Applying Proxy-Re-Encryption to Payments

Sivanarayana Gaddam, Rohit Sinha, Atul Luykx

Visa Research, 2019

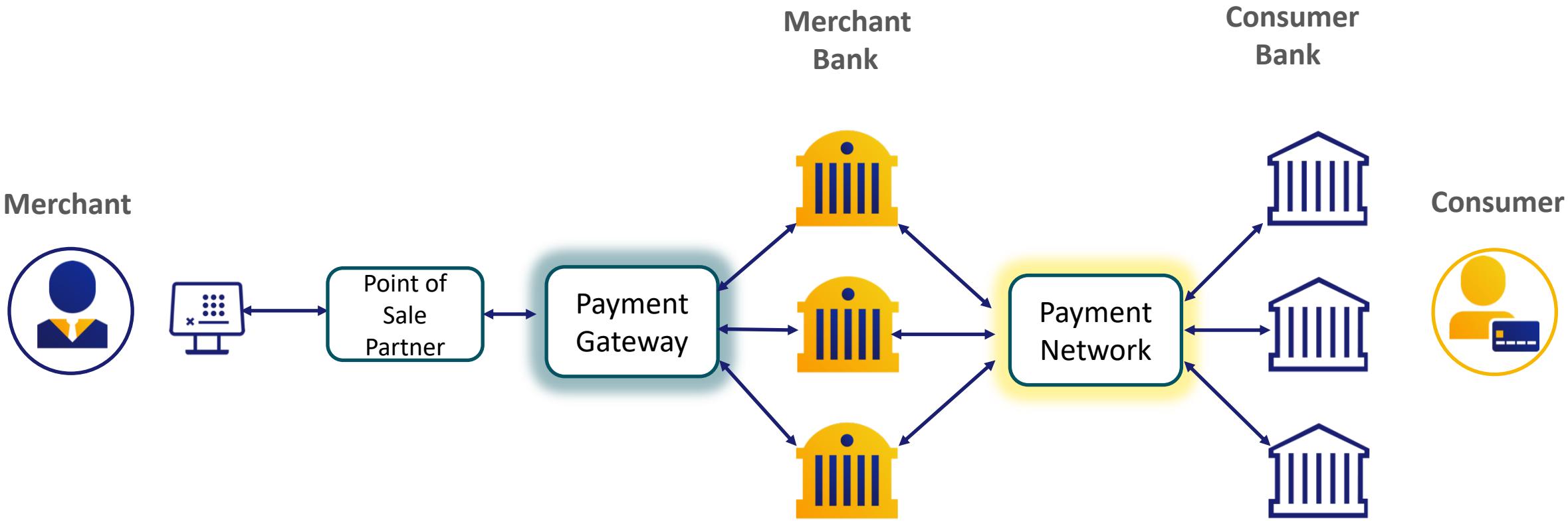
VISA Research

Disclaimer

Case studies, comparisons, statistics, research and recommendations are provided "AS IS" and intended for informational purposes only and should not be relied upon for operational, marketing, legal, technical, tax, financial or other advice. Visa Inc. neither makes any warranty or representation as to the completeness or accuracy of the information within this document, nor assumes any liability or responsibility that may result from reliance on such information. The Information contained herein is not intended as investment or legal advice, and readers are encouraged to seek the advice of a competent professional where such advice is required

