Pay How does it work ?

 Pay was launched in 2014 and is now used by millions of users. In order to understand how Pay works some others actors need to be introduced first:

- **Issuer Bank:** The bank the payment card is associated with.
- **Token Service Provider***(TSP)*: An entity authorized to issue payments tokens according to the data transmission format of EMVCo.
- **Merchant Bank:** The bank of the merchant where the payment card is used.
- **Contactless Point of Sale***(POS)*: A device that bridges the payment card to the merchant bank.
- **Payment Network:** Handles payment transactions between banks, e.g: USA VisaNet

Adding a card to Pay

1) An device sends the card Primary Account Number*(PAN)* and other information to the Pay servers.
2) The Pay servers use the PAN to identify the issuer bank, and request from it authorization*(Payment token - PT)* sending the necessary information, like the PAN.
3) The issuer bank requests a PT to a TSP, sending the information provided in 2.
4) The TSP generates a PT, associates it with the PAN and vaults it. The PT and a Payment Token Key*(PTK)* used as public key, are sent to the issuer bank.
5) The issuer banks gets the information from 4 and adds an additional public key called CVV-Key. It then returns all the information to the servers.
6) All the data is sent back to the device and saved in its Secure Element(SE). This final token is called a Device Account Number*(DAN)*.

Paying with Pay

1) Biometric authentication to the device SE.
2) SE generates:
    1) A Dynamic Cryptogram : Combination of PT, PTK, transaction amount, country code, date, …
    2) Dynamic CVV with the help of CVV-Key.
2) Transfer of Dynamic Cryptogram, Dynamic CVV, DAN, and other payment information to the POS trough NFC. The POS sends it to the merchant bank which forwards it to the payment network.
3) The payment network sends the Dynamic Cryptogram to the TSP which if successful returns the PAN to the payment network.
4) The Payment network sends the PAN and the Dynamic CVV to the issuer bank.
5) The issuer bank verifies the request and authorizes the transaction based on the user's balance.
6) The payment network gets a response from the issuer bank. The payment network sends the response to the merchant bank which allows the transaction on his side.
7) The merchant bank passes the response to the POS, which in turn transmits the response to the device where the payment was initiated. The transaction is finally completed.

LEGEND

ISSUER BANK

MERCHANT BANK

TSP

POS

PAYMENT NETWORK

Adding a card to Pay

START

DAN saved in SE

END

I PAN

6 PT, PTK, CVV-Key

Sends PAN, requests PT 2

5 PT, PTK, CVV-Key

Sends PAN, requests PT 3

4 PT, PTK

 Servers

Paying with Pay

START I

Biometric auth

SE

Generation of Dynamic Cryptogram(DC) & Dynamic CVV (DCVV) 2

DAN, DC, DCVV, payment 3

When authorisation received, notifies device trough NFC

II END Transaction authorisation

DAN, DC, DCVV, payment info 4

10 Transaction authorisation

DAN, DC, DCVV, payment info 5

Decrypts DCVV, validates transaction

8 PAN, payment info, DCVV

Transaction authorisation 9

PAN 7

DAN & DC 6

REFERENCES

- [Pay security and privacy overview]
- [Will dynamic CVVs become the ultimate in CC security?]
- [EMV-Cryptogram-ARQC Explained]
- [How Apple Pay works under the hood?]

REMARKS

- The issuer bank pays a small fee per transaction.
- Several devices support Pay, including watches.

Author

- Pedro Gomes: Github profile, webpage, pegomo896@zoho.eu, PGP fingerprint: 72EDA4D14F94A284C48B4D2BE64A43FDFC17827C