

SSL And The Future Of Authenticity

Moving beyond Certificate Authorities

Comodo

Web Firm Suspects Iran Hacked Into It

Internet-Security Company Says It Was Tricked Into Authenticating Fake Sites, Opening Access to Data, Not Money

Wall Street Journal, March 15th, 2011

The Damage

★ mail.google.com

★ www.google.com

★ login.yahoo.com

★ login.skype.com

★ addons.mozilla.org

★ login.live.com

“ This [attack] was extremely sophisticated and critically executed...it was a very well orchestrated, very clinical attack, and the attacker knew exactly what they needed to do and how fast they had to operate.”

-- Melih Abdulhayoglu, Comodo Founder

“All the IPs were from *Iran*...”

-- Melih Abdulhayoglu, Comodo Founder

cyber

“All of the above leads us to one conclusion only:
that this was likely to be a state-driven attack.”

-- Melih Abdulhayoglu, Comodo Founder

picture

hack --> war

“What does this mean?”

“How would they use them?”

sslsniff

“

The attack came from several IP addresses, but mainly from Iran.

IP Address Location	
IP Address	212.95.136.18
City	Tehran
State or Region	Tehran
Country	Iran, Islamic Republic of
ISP	Pishgaman TOSE Ertebatat Tehran Network.
Latitude & Longitude	35.696111 51.423056

”

212.95.136.18 [16/Mar/2011:09:56:03 +0000] "GET http://www.thoughtcrime.org/software/sslsniff/index.html HTTP/1.1" 200
"Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.13
Gecko/20101203 Firefox/3.6.13 (.NET CLR 3.5.30729; .NET4.0E) "

212.95.136.18 [16/Mar/2011:09:56:03 +0000] "GET http://www.thoughtcrime.org/software/sslsniff/index.html HTTP/1.1" 200
"Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.13
Gecko/20101203 Firefox/3.6.13 (.NET CLR 3.5.30729; .NET4.0E) "

```
212.95.136.18 [16/Mar/2011:09:56:03 +0000] "GET http://  
www.thoughtcrime.org/software/sslsniff/index.html HTTP/1.1" 200  
"Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.13  
Gecko/20101203 Firefox/3.6.13 ( .NET CLR 3.5.30729; .NET4.0E) "
```

212.95.136.18 [16/Mar/2011:09:56:03 +0000] "GET http://
www.thoughtcrime.org/software/sslsniff/index.html HTTP/1.1" 200
"Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.13
Gecko/20101203 Firefox/3.6.13 (.NET CLR 3.5.30729; .NET4.0E) "

referrer

Episode 610 – Man in the Middle fun with SSL Strip

Submitted by Darren Kitchen on October 21, 2009 – 6:49 am

38 Comments

This time on the show Darren's having a little man-in-the-middle fun with a demonstration of SSLStrip, an epic tool for removing that pesky encryption from your victims browsing session.

19

tweets

0

f Share

retweet

+1



[Download HD](#)



[Download MP4](#)



[Download XviD](#)



[Download WMV](#)



Moxie Marlinspike's SSLStrip, released at Blackhat/DEFCON this year, is a tool that transparently hijacks HTTP traffic and redirects HTTPS links to look-alike HTTP links. While this description barely scratches the surface, Darren's segment takes a closer look including a practical demonstration of a man-in-the-middle attack using ~~openssl and a~~

“...it was a very well orchestrated, very clinical attack, and the attacker knew exactly what they needed to do and how fast they had to operate.”

-- Melih Abdulhayoglu

vs



And more embarrassing Google search referrers...

“SSL protocol mitm howto iptables prerouting”

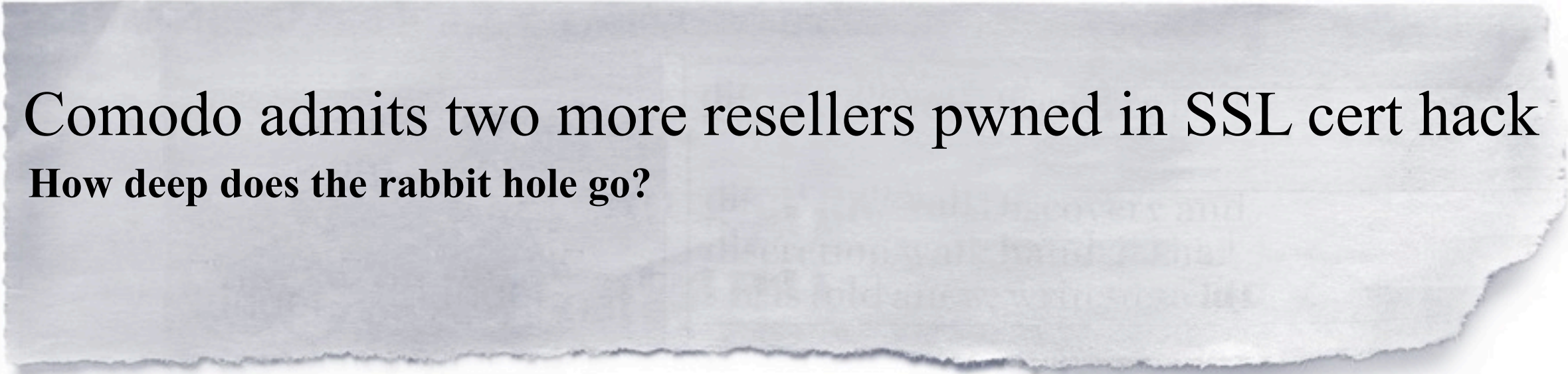
1. Hello
2.
3. I'm writing this to all the world, so you'll know more about us..
4.
5. At first I want to give some points, so you'll be sure I'm the hacker:
6.
7. I hacked Comodo from InstantSSL.it, their CEO's e-mail address mfpenco@mfpenco.com
8. Their Comodo username/password was: user: gtadmin password: globaltrust
9. Their DB name was: globaltrust and instantsslcms
10.
11. Enough said, huh? Yes, enough said, someone who should know already knows...
12.
13. Anyway, at first I should mention we have no relation to Iranian Cyber Army, we don't change DNSes, we
14.
15. just hack and own.
16.
17. I see Comodo CEO and other wrote that it was a managed attack, it was a planned attack, a group of
18.
19. cyber criminals did it, etc.
20.
21. Let me explain:
22.
23. a) I'm not a group, I'm single hacker with experience of 1000 hacker, I'm single programmer with
24.
25. experience of 1000 programmer, I'm single planner/project manager with experience of 1000 project
26.
27. managers, so you are right, it's managed by 1000 hackers, but it was only I with experience of 1000
28.
29. hackers.
30.
31. b) It was not really a managed hack. At first I decided to hack RSA algorithm, I did too much
32.

He just wouldn't shut up!

NAME / TITLE	ADDED	EXPIRES	SIZE	SYNTAX	STATUS	OPTIONS
 PROBLEM OF WORLD: MISSING EQUA...	Mar 31st, 11	Never	3.49 KB	None	Public	-
 Response to comments from Como...	Mar 29th, 11	Never	5.46 KB	None	Public	-
 Comodo Hacker: Mozilla Cert Re...	Mar 28th, 11	Never	2.40 KB	None	Public	-
 Just Another proof from Comodo...	Mar 28th, 11	Never	4.46 KB	None	Public	-
 Another proof of Hack from Com...	Mar 27th, 11	Never	12.54 KB	C#	Public	-
 A message from Comodo Hacker	Mar 26th, 11	Never	5.50 KB	None	Public	-

“ If there were a Secure and Trusted
DNS this issue would be a moot point!
We need a Secure and Trusted DNS! ”

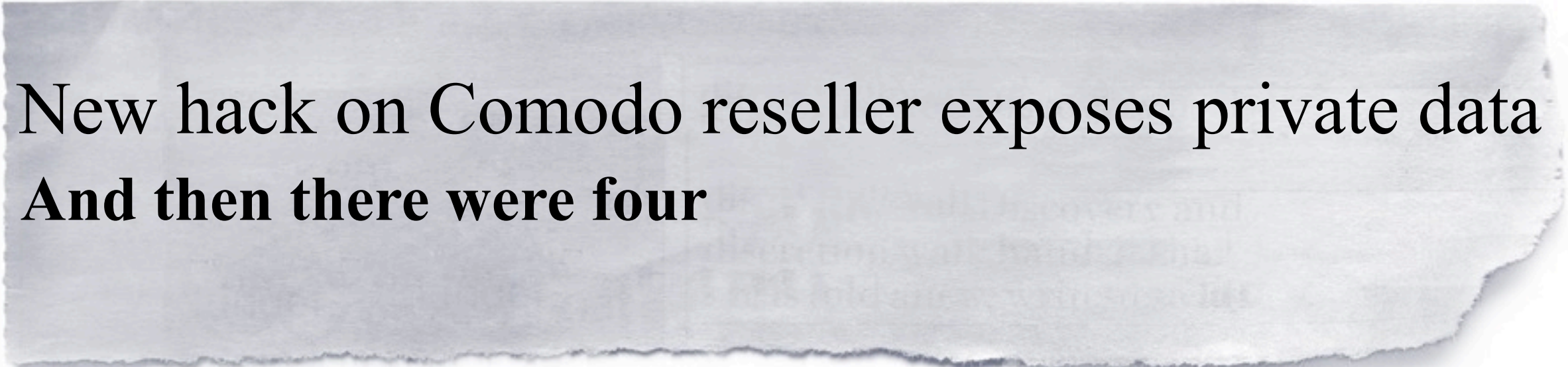
-- Melih Abdulhayoglu, Comodo Founder



Comodo admits two more resellers pwned in SSL cert hack

How deep does the rabbit hole go?

The Register, March 30th, 2011



New hack on Comodo reseller exposes private data
And then there were four

The Register, May 24th, 2011

What happened to Comodo?

nothing

“ Melih Abdulhayoglu named
entrepreneur of the year at RSA
2011. ”

problem

A Secure Protocol

- Secrecy
- Integrity
- Authenticity



early 90's

! information

! e-commerce

! web applications

tiny

< 5 million

> 4 billion

< 10 “secure” sites

> 2 million

intense pressure

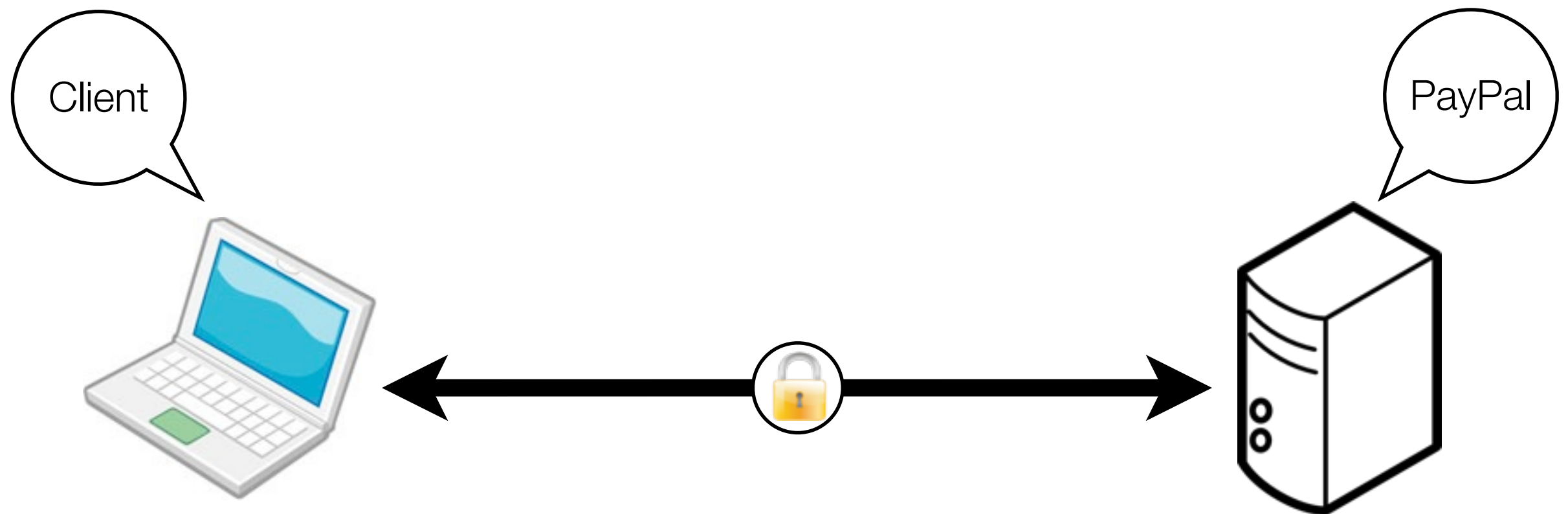
4am decisions == javascript

A Secure Protocol

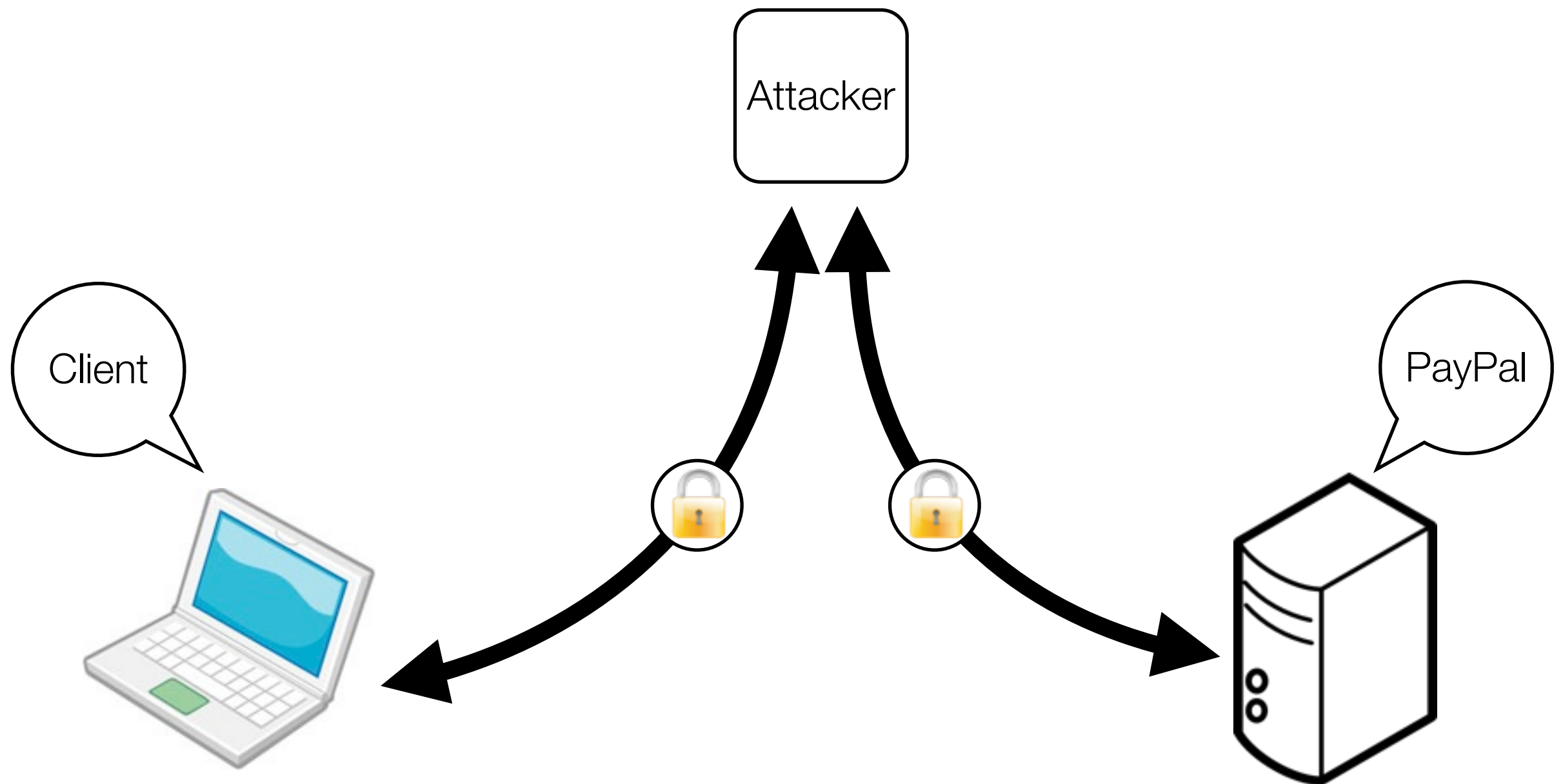
- ✓ Secrecy
- ✓ Integrity
- ▶ Authenticity



A Secure Connection



A Secure Connection

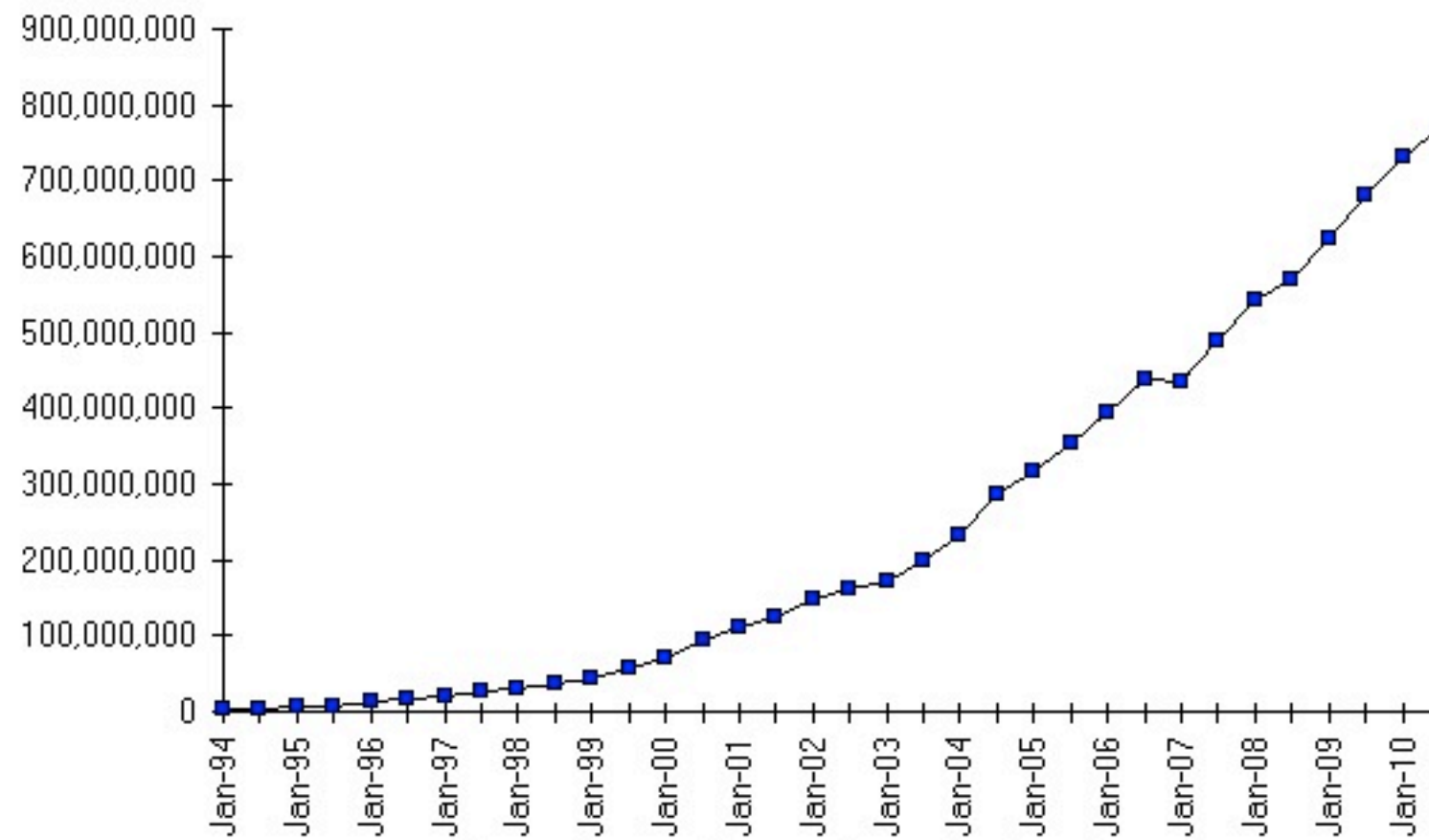


entirely theoretical

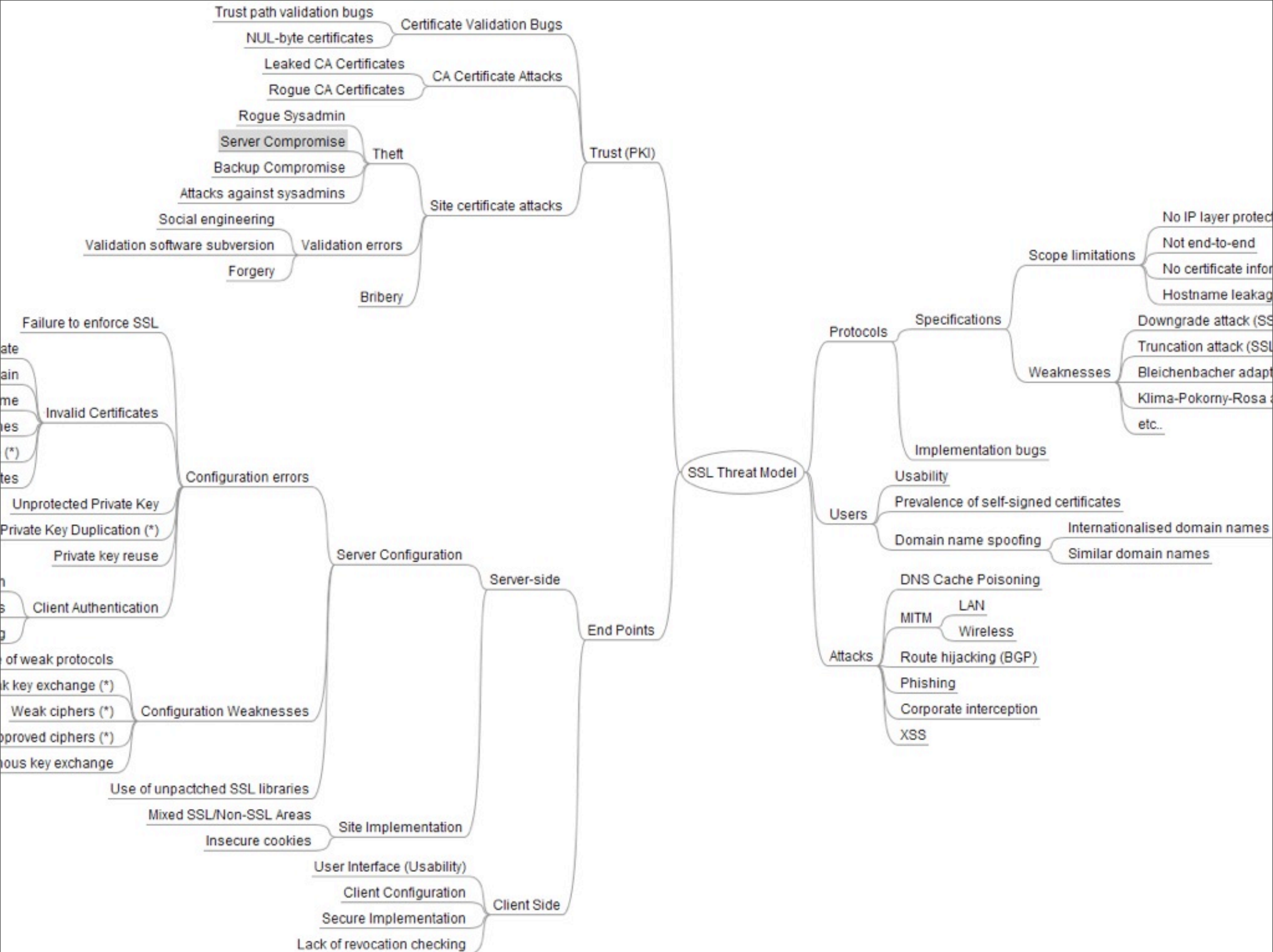
certificates and certificate authorities

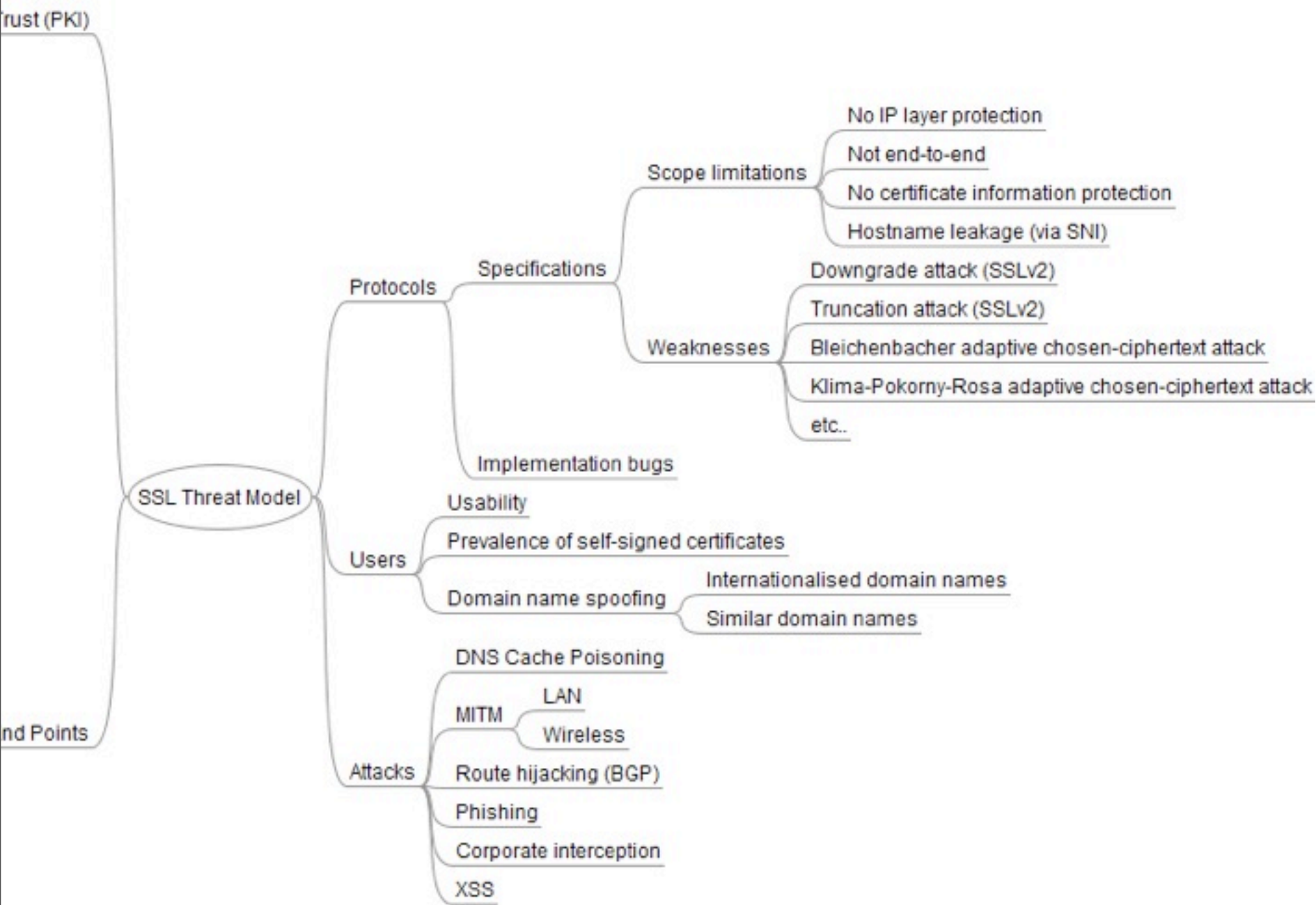
“...a bit of a hand wave.”

