EMV-Compatible Anonymous Payments

Charles Olivier-Anclin

Journées de l'Axe SIC 2024

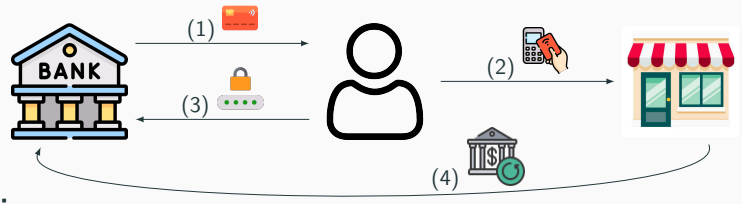
be ys Pay

Université Clermont-Auvergne, CNRS, Clermont-Auvergne-INP, LIMOS, Clermont-Ferrand, France

INSA Centre Val de Loire, Laboratoire d'informatique fondamental d'Orléans, France

Card payments & regulations

Payment processing standards:

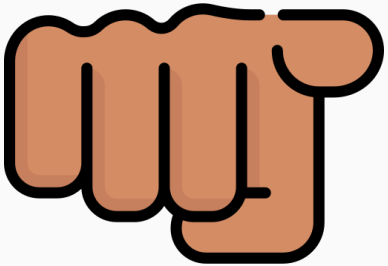


Regulations:

KYC: Know Your Customer

SCA: Strong Customer Authentication

AML: Anti-Money Laundering



You have no anonymity.

More generally, there is no anonymity.

Payments reveal the PAN

```
  5A | len:8  Application Primary Account Number: 1234567898765432

5F24 | len:3  Application Expiration Date YYMMDD: 240430
5F25 | len:3  Application Effective Date YYMMDD: 200401
5F28 | len:2  Issuer Country Code: 0826
9F02 | len:6  Amount, Authorised (Numeric):
       000000004600
9F1A | len:2  Terminal Country Code: 0826
  95 | len:5  Terminal Verification Results:
       0000008001
5F2A | len:2  Transaction Currency Code: 0826
  9A | len:3  Transaction Date: 210318
```

Payments reveal the PAN

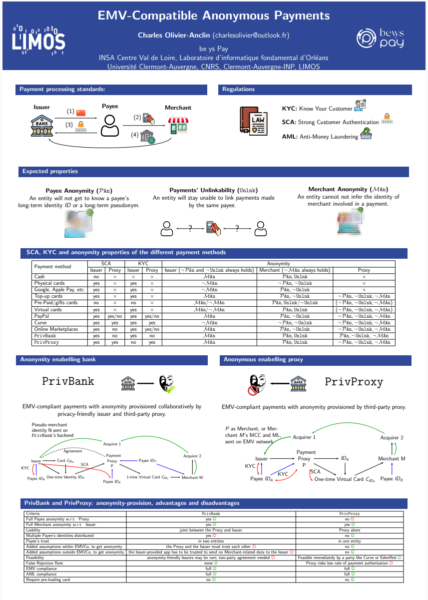
```
  5A | len:8  Application Primary Account Number: 1234567898765432

5F24 | len:3  Application Expiration Date YYMMDD: 240430
5F25 | len:3  Application Effective Date YYMMDD: 200401
5F28 | len:2  Issuer Country Code: 0826
9F02 | len:6  Amount, Authorised (Numer
       000000004600
9F1A | len:2  Terminal Country Code: 08
  95 | len:5  Terminal Verification Res
       0000008001
5F2A | len:2  Transaction Currency Code: 0826
  9A | len:3  Transaction Date: 210318
```

But can we bring (some) anonymity?

Short answer: yes ✓

How? Add an intermediary that we call **Proxy**.

Merci pour votre attention !



EMV-Compatible Anonymous Payments

Charles Olivier-Anclin (charlesolivier@outlook.fr)
be ys Pay
INSA Centre Val de Loire, Laboratoire d'informatique fondamental d'Orléans
Université Clermont-Auvergne, CNRS, Clermont-Auvergne-INP, LIMOS

Payment processing standards:

Regulations

KYC: Know Your Customer
SCA: Strong Customer Authentication
AML: Anti-Money Laundering

Expected properties

Payee Anonymity ($\mathcal{P}$An)
An entity will not get to know a payee's long-term identity *ID* or a long-term pseudonym.

