Reducing HSM Reliance in Payments through Proxy Re-Encryption

Siva Gaddam, Atul Luykx, Rohit Sinha and *Gaven Watson*

VISA Research

PINs and PIN Translation

First, what is a PIN?

User Authentication

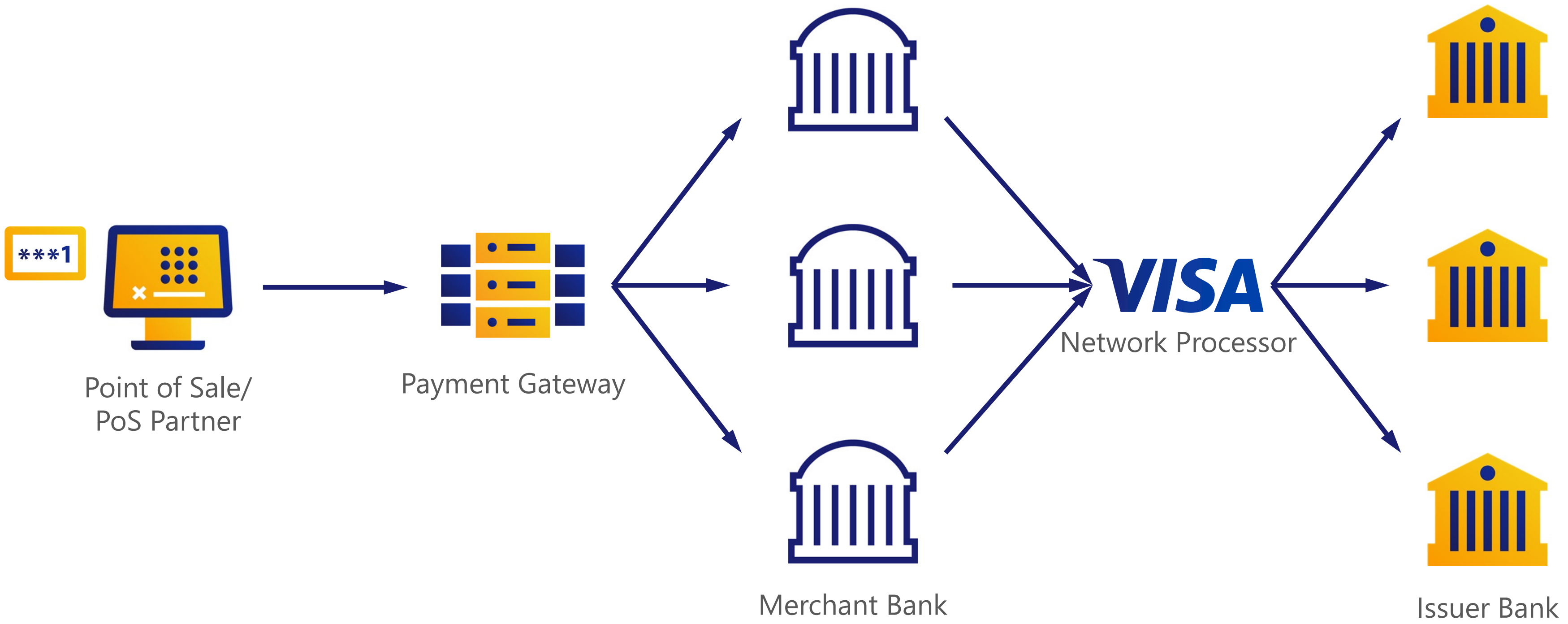
Common method for cardholder verification

