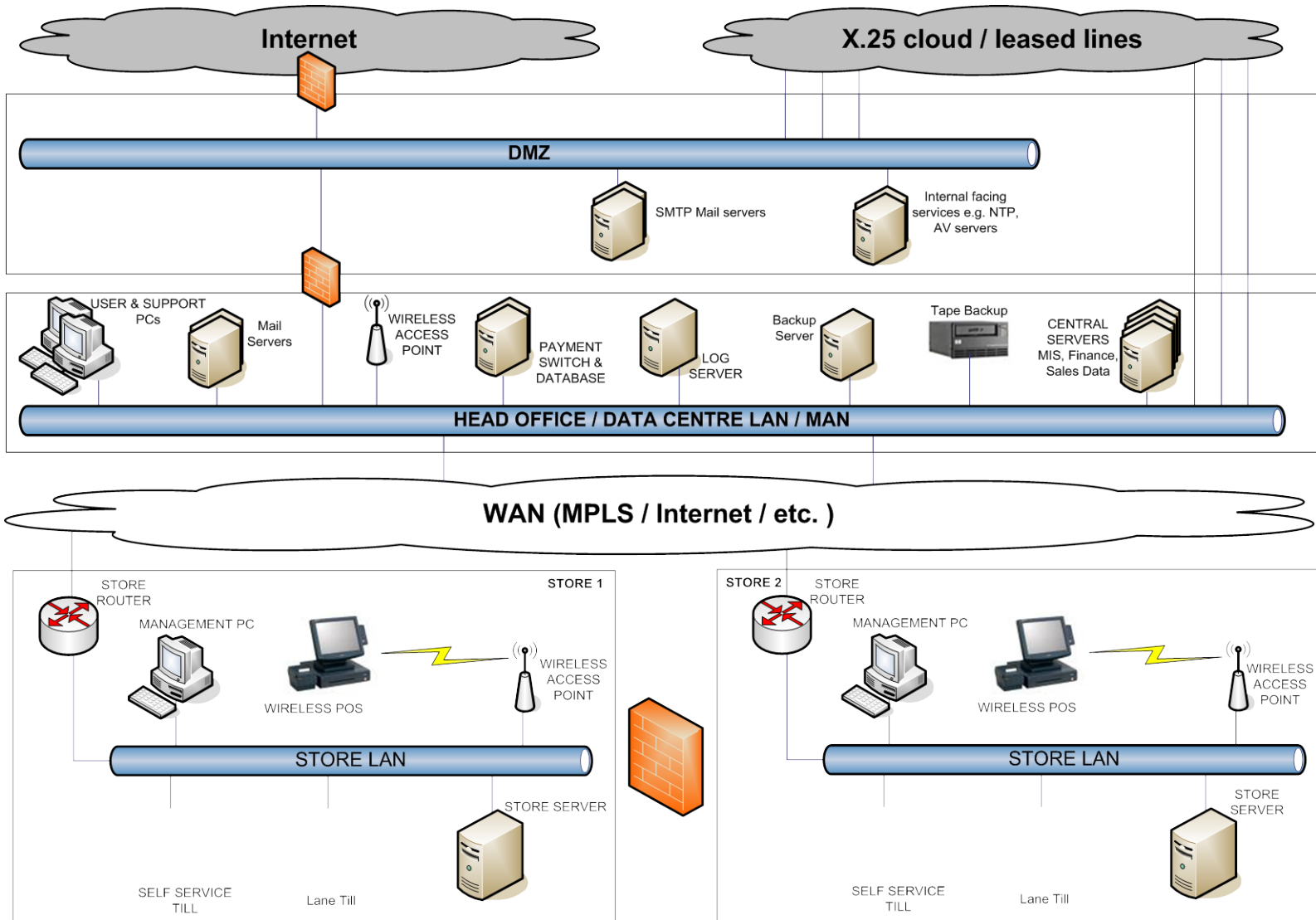


=

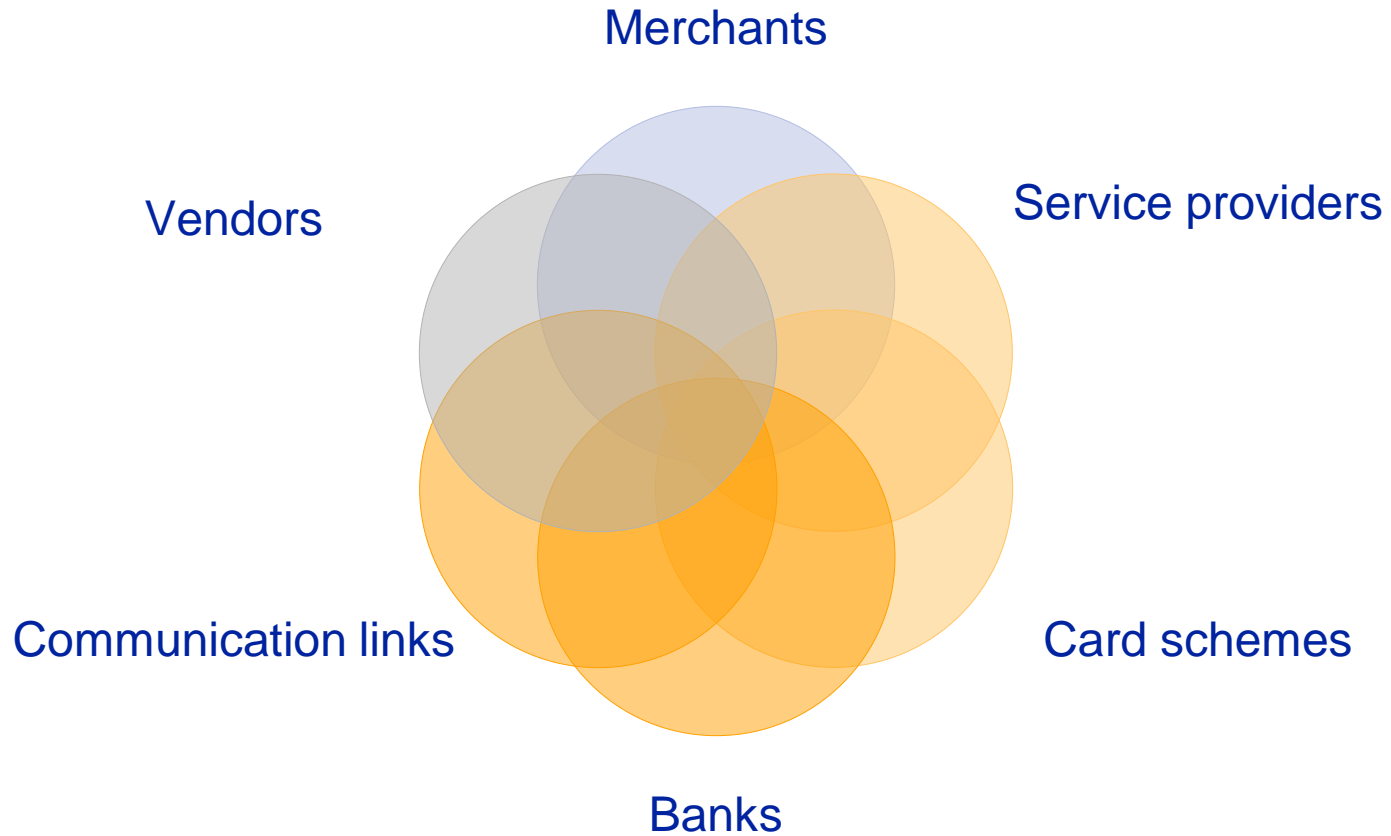




Securing the environment – it's complicated !!!



And it involves a lot of stakeholders



Agenda



- The risk to the payment environment
- Payment Security Risk: getting the simple things right
- Reducing the effort to be secure



