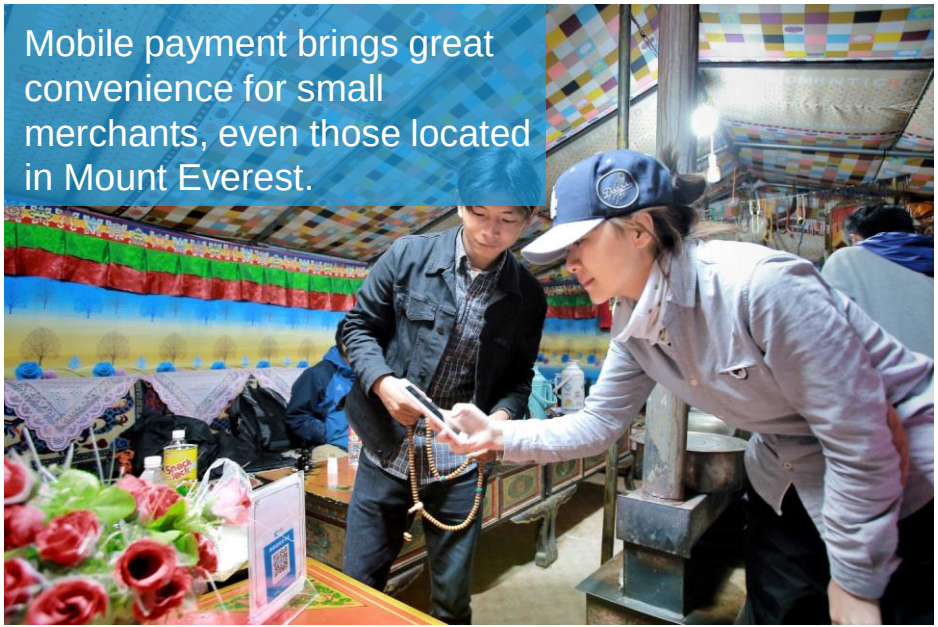
Security aspects of bar code payment

Min ZUO, Alipay

ITU Workshop on Fintech Security
Geneva, Switzerland, 26 August 2019

Global bar code payment prosperity

Practices in several countries/regions



Usage beyond payment

In-store Payment

Public Transportation

Menu Order

Promotion

Coupon

Bar code payment benefits

- Cover **long tail** merchants and users
- Easily combined with **convenient** daily use cases
- Improve Merchant **efficiency**
  Reduce Merchant **costs**




