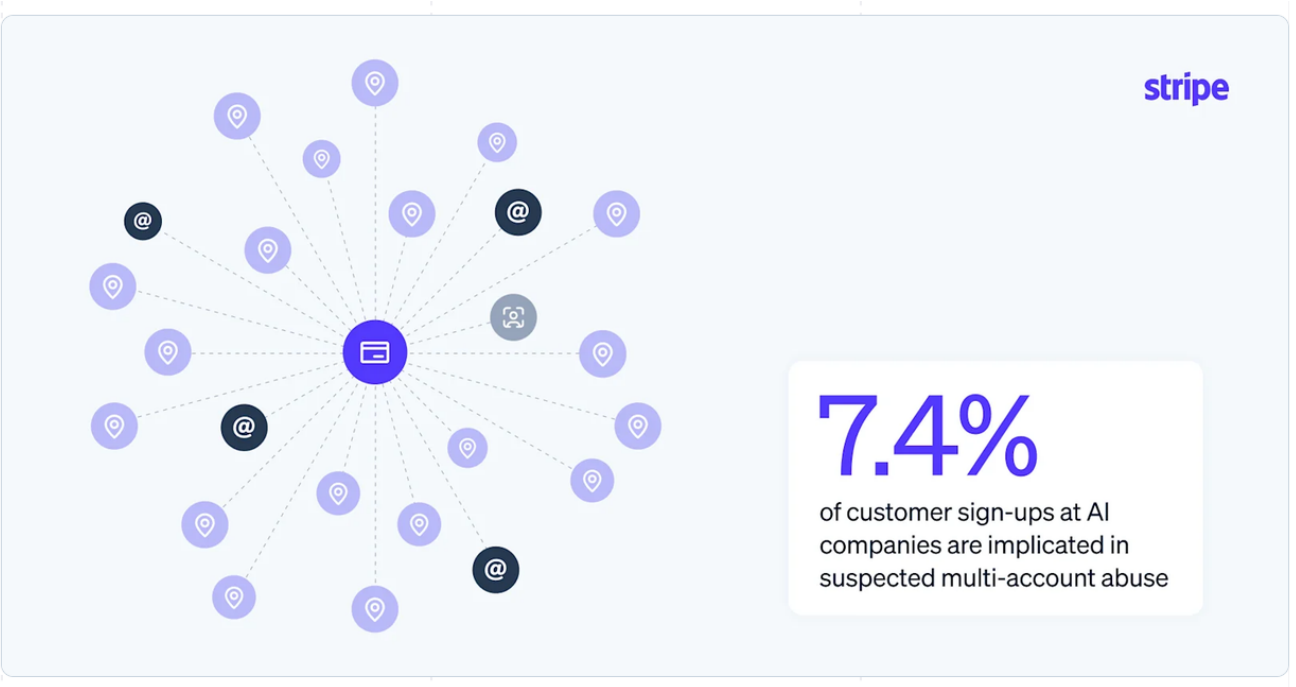
zkEMV: Private Credentials from EMV Offline Data Authentication

Lunch Talk @ Radboud University, Nijmegen
November 6, 2026

Anjan Roy

PhD @ Digital Security Group, Radboud University
and
Engineer @ Avail

Stripe Report from March, 2026 (1/2)



https://stripe.com/blog/analyzing-first-party-fraud-trends-account-free-trial-and-refund-abuse

Stripe Report from March, 2026 (1/2)

Free trial abuse is accelerating, driven by AI companies and the legitimate use of virtual cards

Free trials are necessary for customer evaluation, but they can be abused by users who violate common trial terms, such as cycling through multiple trials to get prolonged free access to a product or service.