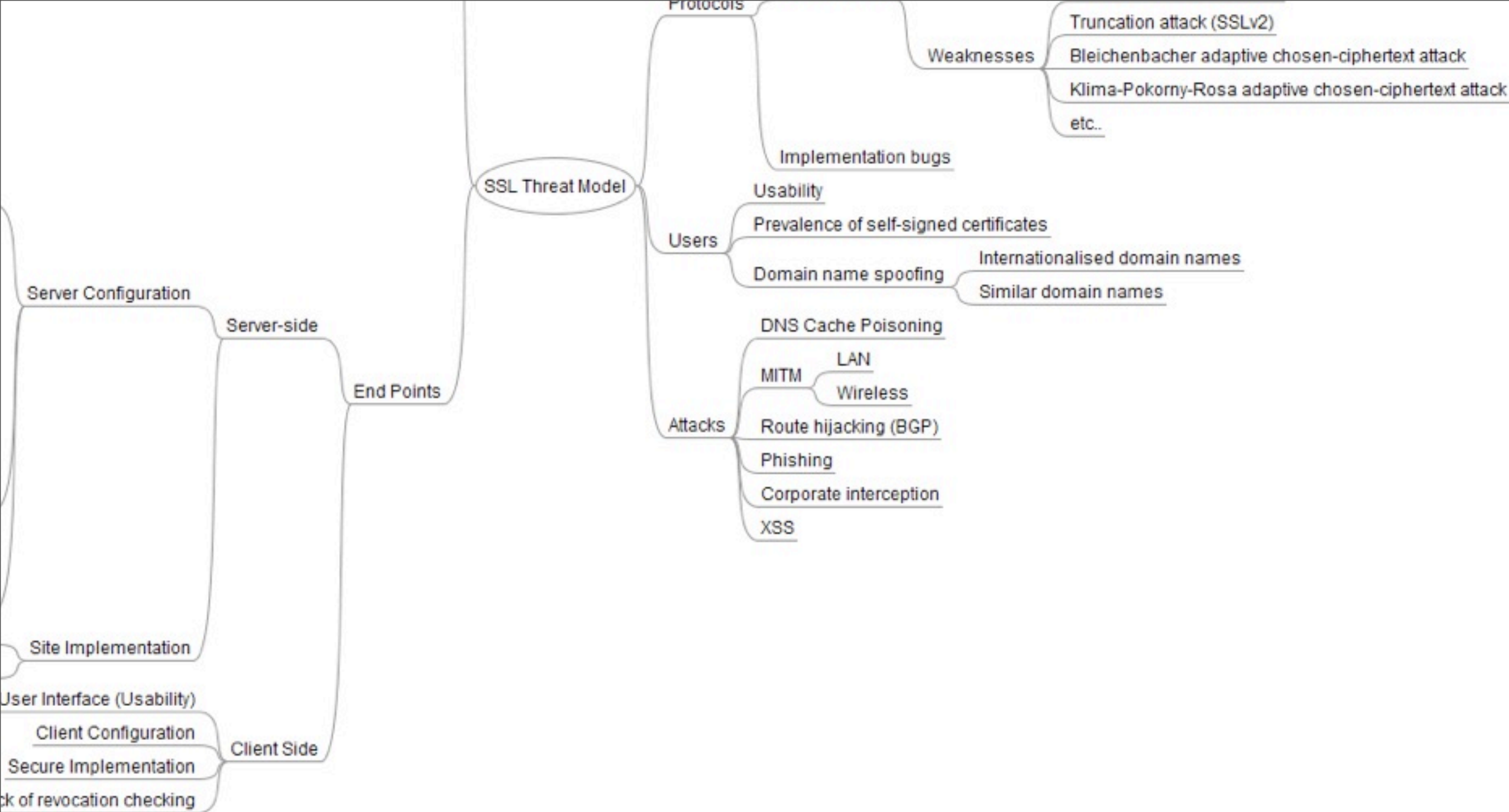
Internet Domain Survey Host Count

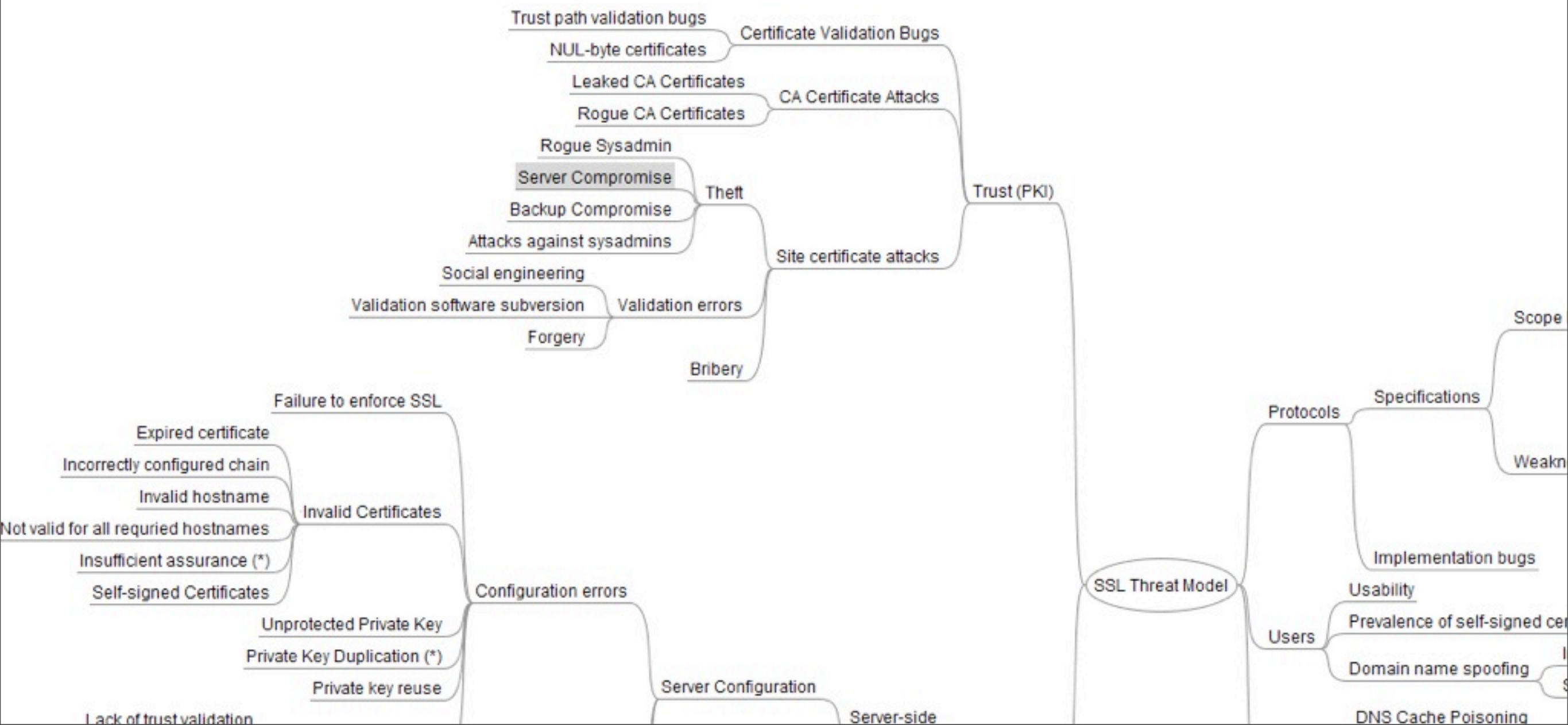


Source: Internet Systems Consortium (www.isc.org)









cyber war

happening every day

login.live.com?

Mike Zussman just asked for it.

Eddy Nigg got mozilla.com
...with no validation

VeriSign issued
“Microsoft Corporation”

SSL-In-A-Box.com

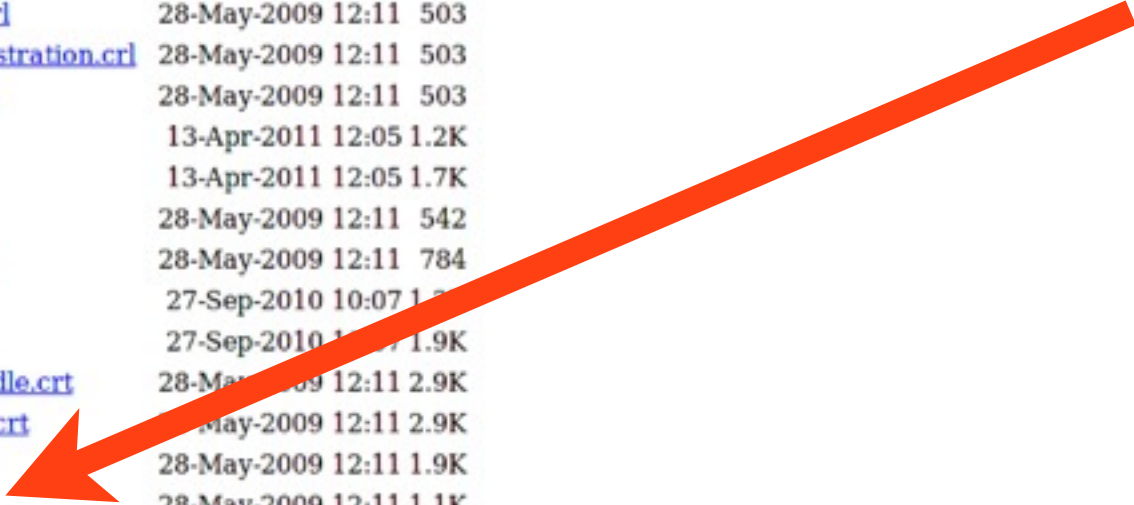
http://www.certigna.fr/crl/

Index of /crl

Name	Last modified	Size	Description
Parent Directory	-	-	-
certigna.crl	18-Aug-2010 11:45	768	
certigna.pem	28-May-2009 12:11	898	
certignachif.crl	13-Apr-2011 12:05	1.5K	
certignachif.pem	13-Apr-2011 12:05	2.0K	
certignahorodatage.crl	13-Apr-2011 12:05	607	
certignahorodatage.pem	13-Apr-2011 12:05	873	
certignaid.crl	13-Apr-2011 12:05	1.8K	
certignaid.pem	13-Apr-2011 12:05	2.5K	
certignaidpris.crl	28-May-2009 12:11	541	
certignaidpris.pem	28-May-2009 12:11	784	
certignaidpris3.crl	28-May-2009 12:11	627	
certignaidpris3.pem	28-May-2009 12:11	898	
certignaidpris3administration.crl	28-May-2009 12:11	503	
certignaidpris3pro.crl	28-May-2009 12:11	503	
certignaidprisadministration.crl	28-May-2009 12:11	503	
certignaidprispro.crl	28-May-2009 12:11	503	
certignassl.crl	13-Apr-2011 12:05	1.2K	
certignassl.pem	13-Apr-2011 12:05	1.7K	
certignasslpris.crl	28-May-2009 12:11	542	
certignasslpris.pem	28-May-2009 12:11	784	
certignatest.crl	27-Sep-2010 10:07	1.2K	
certignatest.pem	27-Sep-2010 10:07	1.9K	
www.certigna.fr-bundle.crt	28-May-2009 12:11	2.9K	
www.certigna.fr-scc.crt	28-May-2009 12:11	2.9K	
www.certigna.fr.crt	28-May-2009 12:11	1.9K	
www.certigna.fr.key	28-May-2009 12:11	1.1K	

Apache/2.2.16 (Debian) Server at www.certigna.fr Port 80

These are the people securing the internet.



StartSSL™ - The Swiss Army Knife of Digital Certificates & PKI

- StartSSL™ Home
- StartSSL™ Products
- Comparison Chart
- How to Enroll
- How to Install
- HTML Examples
- F. A. Q.
- Policies & Resources
- Contact StartCom
- Control Panel

StartSSL™ EV

High Level Trust Indicator
Time Limited Offer

 <https://www.paypal.com/>

Only US\$199.⁹⁰



Maintenance

Due to a security breach that occurred at the 15th of June, issuance of digital certificates and related services has been suspended. Our services will remain offline until further notice.

Subscribers and holders of valid certificates are not affected in any form.

Visitors to web sites and other parties relying on valid certificates are not affected.

We apologize for the temporary inconvenience and thank you for your understanding.



De garantie dat uw privacy gewaarborgd is

Hoe toont u aan dat uw website beveiligd is en dat
persoonsgegevens veilig zijn?

[Meer >>](#)

[Certificaten](#)[Contact](#)[FAQ](#)

Ga direct naar ...

[Digitale Polis](#)[Elektronische handtekening WABO](#)[Overgang certificaten](#)[SHA256 certificaten en sleutellengte 2048](#)[Tarieven certificaten](#)

Lopende projecten

[Ga](#)

DigiNotar®, Internet Trust Provider

Dé onafhankelijke partij voor het identificeren van personen en organisaties op internet en veilig digitaal documenten uitwisselen, ondertekenen en bewaren.

Expertise in o.a. online identiteiten, veilig documenten uitwisselen, privacy services, elektronisch factureren, mobiele pki, (EV)SSL, pseudonimisatie, digitale kluis, authenticatie, elektronische handtekening

[Meer info >>](#)

eHerkenning

Actueel

> Besluit OPTA om de registratie van DigiNotar als certificatie dienstverlener in te trekken

De OPTA heeft op 13 september jl. besloten om de registratie van DigiNotar als leverancier van gekwalificeerde elektronische handtekeningen (certifica...

> Informatie voor gebruikers van DigiNotar certificaten

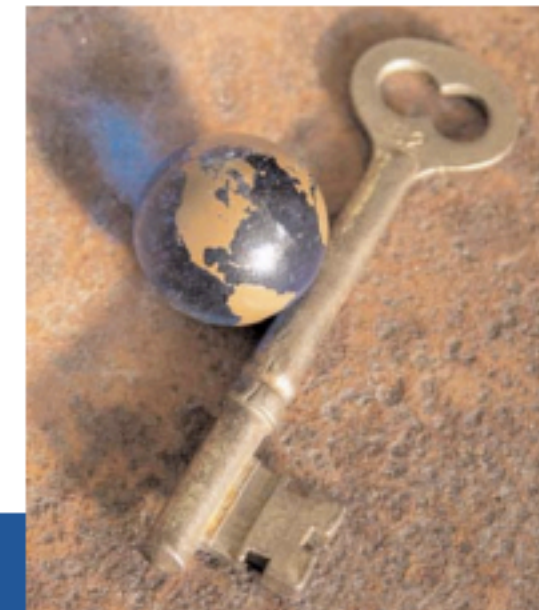
U maakt gebruik van 1 of meer DigiNotar certificaten, onder andere voor de beveiliging van uw internetverkeer. Vrijdag 2 september jl. heeft de overhe...

> Publicatie rapport Fox-IT



GeoRoot™

The power of your own trusted Certificate Authority



FEATURES & BENEFITS

- Complete control over all RA functions for issuance of SSL server certs and client certs
- Globally recognized roots compatible with 99% of all browsers
- Build and maintain a trusted identity with privately-branded certificates
- Predictable and economical yearly costs
- Seamless integration with

PROTECT YOUR BUSINESS WITH YOUR OWN CERTIFICATE AUTHORITY

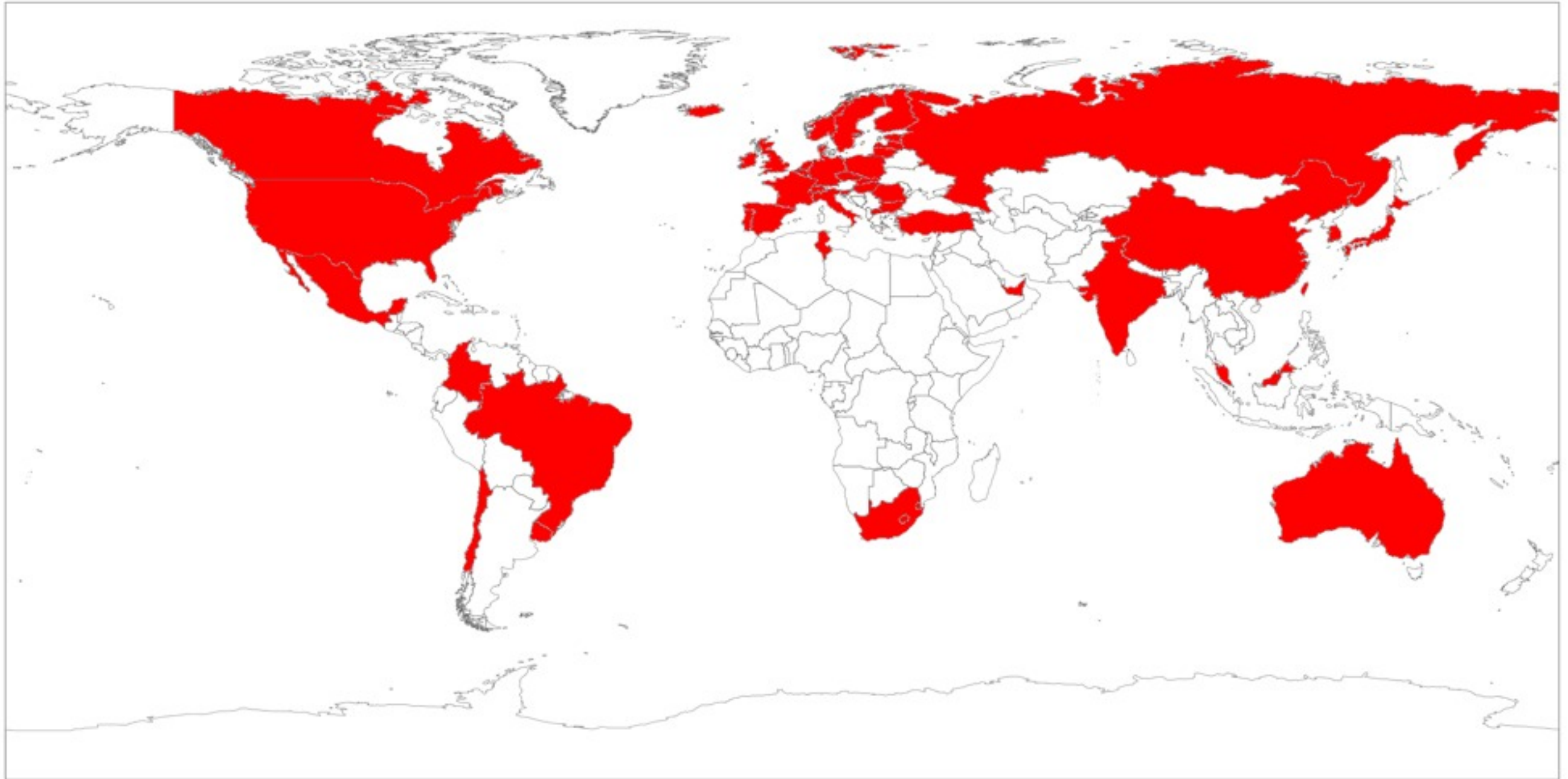
The growing demand for secure e-business environments makes user and transaction identity certification a necessity. One of the most important steps toward achieving enterprise-wide protection is to issue digital certificates through a Certificate Authority (CA). Yet, organizations that choose to run their own private CA often grapple with a common obstacle -- a lack of global recognition for their "self-signed" certificates.

GeoRoot is an ideal solution that allows enterprises to retain full control over Registration Authority (RA) functions for the issuance of SSL server certificates for domains and client certificates (x.509). With GeoRoot, your organization will gain the inherent security, confidence and recognition that result from being chained to one of GeoTrust's trusted roots.

COMPATIBLE WITH 99% OF ALL BROWSERS

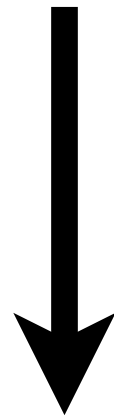
Lack of certificate recognition can be costly resulting in the loss of critical business or the denial of user access to vital information. If a certificate is not recognized, the result is that the recipient may receive an error message or complaint from the browser, and consequently not trust either the server or the source.

State Sponsored?



good news

“total ripoff”



“total ripoff *and* mostly worthless”

problem?





650

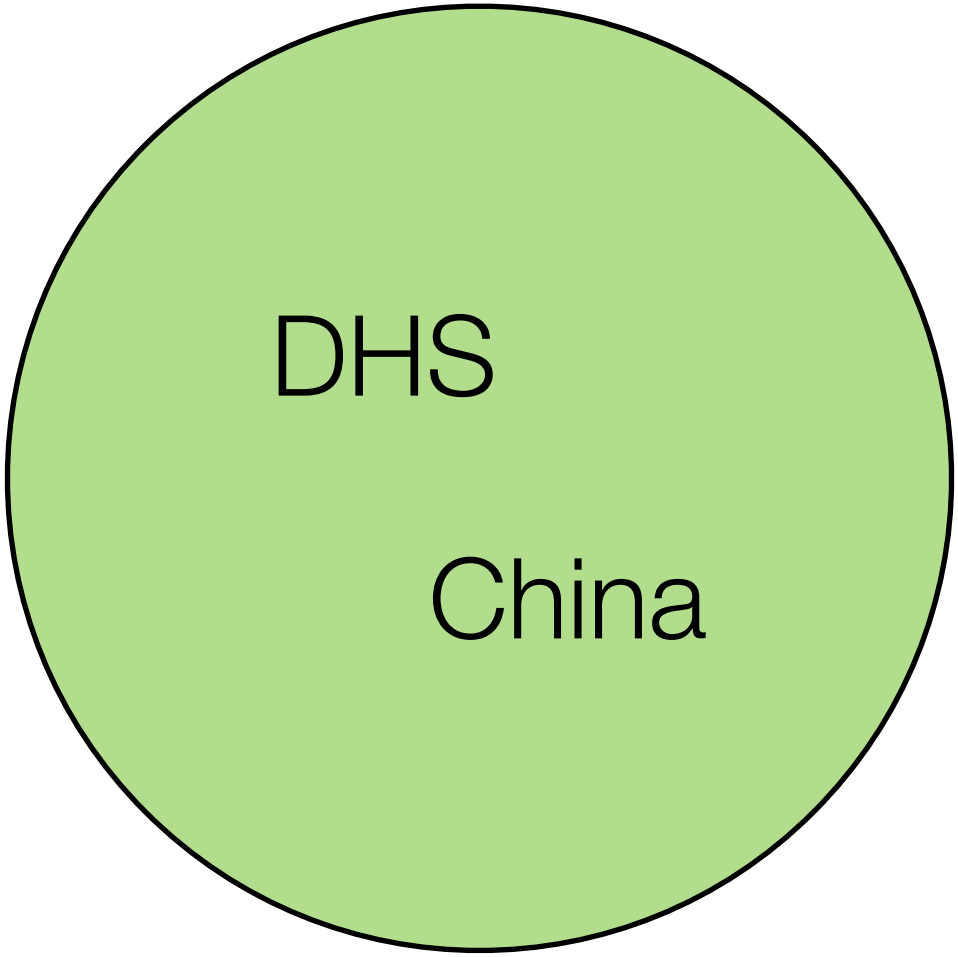


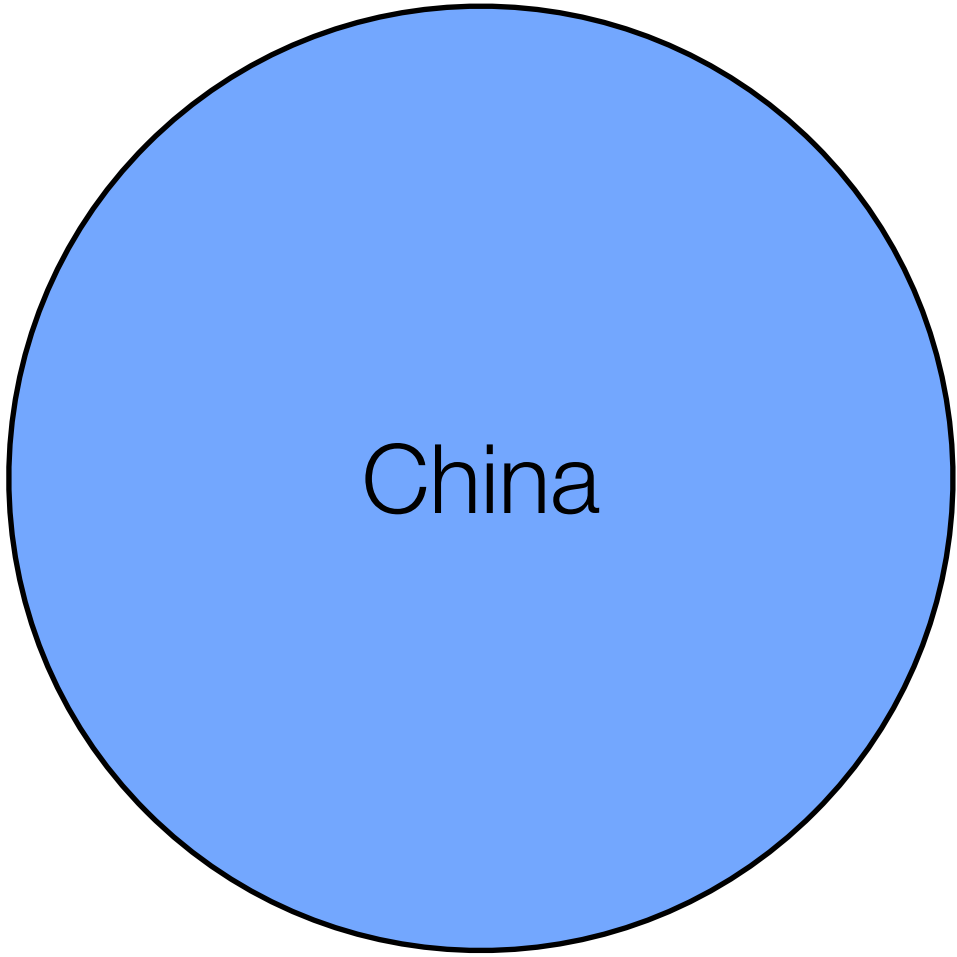
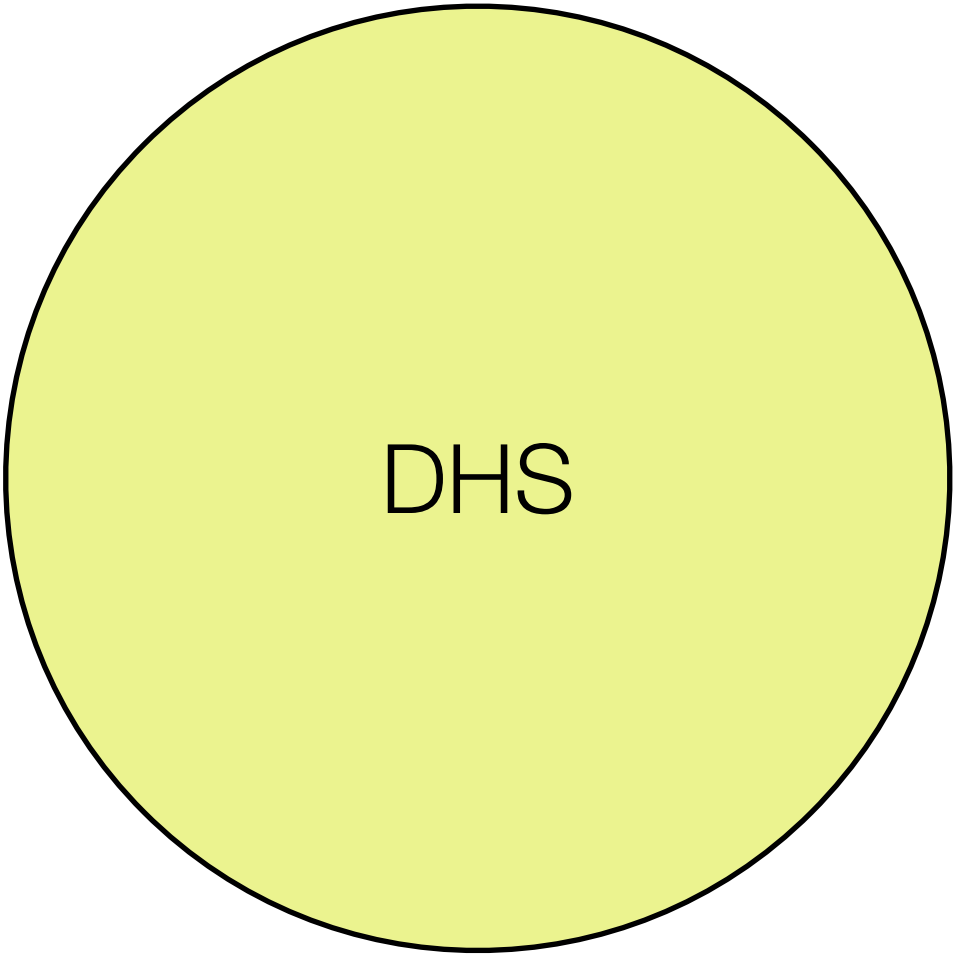
Wednesday, September 28, 2011

VeriSign?

20 $\rightarrow$ 2,000,000









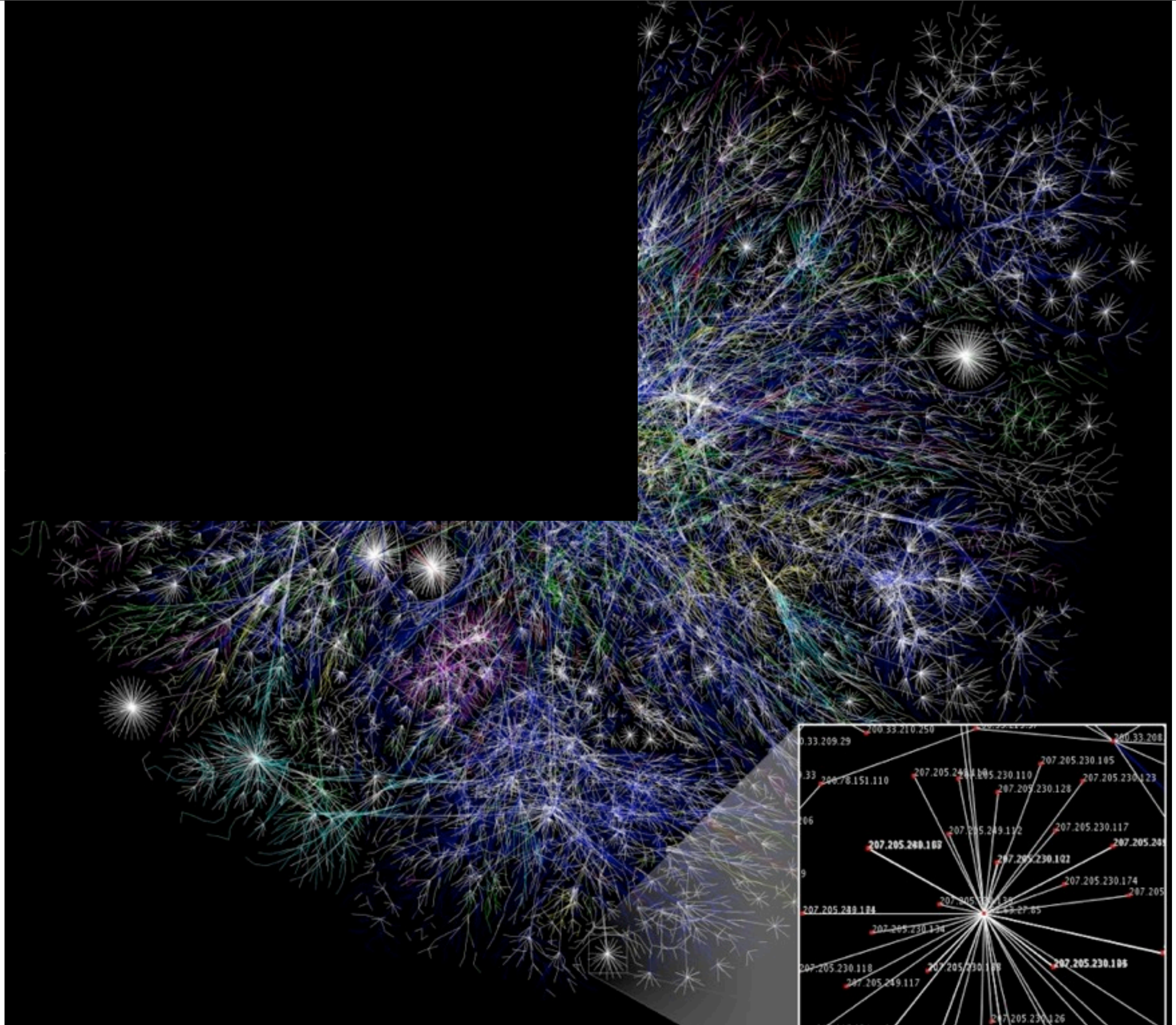
What happened to Comodo?

nothing

What could we have done?