Typical scenarios

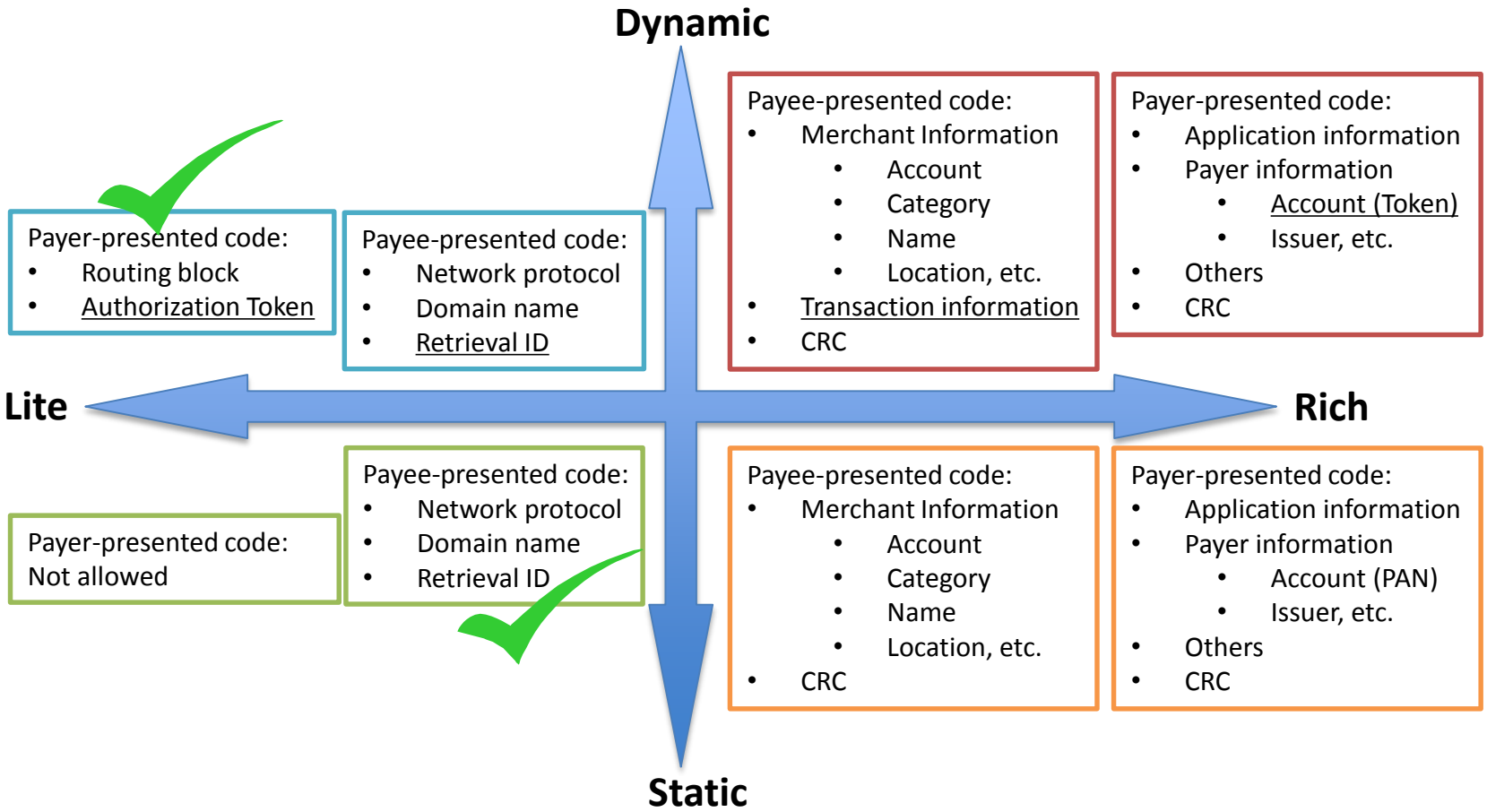
Payee-presented mode

- Identifier for a Payee or service
- Payee could be a merchant or person
- Dynamic or static

Payer-presented mode

- Identifier for a payer or account
- Dynamic

Mainstream formatting of payment bar code



Sample code images

Code value:
https://qr.alipay.com/tsx028...
.....