AI Image Generation Platform Midjourney on March, 2023

Though the Washington Post report initially insinuated that the “abuse” in question was related to a recent slew of viral deepfakes, the company denies that account. “There were some pretty big misunderstandings in the [WaPo] article,” Holz wrote to Gizmodo in an email. “We stopped trials because of massive amounts of people making throwaway accounts to get free images…This happened at the same time as a temporary gpu shortage. The two things came together and it was bringing down the service for paid users,” he added.

https://gizmodo.com/midjourney-deep-fake-ai-trump-arrested-pope-1850283812

Fly.io free tier (1/2)

Free Postgres Databases



Annie Ruygt

Update, September 2026: the free Postgres allowance described in this 2022 post is gone. New accounts get a free trial instead, and today we recommend Managed Postgres for most apps.

https://fly.io/blog/free-postgres/

Fly.io free tier (2/2)

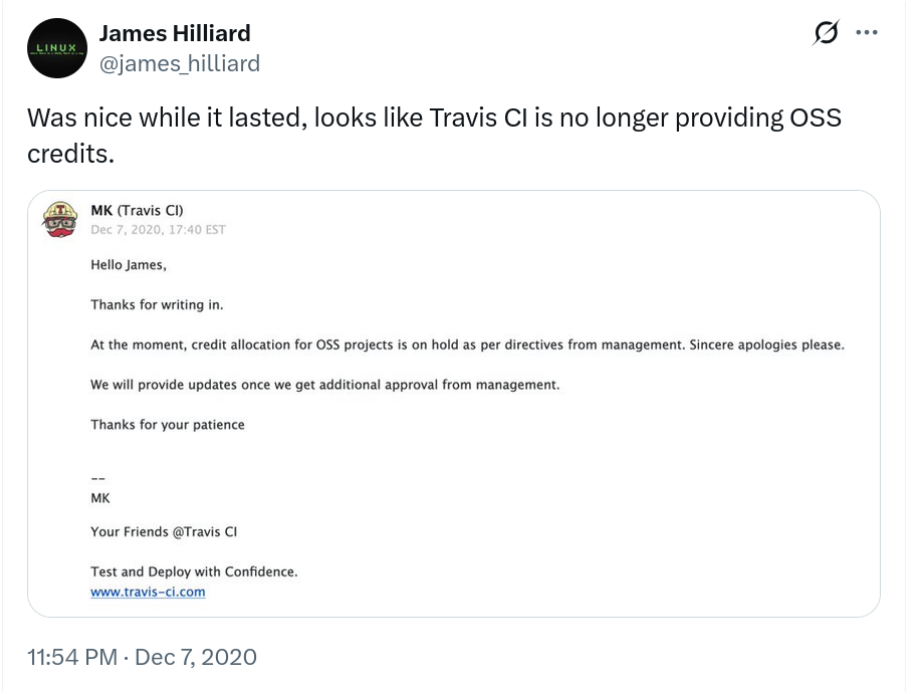
A note about credit cards

Even for our free services, we require a credit card number. We know that's the worst and it gives you heartburn. It's not because we plan to charge you.

But here's what happens if you give people freemium full access to a hosting platform: lots and lots of free VMs mining for cryptocurrencies.

We could tell you we want to prevent crypto mining because we care about the planet, and that would be true. We also have a capitalism nerve that hurts when people spend our money gambling. Your credit card number is the thin plastic line between us and chaos.

Travis CI free tier discontinuation from December, 2020



James Hilliard
@james_hilliard

Was nice while it lasted, looks like Travis CI is no longer providing OSS credits.

MK (Travis CI)
Dec 7, 2020, 17:40 EST

Hello James,

Thanks for writing in.

At the moment, credit allocation for OSS projects is on hold as per directives from management. Sincere apologies please.

We will provide updates once we get additional approval from management.

