PRIVACY PRESERVING RISK CONTROLS

IMDA PET SANDBOX – ANT INTERNATIONAL CASE STUDY

INFOCOMM MEDIA DEVELOPMENT AUTHORITY

Contents

Use Case Background

Current process

1. Processing risk controls for payment requests and marketing discounts require data from partners, e.g. merchants, acquirers, wallet partners to satisfy business rules. Ant International ("Ant") typically works closely with these partners to collect, store and process such data points.

Opportunity

2. Ant is exploring the use of PETs to conduct risk controls without the need to collect and store sensitive data.
3. Alipay+, Ant's payment infrastructure, is being enhanced to include the use of MPC, as an additional data protection safeguard when processing risk control checks.
4. The use of MPC would ensure that the sensitive data belonging to the collaborating merchant and wallet partners will remain in their servers and would not need to be collected and stored by Ant; nevertheless, Ant would still be able to process the relevant risk controls.

Use Case Details

Key POC Stakeholders: (See Annex 1 for overall process flow across all stakeholders)

5. **Payment Infrastructure Provider** - Ant International, owner of payment infrastructure that links between acquirer and payment systems
6. **Merchant** – Provider of services and user interface that customers would interact with to make payment
7. **Acquirer** – Owner of backend system to support merchants in processing transactions.
8. **Wallet** – Facilitate the crediting or debiting of funds following payment risk controls checks by Ant

Proof of Concept and use of MPC

9. Ant will be conducting two POC scenarios to process two different risk control programmes.
   a. **Payment risk control (two-party):** To determine if a transaction, based on data from Acquirer, would be classified as "transport" related.

b. **Market voucher eligibility (three-party):** To determine if a customer, based on data from Acquirer and Wallet Partner would be eligible for a discount

10. Within MPC, specifically Garbled Circuits (GC) and the Oblivious Transfer (OT) Protocol are used as part of the Risk Control Program, to ensure inputs from respective stakeholders, e.g. Acquirer and Wallet remain private, and no data is shared when conducting risk controls.

a. The use of Garbled Circuits is intended to protect the privacy of potentially sensitive input data by transforming them into unintelligible encrypted data. This process primarily hides Acquirer's and Wallet's inputs from Ant.
b. The use of the Oblivious Transfer Protocol ensures that in a scenario with two collaborators, when the sender shares a set of decryption key options to the recipient, the sender does not know which option the recipient was able to gain access to. This process primarily hides Ant's inputs from the Acquirer and Wallet.

Scenario 1 – Payment Risk Control

11. Following the payment request, risk control checks would occur to determine if transaction can be classified under "transport".