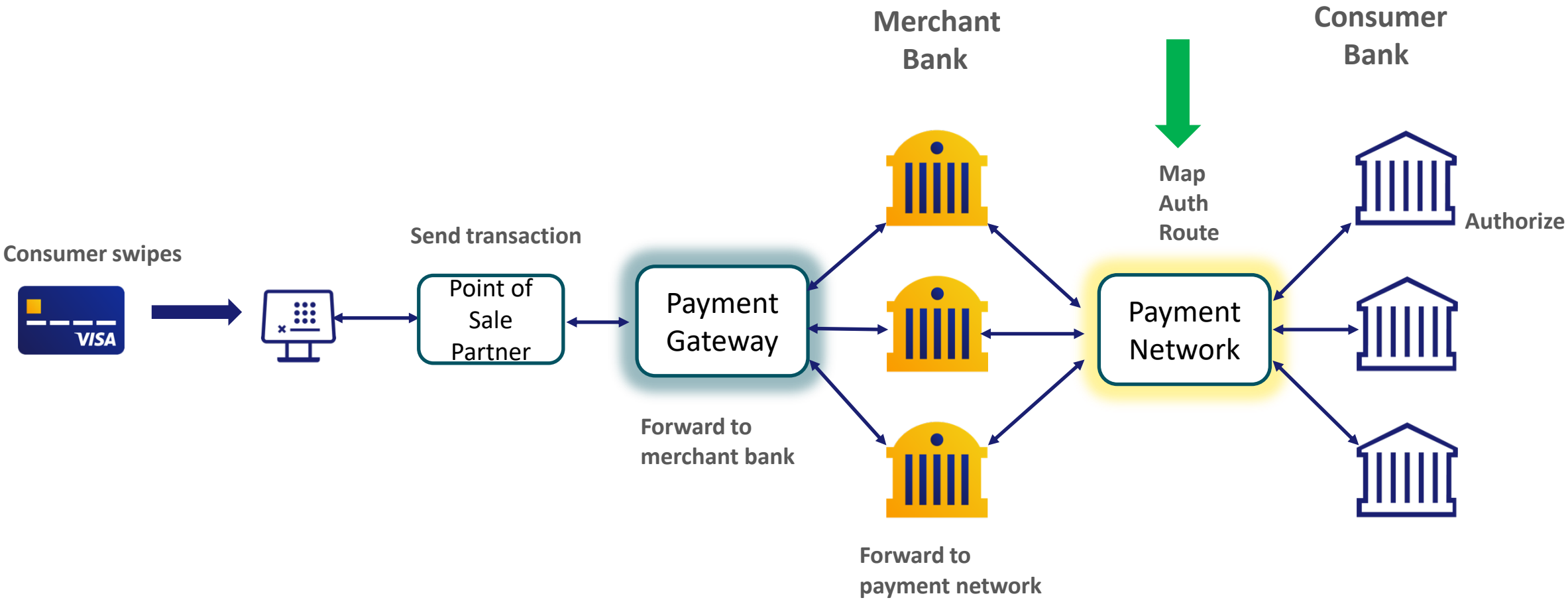
VISA Research

Global Payments Stack



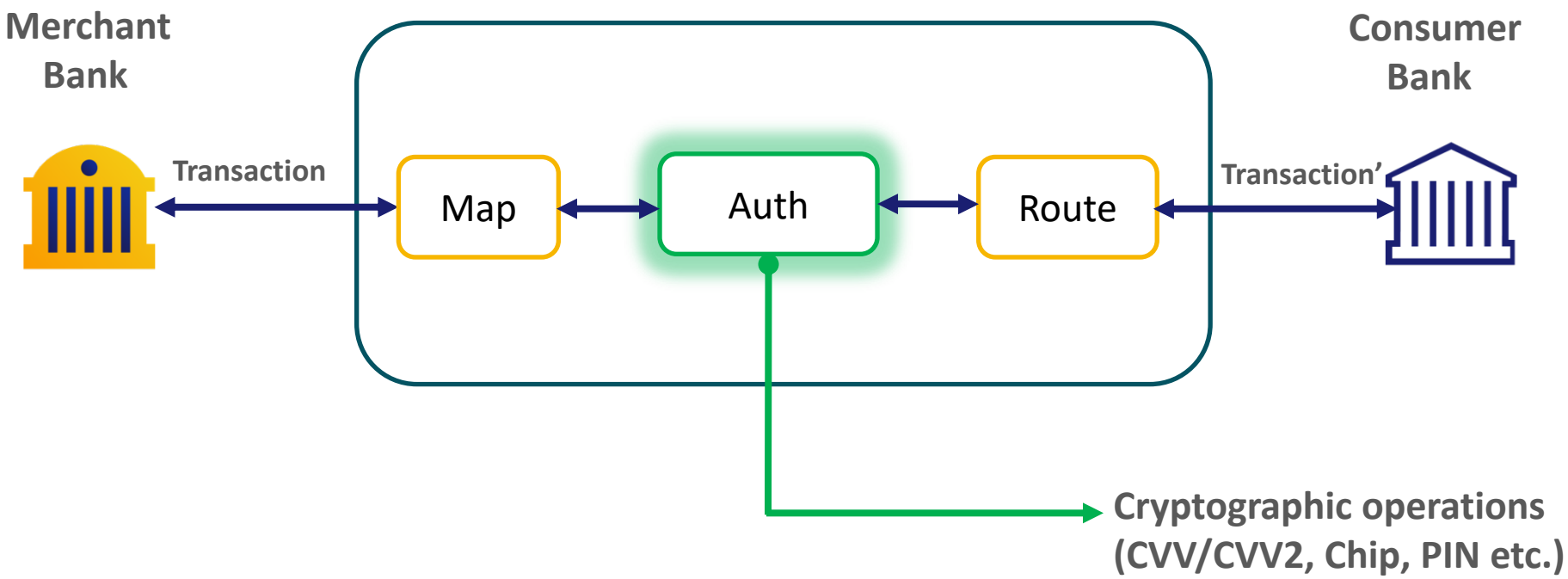
VISA Research

Transaction Flow



VISA Research

Network Functions



VISA Research

Sample Transactions

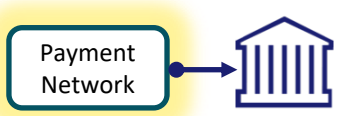
Card Verification Value (CVV/CVV2)

PAN data, CVV → Auth → 1 or 0

Authorization Request Cryptogram (ARQC)

