NEXT GENERATION INTERNET

Blind Signatures

Christian Grothoff

22.05.2026

Learning objectives

How should we pay?

Blind Signatures

Project 2 Topics

Part I: How should we pay?

Surveillance

Surveillance concerns

- Everybody knows about Internet surveillance.
- But is it **that** bad?
  - You can choose when and where to use the Internet
  - You can anonymously access the Web using Tor
  - You can find open access points that do not require authentication
  - IP packets do not include your precise location or name
  - ISPs typically store this meta data for days, weeks or months

Where is it worse?

This was a question posed to RAND researchers in 1971:

> *"Suppose you were an advisor to the head of the KGB, the Soviet Secret Police. Suppose you are given the assignment of designing a system for the surveillance of all citizens and visitors within the boundaries of the USSR. The system is not to be too obtrusive or obvious. What would be your decision?"*

Where is it worse?

This was a question posed to RAND researchers in 1971:

> *"Suppose you were an advisor to the head of the KGB, the Soviet Secret Police. Suppose you are given the assignment of designing a system for the surveillance of all citizens and visitors within the boundaries of the USSR. The system is not to be too obtrusive or obvious. What would be your decision?"*

"I think one of the big things that we need to do, is we need to get a way from true-name payments on the Internet. The credit card payment system is one of the worst things that happened for the user, in terms of being able to divorce their access from their identity." –Edward Snowden, IETF 93 (2015)

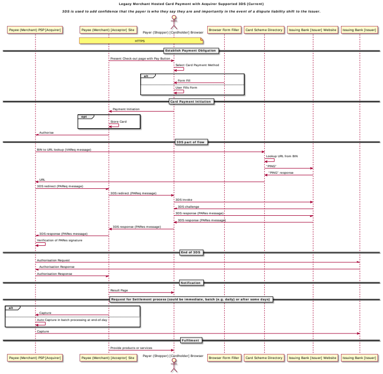
Why is it worse?

- When you pay by CC, the information includes your name
- When you pay in person with CC, your location is also known
- You often have no alternative payment methods available
- You hardly ever can use someone else’s CC
- Anonymous prepaid cards are difficult to get and expensive
- Payment information is typically stored for 6-10 years!

Credit cards have problems, too!

3D secure (“verified by visa”) is a nightmare:

- Complicated process
- Shifts liability to consumer
- Significant latency
- Can refuse valid requests
- Legal vendors excluded
- No privacy for buyers



Legacy Merchant Hosted Card Payment with Acquirer Supported 3DS (Current)

3DS is used to add confidence that the payer is who they say they are and importantly in the event of a dispute liability shift to the Issuer.

Payee (Merchant) PSP [Acquirer]
Payee (Merchant) [Acceptor] Site
Payer (Shopper) [Cardholder] Browser
Browser Form Filler
Card Scheme Directory
Issuing Bank [Issuer] Website
Issuing Bank [Issuer]
HTTPS
Establish Payment Obligation
Present Check-out page with Pay Button
Select Card Payment Method
alt
Form Fill
User Fills Form
Card Payment Initiation
Payment Initiation
opt
Store Card
Authorise
3DS part of flow
BIN to URL lookup (VAReq message)
Lookup URL from BIN
"PING"
"PING" response
URL
3DS redirect (PAReq message)
3DS redirect (PAReq message)
3DS invoke
3DS challenge
3DS response (PARes message)
3DS response (PARes message)
3DS response (PARes message)
3DS response (PARes message)
Verification of PARes signature
End of 3DS
Authorisation Request
Authorisation Response
Authorisation Response
Notification
Result Page
Request for Settlement process (could be immediate, batch (e.g. daily) or after some days)
alt
Capture
Auto Capture in batch processing at end-of-day
Capture
Fulfilment
Provide products or services
Payee (Merchant) PSP [Acquirer]
Payee (Merchant) [Acceptor] Site
Payer (Shopper) [Cardholder] Browser
Browser Form Filler
Card Scheme Directory
Issuing Bank [Issuer] Website
Issuing Bank [Issuer]

The bank's Problem

- Global tech companies push oligopolies
- Privacy and federated finance are at risk
- Economic sovereingity is in danger

支付宝™
Alipay.com

PayPal™

Pay

Pay with Amazon

SAMSUNG pay

pay

Predicting the future

- Google and Apple will be your bank and run your payment system
- They can target advertising based on your purchase history, location and your ability to pay
- They will provide more usable, faster and broadly available payment solutions; our federated banking system will be history
- After they dominate the payment sector, they will start to charge fees befitting their oligopoly size
- Competitors and vendors not aligning with their corporate “values” will be excluded by policy and go bankrupt
- The imperium will have another major tool for its financial warfare

The Bank of International Settlements on CBDC

The Emergency Act of Canada, February 2022, https://www.youtube.com/watch?v=Neh

Part II: Blind Signatures

Reminder: RSA

Generate random p, q primes and e such that

$$GCD((p-1)(q-1), e) = 1 \tag{1}$$

- Define $n = pq$,
- compute d such that $ed \equiv 1 \mod (p-1)(q-1)$.
- Let $s := m^d \mod n$.
- Then $m \equiv s^e \mod n$.