Thanks for your patience

--
MK

Your Friends @Travis CI

Test and Deploy with Confidence.
www.travis-ci.com

11:54 PM · Dec 7, 2020

https://x.com/james_hilliard/status/1336081776691843072

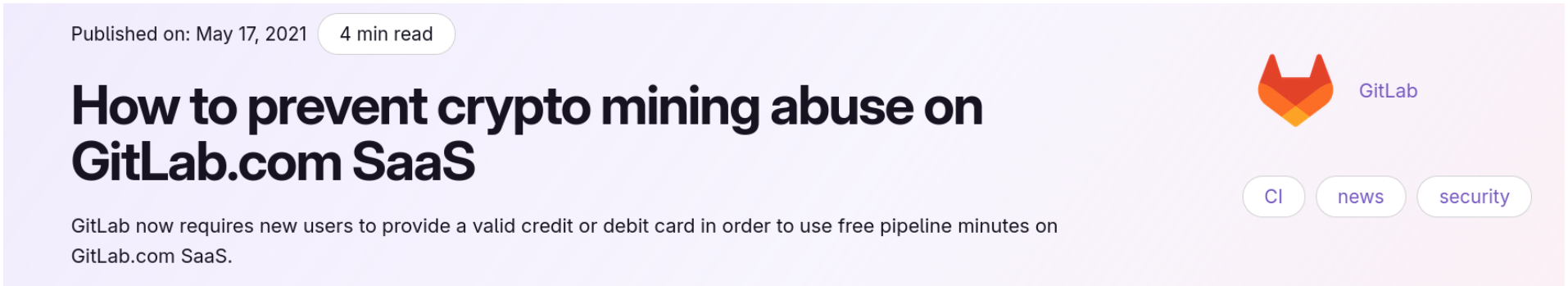
Heroku blog from June, 2024

Our product, engineering, and security teams are spending an extraordinary amount of effort to manage fraud and abuse of the Heroku free product plans. In order to focus our resources on delivering mission-critical capabilities for customers, we will be phasing out our free plan for Heroku Dynos, free plan for Heroku Postgres, and free plan for Heroku Data for Redis®, as well as deleting inactive accounts.

Starting October 26, 2022, we will begin deleting inactive accounts and associated storage for accounts that have been inactive for over a year. Starting November 28, 2022, we plan to stop offering free product plans and plan to start shutting down free dynos and data services. We will be sending out a series of email communications to affected users.

https://www.heroku.com/blog/next-chapter/

GitLab blog from May, 2021



https://about.gitlab.com/blog/prevent-crypto-mining-abuse/

It is called Sybil Attack.

How to resist Sybil attack?

Ask for verifying mobile number, adding a credit card or even showing a Govt. issued ID

Personally Identifiable Information (PII)

Customer

Give out card number, expiry, CVV and card-owner name.

Service Provider

🥲

Hopefully keeps it safe from data breach.