PAN data, ARQC → Auth → 1 or 0

PIN Verification

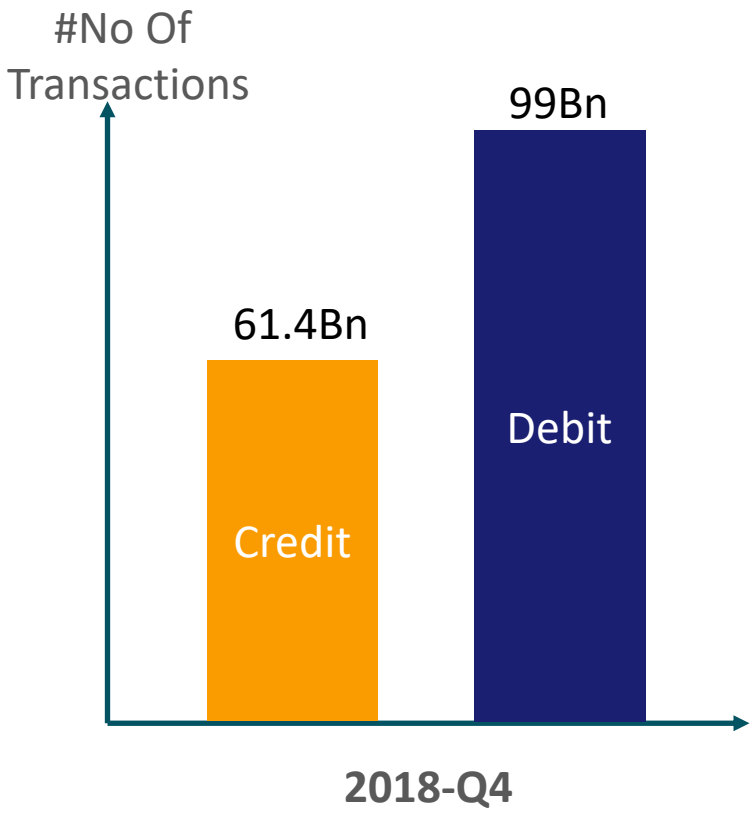


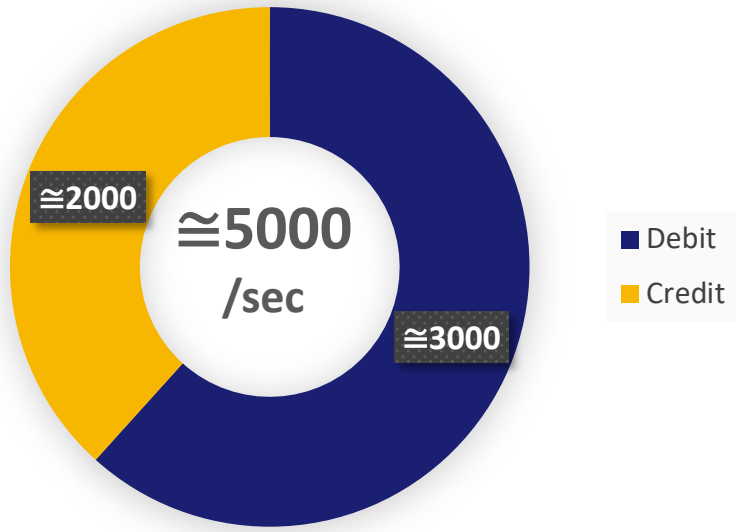
PAN data, PIN → Auth → 1 or 0

https://www.cs.ru.nl/E.Poll/papers/EMVtechreport.pdf

VISA Research

Cryptographic Operations at Scale

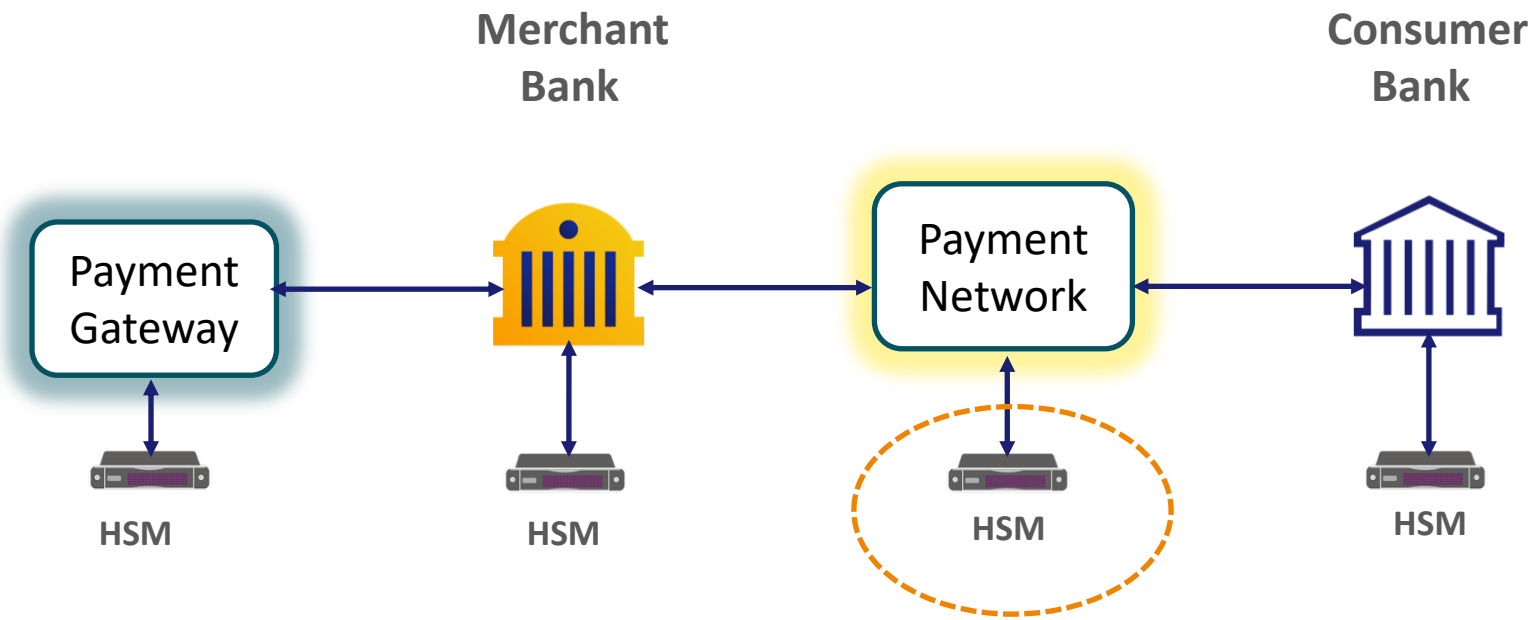




https://s1.q4cdn.com/050606653/files/doc_financials/2018/q4/Visa-Inc.-Q4-2018-Operational-Performance-Data.pdf

VISA Research

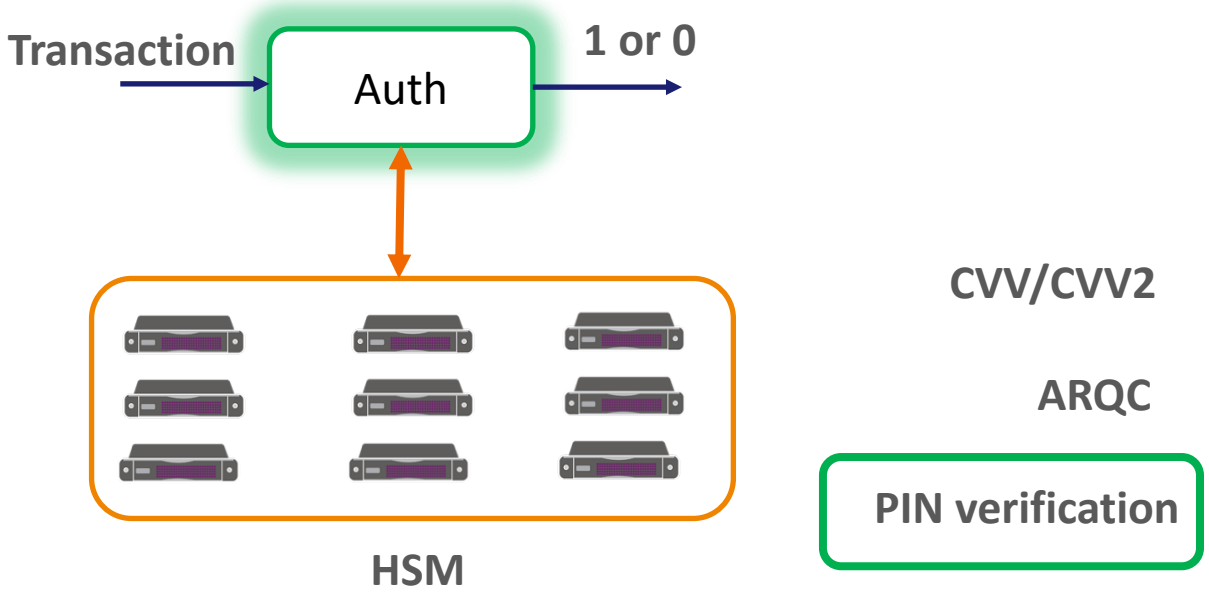
PCI Compliance



https://www.pcisecuritystandards.org/documents/PCI%20HSM%20Security%20Requirements%20v1.0%20final.pdf