RSA Summary

- Public key: n, e
- Private key: $d \equiv e^{-1} \mod \phi(n)$ where $\phi(n) = (p-1) \cdot (q-1)$
- Encryption: $c \equiv m^e \mod n$
- Decryption: $m \equiv c^d \mod n$
- Signing: $s \equiv m^d \mod n$
- Verifying: $m \equiv s^e \mod n$?

These equations are heavily simplified and should not be used like this in production!

Low Encryption Exponent Attack

- e is known
- m maybe small
- $C = m^e < n$?
- If so, can compute $m = \sqrt[e]{C}$

$\Rightarrow$ Small e can be bad!

Padding and RSA Symmetry

- Padding can be used to avoid low exponent issues (and issues with $m = 0$ or $m = 1$)
- Randomized padding defeats chosen plaintext attacks
- Padding breaks RSA symmetry:

$$D_{A_{priv}}(D_{B_{priv}}(E_{A_{pub}}(E_{B_{pub}}(m)))) \neq m \tag{2}$$

- PKCS#1 / RFC 3447 define a padding standard

Blind signatures with RSA [2]

1. Obtain public key (e, n)
2. Compute $f := FDH_n(m)$, $f < n$.
3. Generate random blinding factor $b \in \mathbb{Z}_n$
4. Transmit $f' := fb^e \mod n$

Blind signatures with RSA [2]

1. Obtain public key (e, n)
2. Compute $f := FDH_n(m)$, $f < n$.
3. Generate random blinding factor $b \in \mathbb{Z}_n$
4. Transmit $f' := fb^e \mod n$

1. Receive f'.
2. Compute $s' := f'^d \mod n$.
3. Send s'.

Blind signatures with RSA [2]

1. Obtain public key (e, n)
2. Compute $f := FDH_n(m)$, $f < n$.
3. Generate random blinding factor $b \in \mathbb{Z}_n$
4. Transmit $f' := fb^e \mod n$

1. Receive f'.
2. Compute $s' := f'^d \mod n$.
3. Send s'.

1. Receive s'.
2. Compute $s := s'b^{-1} \mod n$

NGI TALER

Blind signatures with RSA [2]

1. Obtain public key (e, n)
2. Compute $f := FDH_n(m)$, $f < n$.
3. Generate random blinding factor $b \in \mathbb{Z}_n$
4. Transmit $f' := fb^e \mod n$

1. Receive f'.
2. Compute $s' := f'^d \mod n$.
3. Send s'.

1. Receive s'.
2. Compute $s := s'b^{-1} \mod n$

Note:

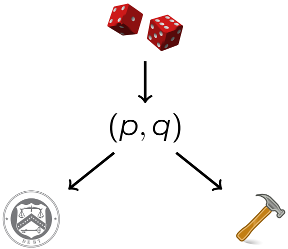
$$\begin{aligned} s'b^{-1} &= f'^d b^{-1} \\ &= f^d b^{ed} b^{-1} \\ &= f^d \end{aligned}$$

Applications for blind signatures

- Untraceable payments
- Unlinkable access tokens (PrivacyPass)

Provider setup: Create a denomination key (RSA)

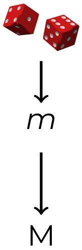
1. Generates random primes p, q.
2. Computes $n := pq$,
   $\phi(n) = (p-1)(q-1)$
3. Picks small $e < \phi(n)$ such that
   $d := e^{-1} \mod \phi(n)$ exists.
4. Publishes public key (e, n).



Merchant setup: Create a signing key (EdDSA)

- Generates random $m \mod o$ as private key
- Computes public key $M := mG$

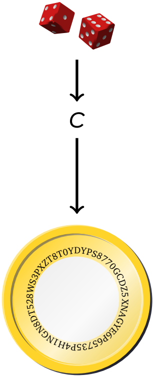
Capability: $m \Rightarrow$ M



Customer: Create a planchet (EdDSA)

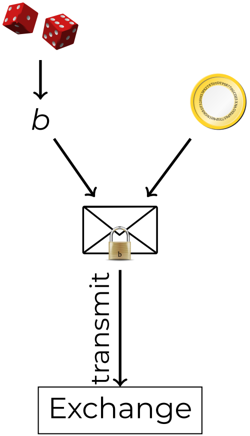
- Generates random $c \mod o$ as private key
- Computes public key $C := cG$