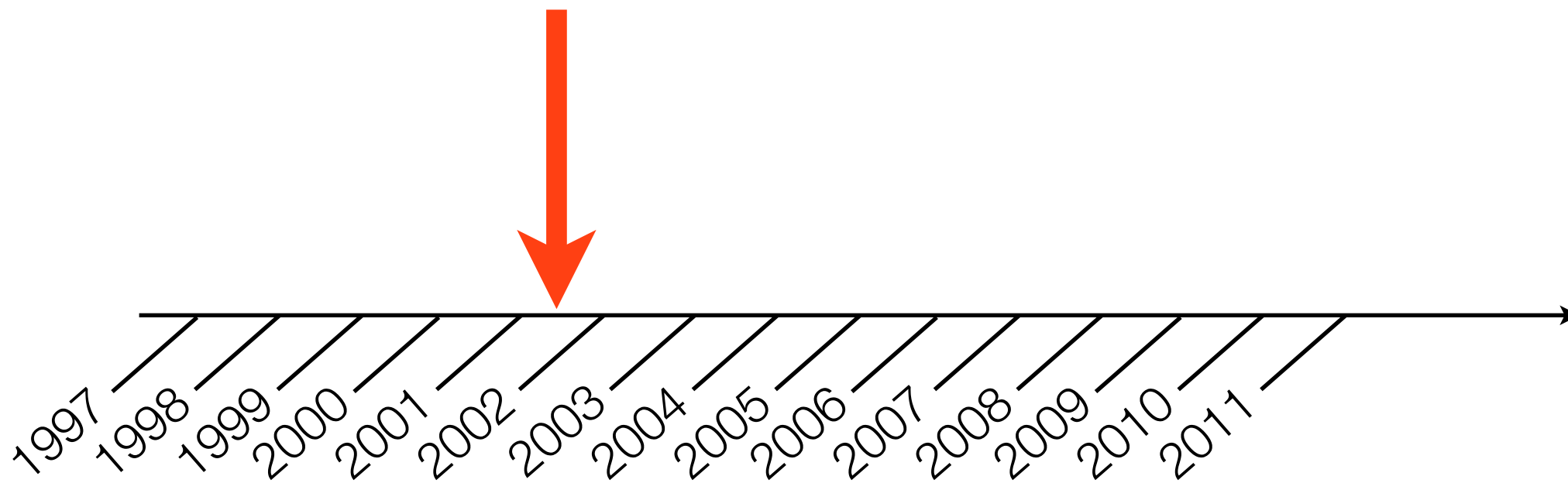
! trust

trustdb -= comodo



ideological

browser vendors



forever



trust agility



Trust Agility Properties

- A trust decision can be easily revised at any time.
- Individual users can decide where to anchor their trust.



Trust Agility Properties

- ▶ A trust decision can be easily revised at any time.
- Individual users can decide where to anchor their trust.

Tor

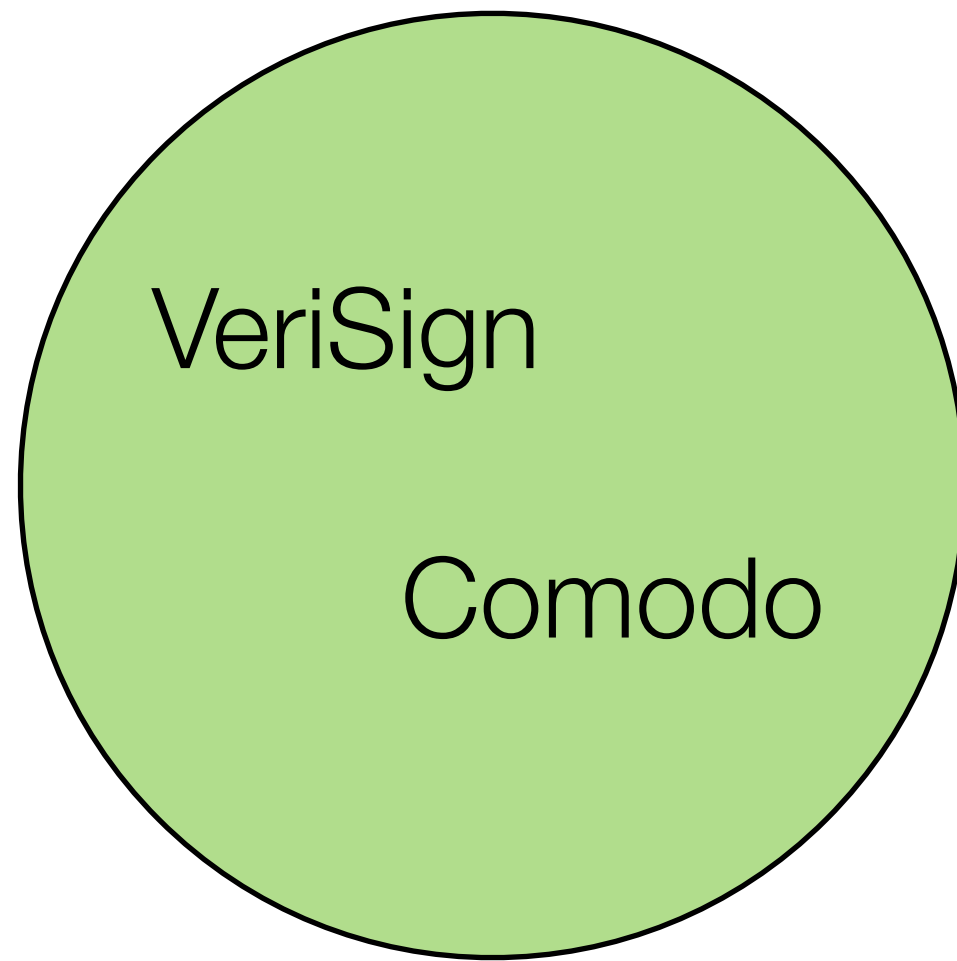


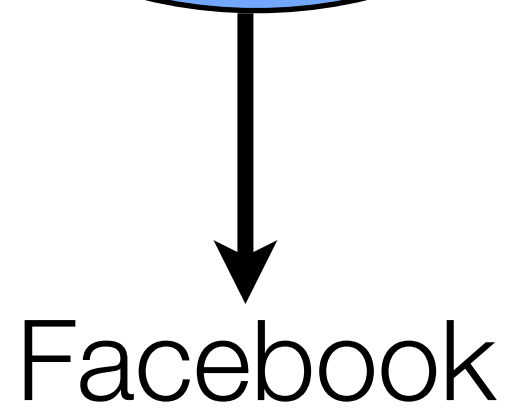
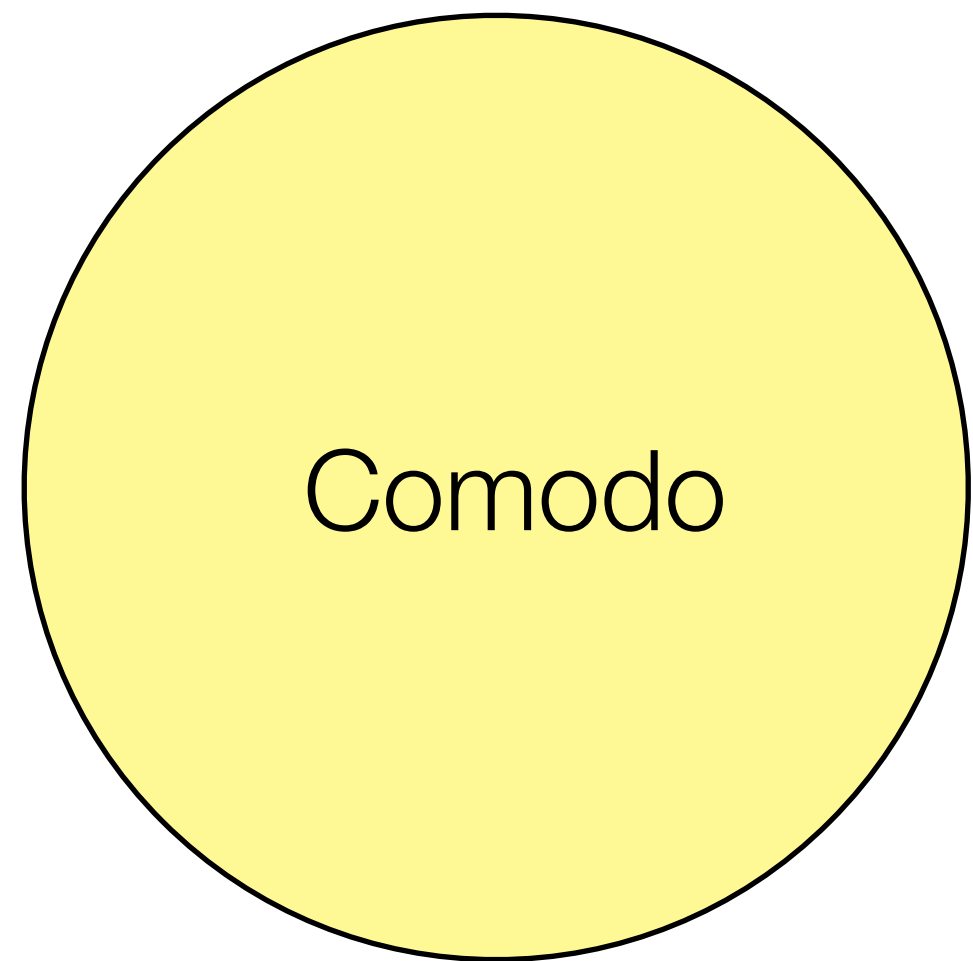
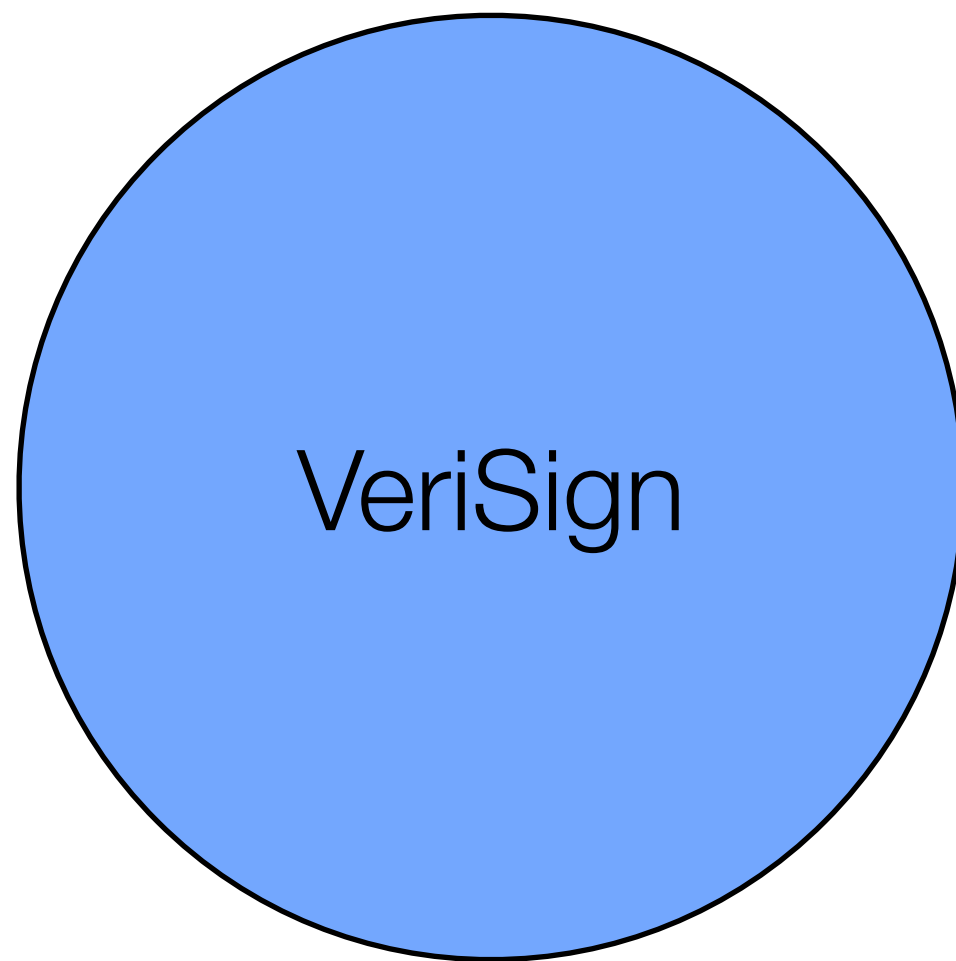


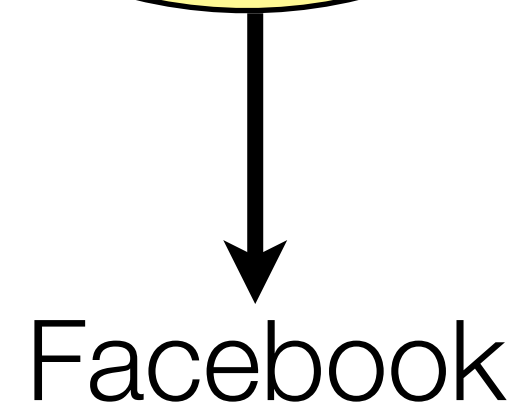
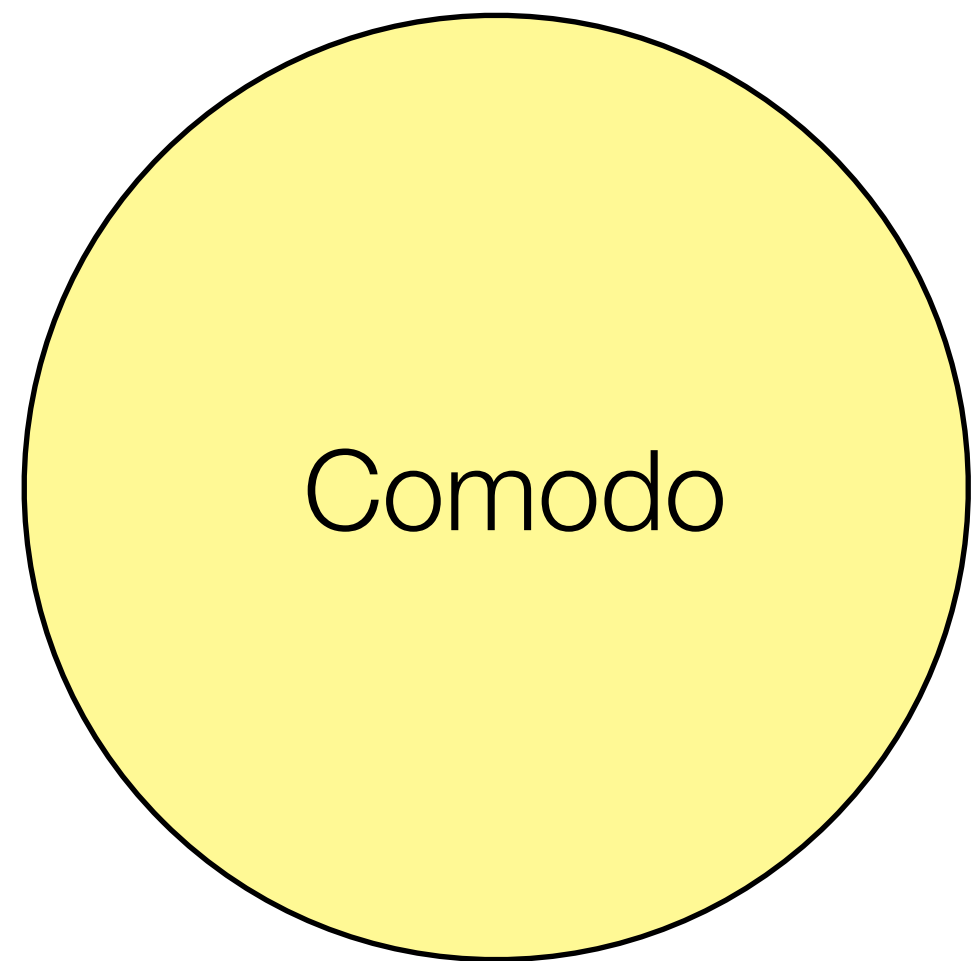
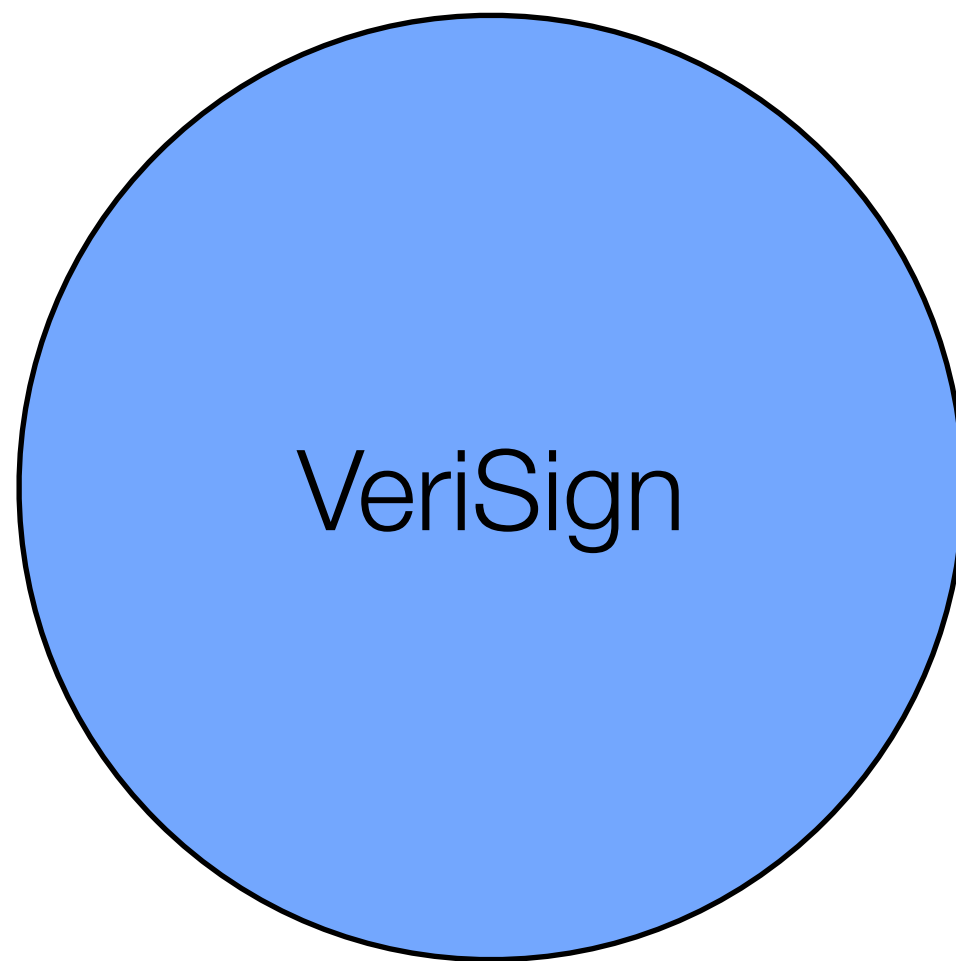


Trust Agility Properties

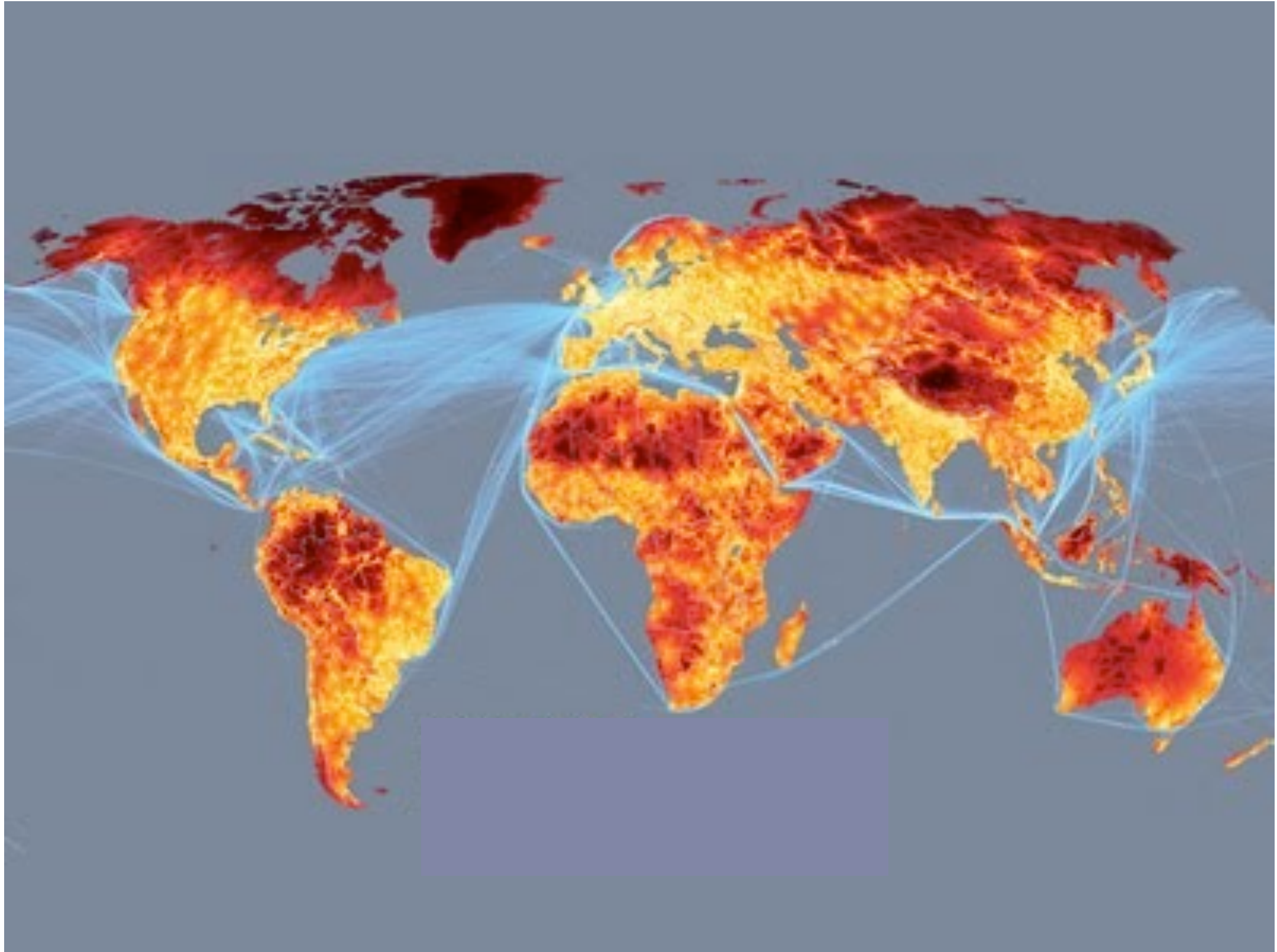
- A trust decision can be easily revised at any time.
- ▶ Individual users can decide where to anchor their trust.







https?

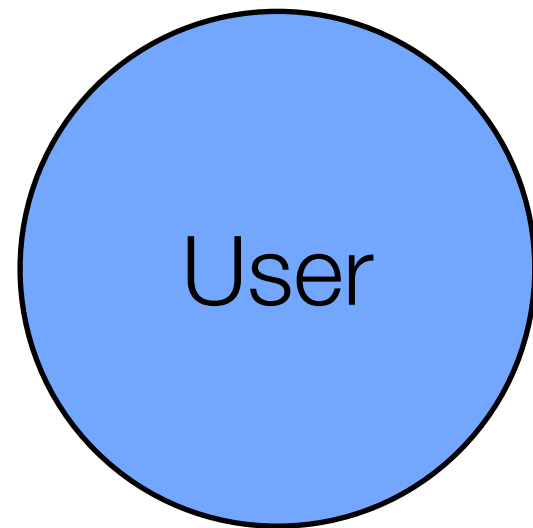
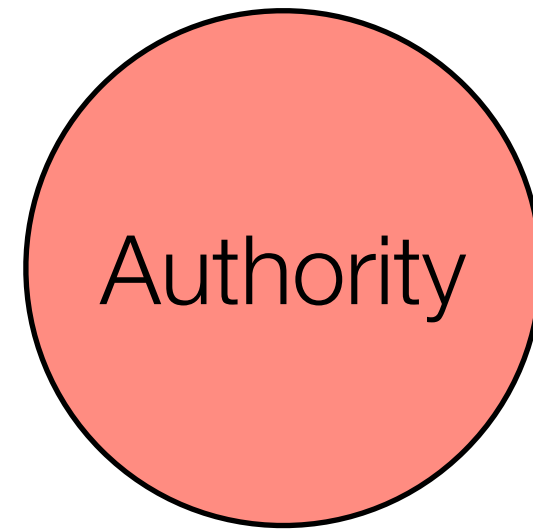
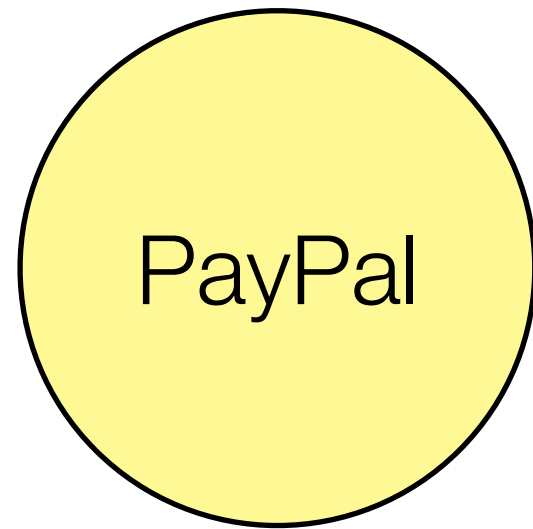


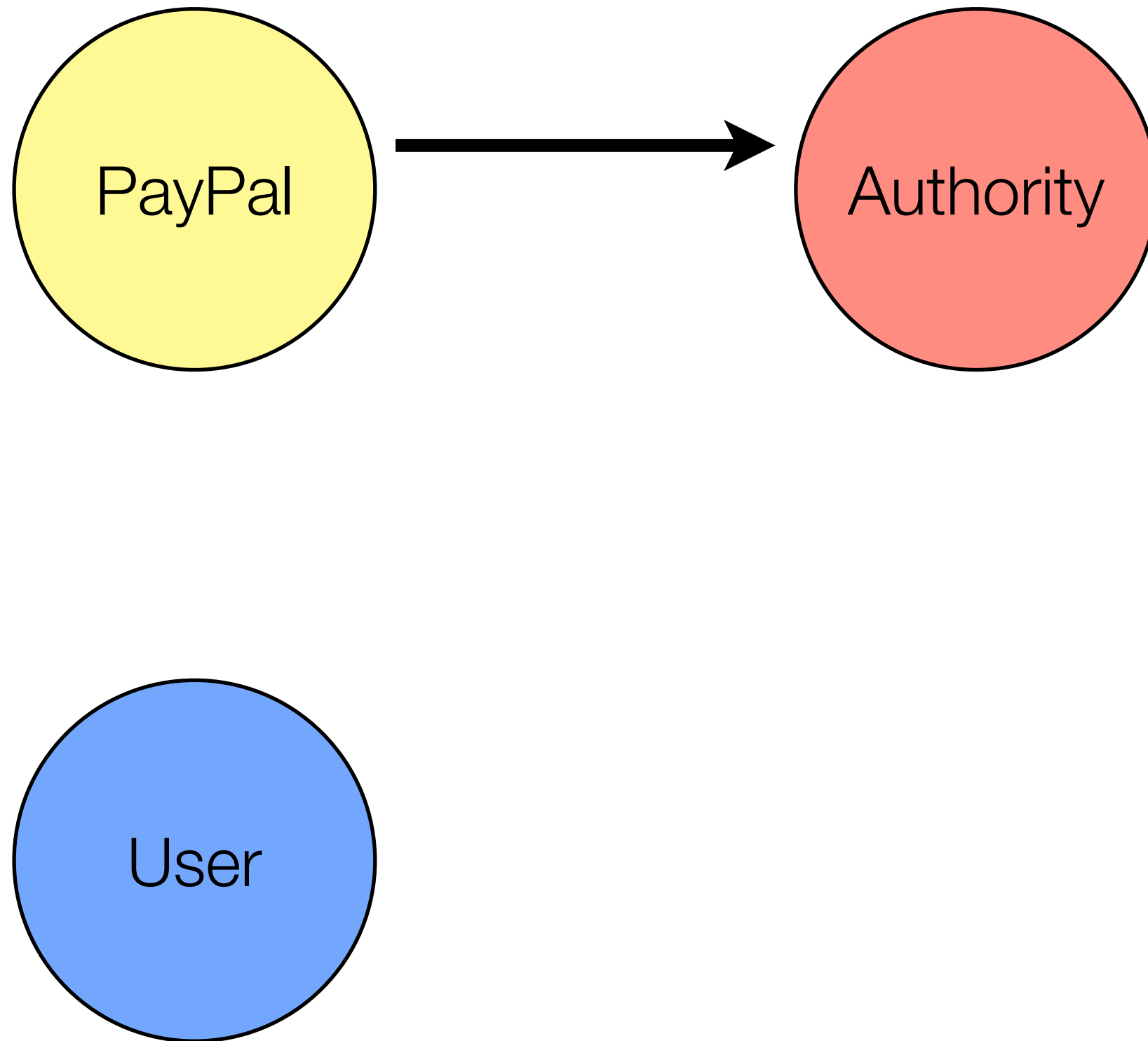
one decision for everyone?