Code value:
https://order.duolabao.com/active/n/10011.....?p=N

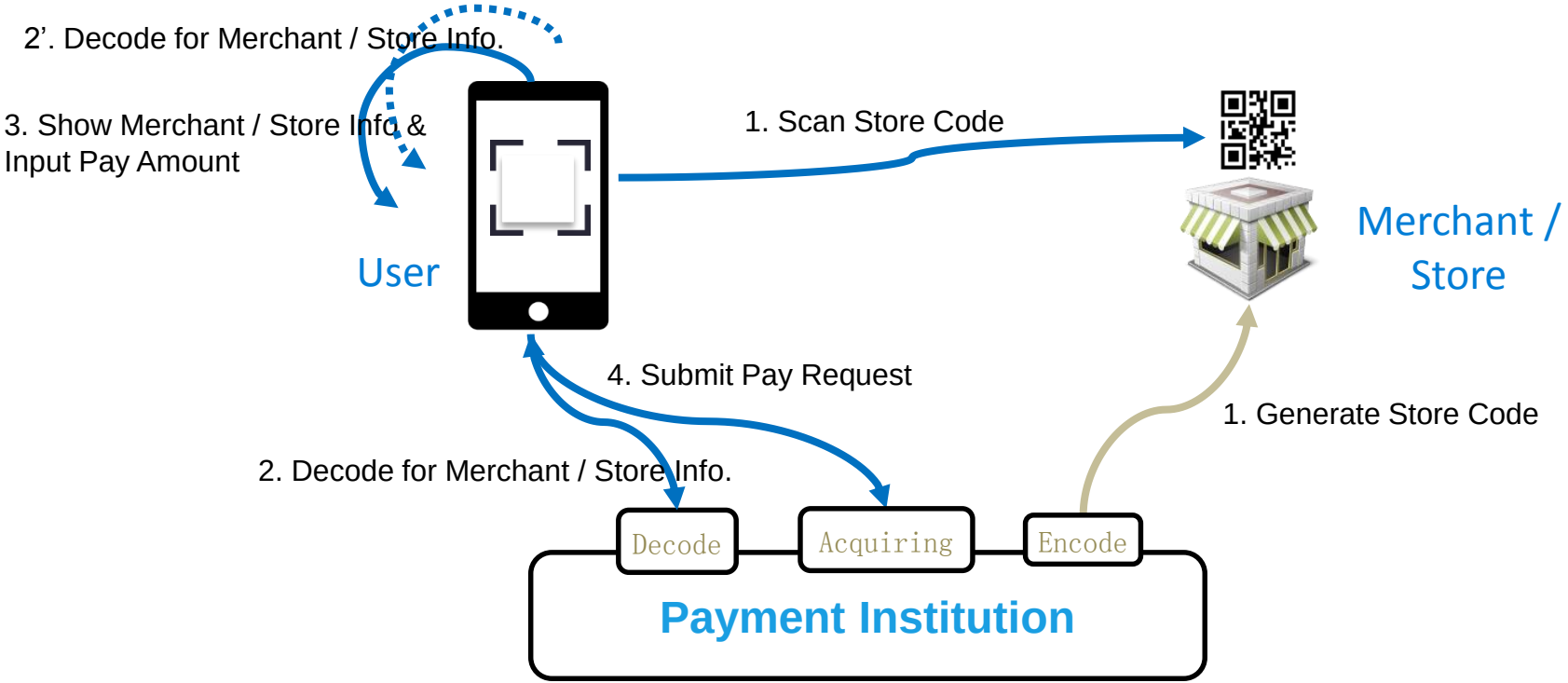
Code value:
28xxxxxxxxxxxxx

Payee-presented code:
- Network protocol
- Domain name
- Retrieval ID

Payer-presented code:
- Routing block
- Authorization Token

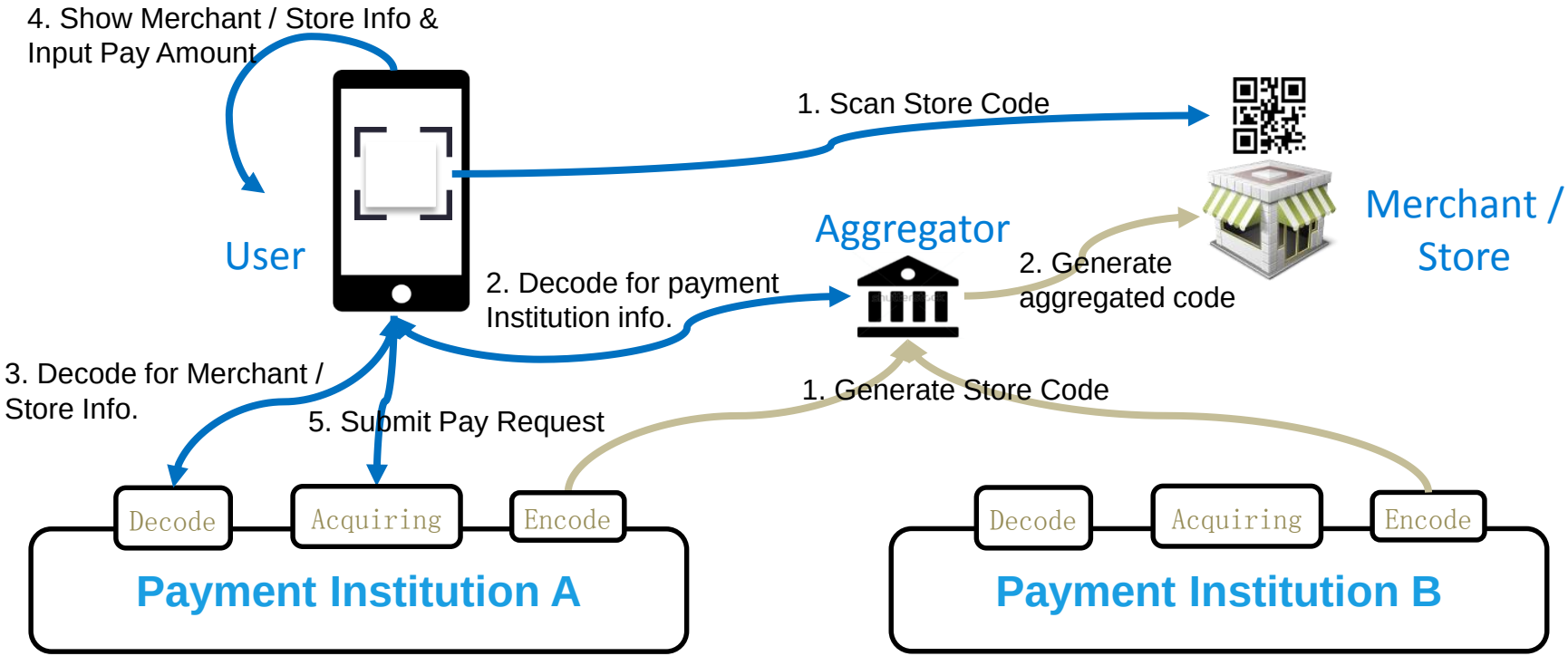
General transaction flow

Payee-presented mode



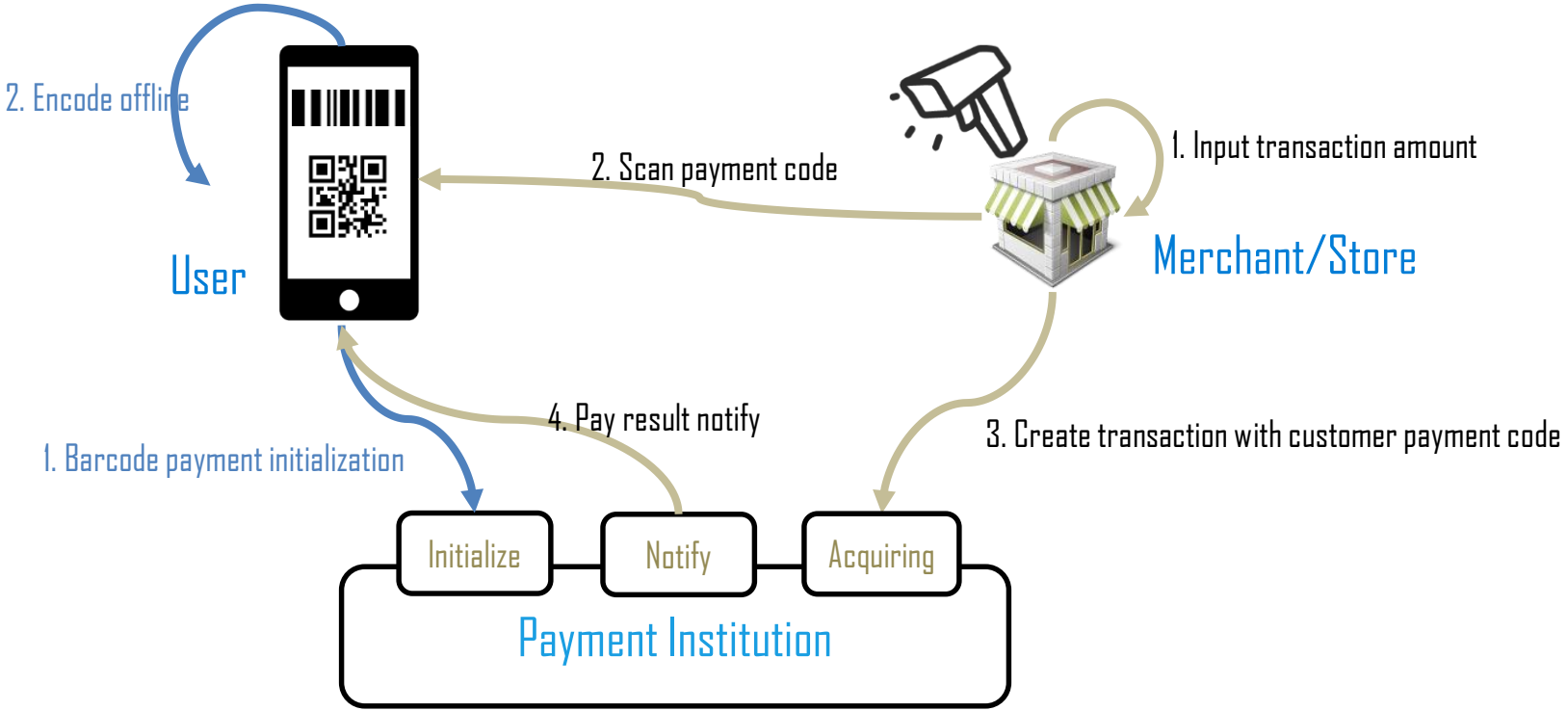
General transaction flow

Payee-presented mode, aggregated code



General transaction flow

Payer-presented mode



Threat analysis (non-exhaustive)

Specific to payee-presented code

- Code containing harmful information
- Code being misplaced, replaced, covered up, stained or altered
- Exposure of merchant business data
- Threats related to URL and redirect
- Threats related to aggregation code

Specific to payer-presented code

- Exposure of user payment account
- Replay of user authorization tokens
- Bar code leakage by screen capture or sharing

Common

- Threats to network communication
- Threats to transactions and user funds
- Threats to sensitive data
- Threats to mobile APPs (user agents)
- Threats to user devices
- Threats to merchant devices
- Threats to servers

Security requirements and measures

Payee-presented mode

Point of Interaction	Payee sensitive data	URL and redirect	Aggregation code
• Secure generating, presenting, and reading of bar codes • Use of anti-counterfeiting technology • etc	• Bar code information organization (what's presented, what's not) • Use of tokenization or similar technology • etc	• Anti-phishing • Verification of transaction information • etc	• Management of sensitive data • Security of user funds • Traceability of transactions • etc

Security requirements and measures

Payer-presented mode

Point of Interaction

- Secure generating, presenting, and reading of bar codes
- Anti-replay
- Screen capture warnings
- etc

Payer sensitive data

- Bar code information organization (what's presented, what's not)
- Use of tokenization or similar technology
- etc