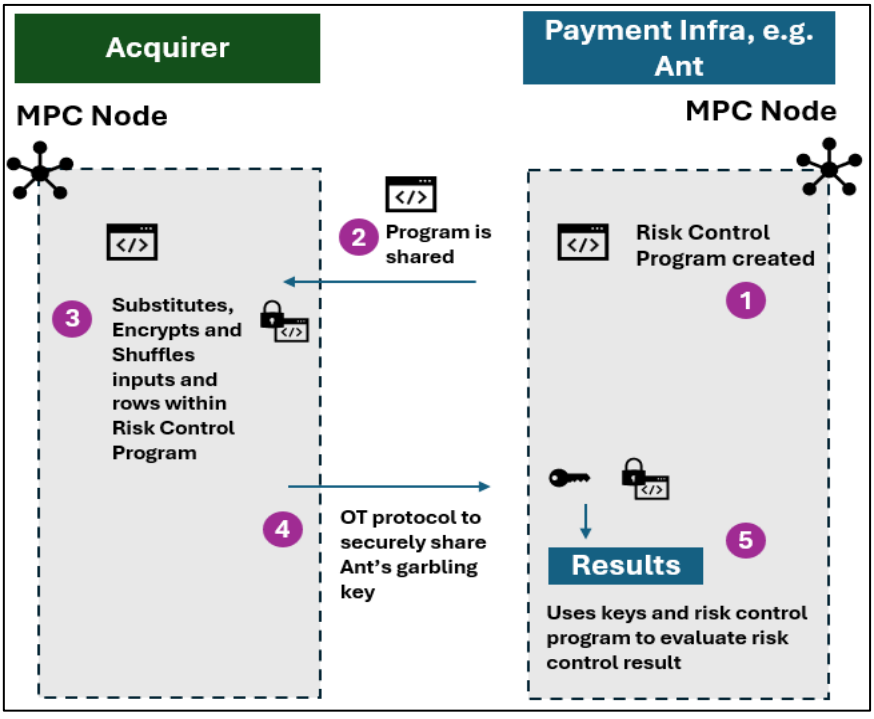


Diagram 2: MPC process in a two-party payment risk control process

a. **Step 1: Setting up of the risk control program that encodes Ant's business rules and thresholds,** e.g. if transaction amount is greater than a certain value, then it fulfils a certain threshold or business rule, and would be classified accordingly. Essentially, the risk control program is a "formula", and the correct inputs from Ant and Acquirer, e.g. X and Y, will produce the risk control evaluation result.

b. **Step 2: Ant sends** the risk control program to the Acquirer in the form of a Truth Table, i.e. a mapping that represents possible permutations of inputs and outputs, represented in a binary form of 0's and 1's. **(See Annex 2 for more information on Truth Tables).** This is done as part of the MPC process to ensure inputs from Ant and Acquirer remain hidden from one another**.**