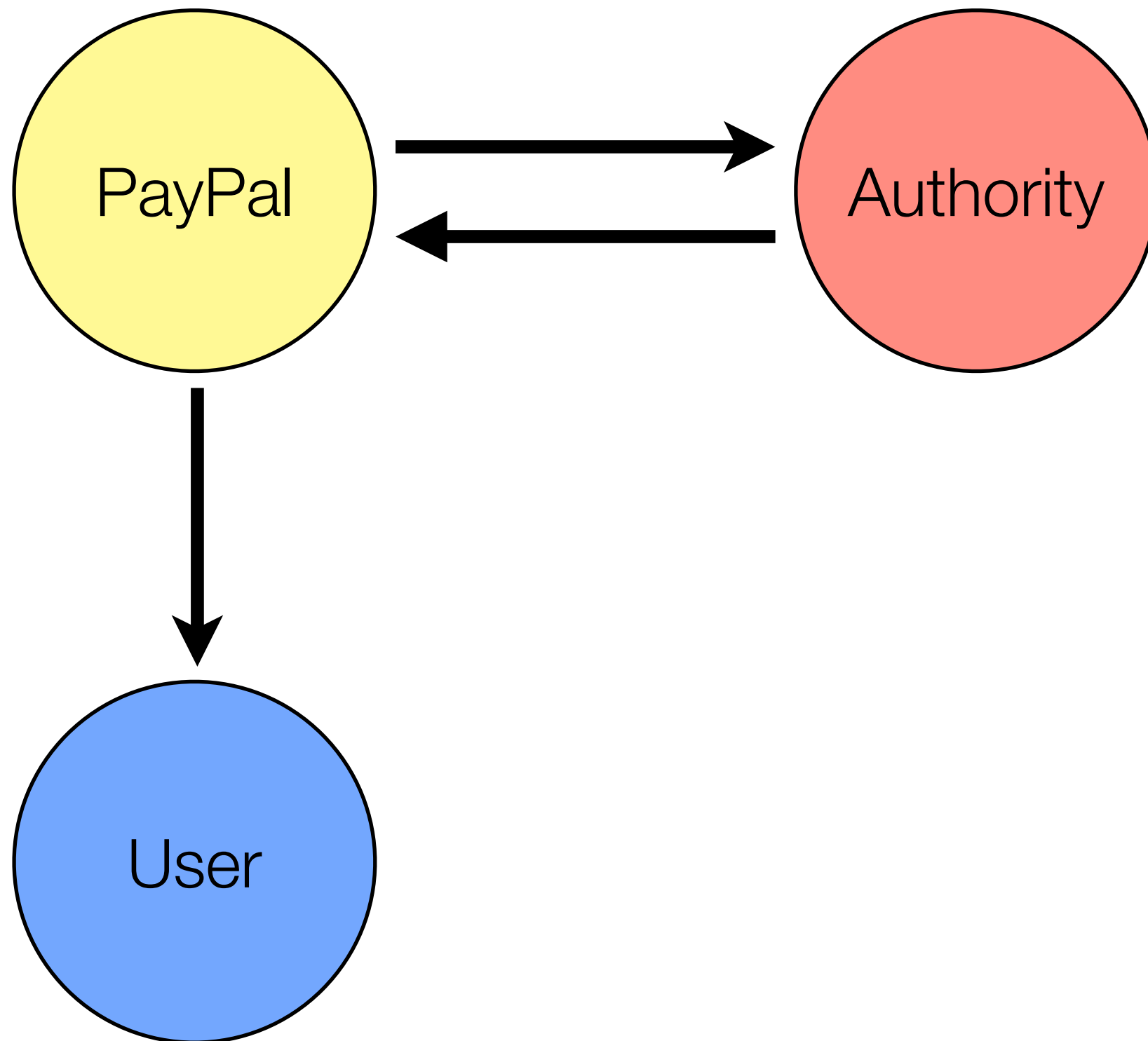
our data, our trust decision

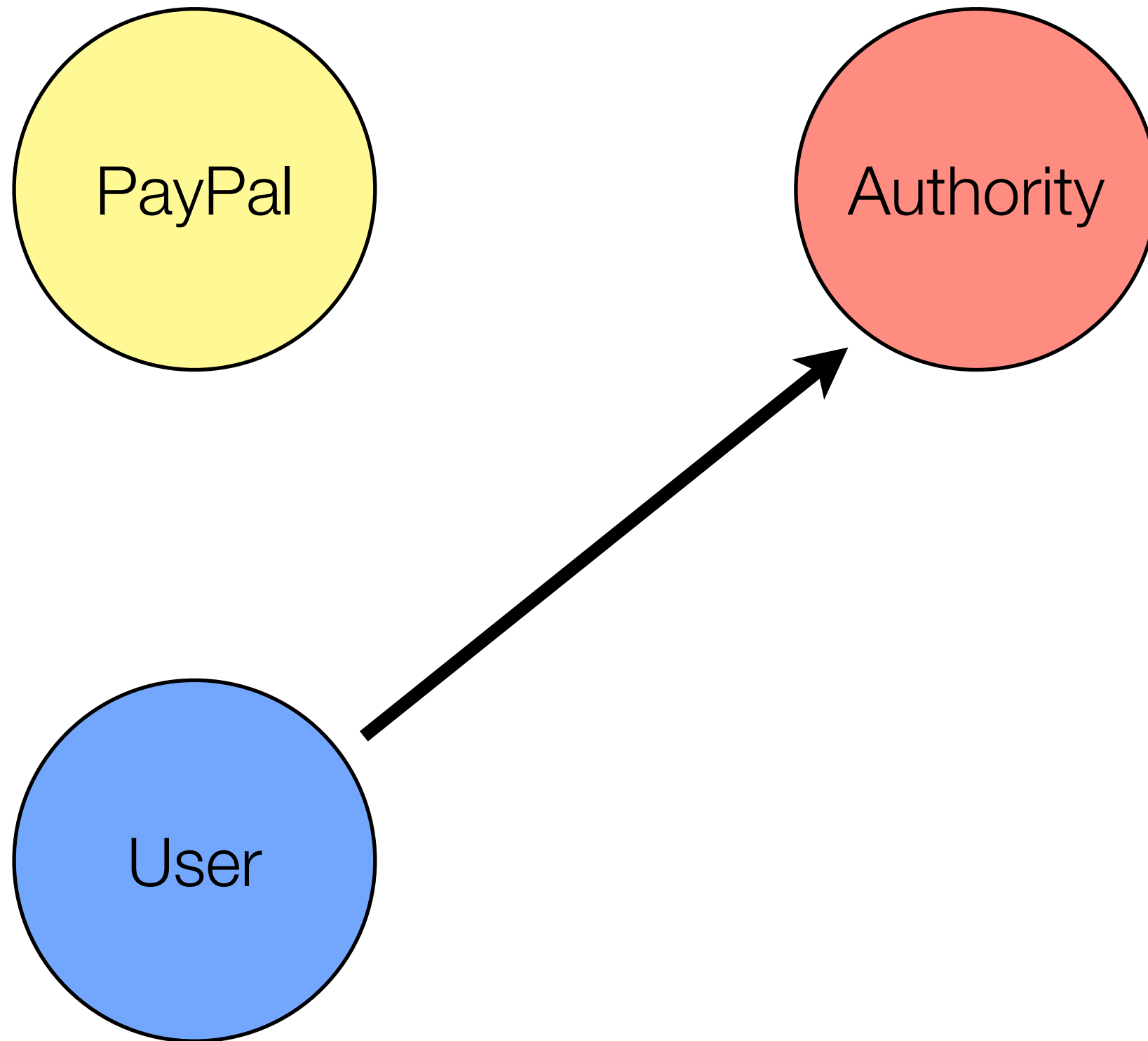
Trust Agility Properties

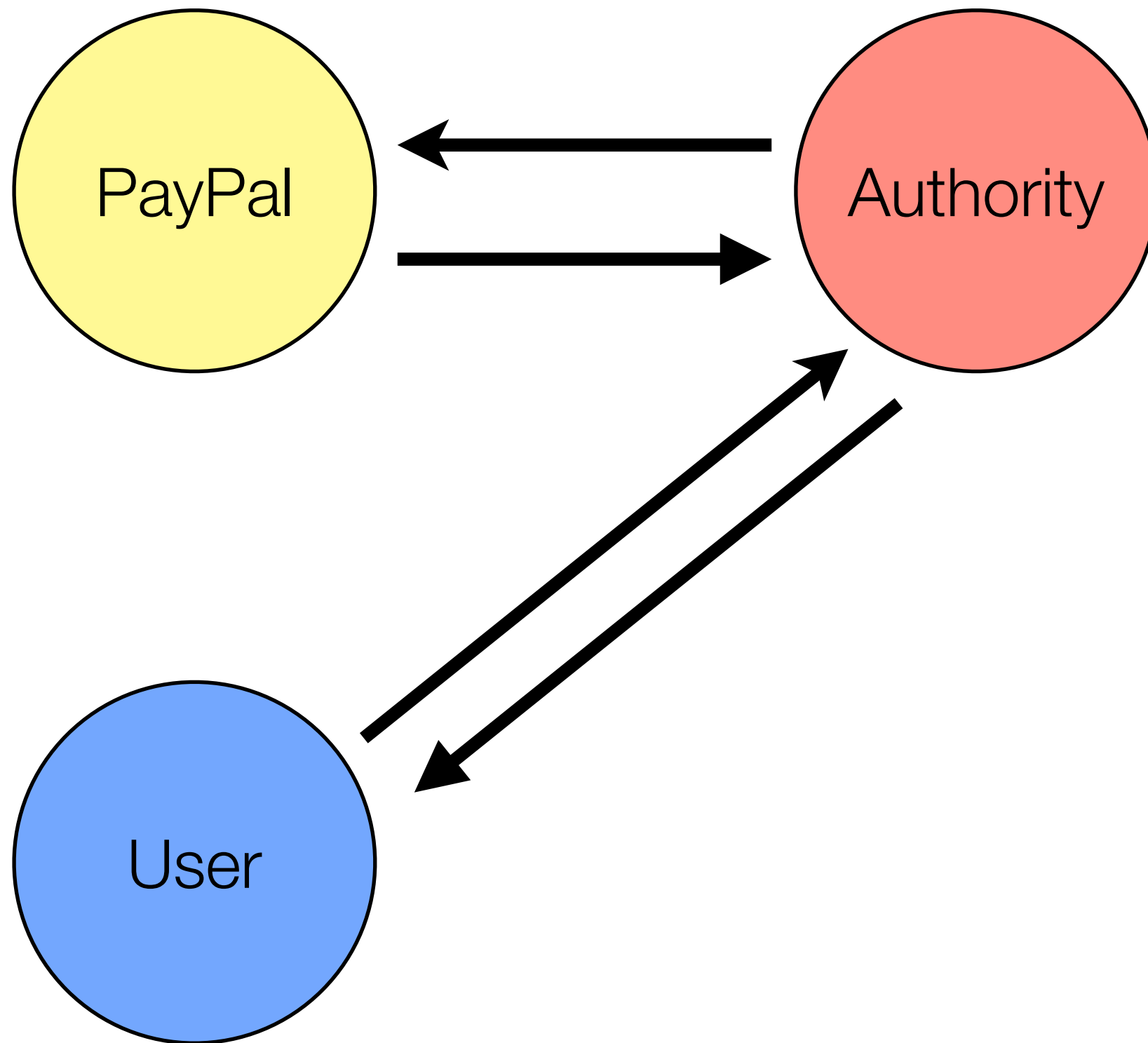
- A trust decision can be easily revised at any time.
- ▶ Individual users can decide where to anchor their trust.

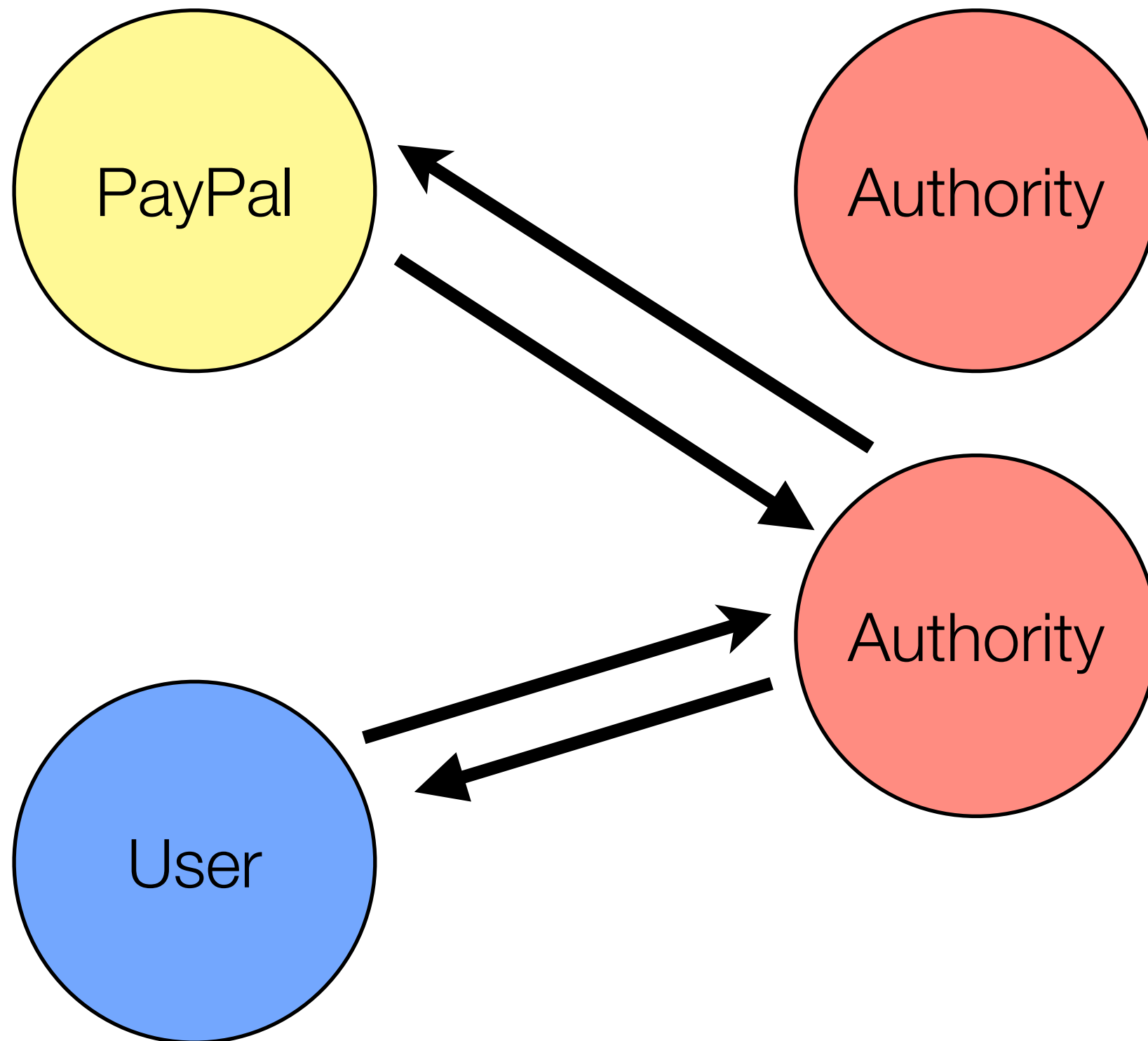


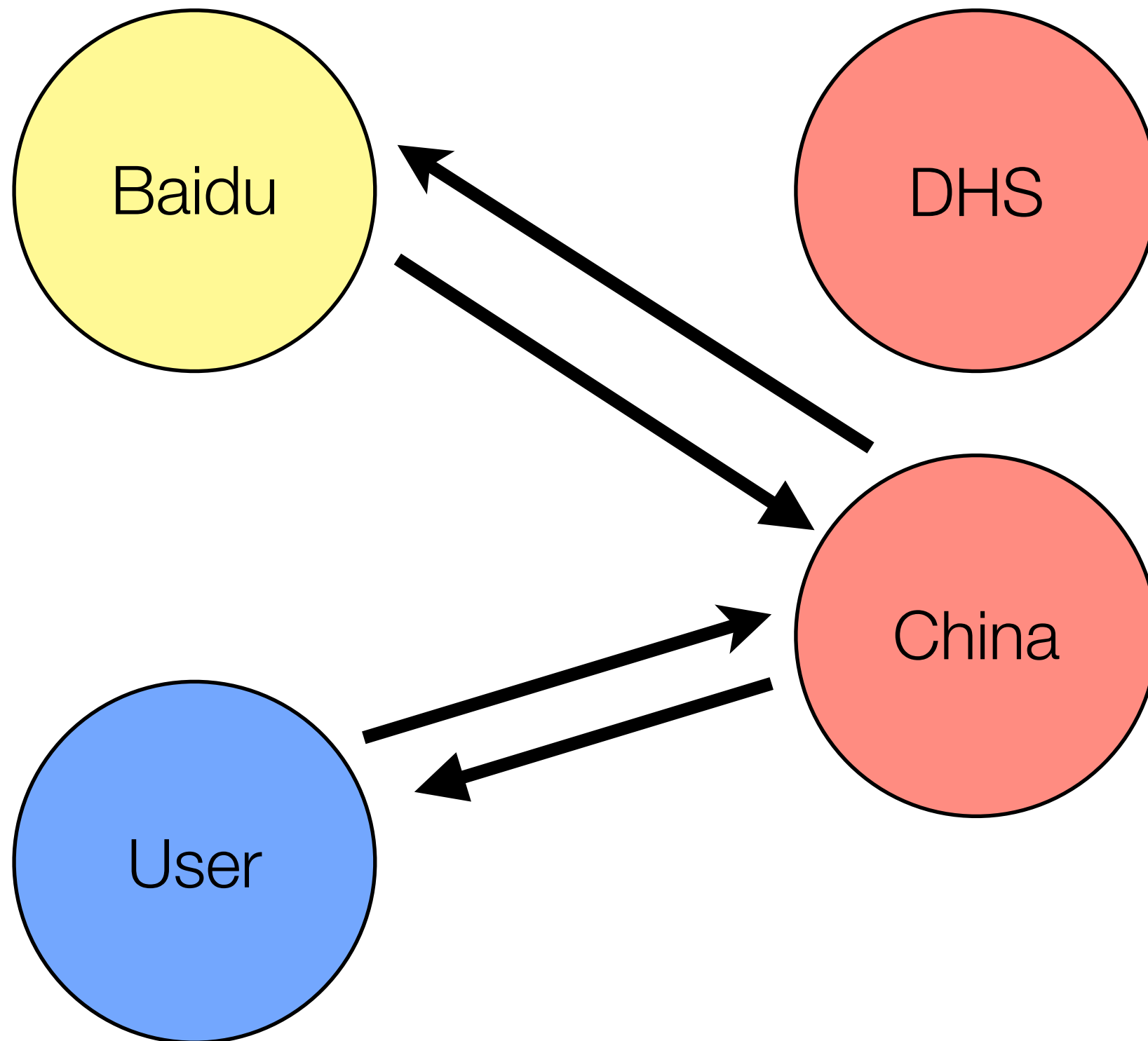


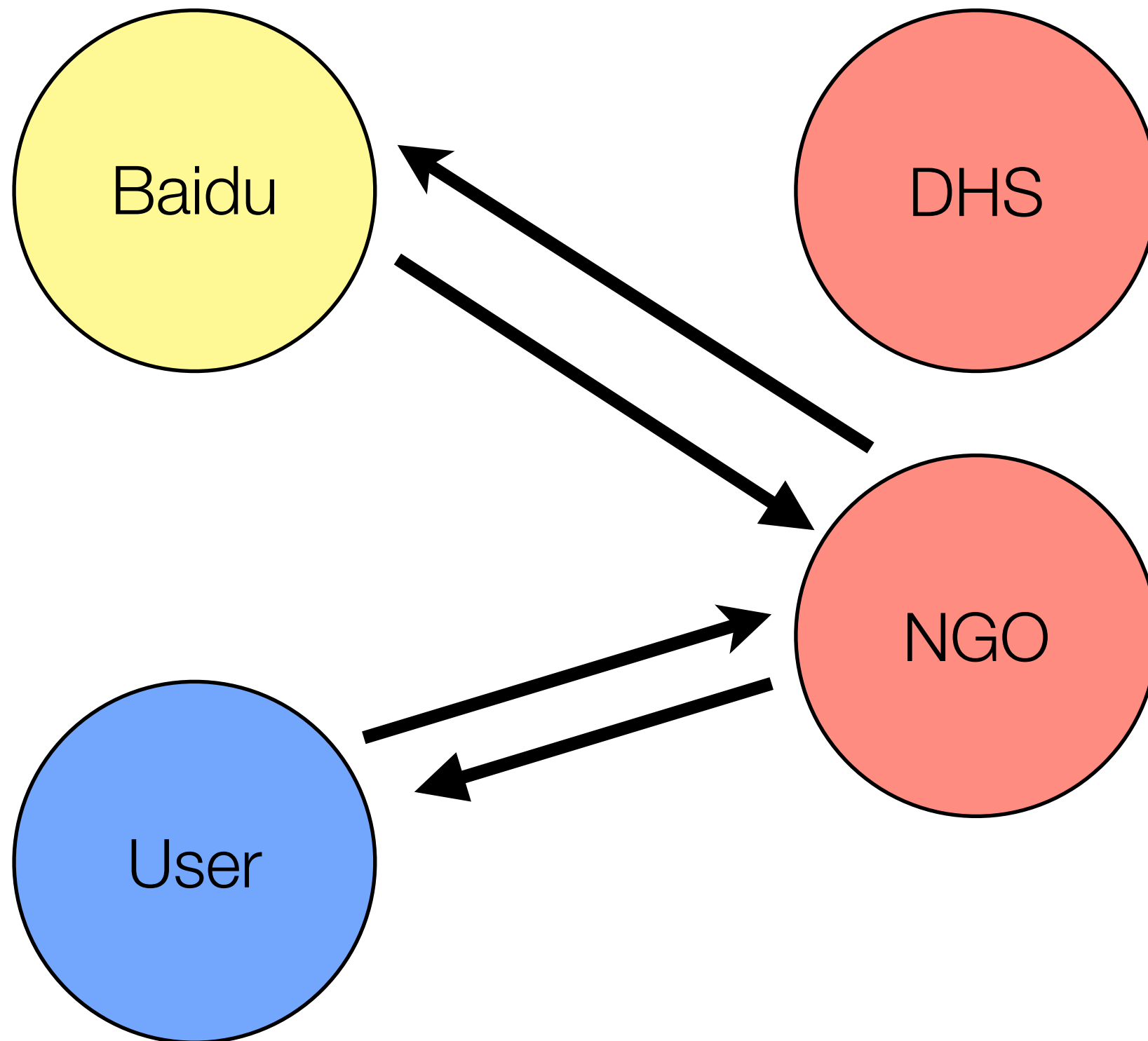












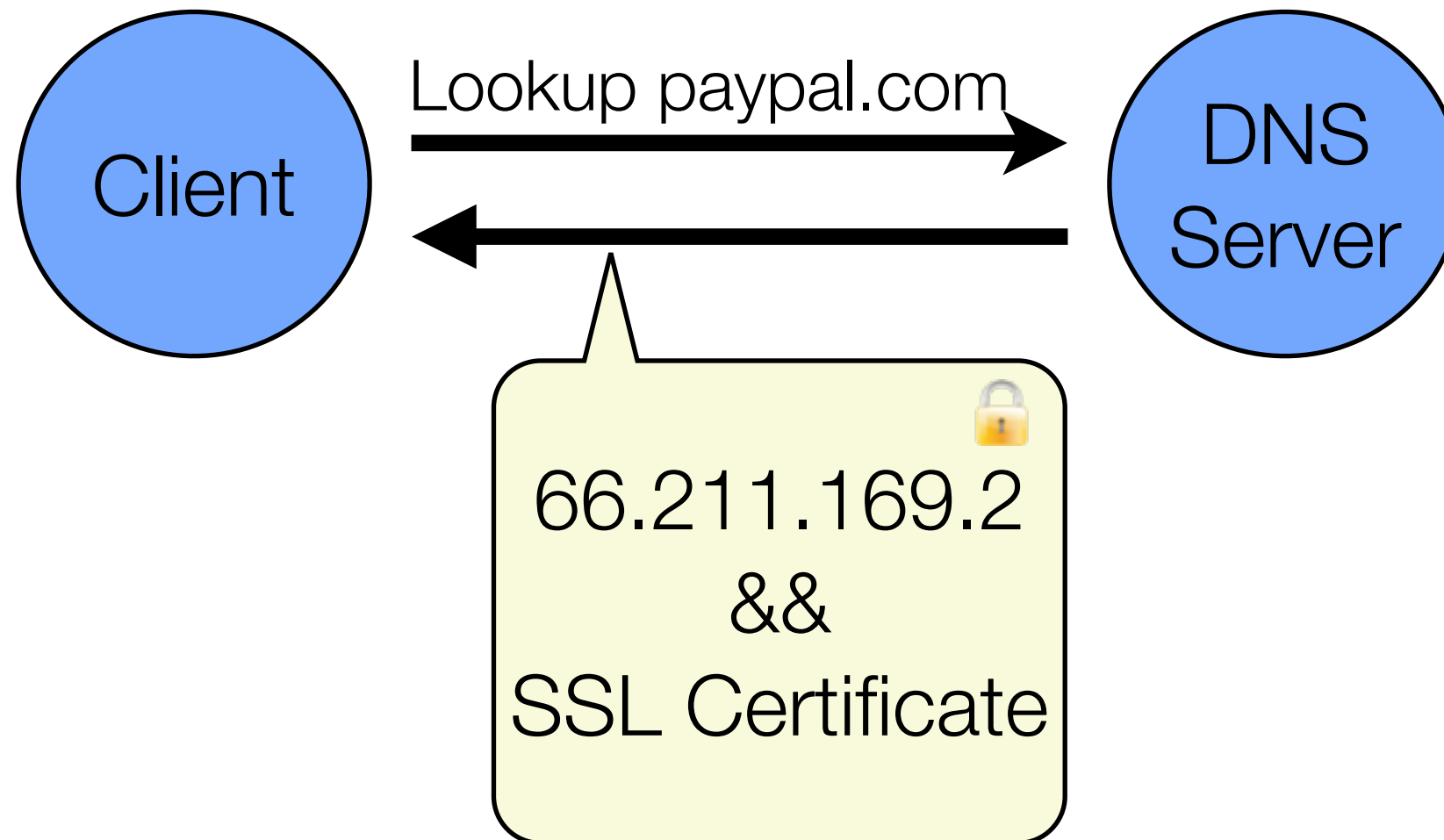
Trust Agility Properties

- ★ A trust decision can be easily revised at any time.
- ★ Individual users can decide where to anchor their trust.

DNSSEC

SSL Cert --> DNS Record





distributed

information --> distributed

trust --> centralized

DNSSEC == CA System

Trust Requirements

- The Registrars.
- The TLDs.
- The root.

Trust Requirements

- ▶ The Registrars.
- The TLDs.
- The root.

sketchy++

GoDaddy



Trust Requirements

- The Registrars.
- ▶ The TLDs.
- The root.