VISA Research

Top Hitters

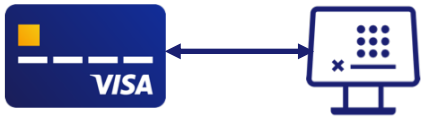


VISA Research

PIN Verification Modes

Consumer
Bank

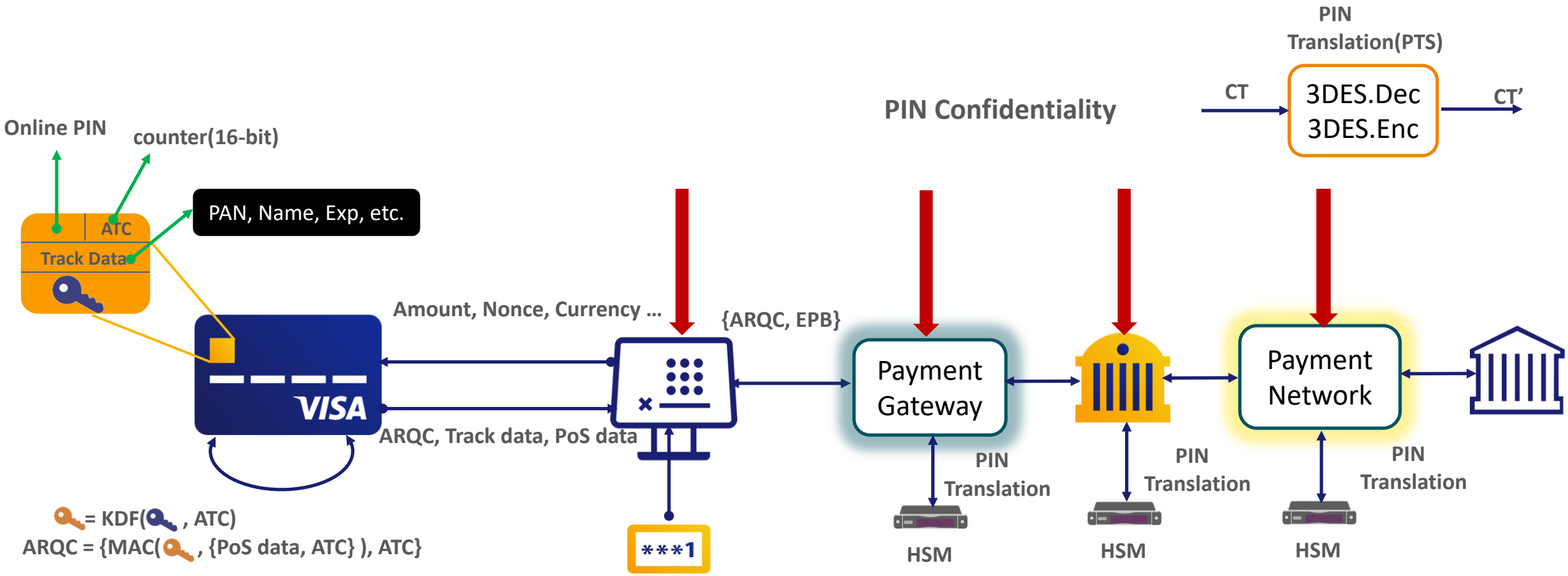
Online



Offline

VISA Research

Chip & PIN Transaction



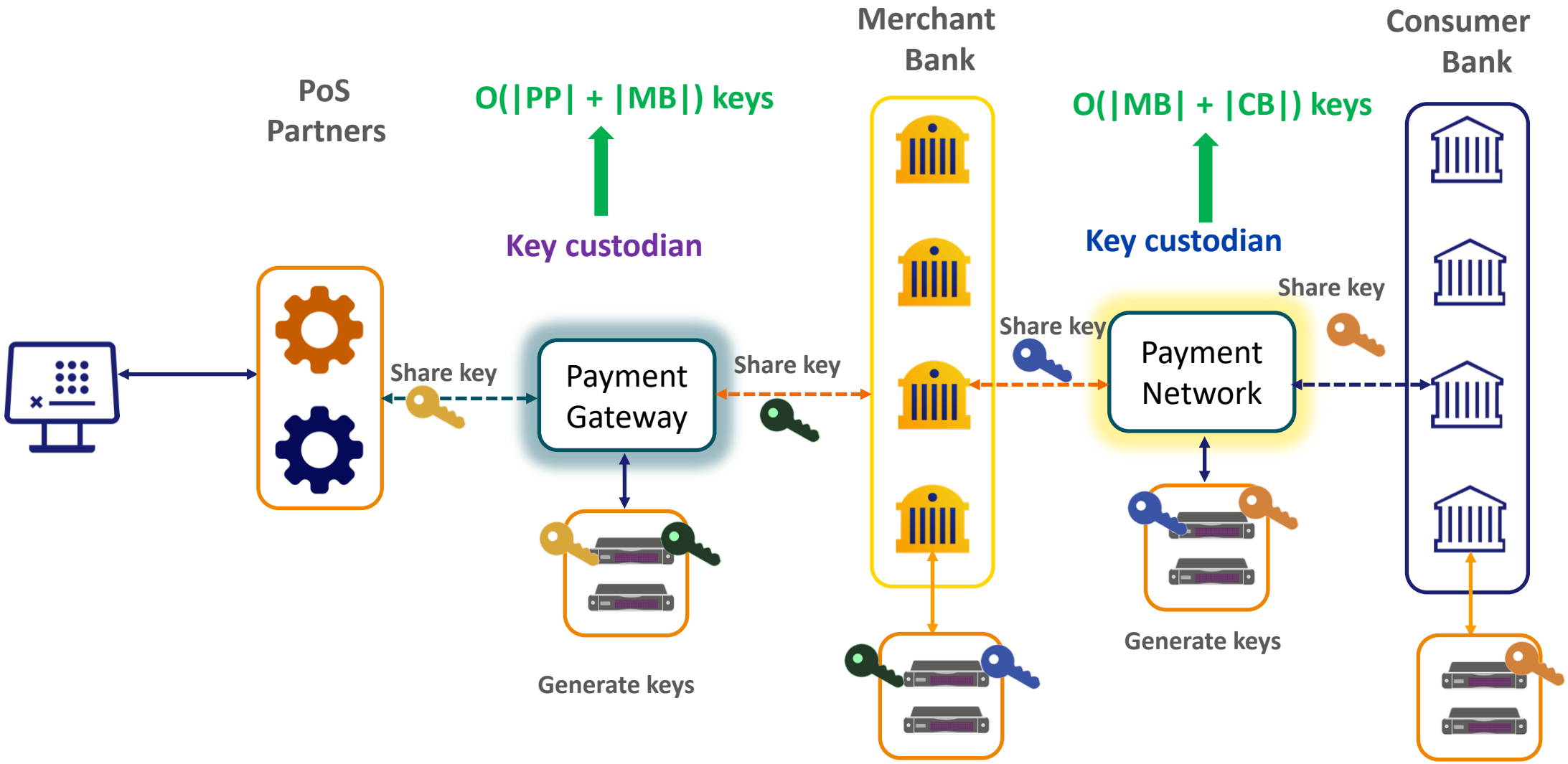
EPB: Encrypted PIN Block

ARQC: Authorization Request Cryptogram

EMV-Book-2_Security And Key Management

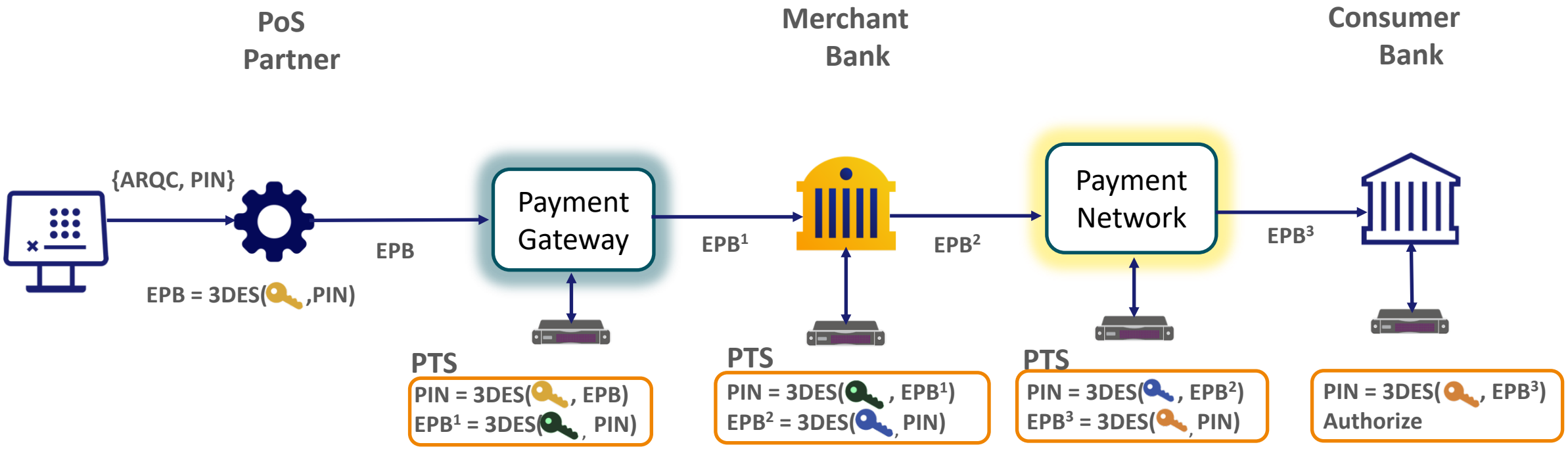
VISA Research