VISA

Transporting PINs

Securing delivery to verifier

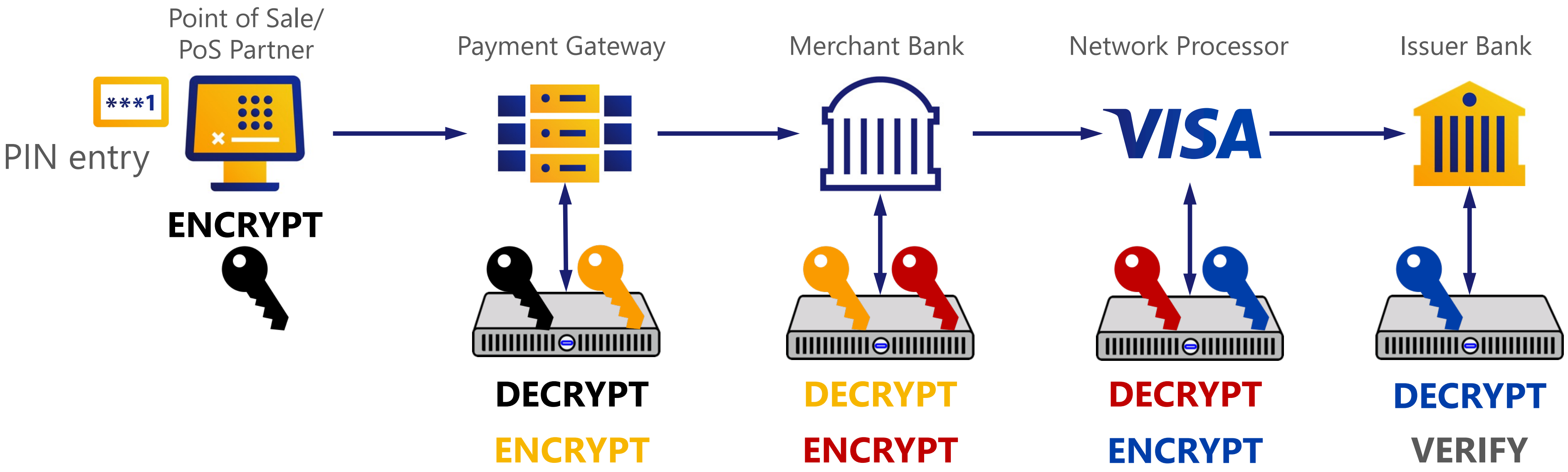
Routing a Transaction



VISA

What happens to PINs during a transaction?

How we use Hardware Security Modules (HSM)



Can we do better?

What are the requirements?

Aim: Reduce reliance on HSMs

Restrictions:

- PINs only in clear inside an HSM
- Pairwise Key Setup
- Ensure backwards compatibility

Finding a Different Solution…

Why not just use Public-Key Encryption?

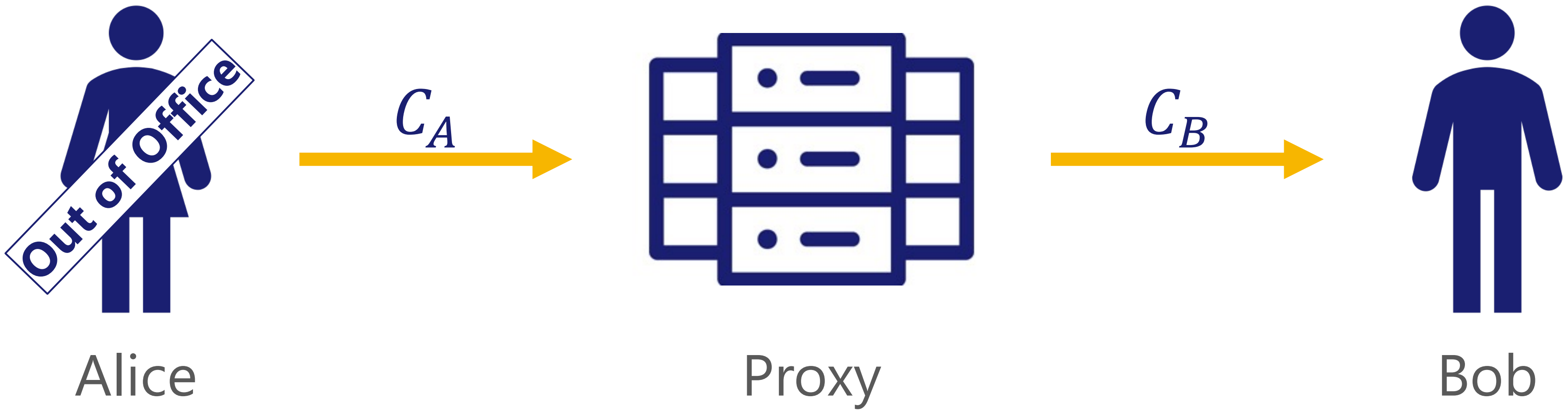
- PoS encrypts under Issuer Bank Public Key provided by the card.
- No PIN translation required.
- *Problem:* Requires significant changes to EMV standard and card re-issuance.