.com, .net

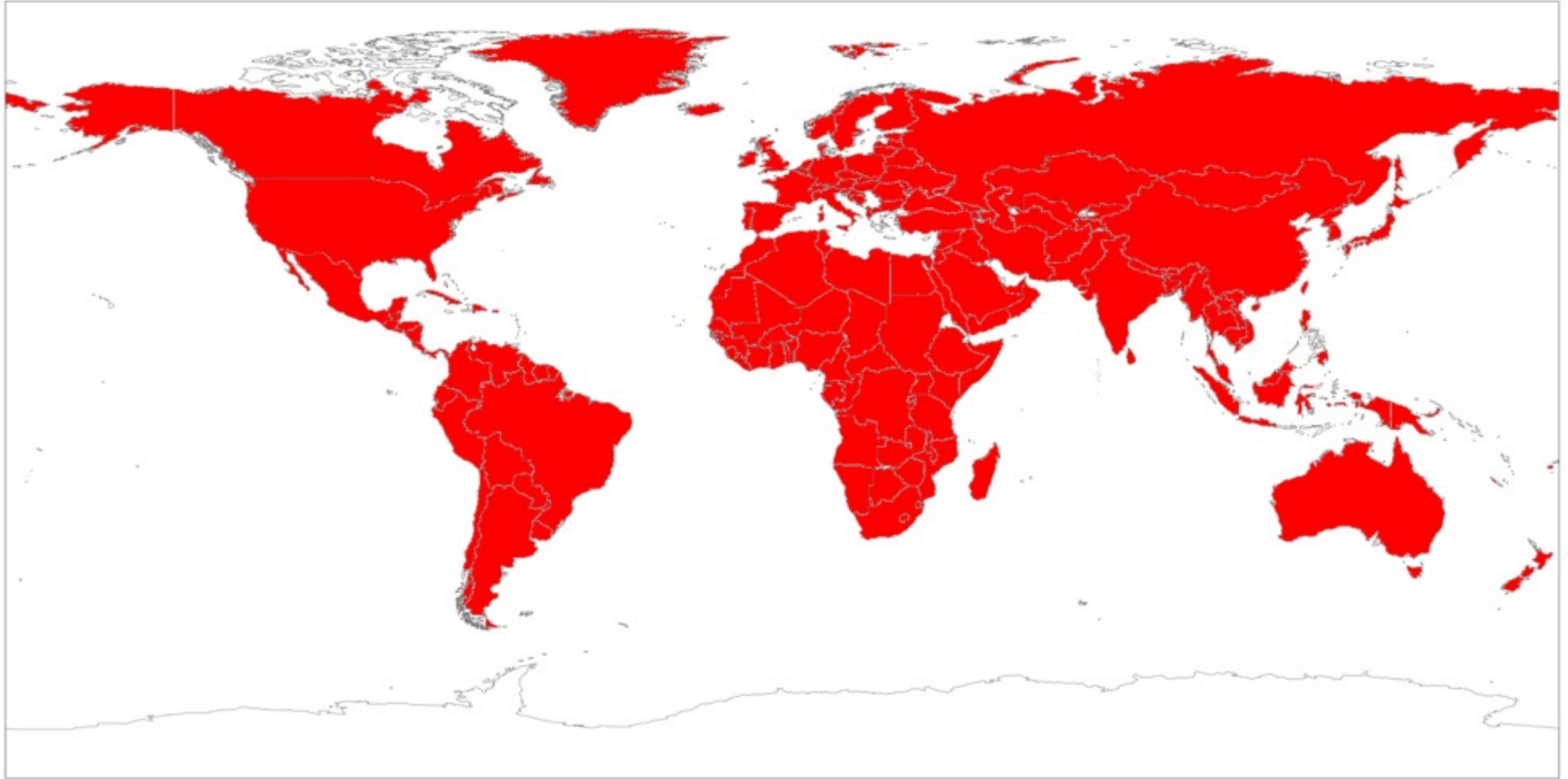
VeriSign

.org, .edu

ccTLDs

.io, .cc, .ly?

.ir, .cn?



domain seizures

Trust Requirements

- The Registrars.
- The TLDs.
- ▶ The root.

ICANN

Global --> California 501(c)(3)

COICA, PROTECT IP, etc...

Trust Requirements

- * The Registrars.

- * The TLDs.

- * The root.

< trust agility

trustdb -= VeriSign

Trust Requirements

- * The Registrars.

- * The TLDs.

- * The root.

forever



Perspectives

Dan Wendlandt, David G. Andersen, Adrian Perrig
Carnegie Mellon University

Perspectives: Improving SSH-style Host Authentication with Multi-Path Probing

Dan Wendlandt David G. Andersen Adrian Perrig
Carnegie Mellon University

Abstract

The popularity of “Trust-on-first-use” (Tofu) authentication, used by SSH and HTTPS with self-signed certificates, demonstrates significant demand for host authentication that is low-cost and simple to deploy. While Tofu-based applications are a clear improvement over completely insecure protocols, they can leave users vulnerable to even simple network attacks. Our system, PERSPECTIVES, thwarts many of these attacks by using a collection of “notary” hosts that observe a server’s public key via multiple network vantage points (detecting localized attacks) and keeps a record of the server’s key over time (recognizing short-lived attacks). Clients can download these records on-demand and compare them against an unauthenticated key, detecting many common attacks. PERSPECTIVES explores a promising part of the host authentication design space: Trust-on-first-use applications gain significant attack robustness without sacrificing their ease-of-use. We

Furthermore, a study by Reis et al. used client-side measurements to confirm that real-time snooping and modification of web traffic is a reality in today’s networks [20].

In this paper, we examine a novel approach to authenticating a server’s public key. Traditional approaches to server key authentication, such as a public-key infrastructure (PKI) [7, 5], rely on trusted entities (e.g., Verisign) that grant certificates based on the validation of real-world identities. When done securely, such verification requires significant (often manual) effort. While some network hosts, primarily commercial websites, can afford to pay the high verification cost for these certificates, clients have no simple and effective means to authenticate connectivity to most other hosts on the Internet.

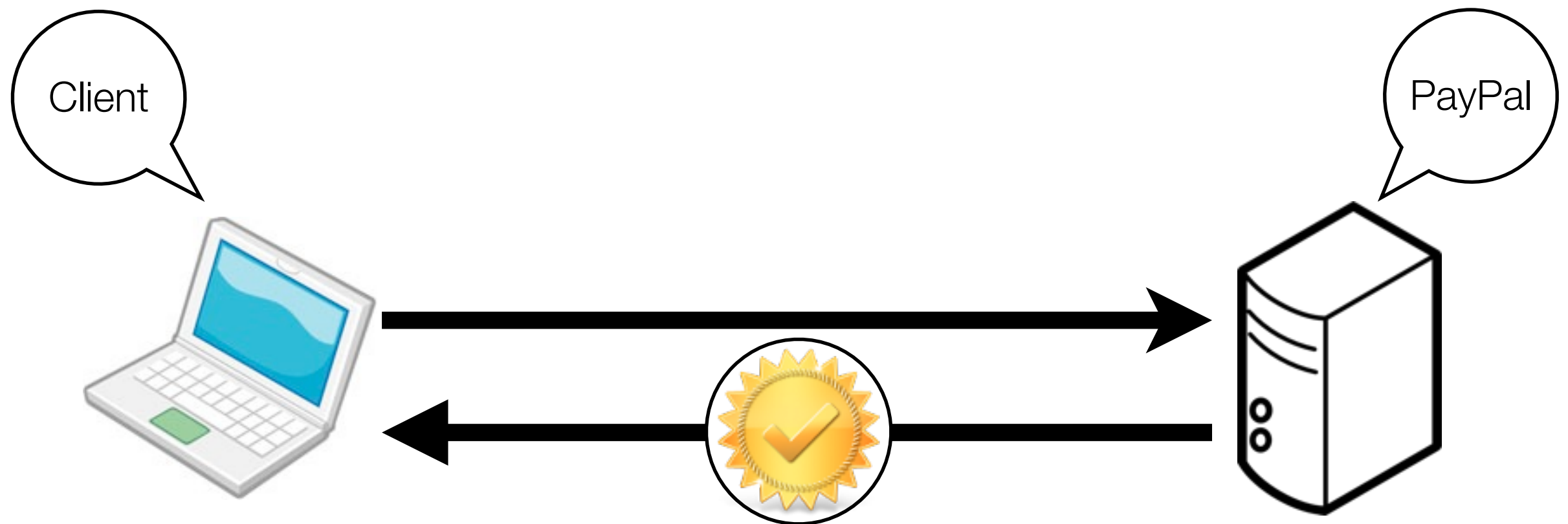
Because the high cost of creating and managing a host PKI presented a substantial barrier to the replacement of completely insecure protocols such as telnet, the *SSH model* of host authentication emerged as a pragmatic so-