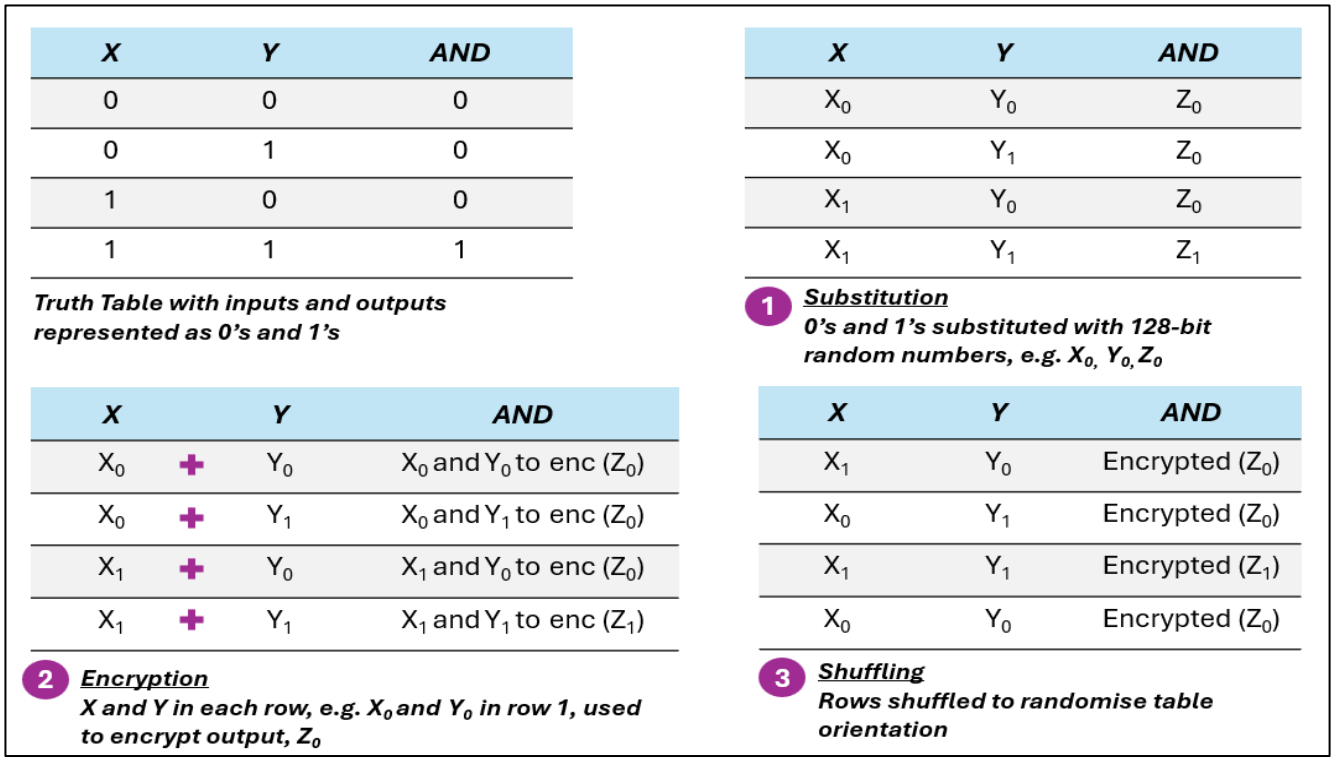


Diagram 3 [for step 3 below]: Value Substitution, Encryption and Shuffling within Simplified Risk Control Program. X and Y represent Acquirer and Ant's private inputs respectively. Z represents Evaluation Results based on X and Y. ***[Note: The Truth Table is a simplified version where columns X and Y are only 1 bit each, for the purpose of explanation. In the POC, X and Y columns in the truth tables used by Ant are usually 64 bit long. This means there are 2^{64} (~18.5 quintillion, 1.84 x 10^{19}) possibilities of Y given a single X input.]***

c. **Step 3:** To ensure inputs from both Acquirer and Ant are kept private but can still be computed to produce an evaluation result, the Acquirer undertakes three steps:

i. **Substitution:** Acquirer substitutes inputs in columns X and Y into four distinct random 128-bit strings, represented as X_0, X_1, Y_0, and Y_1. The intention of

substituting (and shuffling as outlined in iii. below), are key steps to hide Acquirer's input from Ant. Without substitution, knowledge of a "0 or 1" input in the Truth Table may allow for a re-identification of the real value, e.g. "101" corresponds to 5.

ii. **Encryption:** Acquirer uses X_0, X_1, etc as **'garbling (encryption) keys'** to encrypt the output, Z. Each output Z across the four rows is encrypted with two different keys to create **four uniquely encrypted outputs**. The key intention of encryption is to tie X and Y inputs in a row with the output Z, **to allow for uniqueness.** This ensures that only the correct pair of keys when used together, will decrypt a single, correct output.

iii. **Shuffling:** Truth Tables are typically arranged in a standardised format: "0,0", "0,1" "1,0" and "1,1". Shuffling the rows randomises the format, further reducing the risk of re-identification when the table is shared with Ant.

d. **Step 4:** Out of the four rows within the Truth Table, only one evaluation result would be correct. **To decrypt the correct output, e.g. Z, Ant would require:**

i. **Acquirer's garbling key,** e.g. X0
ii. **Ant's garbling key,** e.g. Y_1.

At this point, the Acquirer had been responsible for substituting both X and Y inputs, encryption and shuffling of the Truth Table, and **therefore possesses all the garbling keys, including Ant's**. **The Oblivious Transfer (OT) Protocol** is a privacy preserving protocol that enables the Acquirer to share a set of garbling key options with Ant, **without the Acquirer knowing** which correct option Ant eventually chose.

