Mitigating Risk: Challenges and Opportunities

Chicago Payments Symposium 2015
September 23, 2015
Marianne Crowe
Federal Reserve Bank of Boston
Building Blocks for Authentication and Payment Security

- Card authentication
- Cardholder verification
- Dynamic data
- Protects against counterfeit cards

- Replaces cardholder PAN with limited use token and cryptogram
- Makes PAN less valuable

- P2Pe
- Makes it difficult to extract cardholder data

EMV chip card

Payment Tokenization

Encryption

01100$%#0011#&
1010$%*011#$^01
01100$%#0011#&
1010$%*0110#$01
How tokenization is used to protect cardholder payment data

Replaces high-value payment account credential (PAN) with substitute value for mobile/digital financial transactions

Replaces underlying sensitive value (PAN) post-authorization with non-sensitive token value for data-at-rest stored in merchant/acquirer database

Static: multi-use
Allows merchants to connect cardholder with previous transactions

Dynamic: valid for single or limited number of transactions occurring in very short time

Hybrid: combines static token with uniquely generated cryptogram to add dynamic component for more security (EMVCo model)

PAYMENT TOKEN
SECURITY TOKEN

Card & mobile

Static token
Dynamic token

Hybrid Token

Static: multi-use
Dynamic: valid for single or limited number of transactions occurring in very short time

Dynamic: valid for single or limited number of transactions occurring in very short time

Hybrid: combines static token with uniquely generated cryptogram to add dynamic component for more security (EMVCo model)
Security & Payment Token Transaction Flows

**Provisioning (EMVCo)**

- Token Requestor (TR) sends cardholder PAN to Token Service Provider (TSP) to request a payment token.
- TSP issues payment token on behalf of an FI to TR.
- Token Domain Restriction Controls prevent token misuse.
- Issuer performs Identity and Verification (ID&V) of consumer.
- TSP assigns Token Assurance Level based on ID&V to establish confidence level for token to PAN/cardholder binding.