perspective

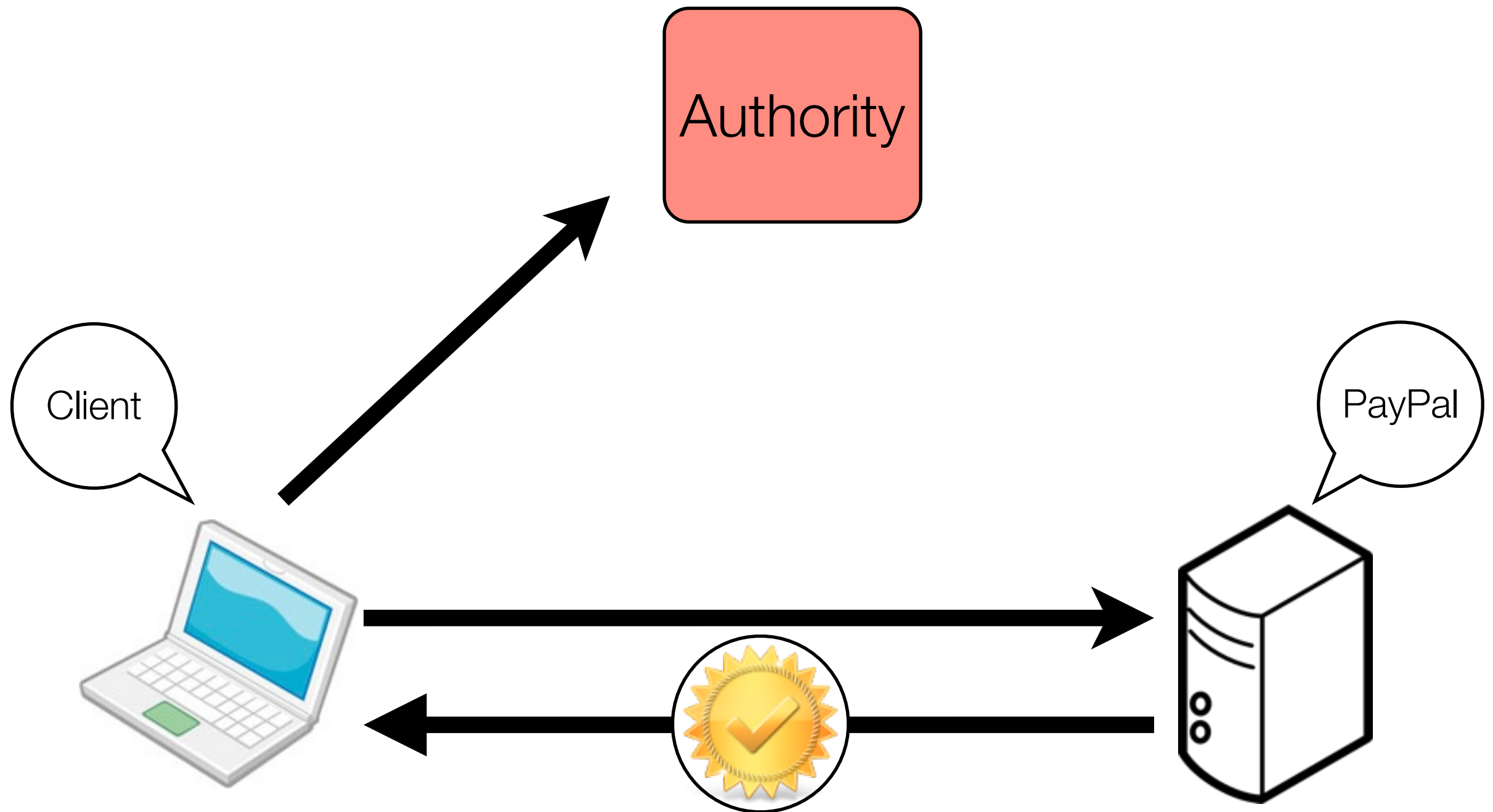
Basic Premise



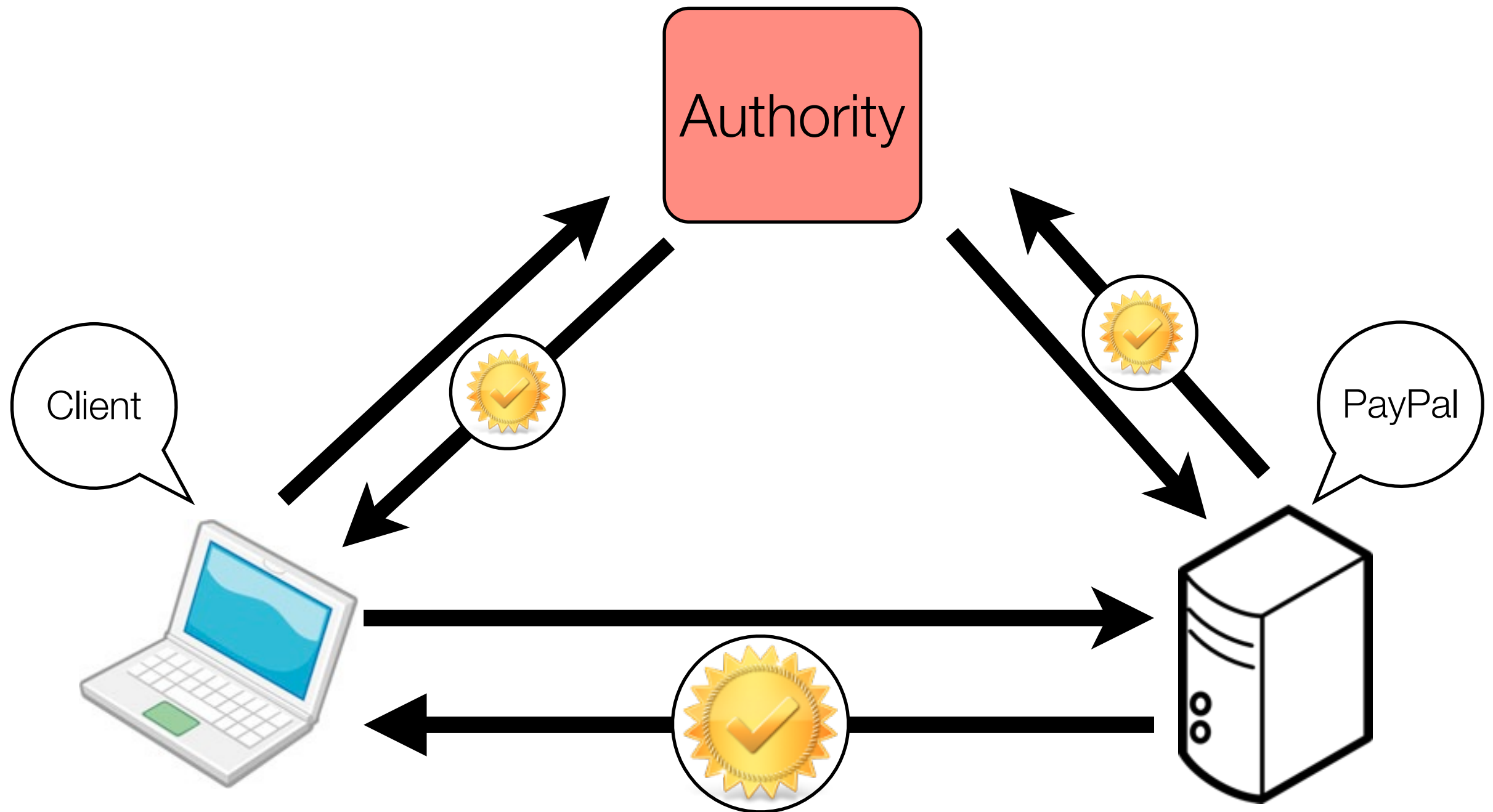
Basic Premise



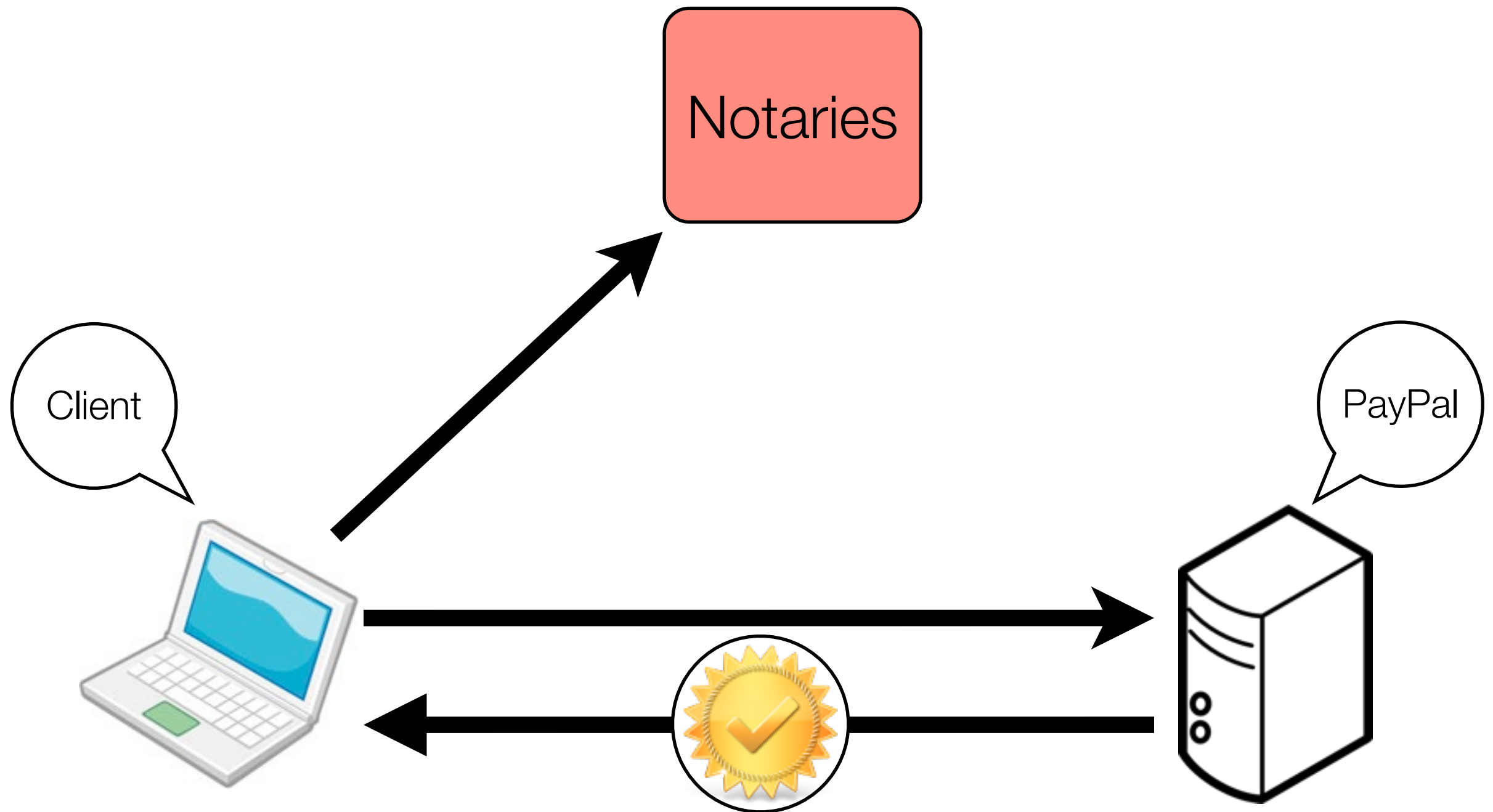
Basic Premise



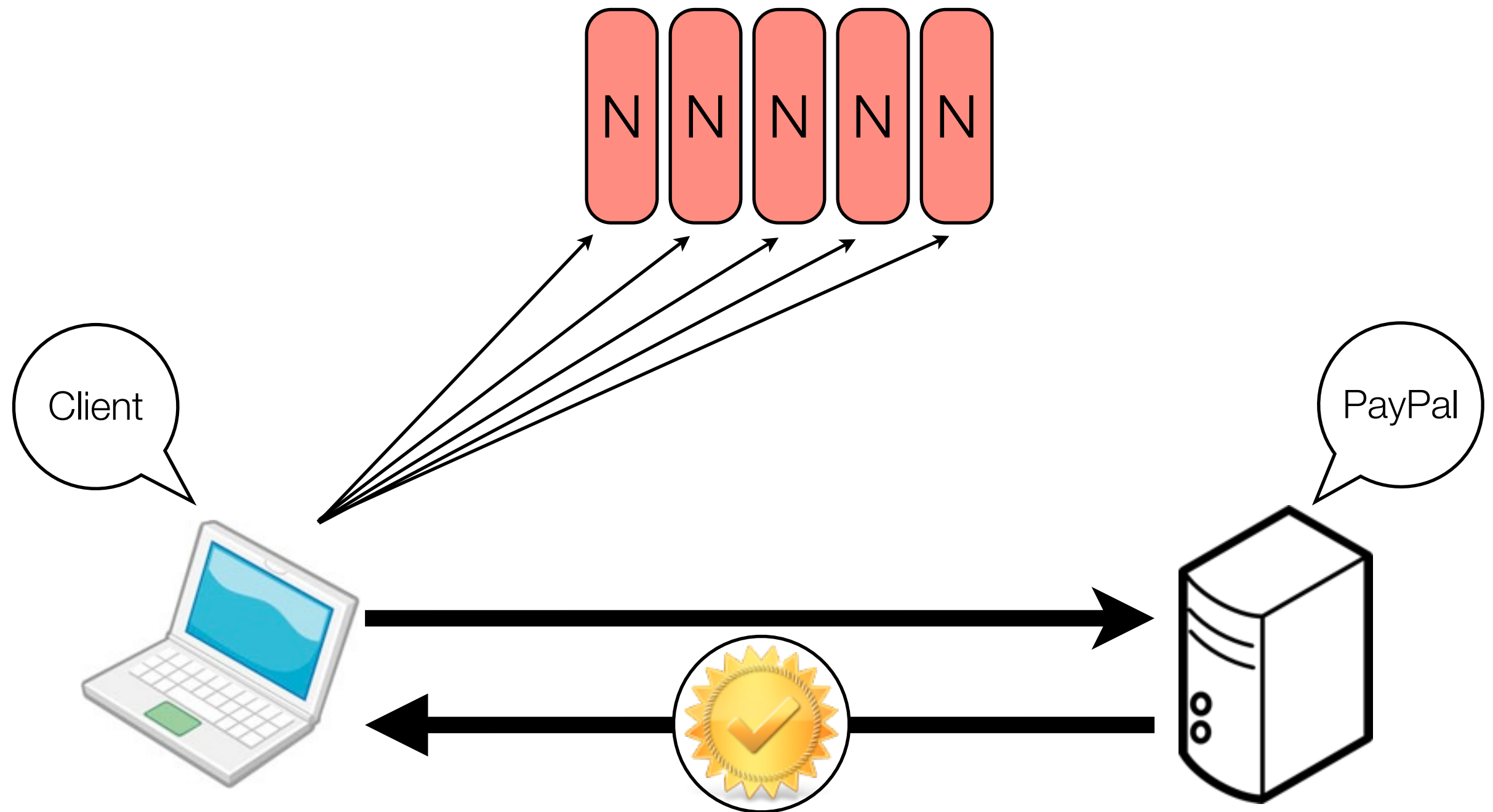
Basic Premise



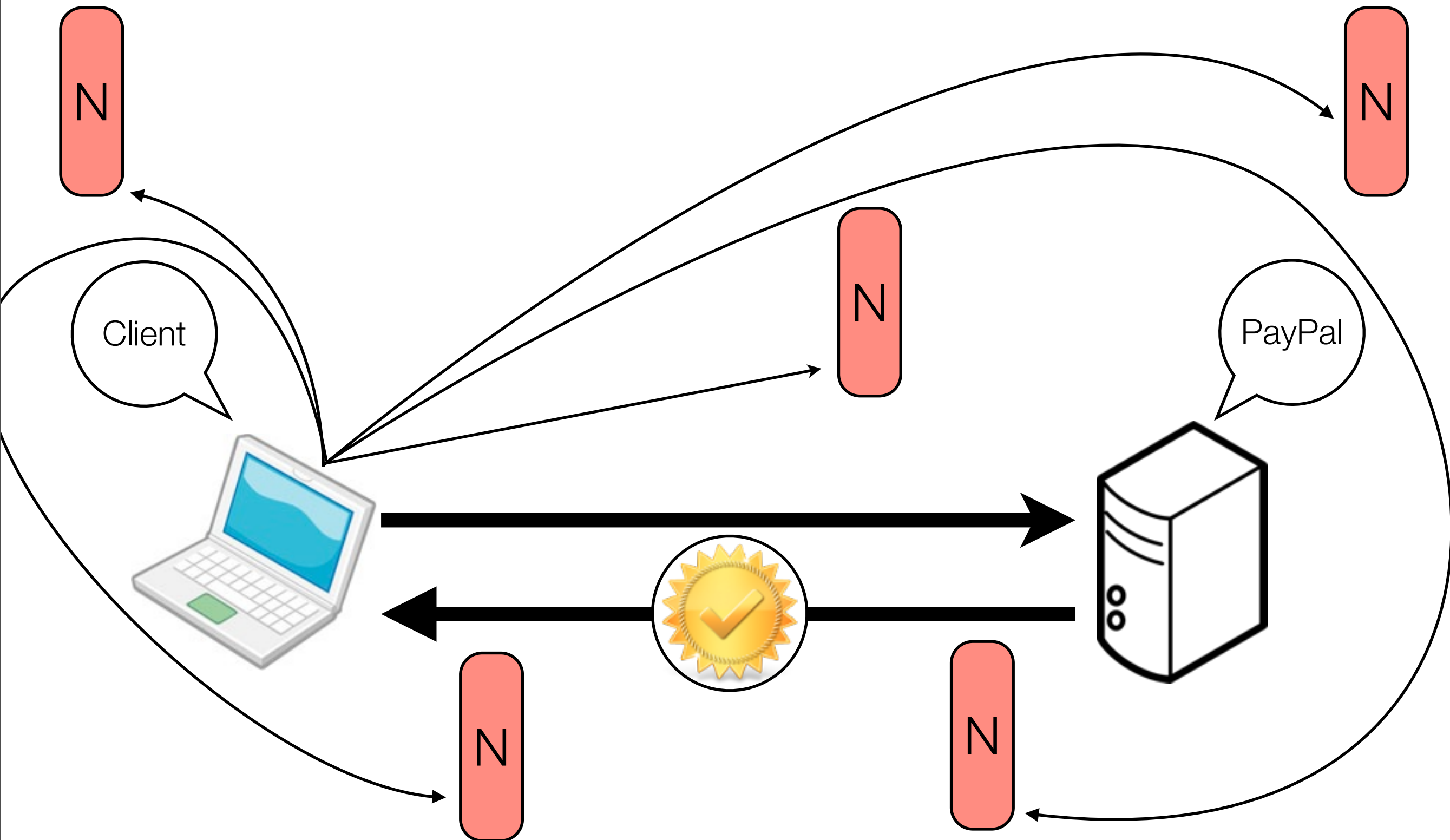
Basic Premise



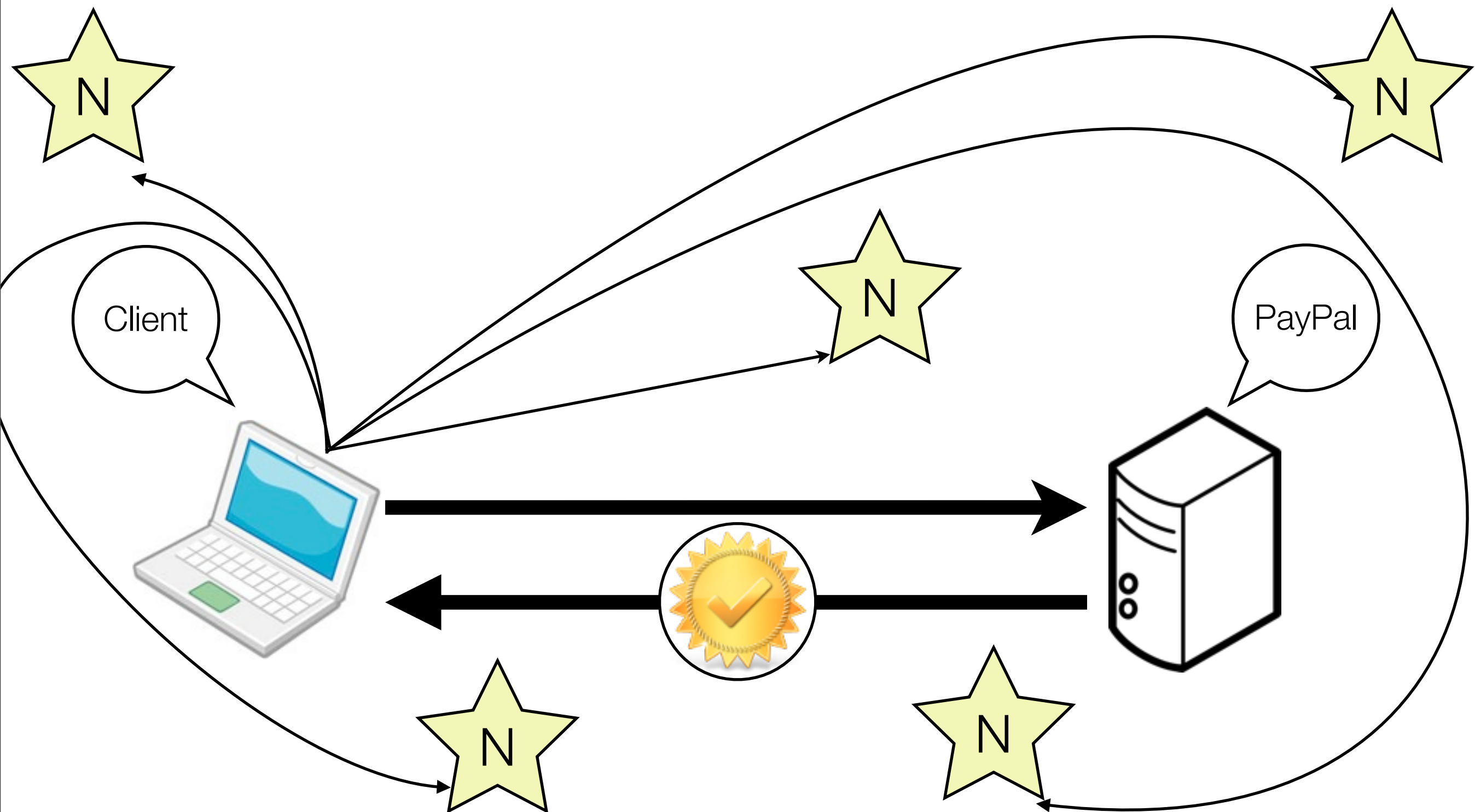
Basic Premise



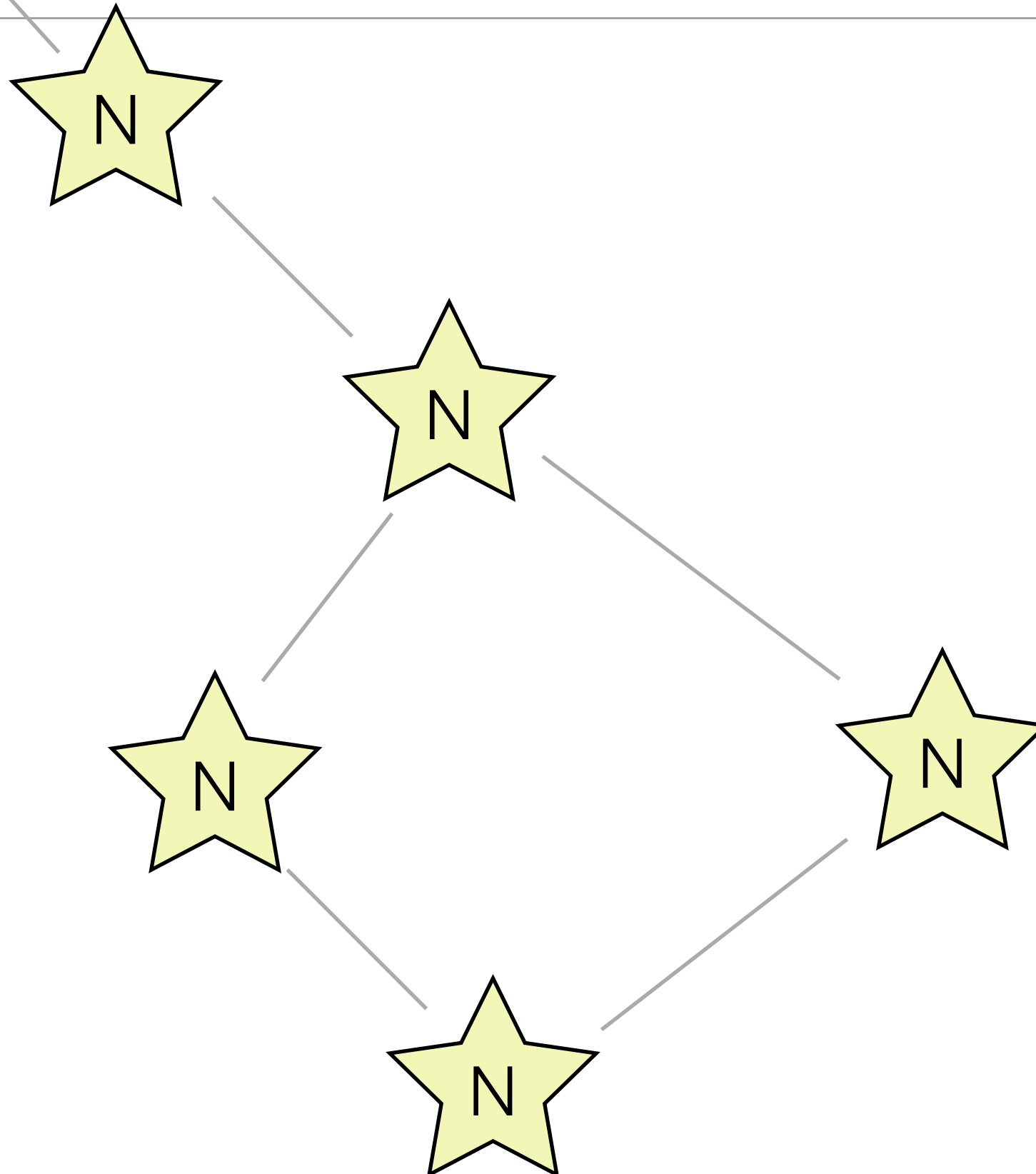
Basic Premise



Basic Premise

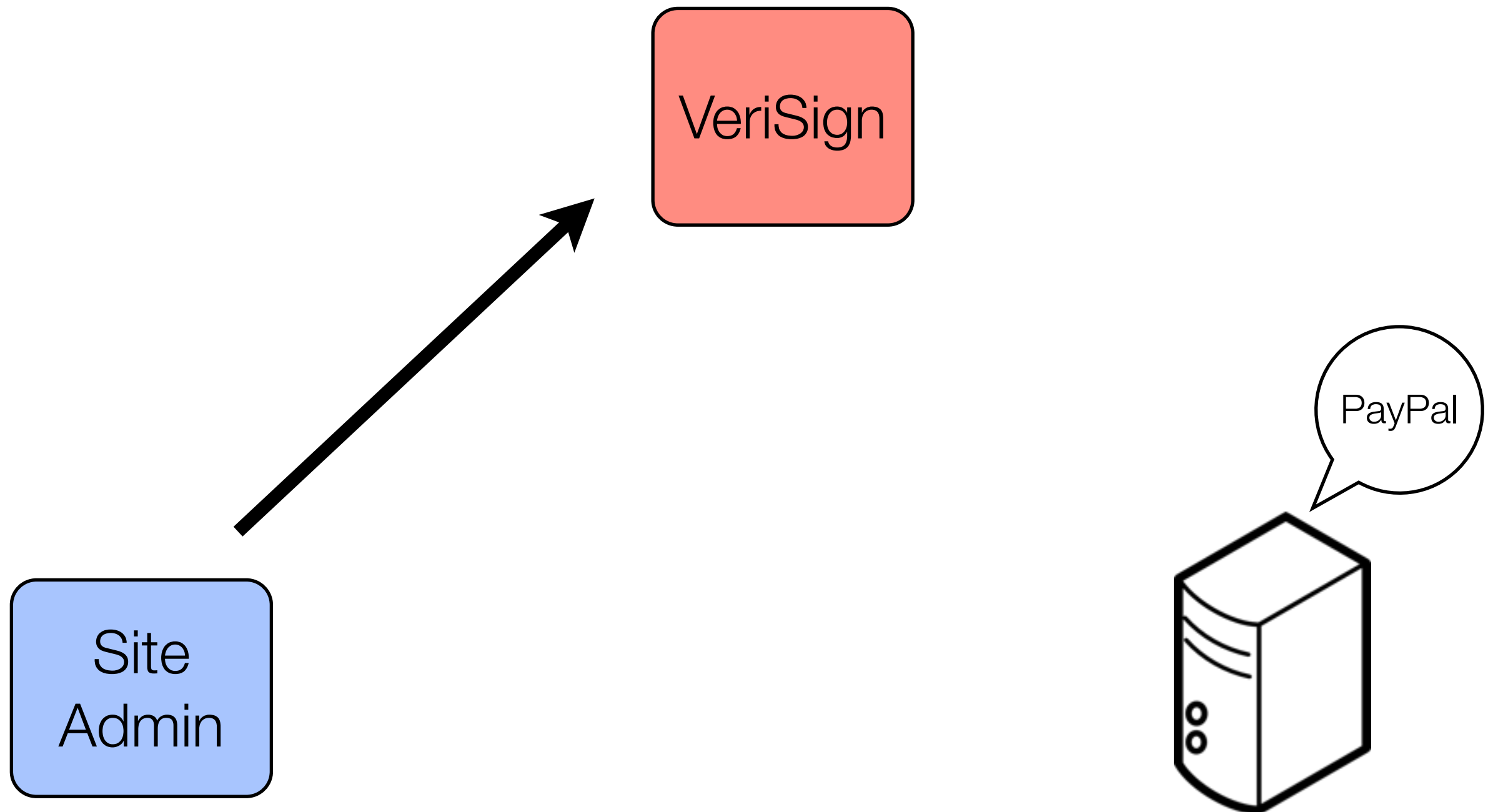


Basic Premise

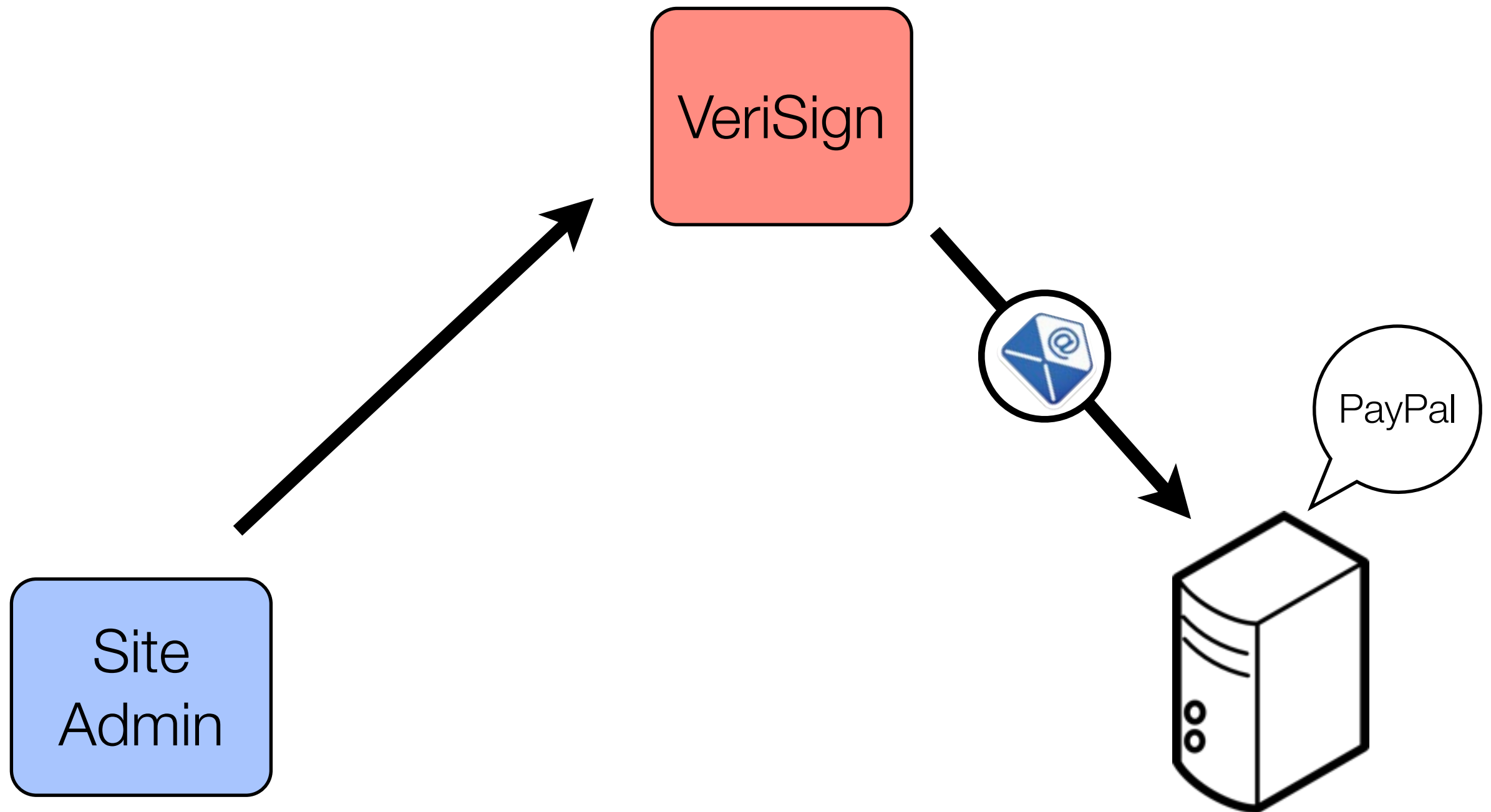


“perspective” is not new

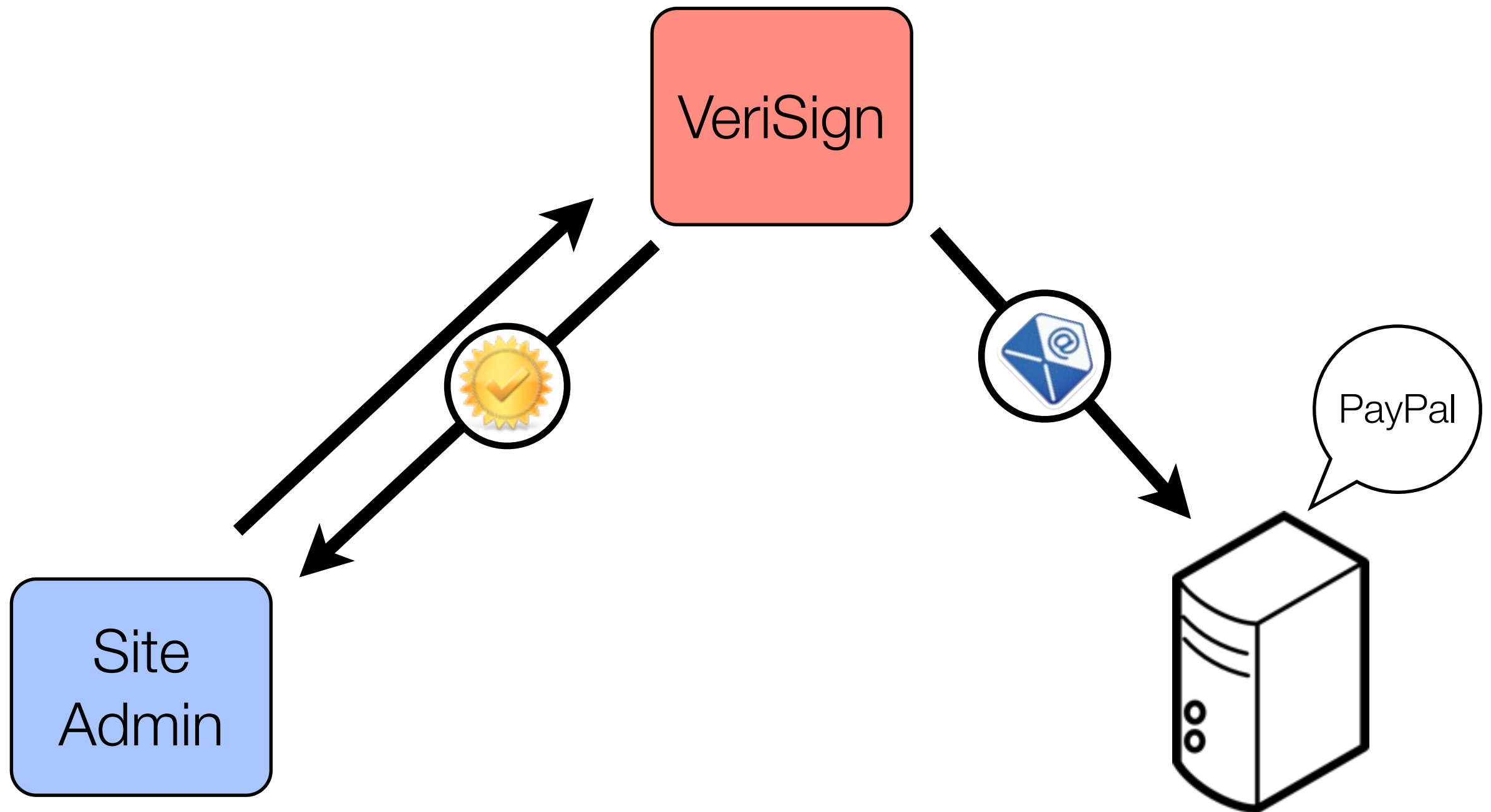
The CA Version Of Perspective



The CA Version Of Perspective



The CA Version Of Perspective



invert

user initiated

implementation

limited

self-signed certs

Perspectives Challenges



Completeness



Privacy



Responsiveness

Perspectives Challenges



Completeness



Privacy



Responsiveness



initial connection

! eliminate CAs entirely

Perspectives Challenges



Completeness

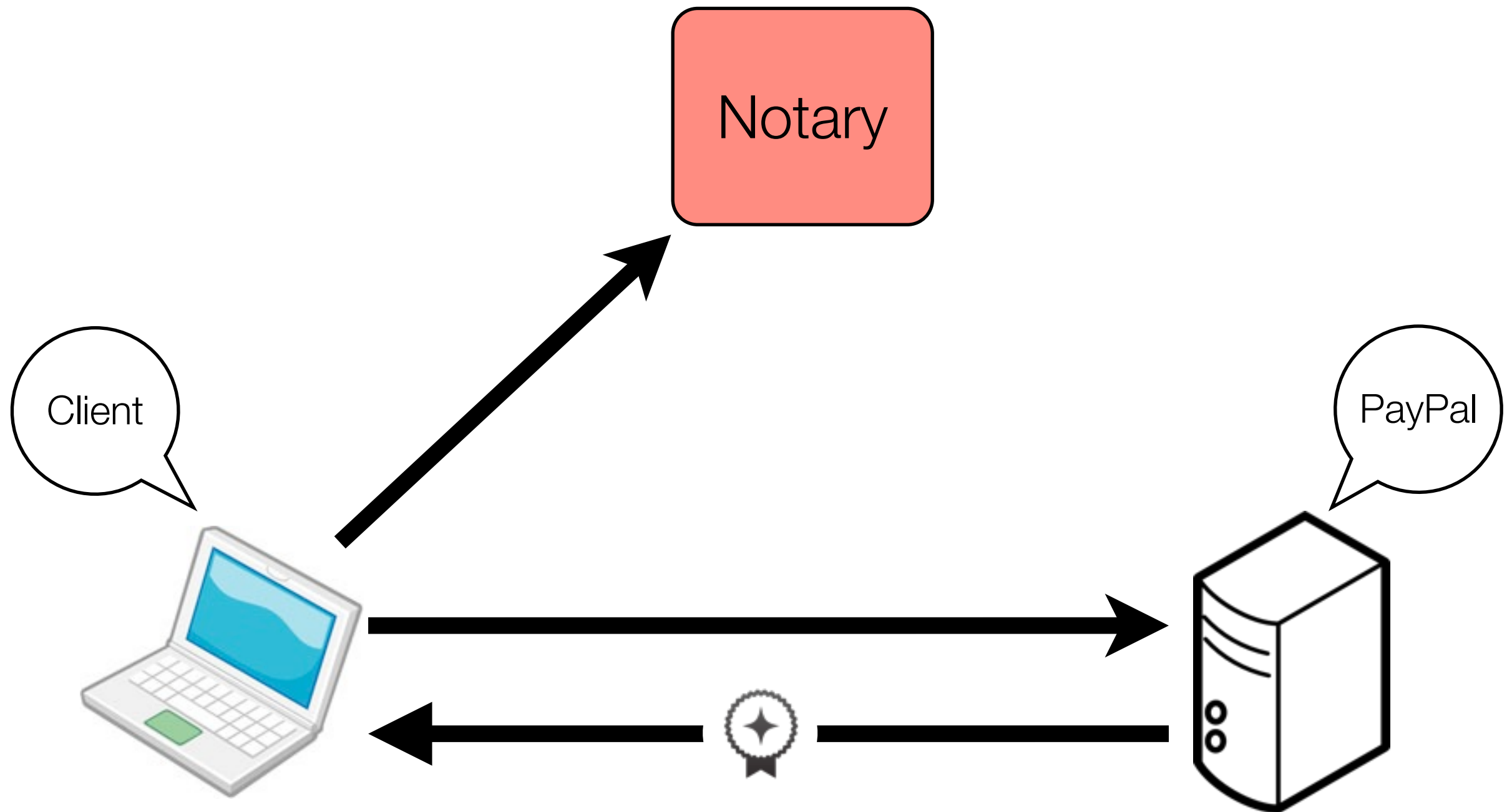


Privacy



Responsiveness

Privacy Problems