Storing cardholder data



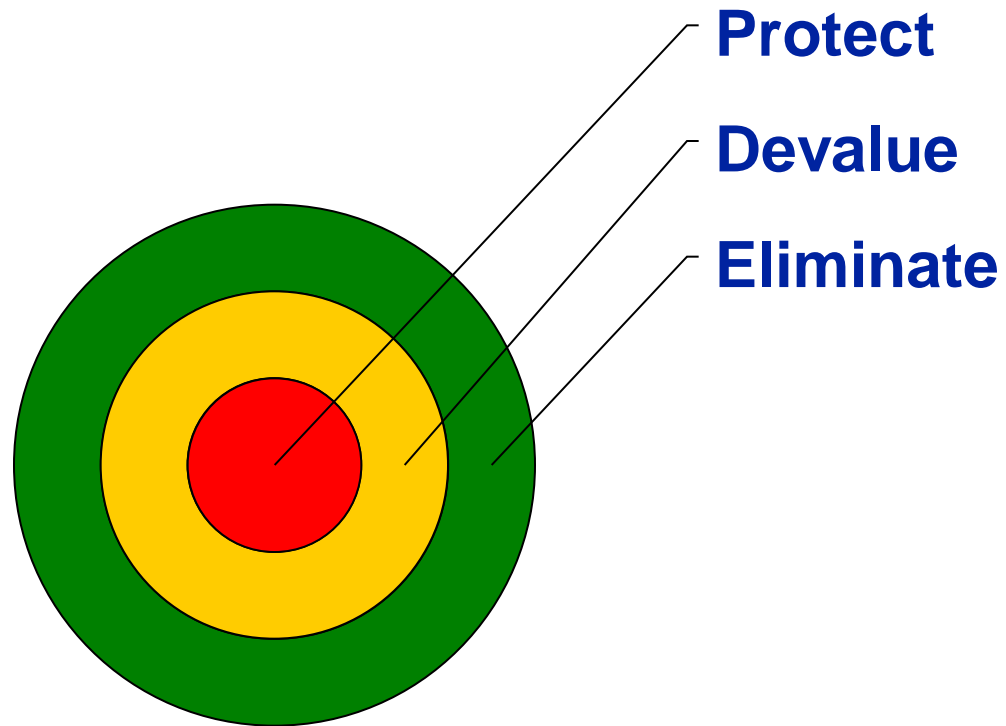
Basic principles:

- If you don't need it don't store it
- Delete sensitive authentication data after authorisation
- If you store cardholder data you must do one or more of the following:

- Truncate
- Hash
- Encrypt



Basic Principles



Sensitive authentication data



- Used in conjunction with card number and expiry date to facilitate card-present and card-absent fraud
- The single biggest invitation you can give to an attacker
- 90%+ of all compromises at entities that are storing sensitive data
- Getting rid of it instantly makes you less attractive – more secure

Default Passwords



One of the biggest root causes of data breaches

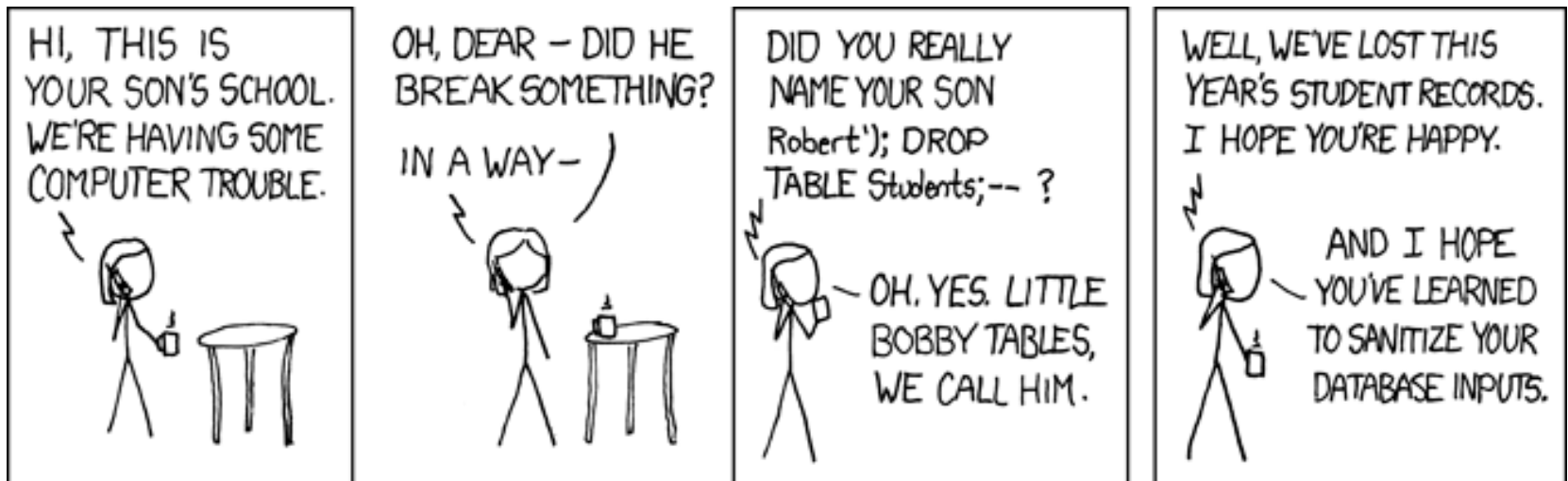
It is crucial to always:

1. Change your default passwords on all systems immediately
2. Use complex passwords
3. Monitor for suspicious activity on your systems

SQL Injection: the threat



- SQL Injection attacks are just as dangerous as default passwords
- **Never** trust user input



Xkcd.com

Agenda



- The risk to the payment environment
- Payment Security Risk: getting the simple things right
- Reducing the effort to be secure



Data Security Strategy



Today



Mid-Term



Long-Term

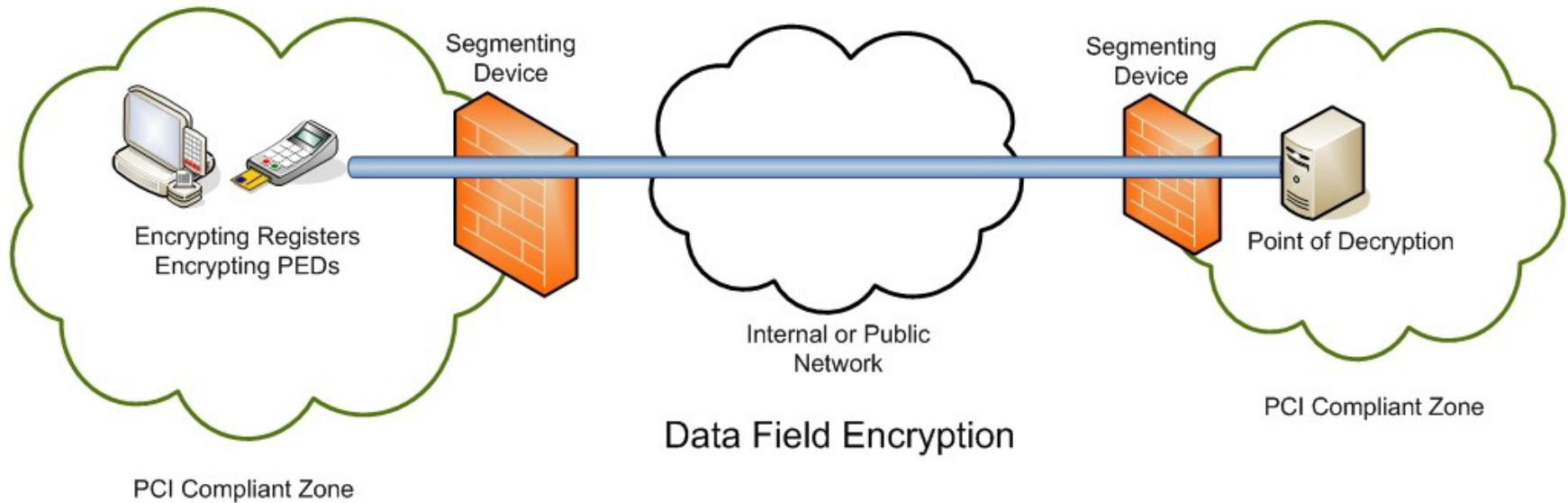
Data Field Encryption:

Encrypting such that the merchant environment has no access to clear-text cardholder data