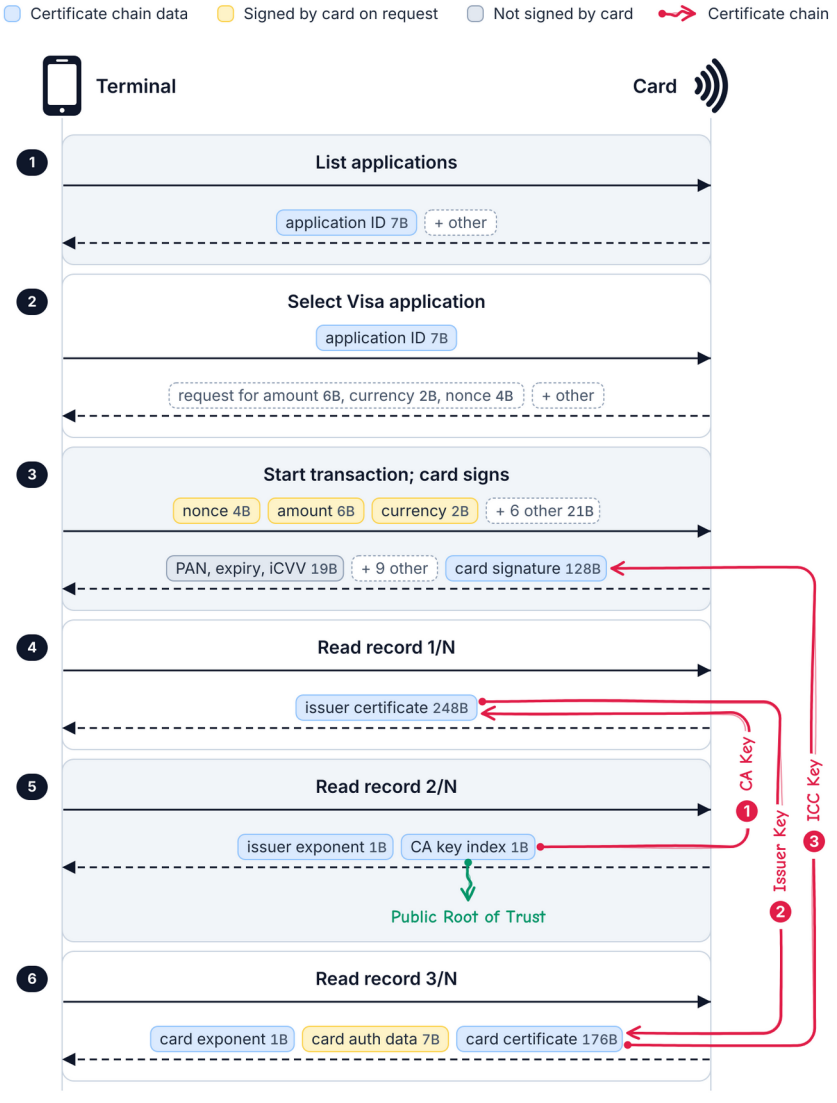
🤓

Privacy-concious customers are left from trying out the product or service.

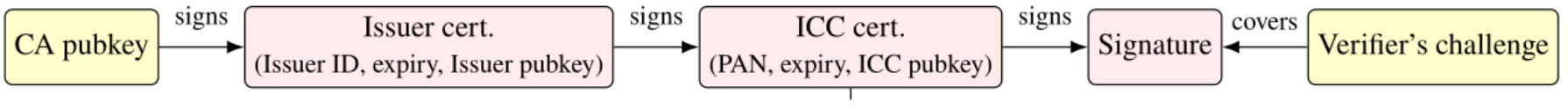
Good news!

EMV chip-cards implement Offline Data Authentication (ODA) protocol.

Visa Fast Dynamic Data Authentication (fDDA)



EMV Certificate-Chain



RSA + SHA-1



But there is a privacy risk with ODA.



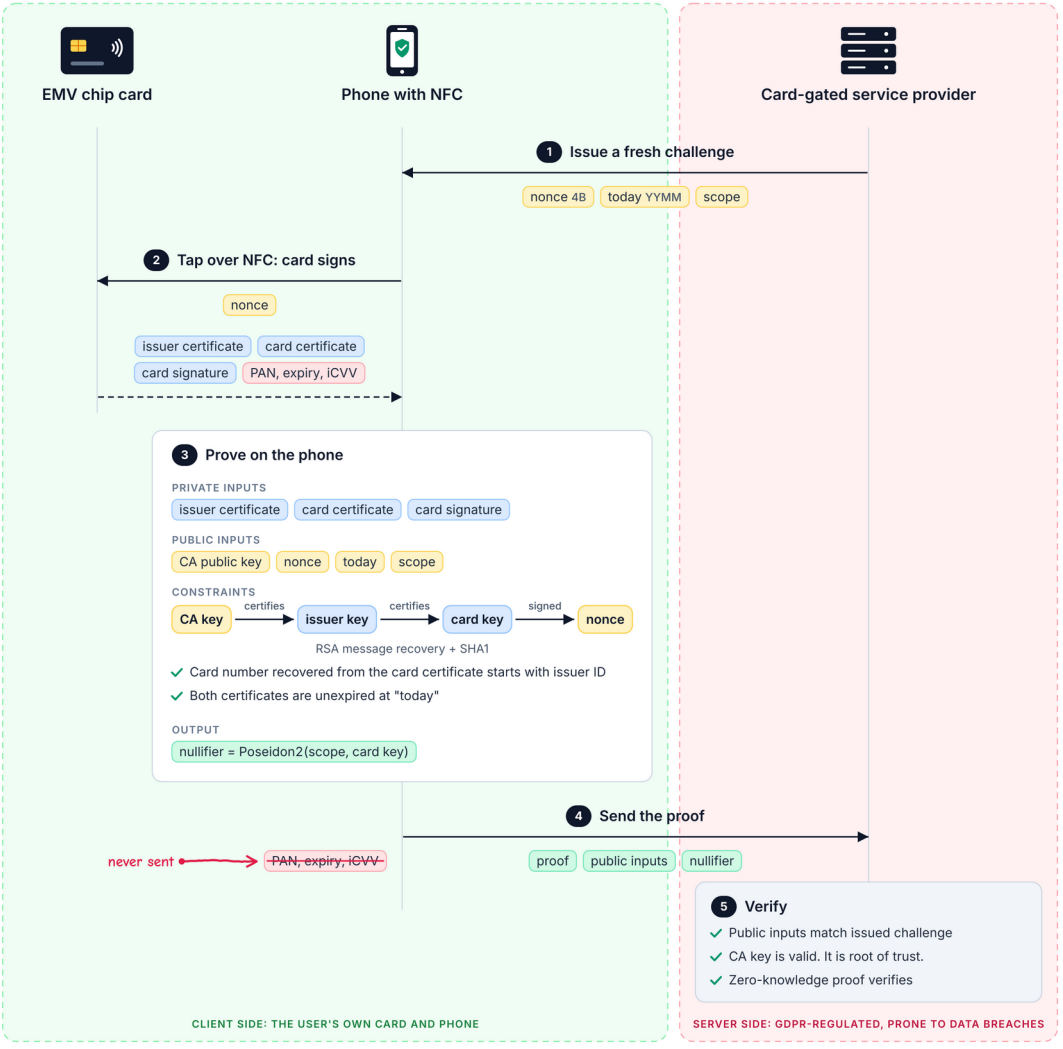
Card number (PAN) is part of the certificate-chain.