OT process

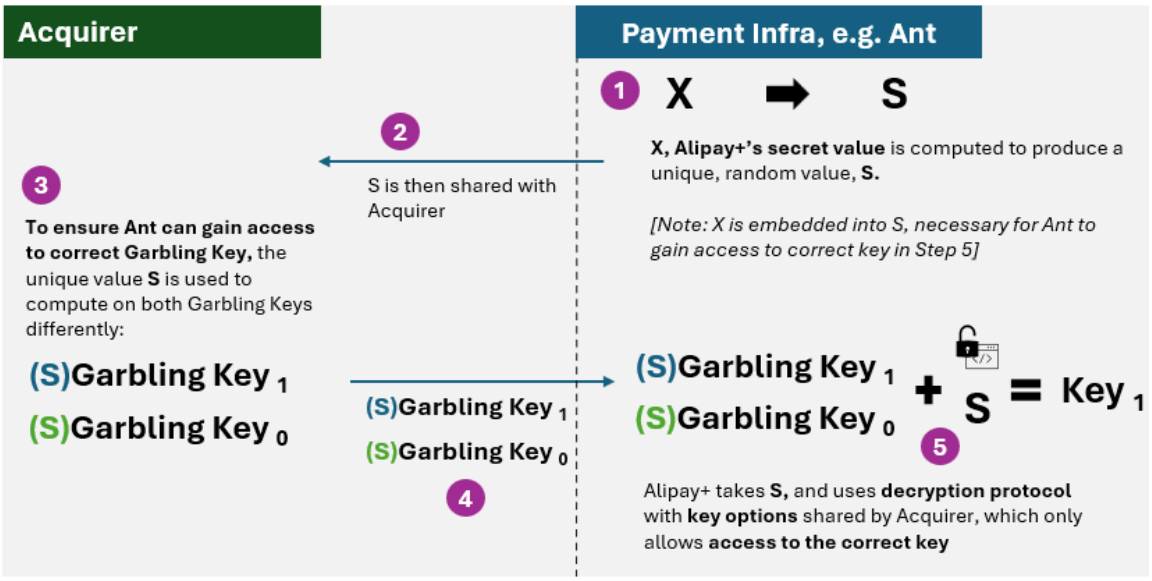


Diagram 4: Simplified OT protocol

i. **Step 1:** Ant's real value, e.g. 5, to be used as part of the risk control process is represented as X. Ant computes X into a unique, random value S. This value S is embedded with Ant's real value, X and is represented as a 128-bit random number. *[Note: Embedding with the real value allows Ant to use S to decrypt the correct garbling key in step 5, when presented with key options]*

ii. **Step 2:** Ant shares S with Acquirer, who holds Ant's garbling keys

iii. **Step 3:** To ensure Ant can only gain access to the correct garbling key, Acquirer uses S and computes on both Keys separately.

iv. **Step 4:** Acquirer sends both garbling keys back to Ant.

v. **Step 5:** Ant uses a **decryption protocol together with S** on both garbling keys, but only the **correct key can be decrypted.** As this step is done privately within Ant's environment, the Acquirer does not know which key Ant ultimately gained access to. **The OT protocol therefore protects the privacy of Ant's real value.**

e. **Step 5: Evaluating the result**

i. Ant requires three components to determine the evaluation result of the risk control program:

A. Ant's garbling key, e.g. Y_1
B. Acquirer's garbling key, e.g. X_0
C. Risk control program with encrypted outputs, e.g. Z

ii. Ant's garbling key was shared by the Acquirer using the OT protocol. The risk control program and Acquirer's garbling key are directly shared with Ant. *[Note:*

Acquirer's garbling key is a 128-bit random number and outputs of risk control program are encrypted. As the values are hidden, Ant does not know Acquirer's values]

iii. With the above three components, Ant can evaluate the result of the risk control program. The use of Garbled Circuits and OT protocol achieved the following:

A. **Protecting Ant's business policy threshold from Acquirer:** Using the OT protocol

B. **Protecting Acquirer's inputs, e.g. Merchant Information, from Ant:** Using the Garbled Circuits in step 3, where Substitution, Encryption and Shuffling was conducted.