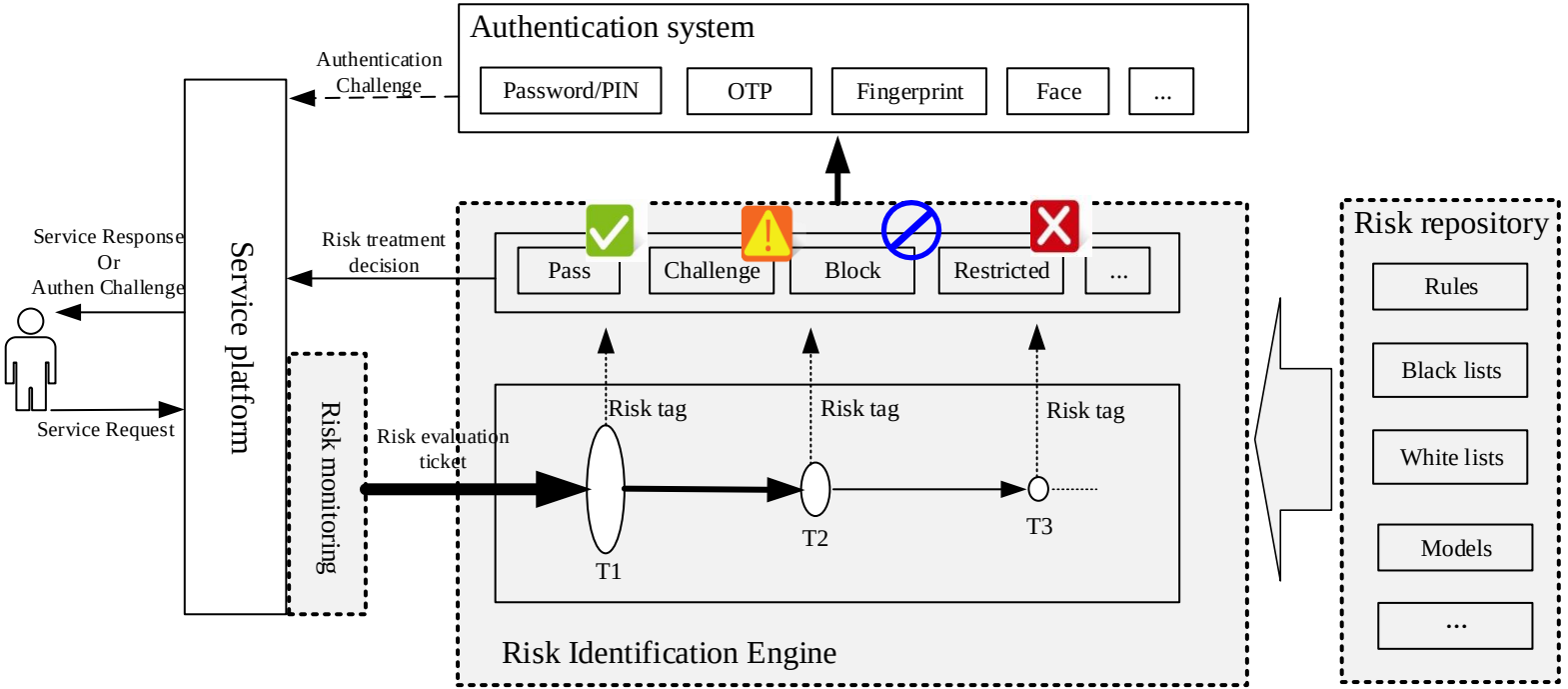
Security requirements and measures

Common

Infrastructure	Mobile devices and APPs	Transactions
• Data security and recovery • Application security (eg. Web) • Host security • Network security • Physical security	• Human-machine interactions • Client software security • Communication security	• Secure processing of transaction data • Payer identification, authentication, authorization • Identifying and handling of transaction risks • etc