Perspectives Challenges



Completeness



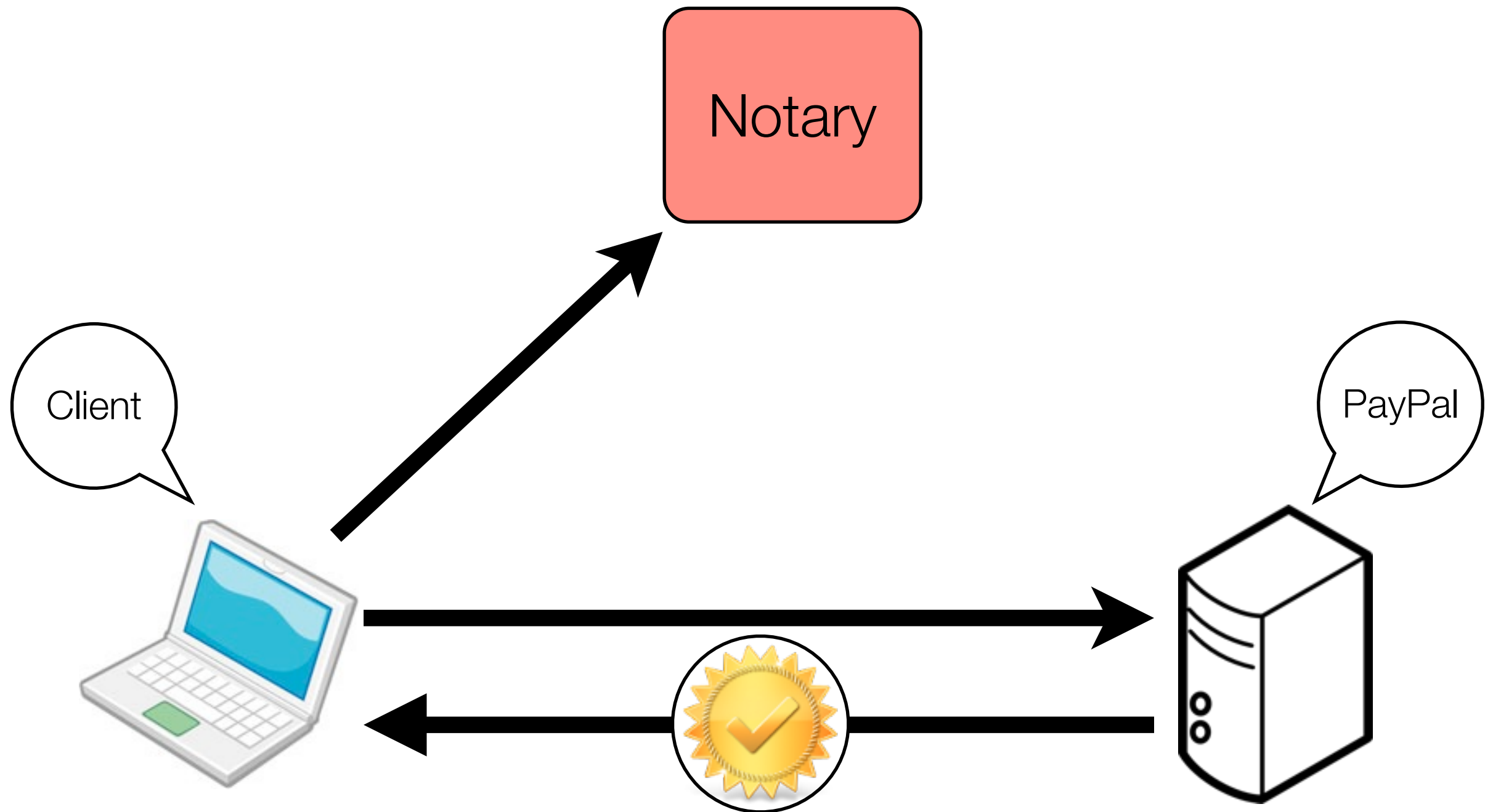
Privacy



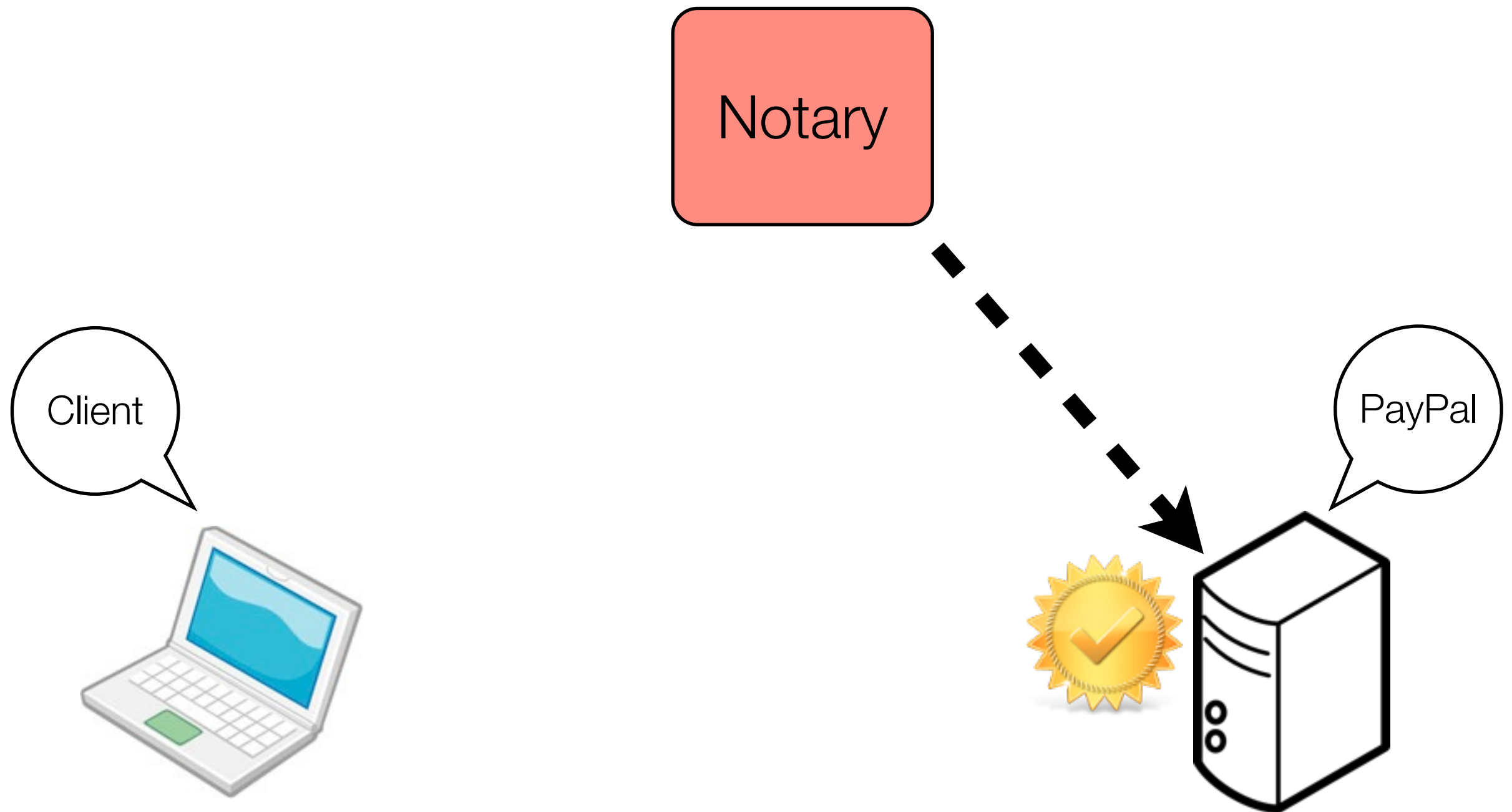
Responsiveness

notary lag

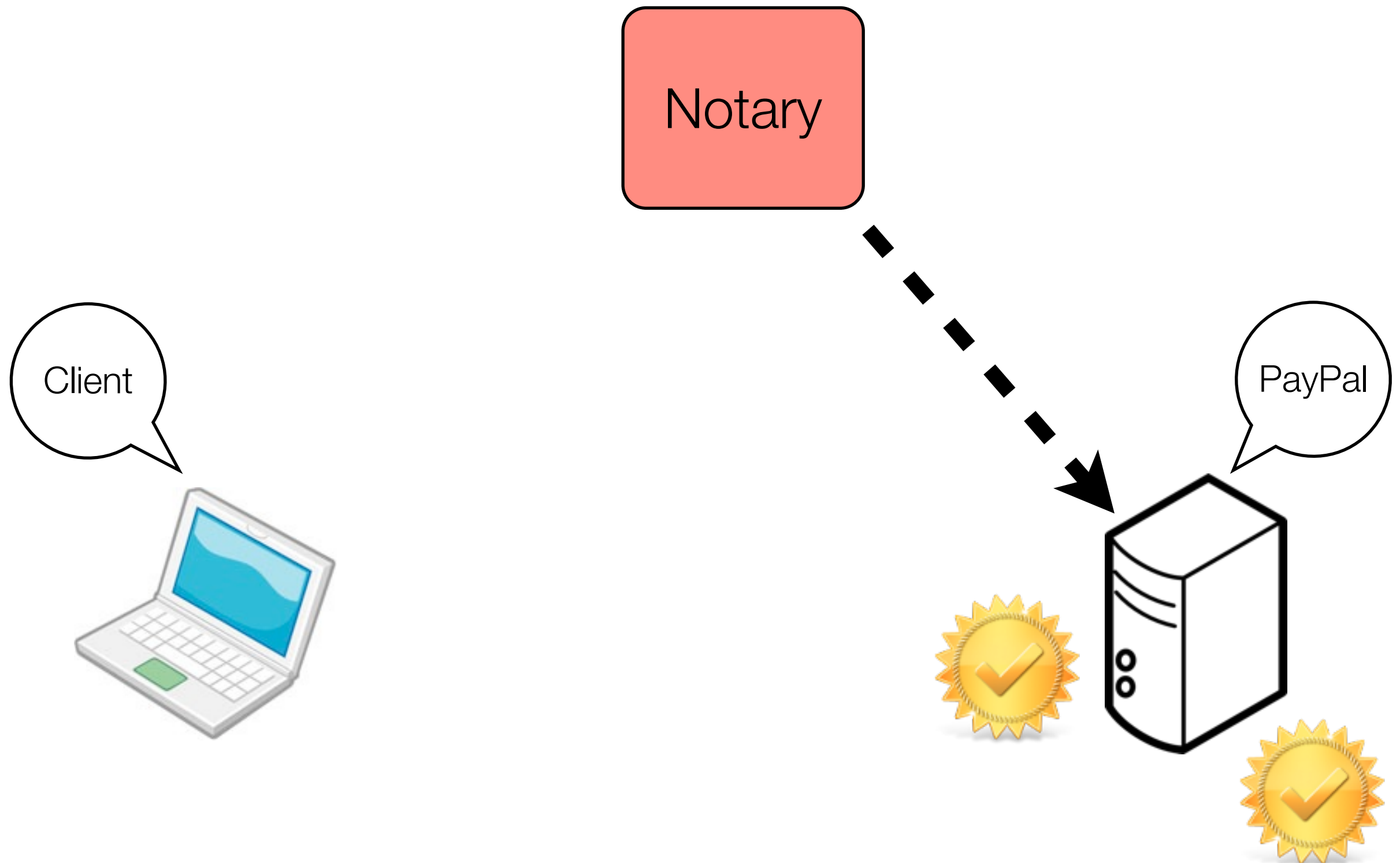
Notary Lag



Notary Lag



Notary Lag





CONVERGENCE



CONVERGENCE

- New Protocol
- New Client Implementation
- New Server Implementation

Perspectives Challenges



Completeness



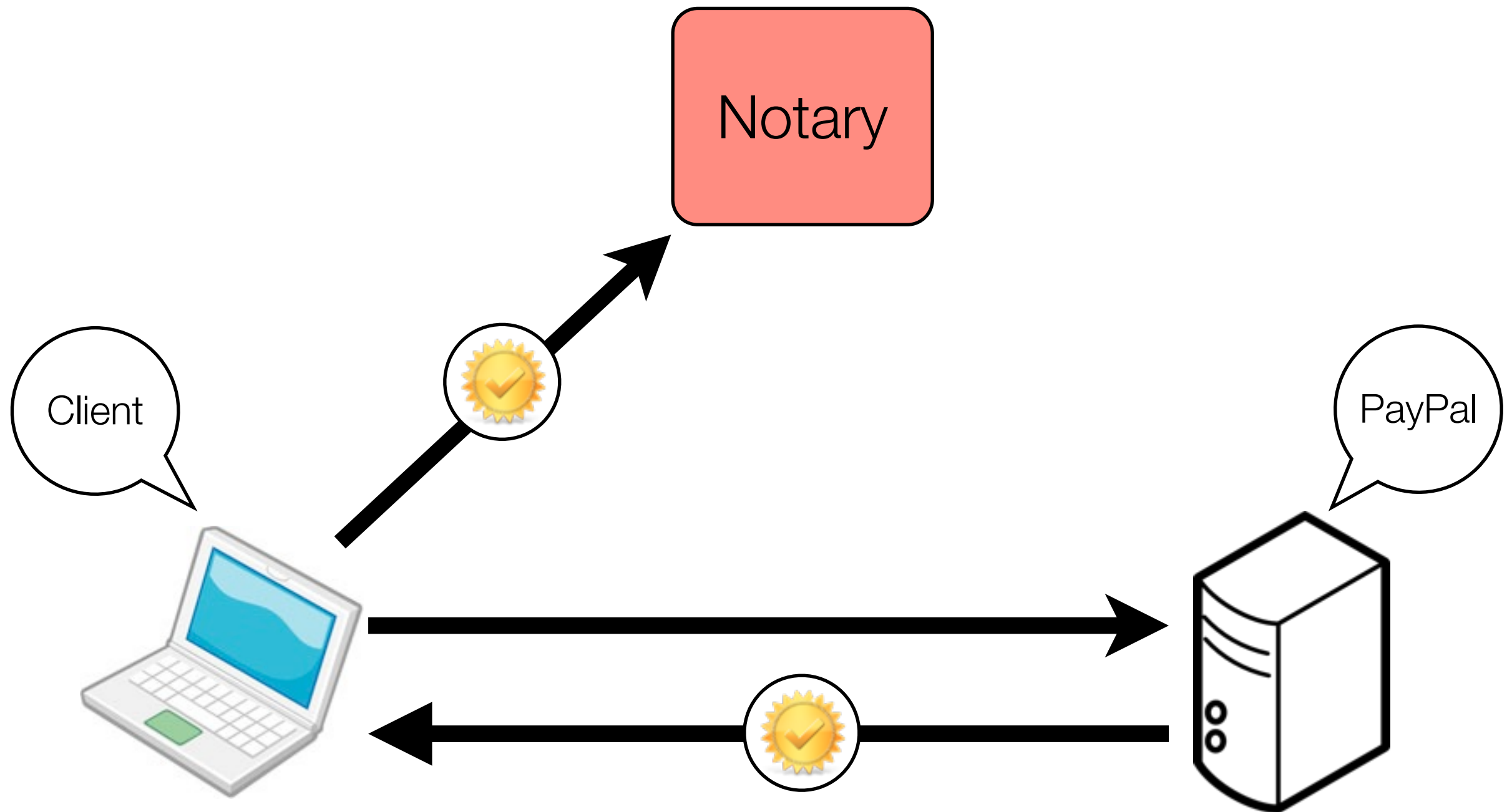
Privacy



Responsiveness

! notary lag

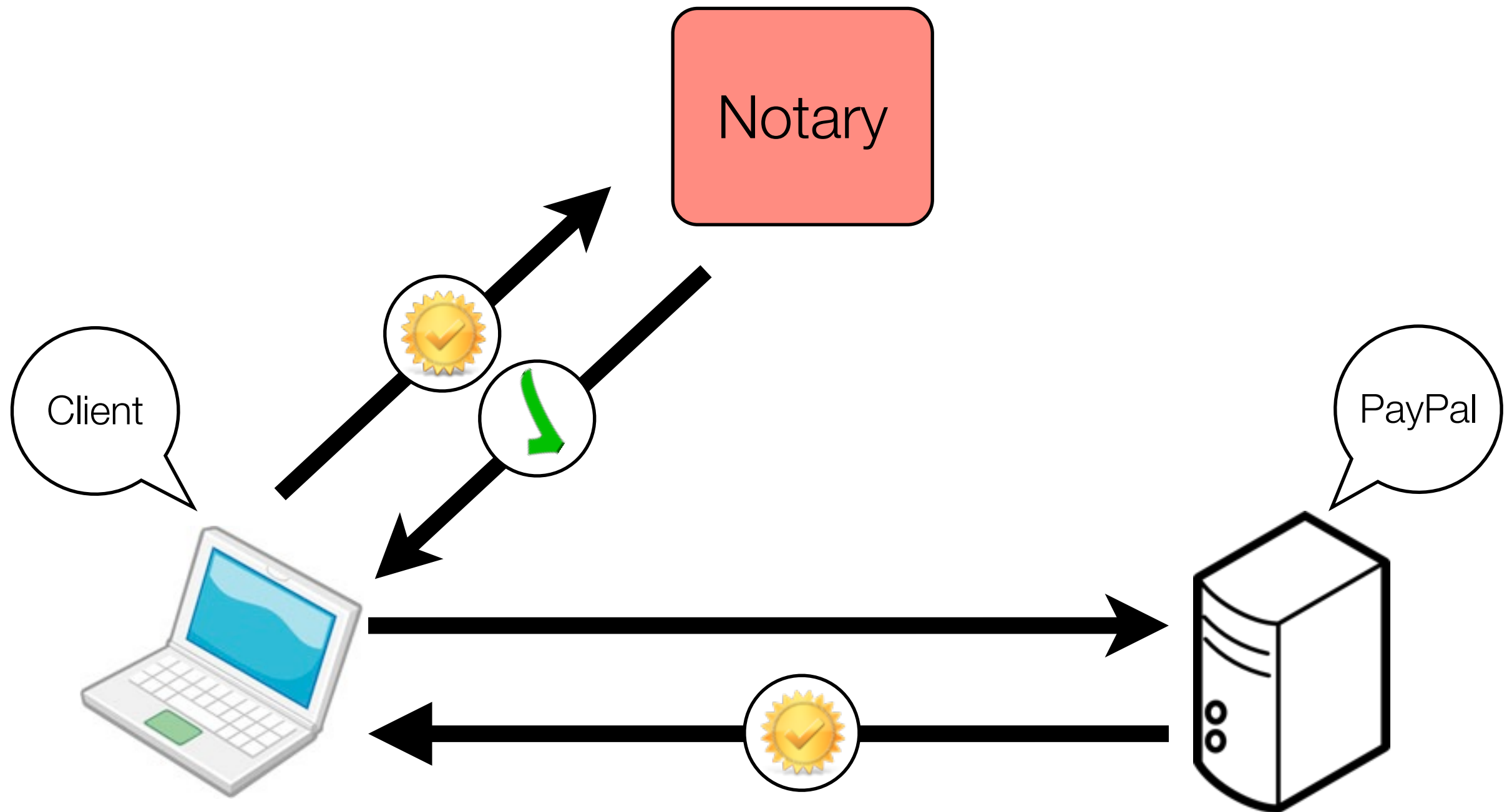
Responsive: Eliminate Notary Lag



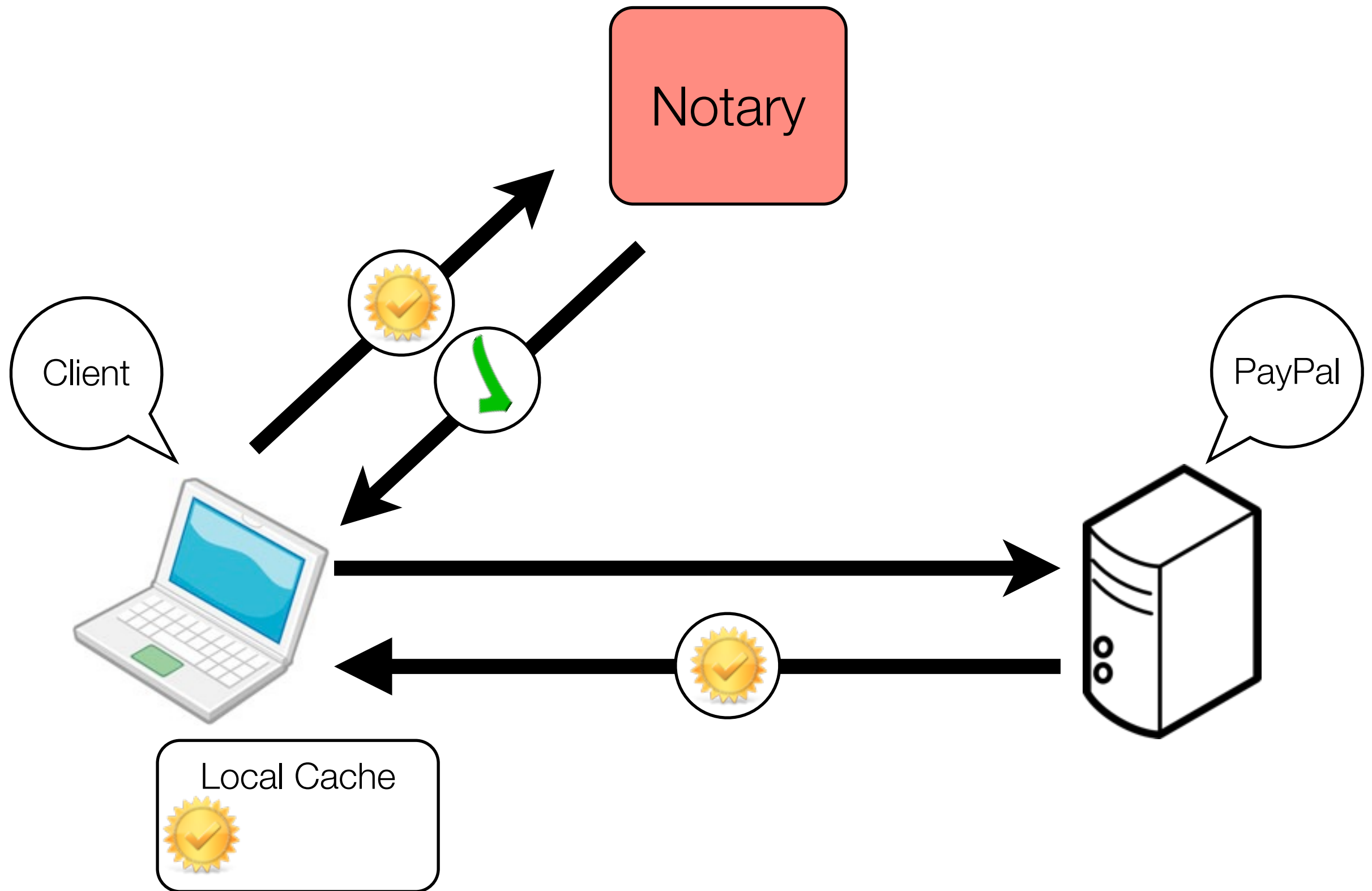
+ privacy

1) local caching

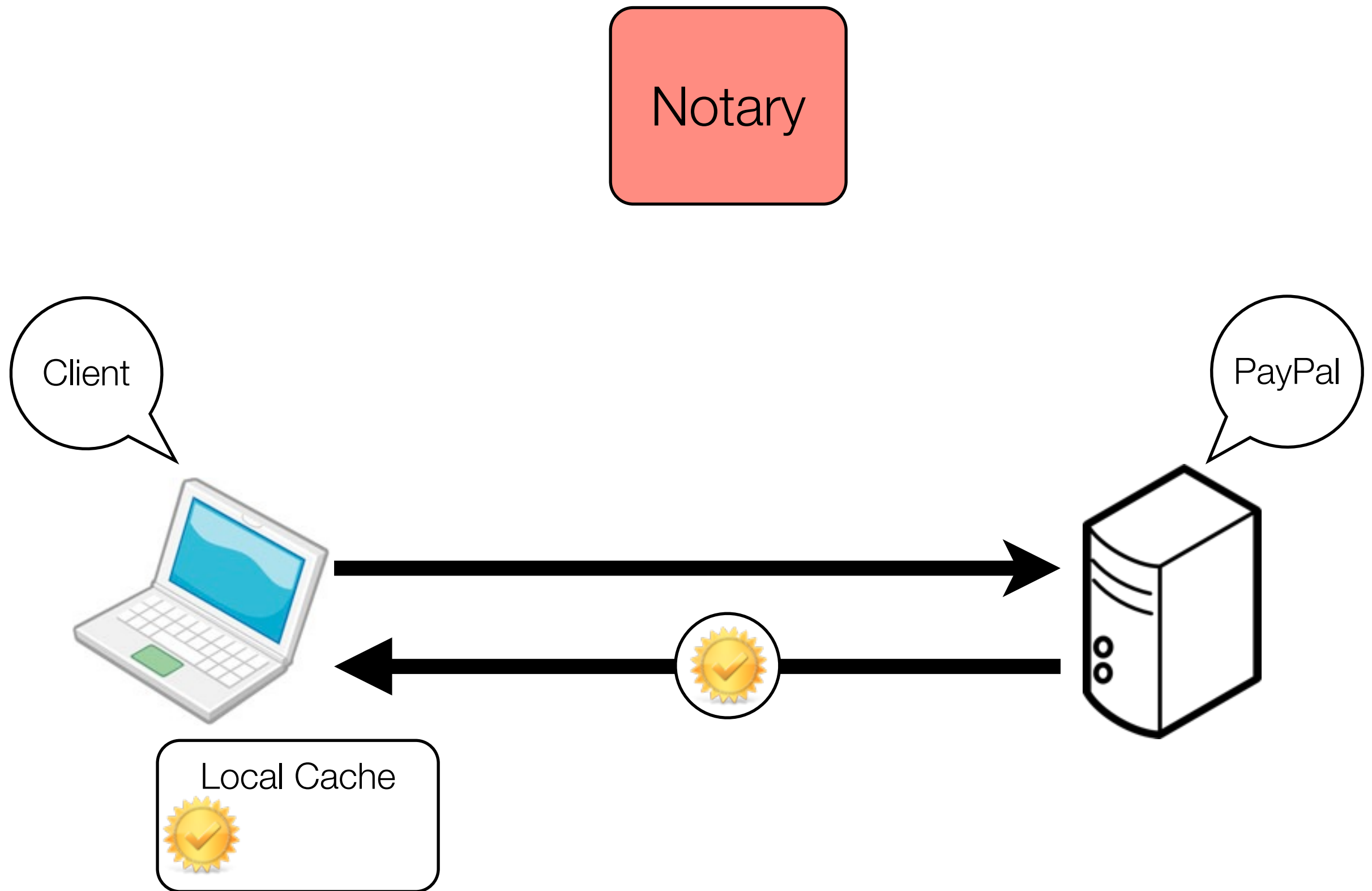
Local Caching



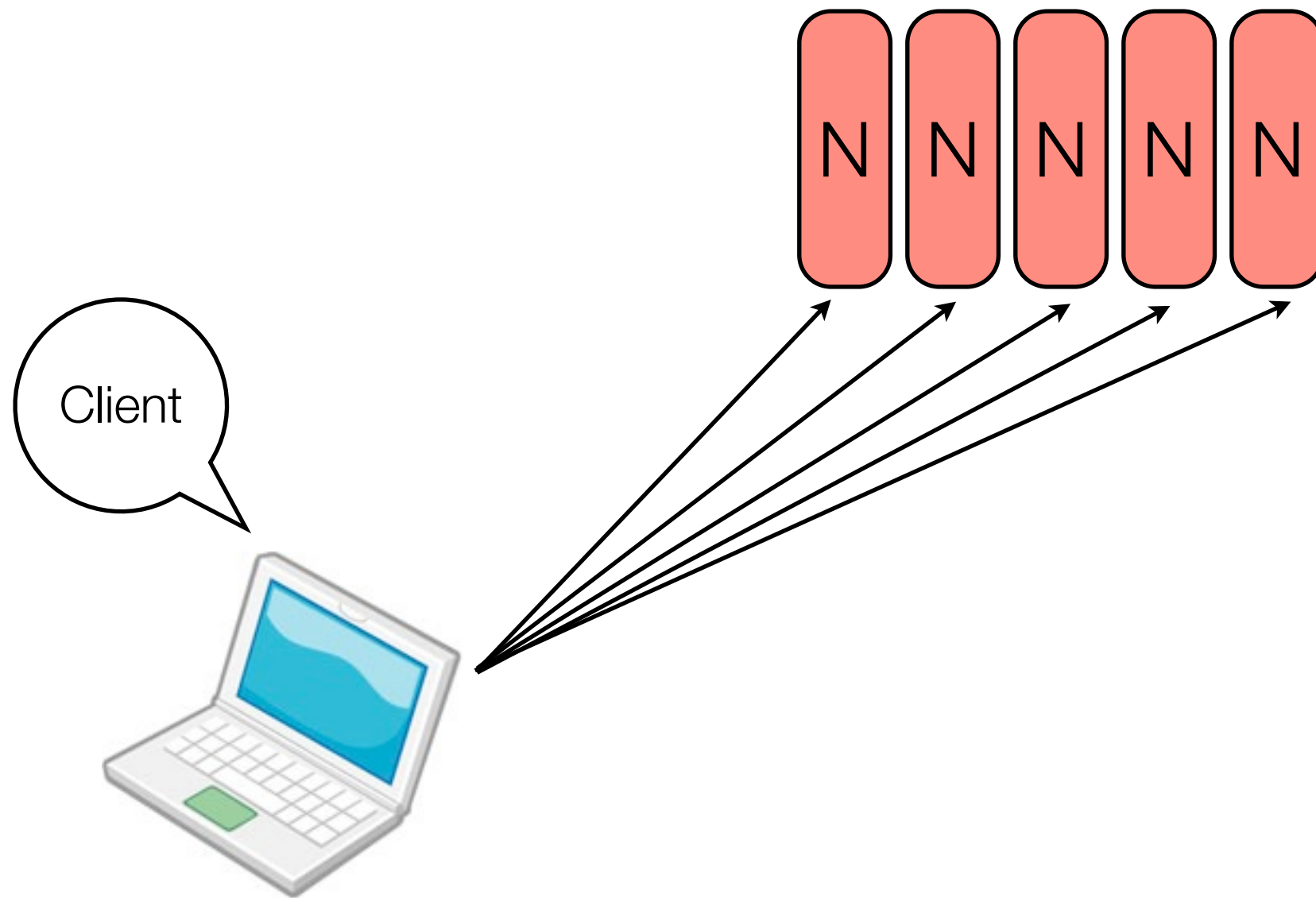
Local Caching



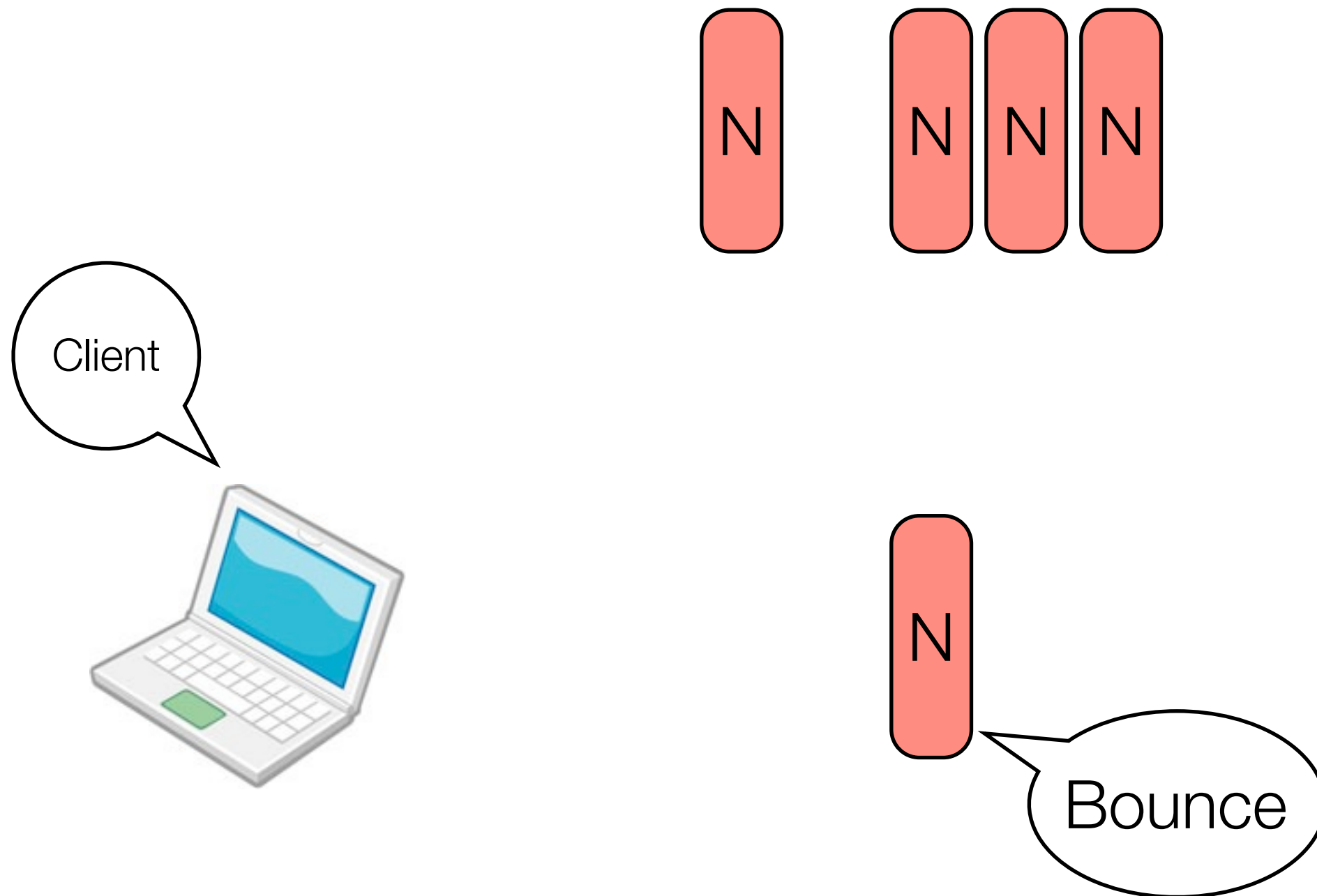
Local Caching



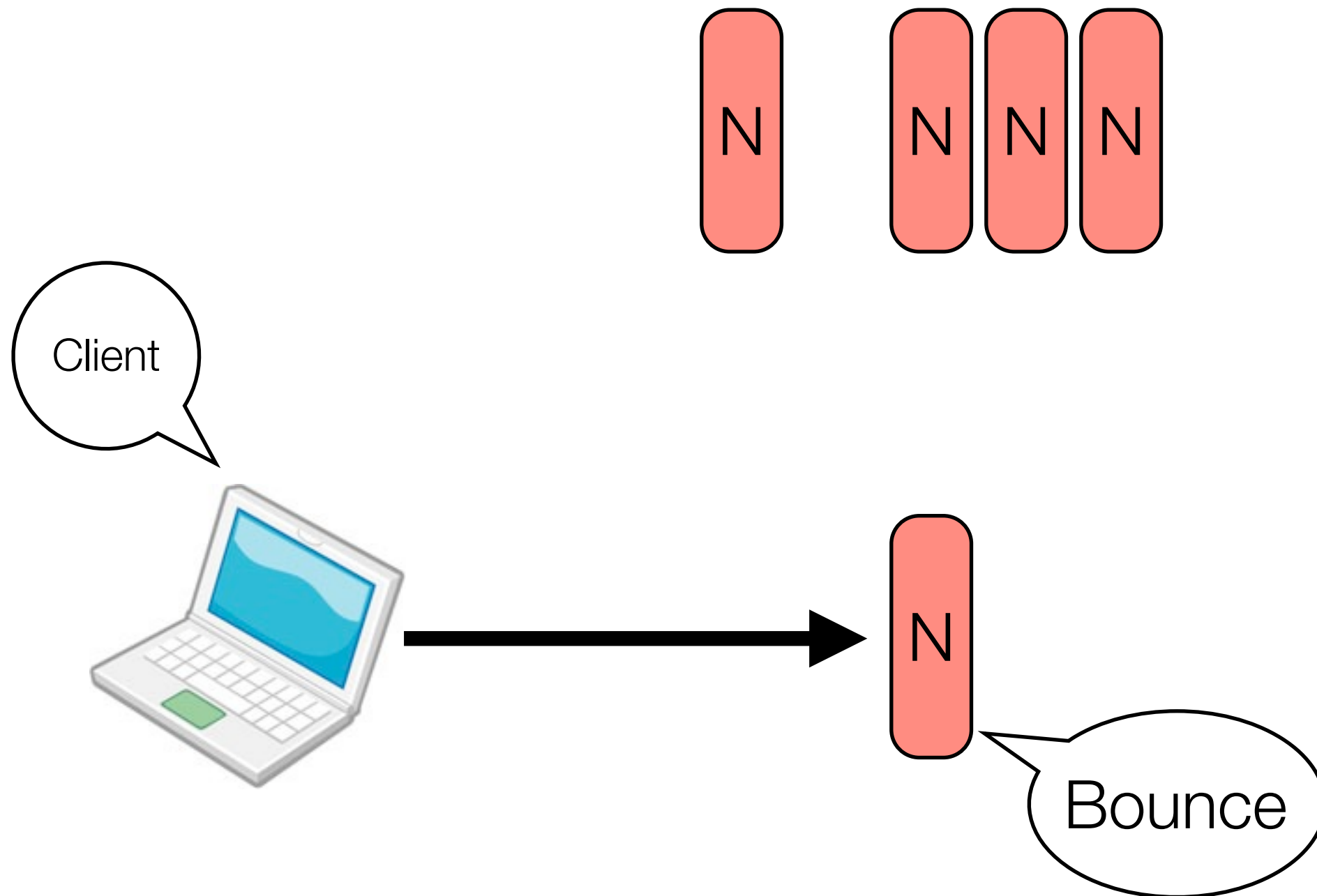
Notary Bounce



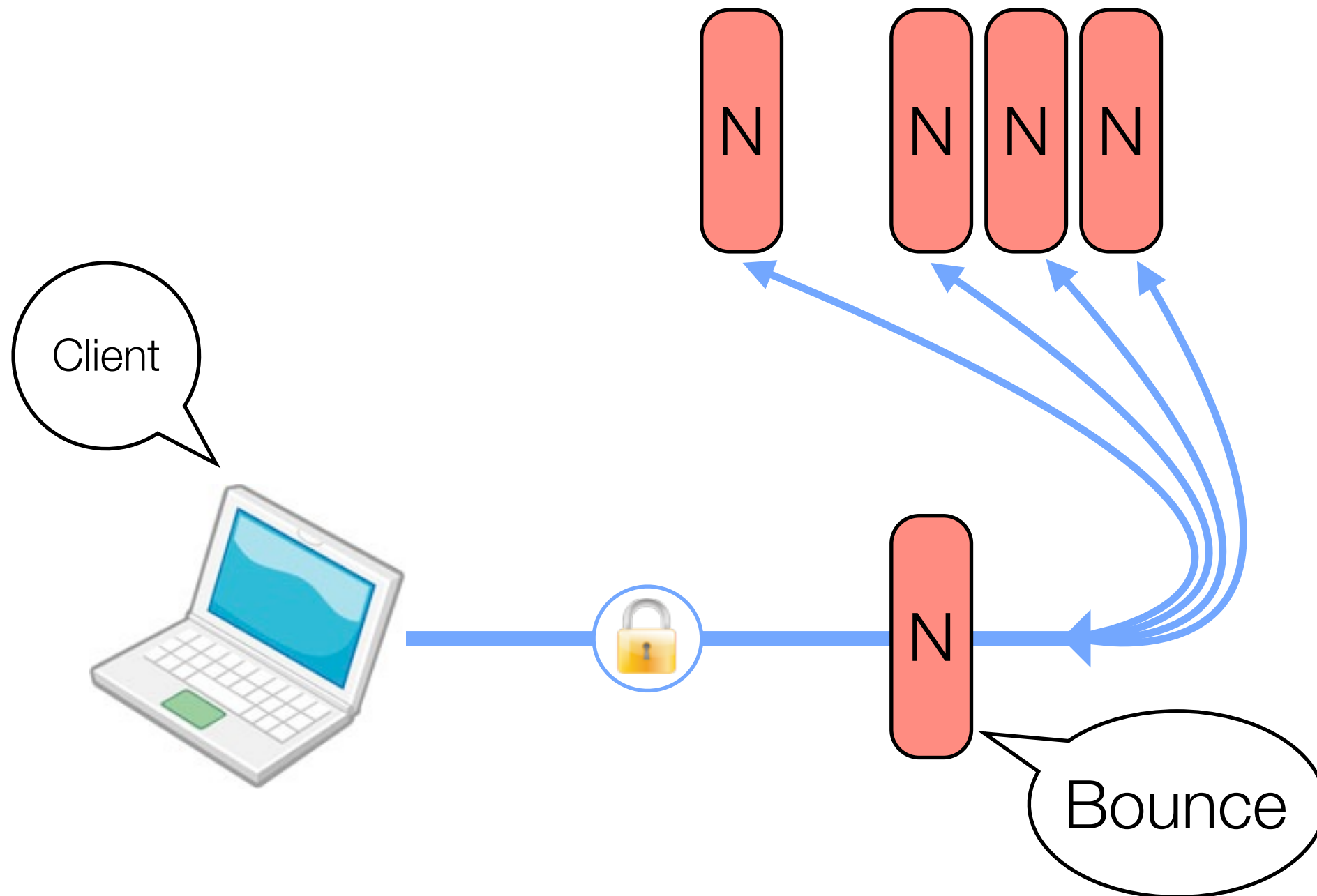
Notary Bounce



Notary Bounce



Notary Bounce



Convergence : Firefox



Send Money, Pay Online or Set Up a Merchant Account with PayPal

Send Money, Pay Online or Set ...