Key Sharing Setup



VISA Research

PIN Confidentiality

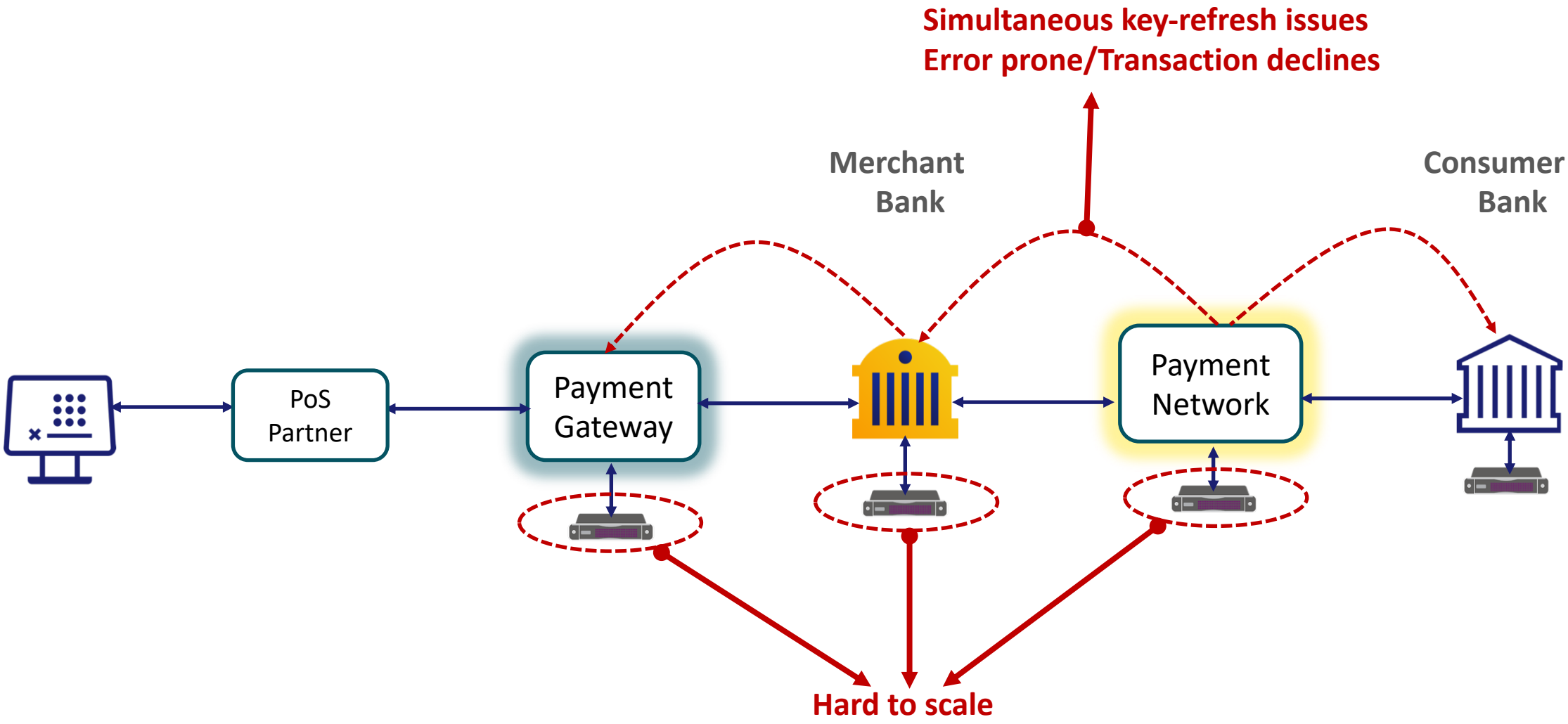


EPB: Encrypted PIN Block

ARQC: Authorization Request Cryptogram

VISA Research

PIN Confidentiality Problem



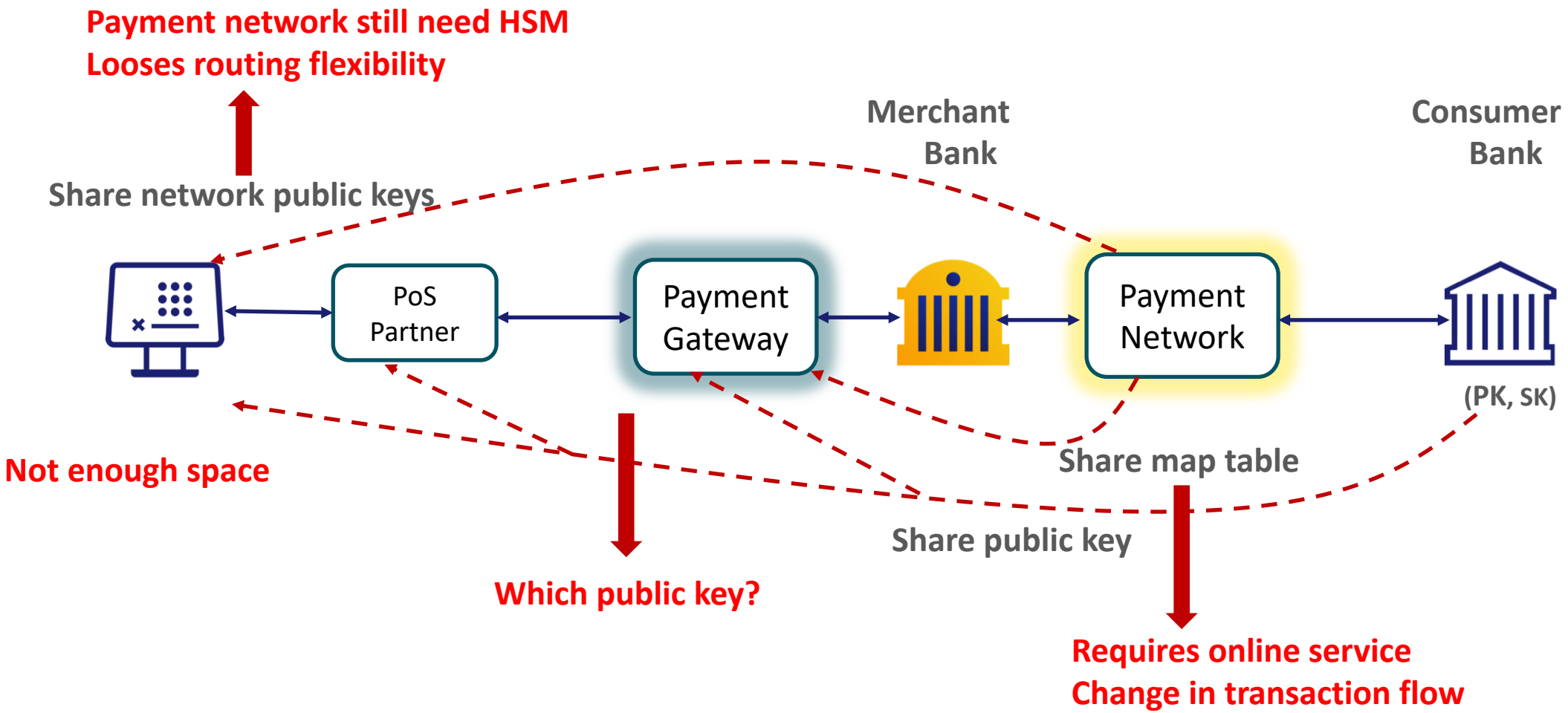
VISA Research

Requirements

- ✓ Support for all payment types(chip/mag-stripe, apple pay etc.)
- ✓ Reduce HSM reliance
- ✓ Incur minimal changes to the ecosystem