Scenario 2 – Marketing Risk Control

12. Evaluating whether a transaction is eligible for a marketing voucher.

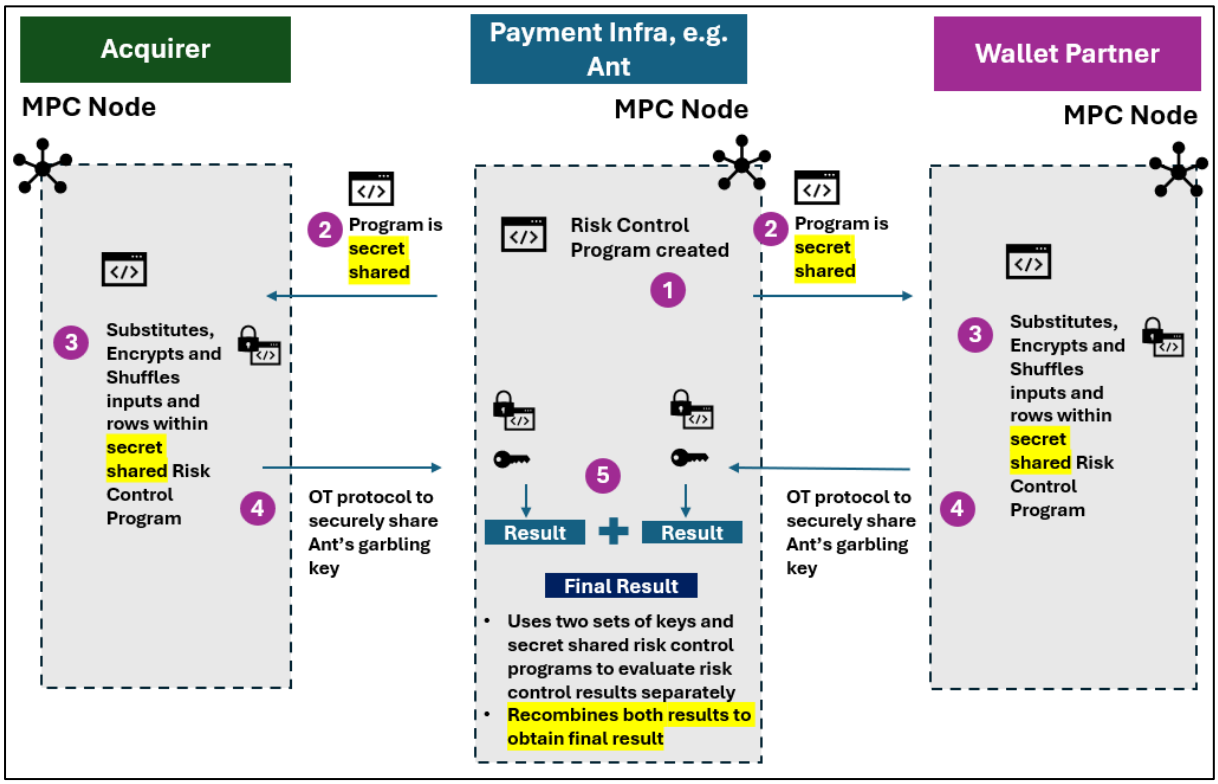


Diagram 4: Three-party marketing risk control to determine voucher eligibility

a. In this scenario, the key differences from Scenario 1 are as follows:

i. Three parties – In this risk control, data from the Wallet partner is also required.

ii. **Secret sharing of risk control program -** In any risk control check, only one risk control program would be created. With three parties, an additional step occurs in **Step 2, – secret sharing of the programme.** The objective of secret sharing is to ensure both parties, Acquirer and Wallet, can compute on their respective secret shared risk control program without Ant seeing either of the Acquirer and Wallet's real data.

iii. **Recombining results from both parties -** In Step 5, Ant would obtain two results from evaluating two sets of garbling keys and risk control program from Acquirer and Ant. The two results would finally be recombined to produce the final evaluation result.

Regulatory Learnings

13. Ant sought Practical Guidance (Guidance) from the Personal Data Protection Commission (PDPC) on the following:

    a. Is the data, e.g. garbling keys, secret value in the Oblivious Transfer (OT) protocol shared via MPC between the Wallet and Acquirer to Ant International considered anonymised data?

    b. Does this MPC workflow satisfy cross-border data transfer regulations by PDPA?

    c. What are the recommended best practices that wallets and acquirers should implement as part of this MPC risk control workflow?

PDPC's assessment

Is the data, e.g. garbling keys, secret values in the Oblivious Transfer (OT) protocol shared via MPC between the Wallet and Acquirer to Ant International considered anonymised data?