Capability: $c \Rightarrow$



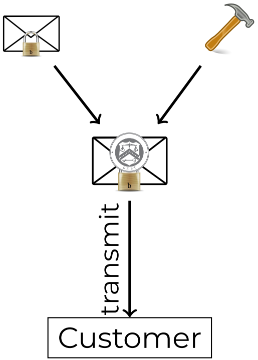
Customer: Blind planchet (RSA)

1. Obtains public key (e, n)
2. Computes $f := FDH_n(C), f < n$.
3. Generates random blinding factor $b \in \mathbb{Z}_n$
4. Transmits $f' := fb^e \mod n$



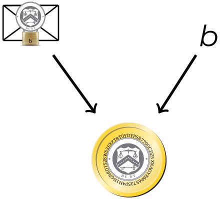
Provider: Blind sign (RSA)

1. Receives f'.
2. Computes $s' := f'^{d} \mod n$.
3. Sends signature s'.

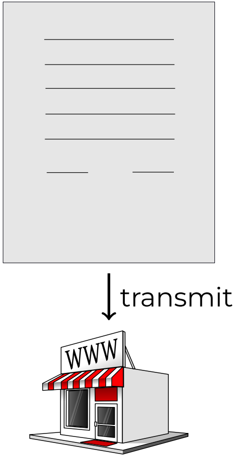


Customer: Unblind signature (RSA)

1. Receives s'.
2. Computes $s := s'b^{-1} \mod n$

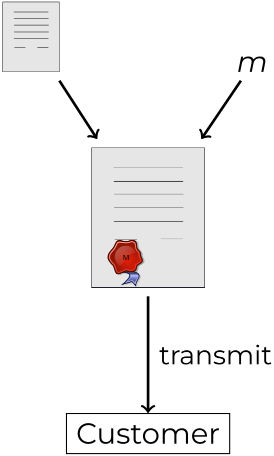


Customer: Build shopping cart



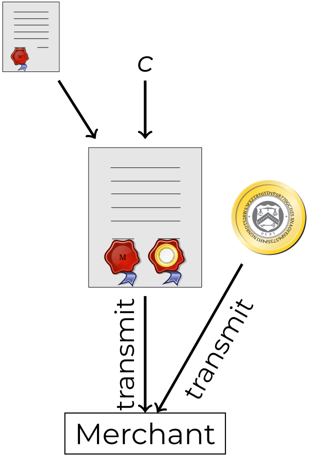
Merchant: Propose contract (EdDSA)

1. Complete proposal *D*.
2. Send *D*, $EdDSA_m(D)$



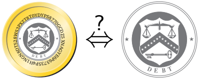
Customer: Spend coin (EdDSA)

1. Receive proposal D, $EdDSA_m(D)$.
2. Send s, C, $EdDSA_c(D)$



Merchant and provider: Verify coin (RSA)

$$s^e \mod n \overset{?}{\equiv} FDH_n(C)$$



The provider does not only verify the signature, but also checks that the coin was not double-spent.

This creates an online payment system.

Part III: Project 2 Topics

Project 2 basics

- Your own ideas are welcome (not too hard, not too easy!)
- Everything you implement must be Free Software
- You need to know **why** it matters
- Usually one meeting per week
- Ideally **de-risks** Bachelor’s thesis
- Good to engage with GNU community
- Project management was good if result is good

Project 2 topics

- TOTP authenticator apps with Taler amounts (easy)
- Secure merchant webhooks (easy)
- 10x Faster RSA signatures (hard)
- Receiver attestation for anti-fraud (**recommended**)
- Taler wallet supply chain security (easy)
- Taler wallet for Tor browser

Project 2 + BS thesis topics

- HSM-encrypted wallet databases on mobile (**recommended**)
- Post-quantum Taler: cipher agility (hard)
- Post-quantum Taler: primitives (hard)
- E-voting on tokenized shares (**recommended**)
- Paivana (**recommended**)
- EBICS server

References I

Jeffrey Burdges, Florian Dold, Christian Grothoff, and Marcello Stanisci.
Enabling secure web payments with GNU Taler.
In Claude Carlet, M. Anwar Hasan, and Vishal Saraswat, editors, *6th International Conference on Security, Privacy and Applied Cryptographic Engineering*, number 10076 in LNCS, pages 251–270. Springer, Dec 2016.

David Chaum.
Blind Signature System, pages 153–153.
Springer US, Boston, MA, 1984.

References II

David Chaum, Christian Grothoff, and Thomas Moser.
How to issue a central bank digital currency.
In *SNB Working Papers*, number 2021-3. Swiss National Bank, February 2021.

Acknowledgements

Co-funded by the European Union (Project 101135475).

Co-funded by the European Union

Co-funded by SERI (HEU-Projekt 101135475-TALER).

Project funded by

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Department of Economic Affairs,
Education and Research EAER
State Secretariat for Education,
Research and Innovation SERI

Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union.

Neither the European Union nor the granting authority can be held responsible for them.