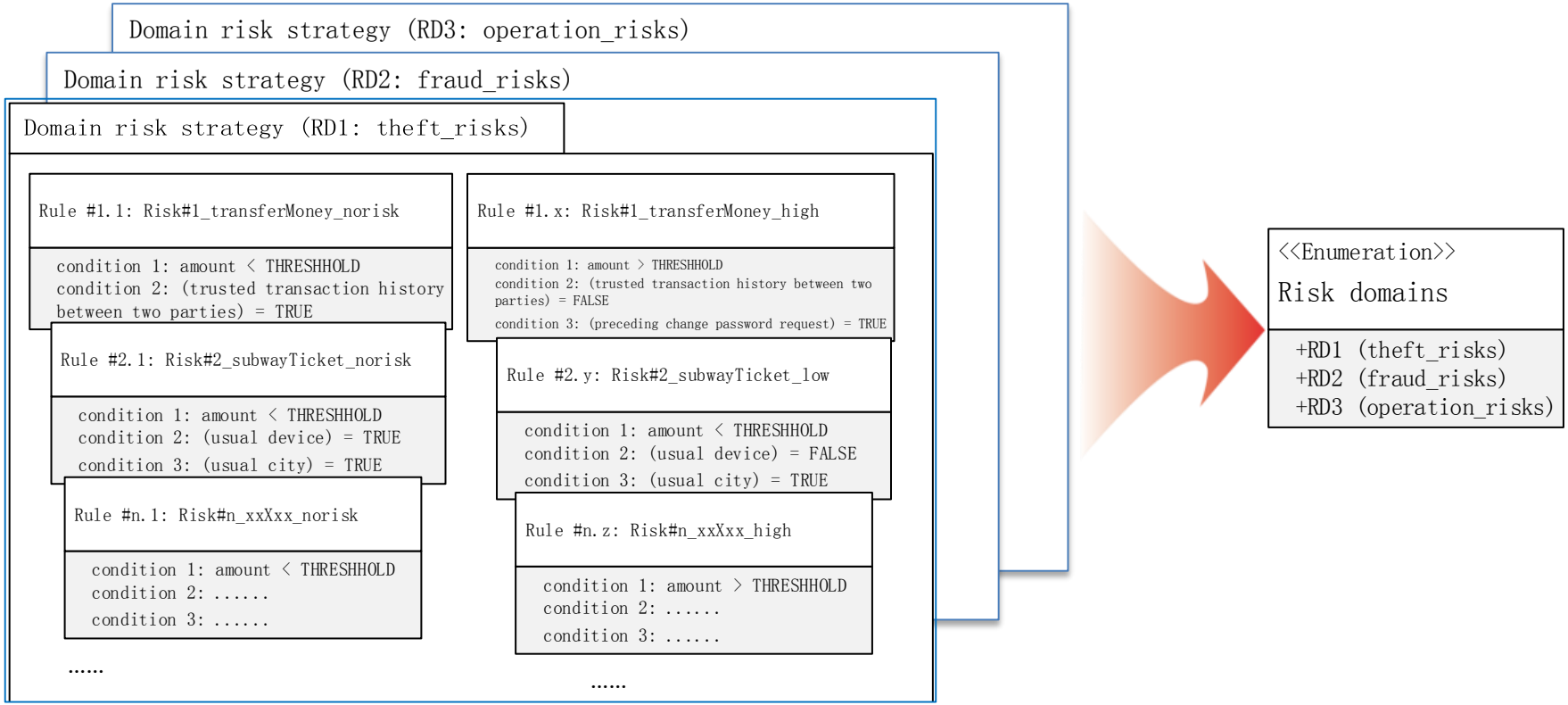
Identifying and handling of transaction risks

- X.tfrca: Technical Framework of risk identification to enhance authentication



Identifying and handling of transaction risks

- X.tfrca: Technical Framework of risk identification to enhance authentication



Other related standardization work

- Payer identification, authentication, authorization
  - ISO/IEC WD 27553 Information technology -- Security techniques -- Security requirements for authentication using biometrics on mobile devices
    @ ISO/IEC JTC1 SC27 WG5
  - IEEE P2790 Biometric Liveness Detection
    @ IEEE Cybersecurity and Privacy Standards Committee
  - Proposed study group on Security aspects of bar code payment
    @ ISO TC68 SC2

- TBD

Thanks!

Contacts:
Min ZUO, zuomin.zm@alipay.com