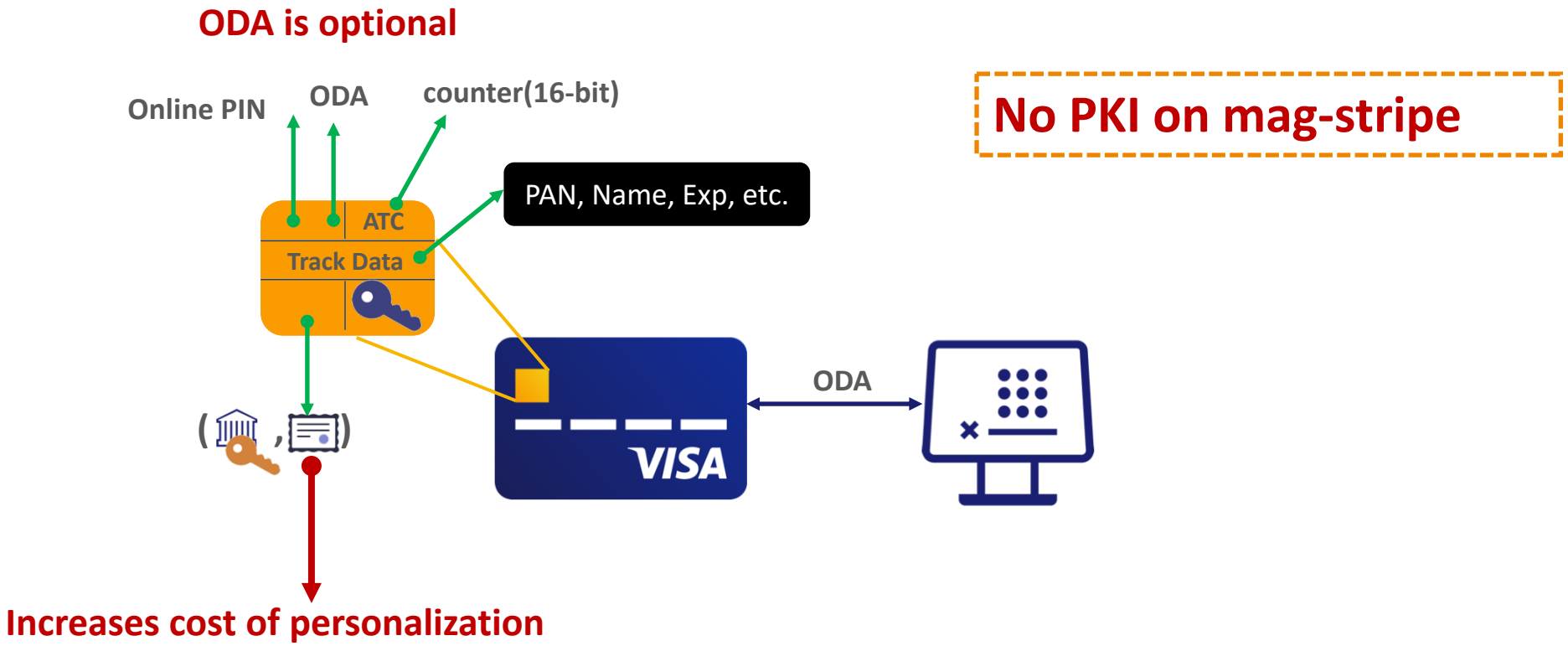
VISA Research

Strawman Solution#1



VISA Research

Strawman Solution#2



ODA: Offline Data Authentication

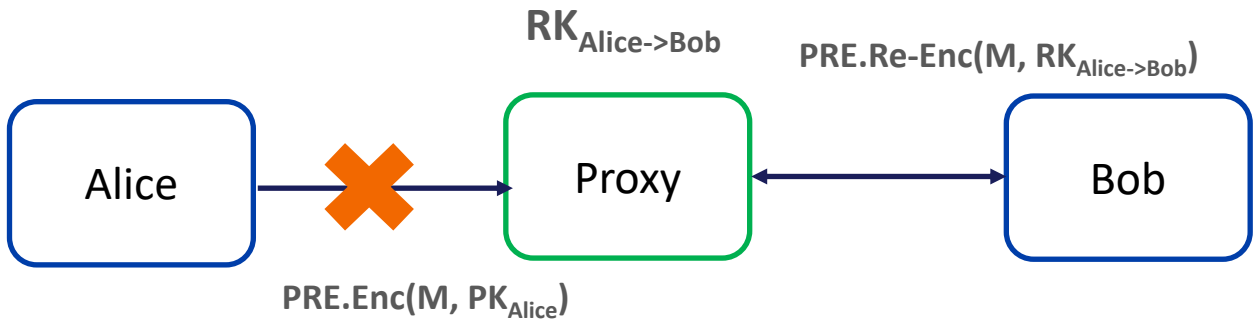
http://www.uspaymentsforum.org/wp-content/uploads/2018/10/Dual-Interface-Card-Personalization-WP-FINAL-Oct-2018.pdf