Can we use more advanced techniques?

- Let's try *Proxy Re-Encryption*!

What is Proxy Re-encryption (PRE)?

Delegate decryption ability to someone else



PKE to PRE

$KeyGen(1^\lambda) \rightarrow (sk_i, pk_i)$

$ReKeyGen(sk_i, sk_j) \rightarrow rk_{i,j}$

Bidirectional

$ReKeyGen(sk_i, pk_j) \rightarrow rk_{i,j}$

Unidirectional

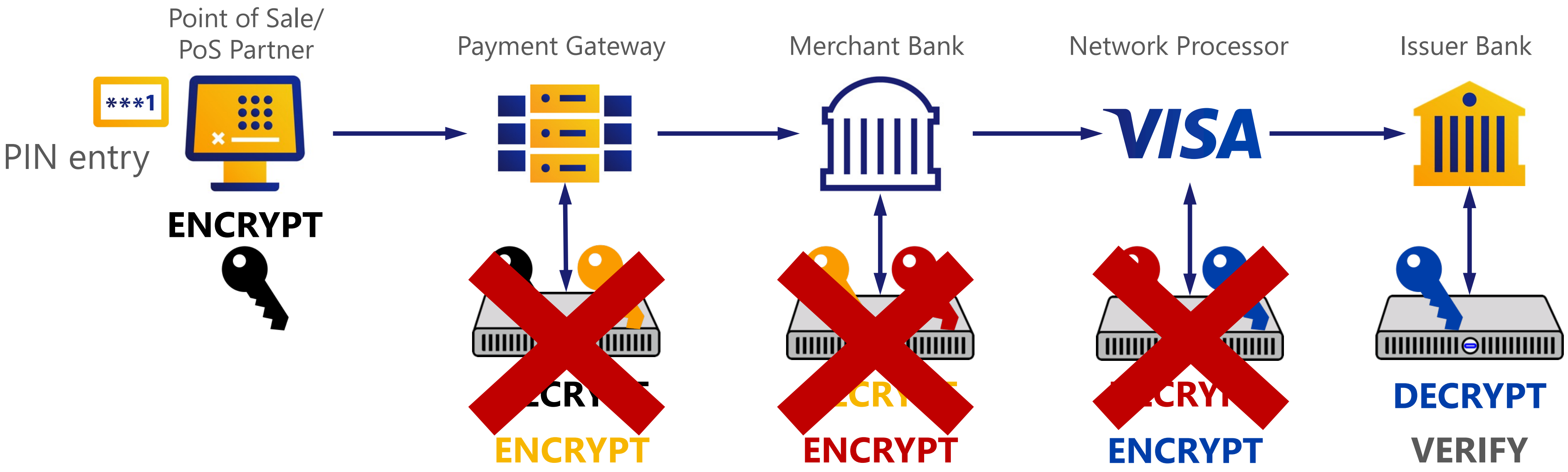
$Encrypt(pk_i, m) \rightarrow c$

$Decrypt(sk_i, c) \rightarrow m$

$ReEncrypt(rk_{i,j}, c) \rightarrow c'$

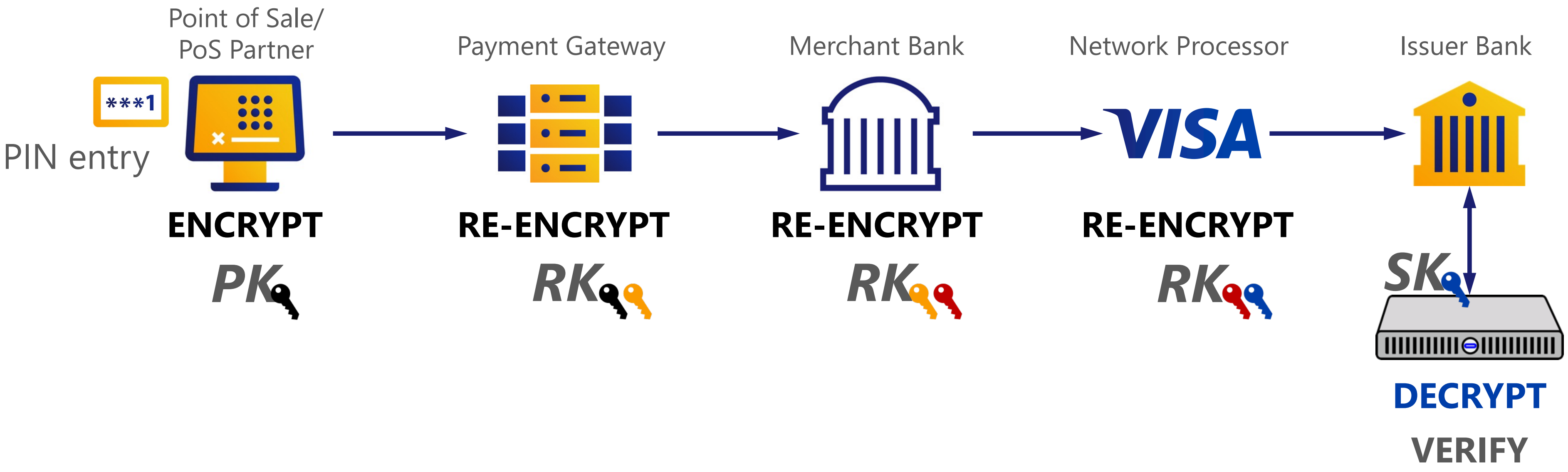
Apply PRE to Payments

Recall the previous setting



Our Approach

Removing HSMs from the online flow



What are the advantages of PRE?

Plan: Replace HSMs with PRE

Advantages:

- Don’t need specialized hardware
- Pure software solution so better scaling, elasticity and reduced costs
- Equivalent Security - re-encrypt operation ensures PIN never exposed

VISA

Our Construction: High-Level Perspective

Bidirectional PRE	Hybrid Encryption KEM-DEM
KEM: Borrows ideas from BBS PRE	DEM: Backwards Compatible with existing PIN Blocks

Our scheme is provable secure in a model which accurately represents the payment setting & extends recent HRA models

Performance Evaluation

Eliminating the Network Latency

	PoS Terminal	Gateway	Merchant Bank	Network	Issuer Bank	Total
HSM-based	98	920	920	920	900	**3758**
PRE-based	348	161	-	161	934	**1604**

Latency (μs)

	Network/Gateway	Issuer Bank
HSM-based	1086	1110
PRE-based	6240	1025

Throughput (txs/sec)

Meeting Our Goals

Goal	Status
Reduce Number of HSMs	All but eliminated in online flow
PINs only in clear inside an HSM	Yes
Ensure backwards compatibility	Yes
Pairwise Key Setup	Partially

Solution: Unidirectional PRE
Roadblock: Efficiency

Thank You!