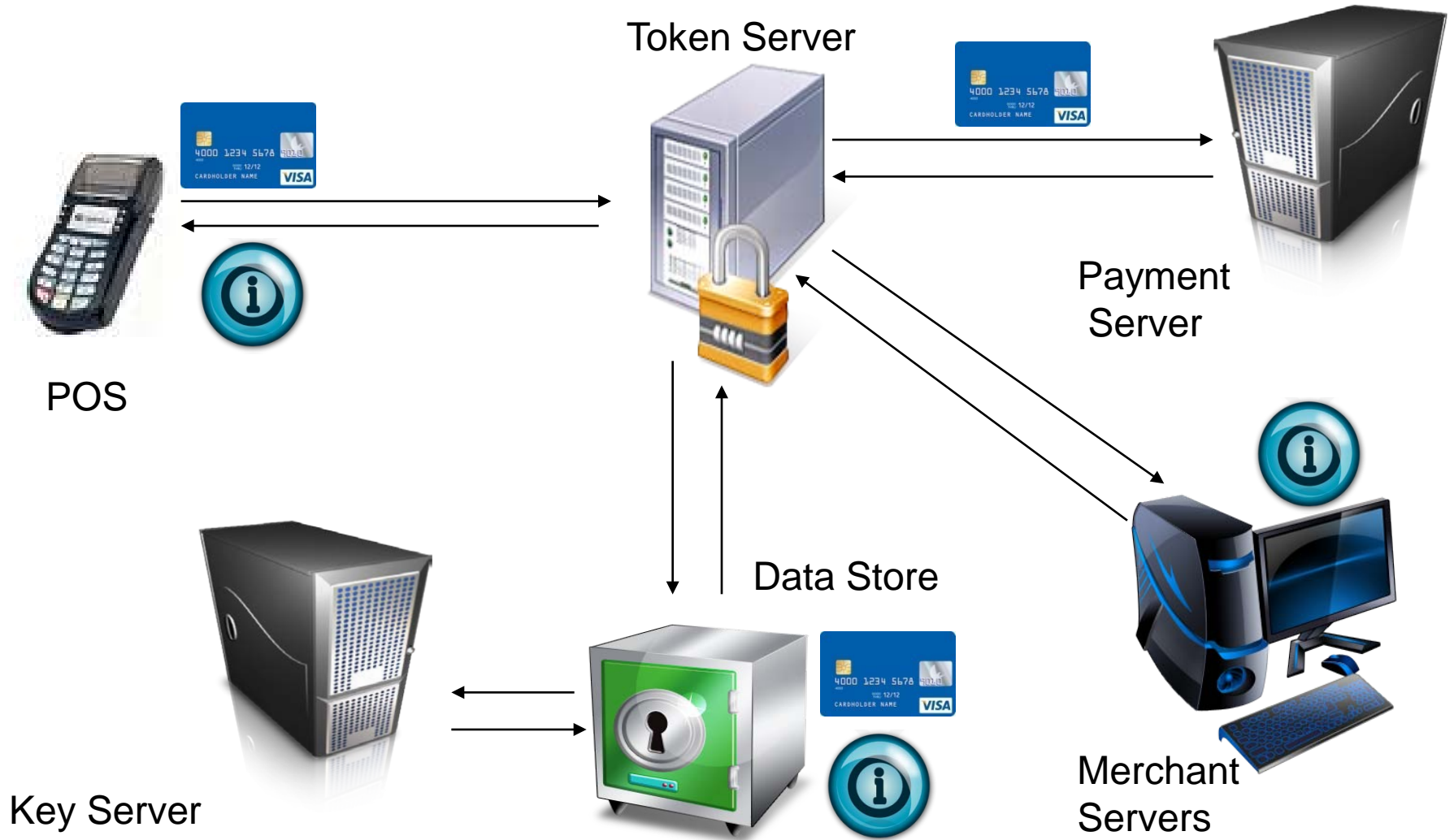
Tokenisation:

The process of replacing cardholder data (i.e. the PAN) with a surrogate token value