The execution of the MPC protocol with implemented technical safeguards and best practices

14. With the use of MPC protocol across both two-party and three-party scenarios, PDPC understands that Ant International would now not need to collect the following datapoints: Merchant MCC, Merchant Legal Name, Merchant ZIP Code and Merchant Registration Region from the Acquirer, and Payment History from Wallet Partner, as these datapoints would constitute the inputs provided by the Acquirer and Wallet Partner into the Risk Control Program. In doing so, PDPC notes that less data is being collected, aligning with the data minimisation principle, whilst still enabling the processing of risk controls. In addition, the following data protection safeguards have been put in place:

a. **Substitution of inputs:** Acquirer and Wallet Partner would substitute Risk Control Program inputs, e.g. 0 or 1's in the Truth Table into 128-bit random strings. The random strings are unintelligible to either party to prevent association and re-identification of inputs.

b. **Shuffling of Truth Table:** The shuffling process helps to further reduce the possibility of re-identification by randomising the usually standardised format and patterns in which a Truth Table is set up.

c. **Use of sufficiently large Truth Tables**: Ant International uses Truth Tables that have X and Y inputs which are 64-bit long, e.g. X_1, X_2…. $X_{64.}$ Doing so greatly increases the number of possible inputs in the risk control program and is another measure to reduce the probability to re-identify the other party's corresponding input.

d. **Oblivious Transfer Protocol**: A well-recognized cryptographic algorithm that ensures a sender (Acquirer/Wallet) of a set of garbling keys would not be aware which single key within the set was selected by the recipient (Ant), and the sender remains unaware of the keys which were not selected, thereby protecting the privacy of the recipient's (Ant) input.

e. **Secret Sharing of Truth Table:** In the three-party scenario, the risk control program is further secret shared to ensure that the Acquirer and Wallet can compute on their respective parts of the risk control program without Ant or either the Acquirer or Wallet seeing each other's real data.

15. PDPC also notes that Ant International has implemented MPC in accordance with industry recognised practices and standards.[1]

16. Personal data is defined in section 2 of the PDPA to refer to data, whether true or not, about an individual who can be identified (a) from that data; or (b) from that data and other information to which the organization has or is likely to have access.

17. Based on the above, PDPC is of the view that there is **no serious possibility that the Acquirer, Wallet Partner and Ant would be able to identify individuals from the data that it receives from each other within the MPC workflow, or that a third party who obtains the data will be able to identify individuals from it.** Hence, the datapoints (Merchant MCC, Merchant Legal Name, Merchant ZIP Code and Merchant Registration Region from the Acquirer, and Payment History from Wallet Partner) shared between

[1] Two-party scenario implemented in accordance with draft ISO/IEC 4922-3 Mechanisms based on garbled circuit

Acquirer and Wallet Partner to Ant International in the MPC workflows **would not be considered personal data** and sharing it between the Acquirer, Wallet Partner and Ant for the purpose of the two risk control scenarios would not constitute disclosure of personal data.

18. However, if additional data which makes it possible to identify an individual will be included in the MPC workflow in the future, Ant should seek further guidance from PDPC.

Recommended Best Practices

19. In the design of the risk control program, PDPC notes that the input data used for both the two-party scenario for payment risk control and three-party scenario for market eligibility are necessary for the risk control evaluation. However, where personal data may be used as part of the input dataset for the purpose of the risk control evaluation, only necessary and relevant datasets should be used to ensure purpose limitation.

20. All parties collaborating within the MPC workflow should ensure that the measures and security arrangements implemented to prevent the risk of re-identification and protect against data protection threats remain effective and up to date. This includes keeping the PETs used in the POC updated with prevailing industry-recognised processes and standards and ensuring "cryptographic agility" by replacing cryptography algorithms that are found to be vulnerable.

21. When implementing cryptographic algorithms, to consider choosing the maximum supported encryption key length and randomness defined within the cryptographic specification and reference standards as far as practicable.

22. It is recommended that the Acquirer and Wallet employ sufficient measures to protect the garbling mapping of the control circuit to garbled circuit using industry standard encryption measures e.g. AES-256 and to securely protect the encryption keys by storing them separately away from the encrypted data.

23. PDPC recognises that the use of MPC has been useful towards protecting business sensitive data by minimising amount of data collected. Its use has also made more data available for analysis that otherwise may have been challenging to be directly shared, e.g. payment history data in three-party scenario.

Does this MPC workflow satisfy cross-border data transfer regulations by PDPA (i.e. would the Transfer Limitation Obligation under the PDPA apply to the MPC workflow)?

24. As per paragraph 17 above, since datapoints shared in the MPC workflow would not be considered personal data, PDPA data protection obligations will not apply.