Solution

Zero-knowledge proof of EMV ODA.

ZKP of Possession of Genuine Chip-Based Contactless Card

Without revealing card number (PAN), expiry or CVV



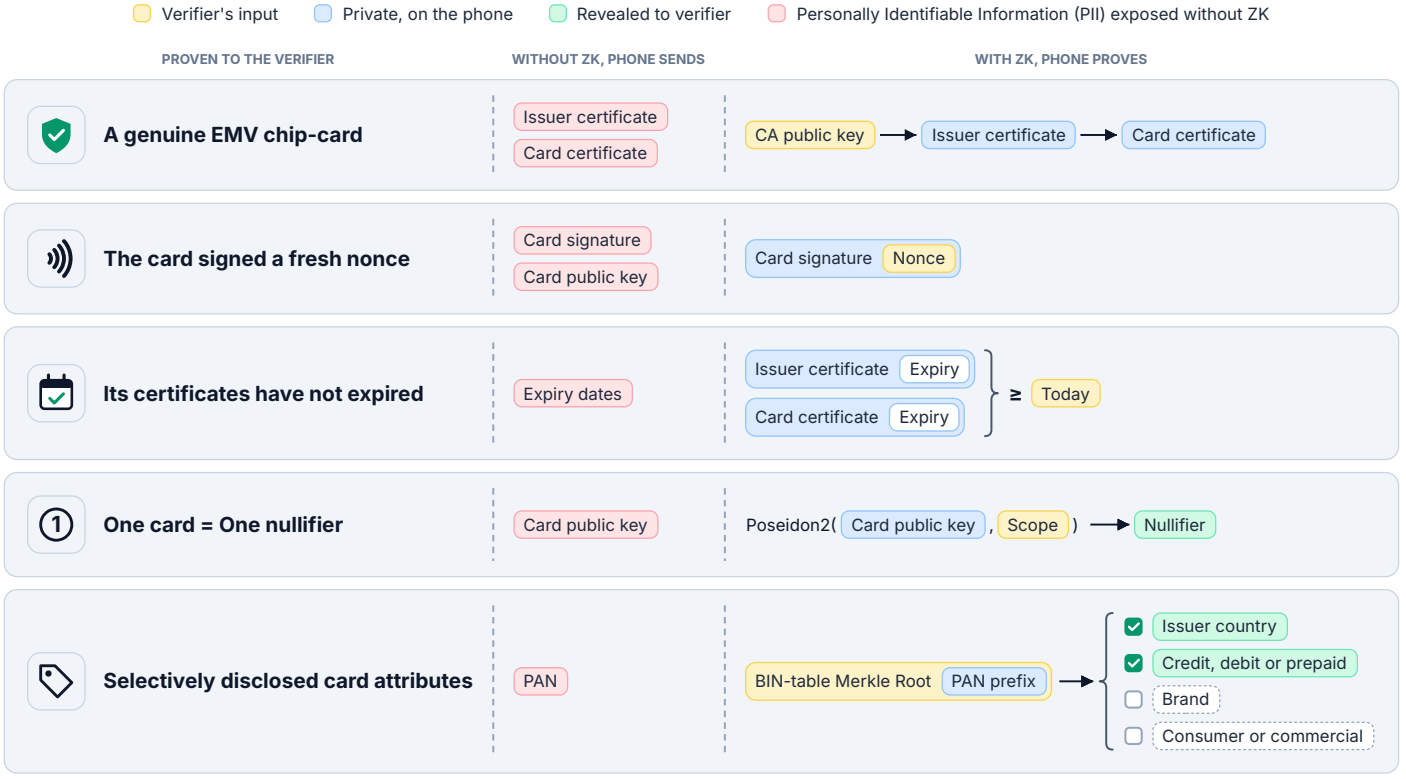
What is the nullifier?