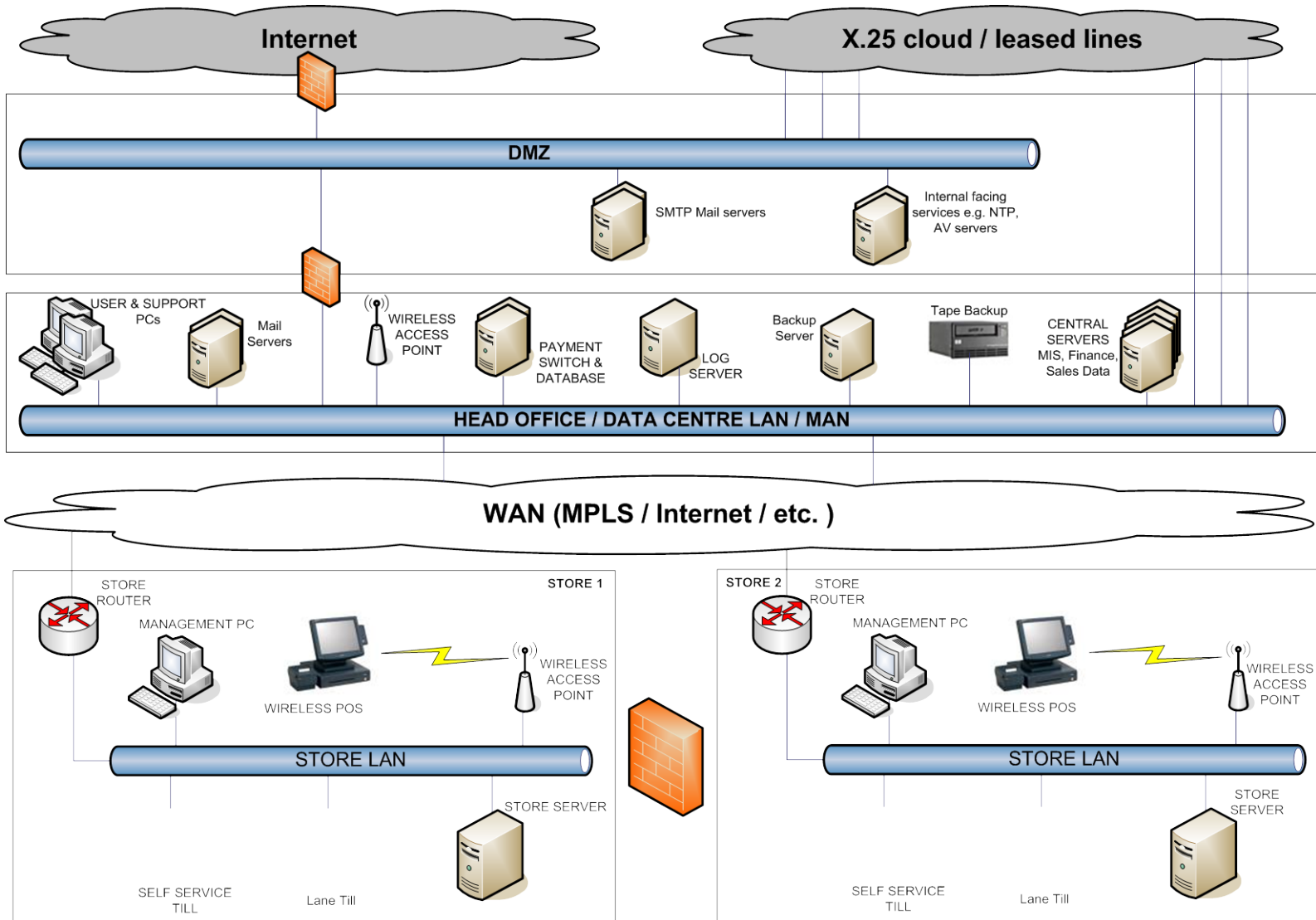
Data field encryption



Tokenization



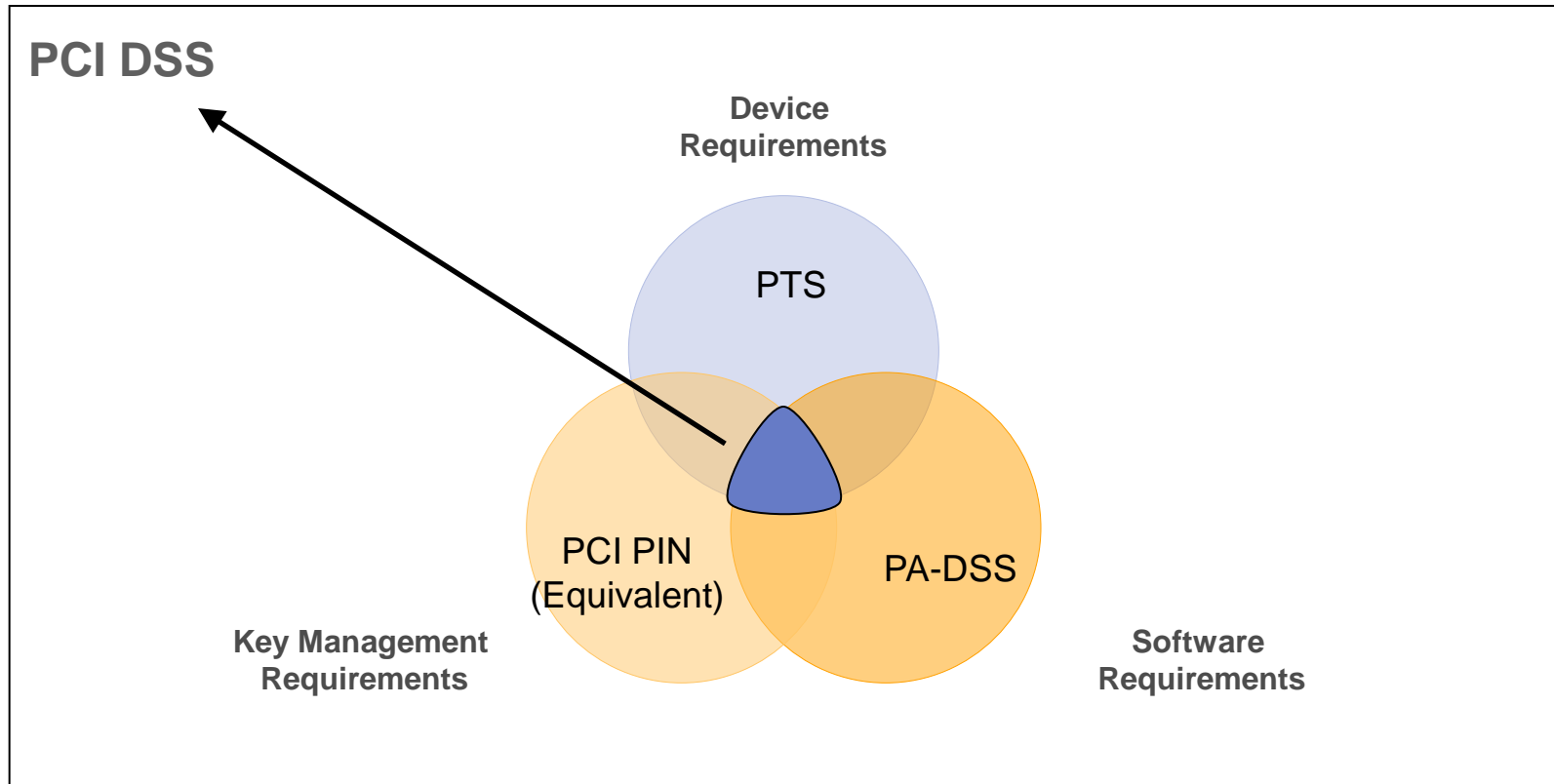
Securing the environment – it's complicated !!!



Data field encryption



Treating Account Data like PIN data



Fully validated End-to-End Encryption Solution

The industry's first specification for Data Field Encryption



- A comprehensive guidance document describing the key management practices that would be necessary to support encryption solutions
- Based on 5 key security objectives
- Aimed at consolidating industry best practice
- All resources available at <http://www.visaeurope.com/aboutvisa/security/ais/resourcesanddownloads.jsp>



Summary



- The way criminals commit fraud has evolved and is more organised and innovative
- Wholesale thefts of cardholder data means that data compromise is high on the risk agenda
- There are more touch points in the flow of transactions, each one of them representing a potential risk
- Security is everyone's responsibility - but there are standards and guidelines to help consolidate the industry
- Emerging technologies such as data field encryption provide new ways to comply with PCI DSS
- Visa is working alongside others in the payment industry to support retailers in reducing losses through fraud

Your questions