Payments' Unlinkability (Unlnk)
An entity will stay unable to link payments made by the same payee.

Merchant Anonymity ($\mathcal{M}$An)
An entity cannot not infer the identity of merchant involved in a payment.

SCA, KYC and anonymity properties of the different payment methods

Payment method	SCA		KYC		Anonymity		
	Issuer	Proxy	Issuer	Proxy	Issuer ($\neg\mathcal{P}$An and $\neg$Unlnk always holds)	Merchant ($\neg\mathcal{M}$An always holds)	Proxy
Cash	no	×	×	×	$\mathcal{M}$An	$\mathcal{P}$An, Unlnk	×
Physical cards	yes	×	yes	×	$\neg\mathcal{M}$An	$\neg\mathcal{P}$An, $\neg$Unlnk	×
Google, Apple Pay, *etc.*	yes	×	yes	×	$\neg\mathcal{M}$An	$\mathcal{P}$An, $\neg$Unlnk	×
Top-up cards	yes	×	yes	×	$\mathcal{M}$An	$\mathcal{P}$An, $\neg$Unlnk	$\neg\mathcal{P}$An, $\neg$Unlnk, $\neg\mathcal{M}$An
Pre-Paid/gifts cards	no	×	no	×	$\mathcal{M}$An/$\neg\mathcal{M}$An	$\mathcal{P}$An, Unlnk/$\neg$Unlnk	($\neg\mathcal{P}$An, $\neg$Unlnk, $\neg\mathcal{M}$An)
Virtual cards	yes	×	yes	×	$\mathcal{M}$An/$\neg\mathcal{M}$An	$\mathcal{P}$An, Unlnk	($\neg\mathcal{P}$An, $\neg$Unlnk, $\neg\mathcal{M}$An)
PayPal	yes	yes/no	yes	yes/no	$\mathcal{M}$An	$\mathcal{P}$An, $\neg$Unlnk	$\neg\mathcal{P}$An, $\neg$Unlnk, $\neg\mathcal{M}$An
Curve	yes	yes	yes	yes	$\neg\mathcal{M}$An	$\neg\mathcal{P}$An, $\neg$Unlnk	$\neg\mathcal{P}$An, $\neg$Unlnk, $\neg\mathcal{M}$An
Online Marketplaces	yes	no	yes	yes/no	$\mathcal{M}$An	$\mathcal{P}$An, $\neg$Unlnk	$\neg\mathcal{P}$An, $\neg$Unlnk, $\neg\mathcal{M}$An
PrivBank	yes	no	yes	no	$\mathcal{M}$An	$\mathcal{P}$An, Unlnk	$\mathcal{P}$An, $\neg$Unlnk, $\neg\mathcal{M}$An
PrivProxy	yes	yes	no	yes	$\mathcal{M}$An	$\mathcal{P}$An, Unlnk	$\neg\mathcal{P}$An, $\neg$Unlnk, $\neg\mathcal{M}$An

Anonymity enabelling bank

PrivBank

EMV-compliant payments with anonymity provisioned collaboratively by privacy-friendly issuer and third-party proxy.

Anonymous enabelling proxy

PrivProxy

EMV-compliant payments with anonymity provisioned by third-party proxy.

PrivBank and PrivProxy: anonymity-provision, advantages and disadvantages

Criteria	PrivBank	PrivProxy
Full Payee anonymity w.r.t. Proxy	yes	no
Full Merchant anonymity w.r.t. Issuer	yes	yes
Liability	joint between the Proxy and Issuer	Proxy alone
Multiple Payee's identities distributed	yes	no
Payee's trust	in two entities	in one entity
Added assumptions within EMVCo, to get anonymity	the Proxy and the Issuer must trust each other	no
Added assumptions outside EMVCo, to get anonymity	the Issuer-provided app has to be trusted to send no Merchant-related data to the Issuer	no
Feasibility	anonymity-friendly Issuers may be rare; two-party agreement needed	Feasible immediately by a party like Curve or EdenRed
False Rejection Rate	none	Proxy risks low rate of payment authorisation
EMV compliance	full	full
AML compliance	full	full
Require pre-loading card	no	no