A 32-byte unique identifier for a EMV card under a specific verifier-scope.

Unlinkable across verifier-scopes.

A domain separator.

What Can an EMV Card Tap Prove, Without Exposing PII?



What can zkEMV not prove?

- No proof of personhood.
- No privacy from card issuer or network.
- No payments use case.

What are the use cases of zkEMV?

- Privacy-respecting free tier service.
- Bot-free Discord-like communities.
- 2-factor authentication.

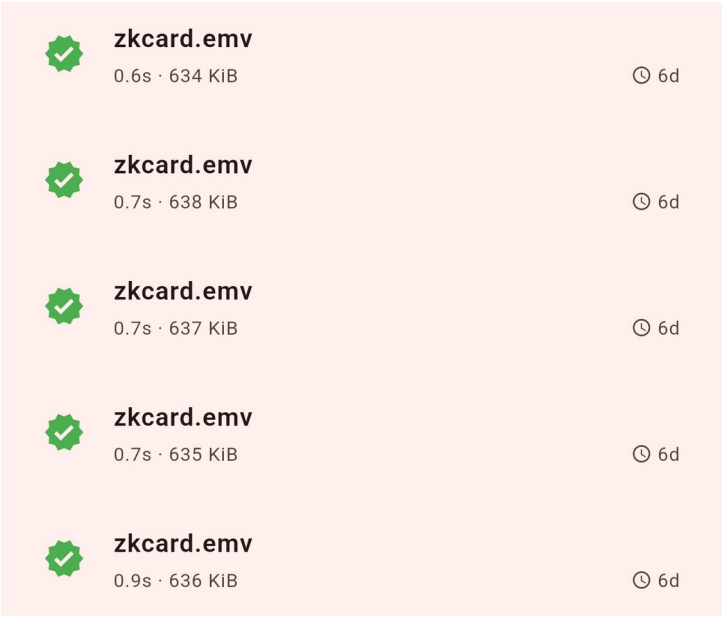
How to zk prove?

```
fn main(trust_anchors: pub TrustAnchors, challenge: pub Challenge, card: Card, bin_membership: BinMembership) -> pub Revealed {
    CaKey::from_limbs(trust_anchors.ca_modulus)
        .recover_issuer_cert(card.issuer_pubkey_cert)
        .verify::<ISSUER_PUBKEY_BYTE_LEN, _>(card.issuer_pubkey_remainder, card.issuer_pubkey_exponent, challenge.today_yymm)
        .key()
        .recover_icc_cert(card.icc_pubkey_cert)
        .verify::<ICC_PUBKEY_BYTE_LEN, _, _>([], card.icc_pubkey_exponent, card.static_data_to_authenticate, challenge.today_yymm)
        .key()
        .recover_sdad(card.signed_dynamic_app_data)
        .verify([FMT_SDAD_DDA], challenge.nonce)
        .reveal(trust_anchors.bin_root, challenge, bin_membership)
}
```

Circuit in Noir Programming Language: https://noir-lang.org

How is the zk proving performance?

Visa	Mastercard
R1CS constraints 64,702	R1CS constraints 93,054



Proof generated using ProveKit: https://provekit.org on Samsung Galaxy S25 Ultra

Any downsides of zkEMV?

- No privacy from terminals who already know the card.
- Card skimming attack.
- Only 4-byte challenge in EMV ODA.
- Most circulated cards have legacy crypto. of RSA + SHA-1.

Where to go from here?

- Deploy zkEMV. Respect user privacy. Hold less data to leak.
- Extend zkEMV to support new ECC-based EMV spec.
- Add support for more cards.

Feedback and questions?