VISA Research

Our Solution: Proxy-Re-Encryption based PIN Confidentiality

PRE

- PRE.KeyGen
- PRE.Enc
- PRE.Dec
- PRE.Re-Key
- PRE.Re-Enc

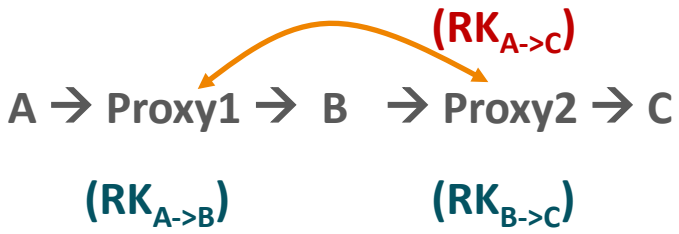


Uni/Bi-Directional

Collusion-Safe

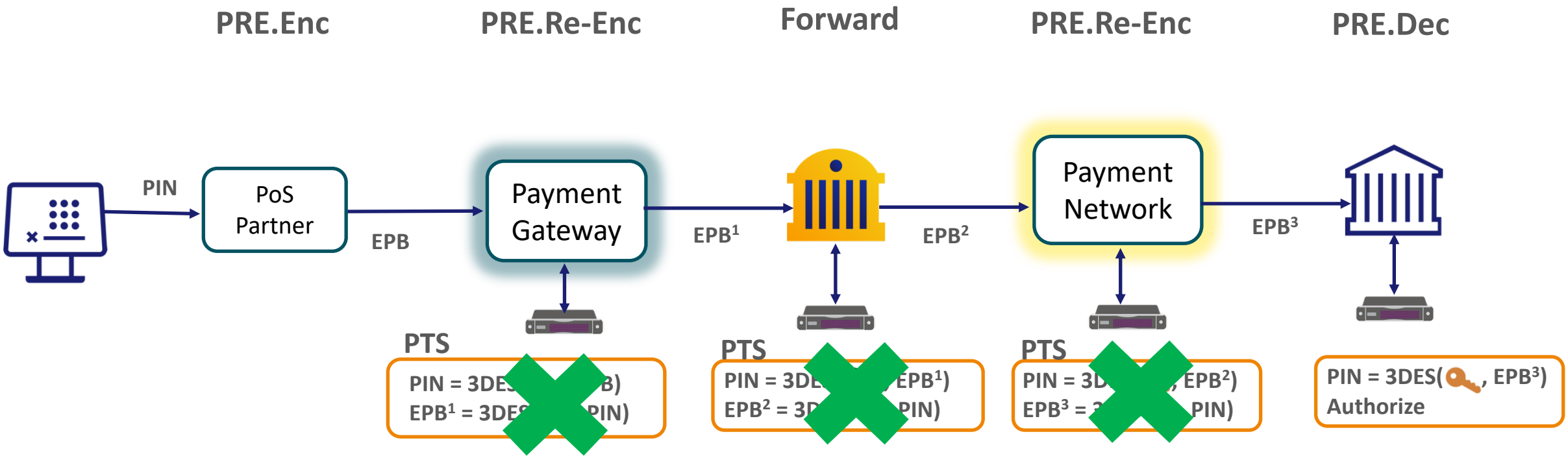
Non-Interactive

Non-Transitive



VISA Research

Our Solution: Proxy-Re-Encryption based PIN Confidentiality



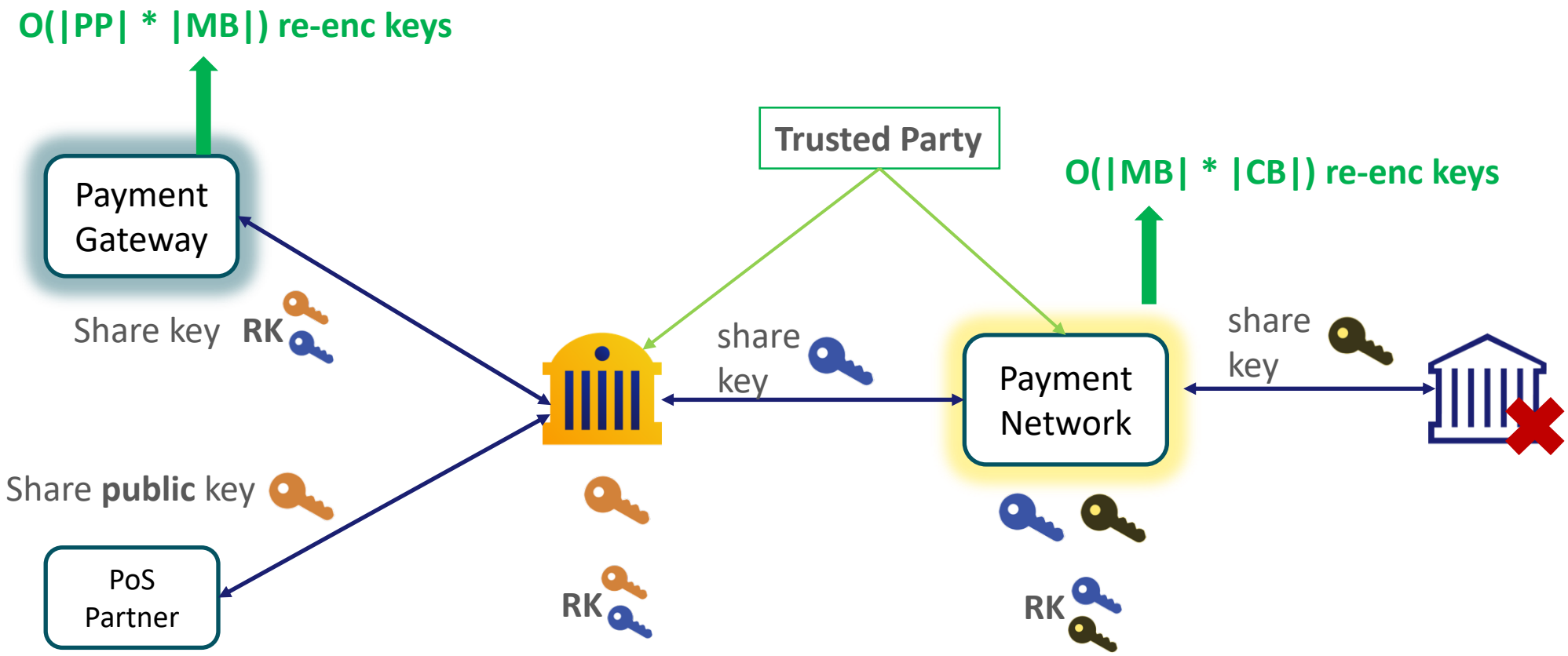
VISA Research

Desired PRE Scheme

Matt Blaze, Gerrit Bleumer, and Martin Strauss. Divertible protocols and atomic proxy cryptography. In Kaisa Nyberg, editor, EUROCRYPT'98

VISA Research

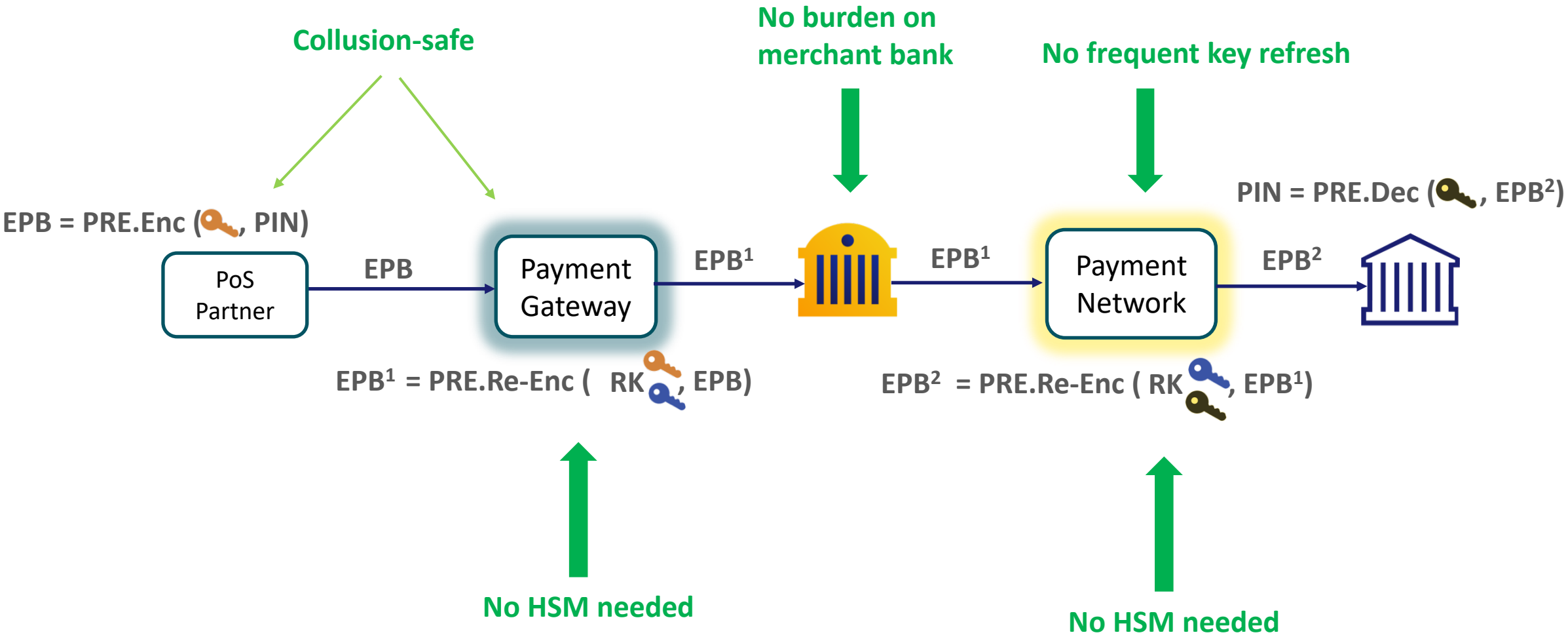
Key Setup



Matt Blaze, Gerrit Bleumer, and Martin Strauss. Divertible protocols and atomic proxy cryptography. In Kaisa Nyberg, editor, EUROCRYPT'98