Results and Next Steps

25. The use of MPC helped to minimise data collected by Alipay+ for risk control purposes, ensuring that sensitive information from the Acquirer is stored locally, and that Alipay+ does not see any of it.

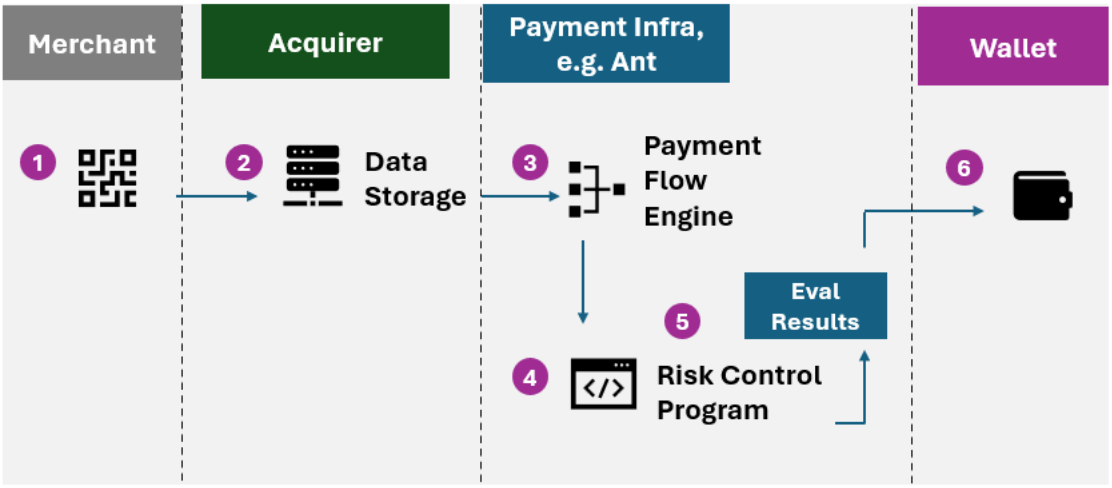
26. In terms of latency, the total time added to each transaction **increased by 200ms** after using MPC, which was deemed suitable and within performance thresholds, **with negligible impact to customer experience.**

27. **With the success of privacy preserving risk control processing, Ant can also support other business scenarios such as:**

    a. Fraud Detection - Stolen cards can be detected and corresponding transactions would be halted.
    b. Anti-Money Laundering - Suspicious large transactions can be flagged and reported.
    c. Sanction List - Identifying sales of prohibited items or transactions involving sanctioned personnel
    d. Credit Risk Assessment - Assessing credit risk of acquirers or wallet partners

28. The use of PETs is a critical part of Ant's privacy upgrade for their Acquirer and Wallet partners, and its success would continue to enable more production use cases, with privacy a cornerstone of all products.

Annex 1 – End to end payments flow



Details:

1 – Customer scans QR code to pay
2 – Customer data stored locally
3 – Scanning triggers payment request to Ant
4 – Risk control checks happen (Where MPC happens)
5 - 6 – Depending on result (e.g. true or false), payment request would flow to payment provider to complete the transaction, or it may be cancelled.

Annex 2 – More info on Truth Table

X – Acquirer ***(Input - Merchant Code to compare against, e.g. 345)***	**Y – Ant Intl** ***(Input - Ant's Threshold to compare against, e.g. $200)***	**Result** **(AND)**
300 =/= 345, therefore **0**	150 =/= 200, therefore **0**	**0**
300 =/= 345, therefore **0**	200 = 200, therefore **1**	**0**
345 = 345, therefore **1**	150 =/= 200, therefore **0**	**0**
345 = 345, therefore **1**	200 = 200, therefore **1**	**1**

Diagram: An example of a 1-bit x 1-bit AND Truth Table

Creation of the "Risk Control Program", i.e. the Truth Table

It includes a mapping of all possible permutations of inputs and outputs from both parties, represented in binary format, 0 and 1s.

Each column includes "encoded business rules" that inputs would be compared against, e.g. transaction value needs to be more than $200