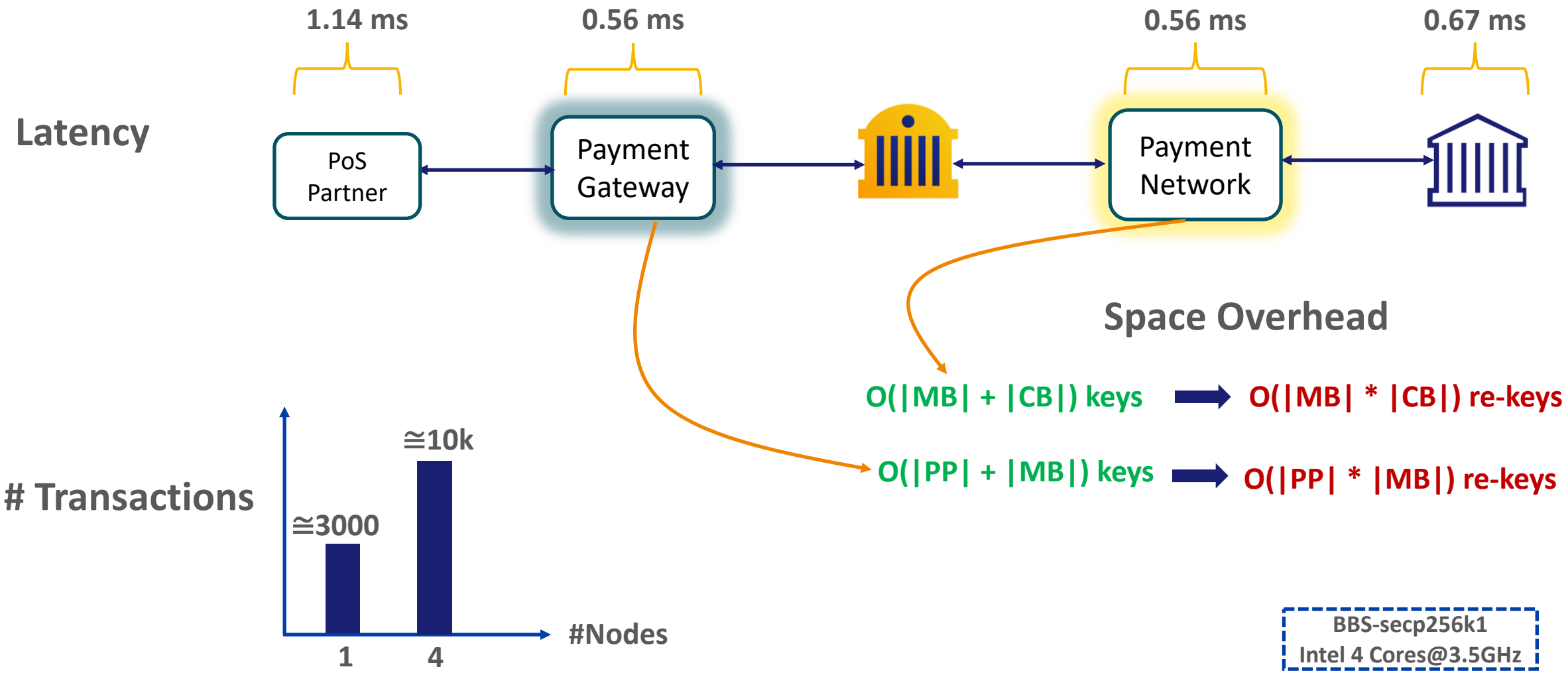
VISA Research

Transaction Flow



VISA Research

Benchmarks*



BBS-secp256k1
Intel 4 Cores@3.5GHz

* Representative results based on the configuration shown

VISA Research

Solution Summary

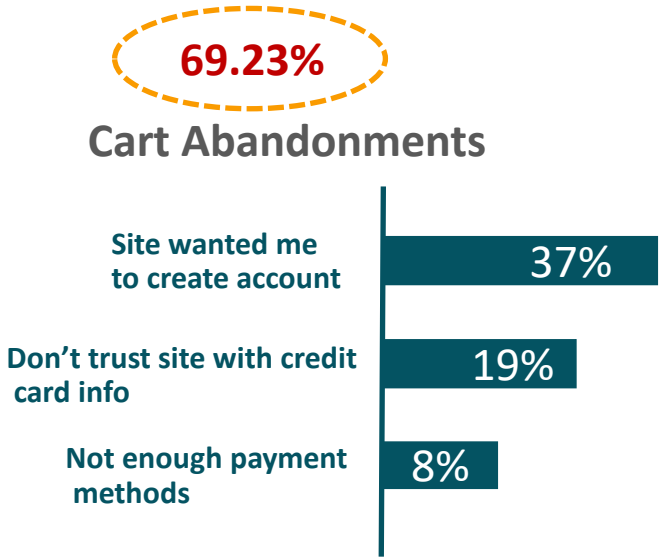
Supports all payment types(chip/mag-stripe, token-based etc..)

Reduced HSM reliance during online phase

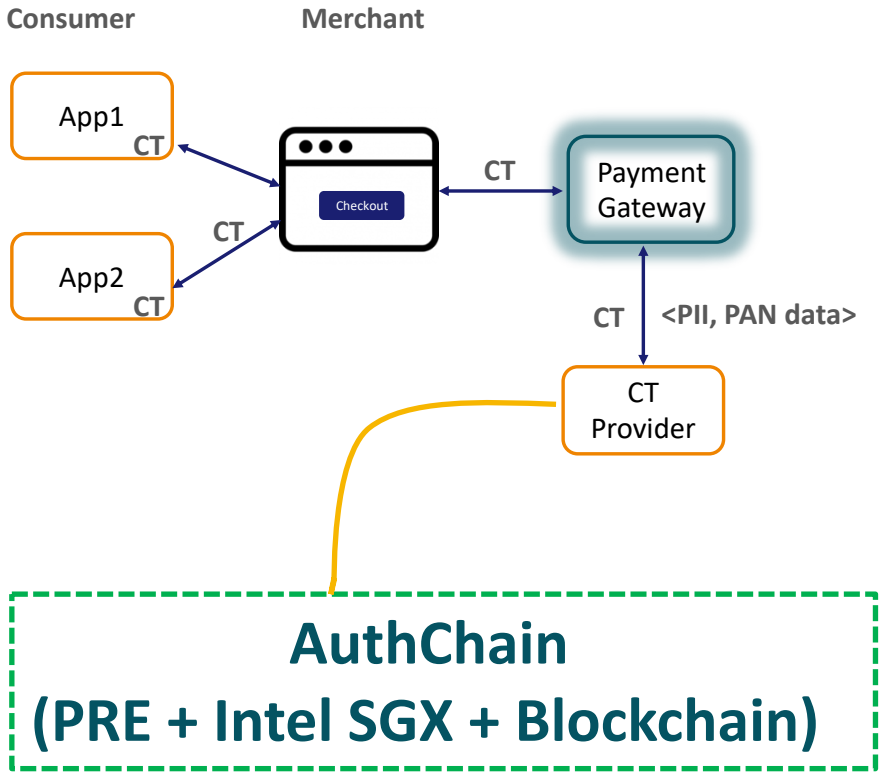
Incurs minimal change [Domestic Card Processing Network]

VISA Research

Problem: Cart-Abandonments



Help merchants accept unknown payment types?



https://baymard.com/lists/cart-abandonment-rate
LexisNexis-True-Cost-Of-Fraud-Study, 2017

VISA Research

Conclusion

PIN Translation: PRE reduces HSM burden on intermediaries

E-Commerce: PRE helps consumers choose any preferred mobile app for checkout

VISA Research

?

VISA Research