+

paypal.com

https://www.paypal.com/

☆

↺

Google

🔍

🔒

+

+

Sign Up

Log In

Help

Security and Protection

Search

English

▼

PayPal

Home

Personal

Business

Developers

Get to Know PayPal

Pay Online

Send Money

Get Paid

Products & Services

Account login

🔒

Email address

PayPal password

Go to

My account

▼

Log In

Problem with login?

New to PayPal? Sign up.

94.4 million

people worldwide using PayPal

Sign Up

Get to Know PayPal

How PayPal Works

Getting Started

WELCOME TO PayPal

The world's most loved way to pay and get paid. [Learn More](#)



Necklace selected.

Privacy protected.

Pay with PayPal

Go for the things you love with confidence.

Pay Online

Shop and pay online quickly and securely.

Send Money

Send money to just about anyone, anywhere.

Get Paid

Accept online payments for items you sell.

Wednesday, September 28, 2011

Send Money, Pay Online or Set Up a Merchant Account with PayPal

Send Money, Pay Online or Set ...

+

paypal.com

https://www.paypal.com/

☆

↺

Google

Q

🔒

+

+

+

[Sign Up](#) | [Log In](#) | [Help](#) | [Security and Protection](#)

Search

English ▾

PayPal

Home | Personal | Business | Developers

Get to Know PayPal | Pay Online | Send Money | Get Paid | Products & Services

Account login 🗝

Email address

PayPal password

Go to

My account ▾

Log In

[Problem with login?](#)

New to PayPal? [Sign up.](#)

94.4 million

people worldwide using PayPal

➕ Sign Up

Get to Know PayPal

[How PayPal Works](#)

[Getting Started](#)

WELCOME TO PayPal

The world's most loved way to pay and get paid. [Learn More](#)



Necklace selected.
Privacy protected.

Pay with PayPal

Go for the things you love
with confidence.

Pay Online

Shop and pay online quickly
and securely.

Send Money

Send money to just about
anyone, anywhere.

Get Paid

Accept online payments
for items you sell.

Send Money, Pay Online or Set Up a Merchant Account with PayPal

Send Money, Pay Online or Set ...

+

paypal.com

https://www.paypal.com/

☆

↺

Google

🔍

🔒

⌵

Sign Up

Log In

Help

Security and Protection

Search

English ⌵

PayPal

Home

Personal

Business

Developers

Get to Know PayPal

Pay Online

Send Money

Get Paid

Products & Services

Account login 🗝

Email address

PayPal password

Go to

My account ⌵

Log In

[Problem with login?](#)

New to PayPal? [Sign up.](#)

94.4 million

people worldwide using PayPal

➕ Sign Up

Get to Know PayPal

[How PayPal Works](#)

[Getting Started](#)

WELCOME TO PayPal

The world's most loved way to pay and get paid. [Learn More](#)



Necklace selected.
Privacy protected.

Pay with PayPal

Go for the things you love
with confidence.

Pay Online

Shop and pay online quickly
and securely.

Send Money

Send money to just about
anyone, anywhere.

Get Paid

Accept online payments
for items you sell.

A red arrow pointing from the top right corner of the browser window towards the address bar area.

A vertical scrollbar on the right side of the browser window, indicating the page content extends beyond the visible area.

Wednesday, September 28, 2011

Wells Fargo - Personal & Business Banking - Student, Auto & Home Loans - Investing & Insurance

Wells Fargo - Personal & Busine...

+

WT wells Fargo - Personal & Busine...

wellsfargo.com https://www.wellsfargo.com/

★ ↻ 🔍 Google

🔒

Verified by: VeriSign Trust Network

Find Locations | Customer Service | En Español

Search

WELLS FARGO

Personal Small Business Commercial About Us

🔒 View Your Accounts

Go to: Account Summary

Username:

Password:

Go

Username / Password Help

Need to set up online access?
Sign Up Now or Take a Tour

Account Services

Free* Mobile Banking at wf.com

Set up Account Alerts

Get Online Statements

More >

Find ATMs/Locations

Enter Zip code or City & State

Go

Fraud Prevention & Online Security

Report Fraud

Visit Our Fraud Information Center

Read Our Online Security Guarantee

Banking

Online Banking [Get Free Access](#)

Bill Pay

Checking [Open In Minutes](#)

Savings & CDs

Credit Cards [Earn Rewards](#)

More >

Loans

Home Mortgage [Free Prequalification](#)

Home Equity [Low Payment Options](#)

Student Loans [Apply Now](#)

Personal Loans

Auto Loans

More >

Investing & Insurance

Retirement [Compare IRAs](#)

Investment Services [Invest Online](#)

The Private Bank

Mutual Funds

Insurance [Protect Your Identity](#)

More >

Open an Account

Checking

Go

Applications

Finish Application or View Status

Check Today's Rates

Mortgage

Go

Notice

ADA Settlement Agreement Notice

Make your money go further

Achieve your financial goals with our free tools and resources

▶ Learn More

Featured CD rates

Buying a house?

Free account access

Checking and much more

Choose a Wells Fargo Checking Package®

Get Started

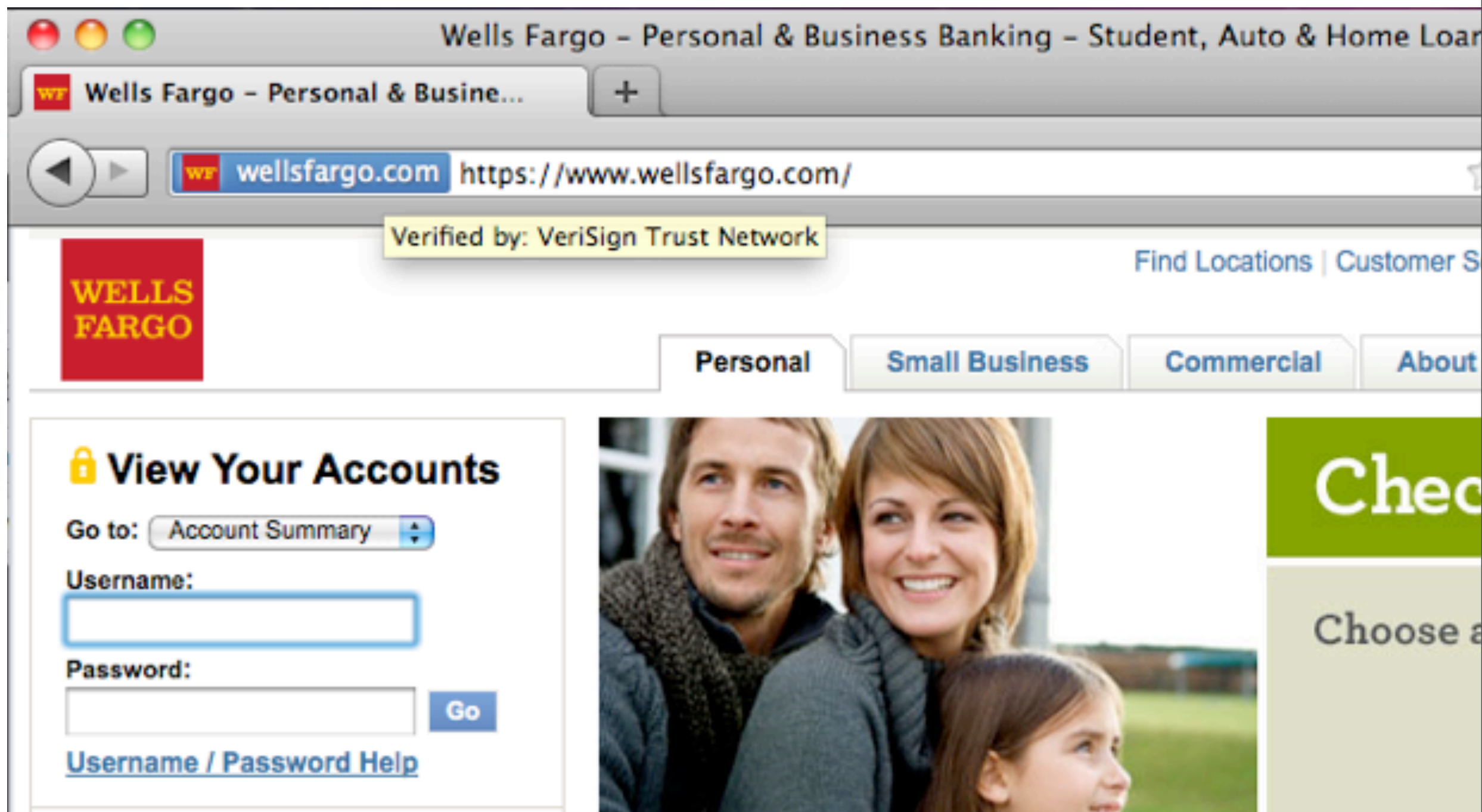


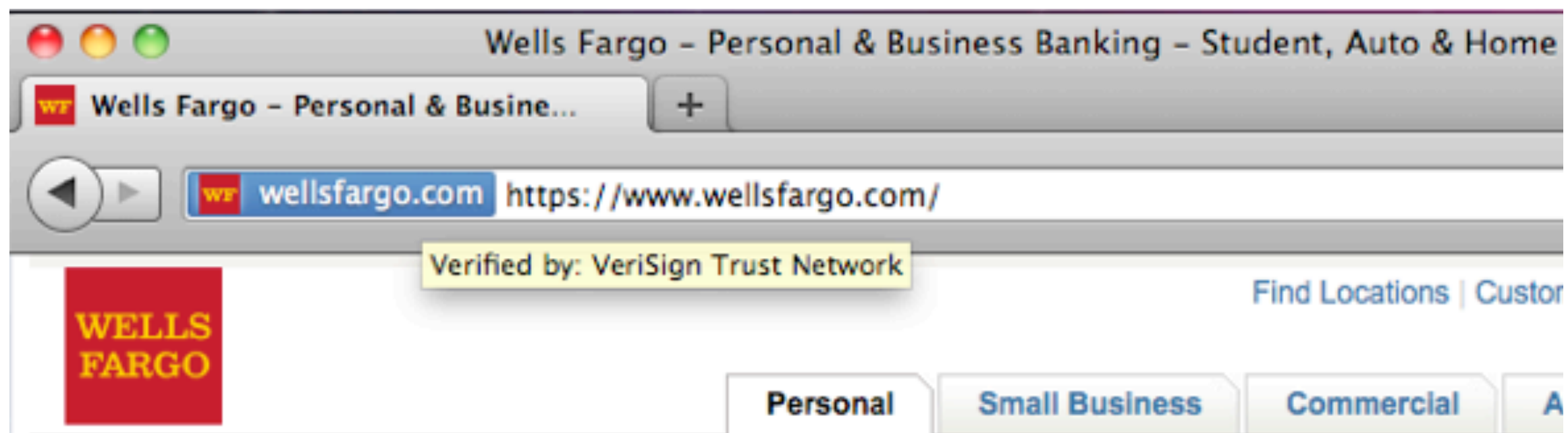
Banking

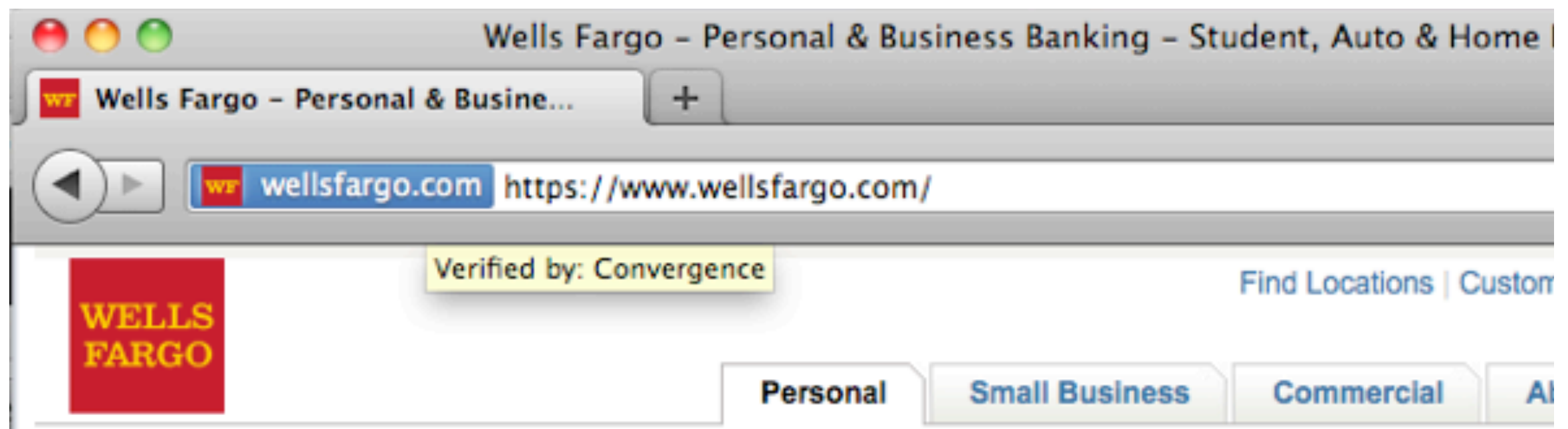
Loans

Investing & Insurance

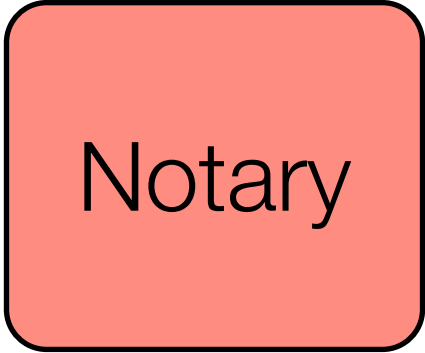
Wednesday, September 28, 2011





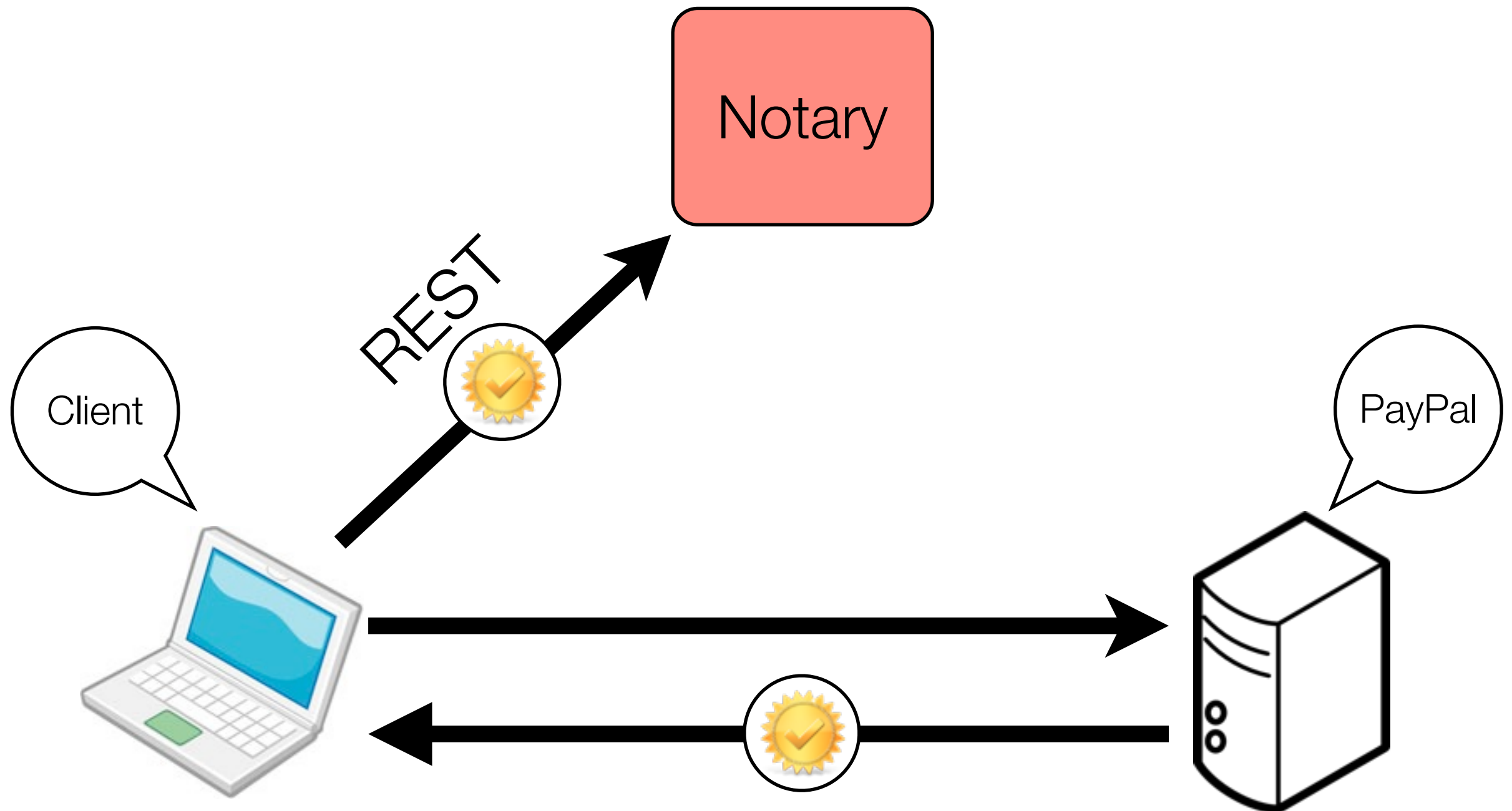


Convergence: Extensible for the future.

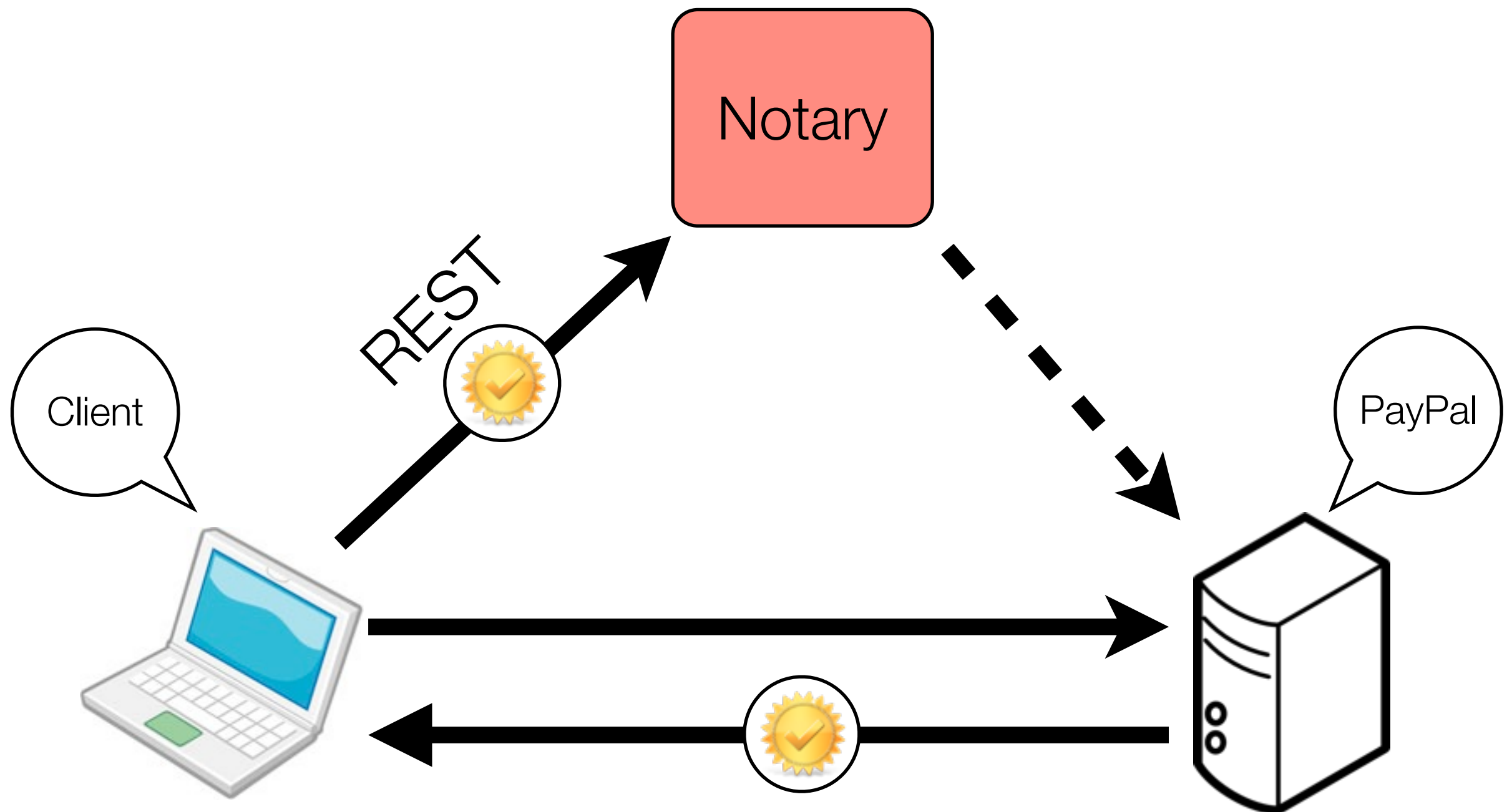


Notary

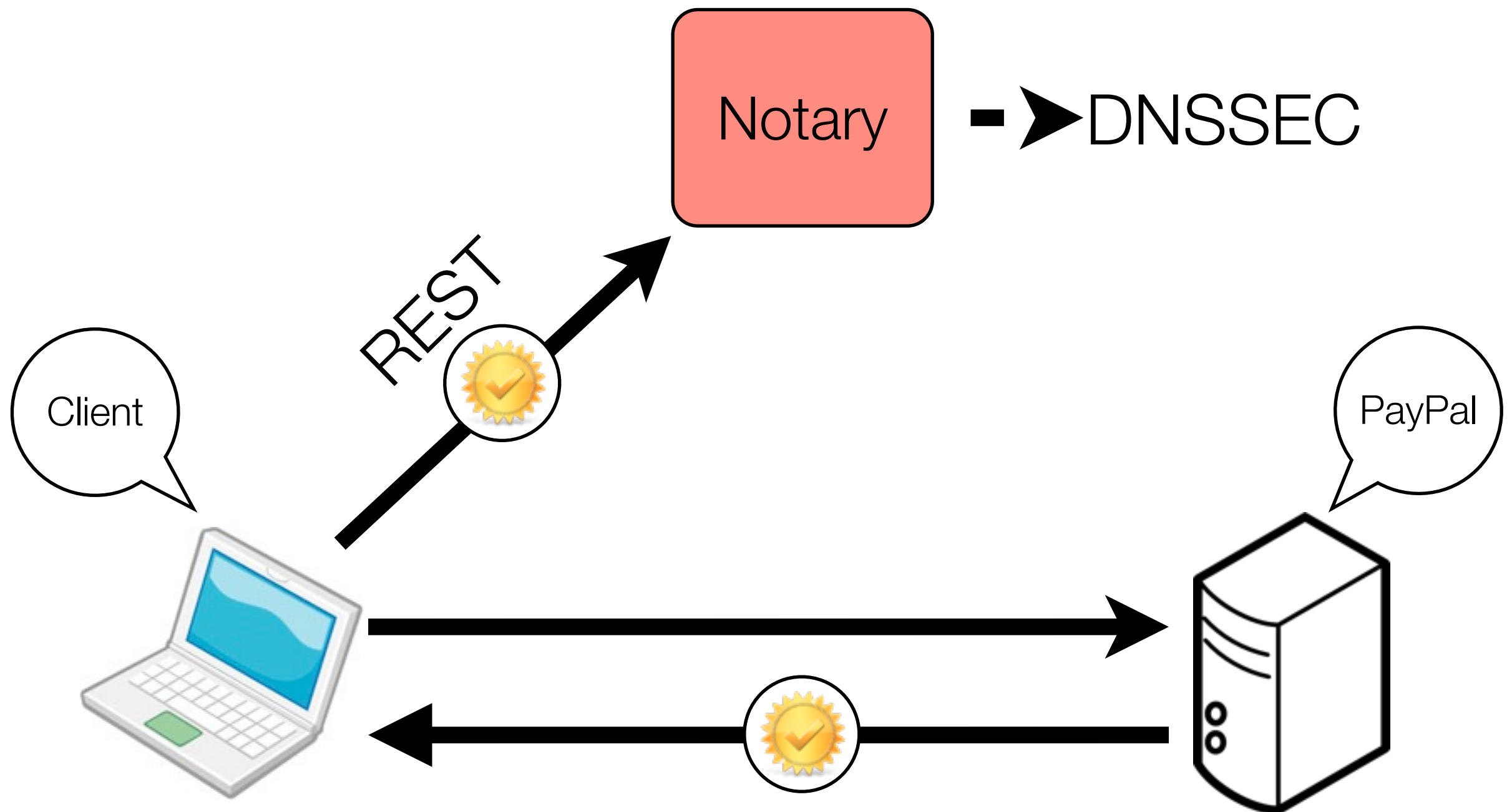
Convergence: Extensible for the future.



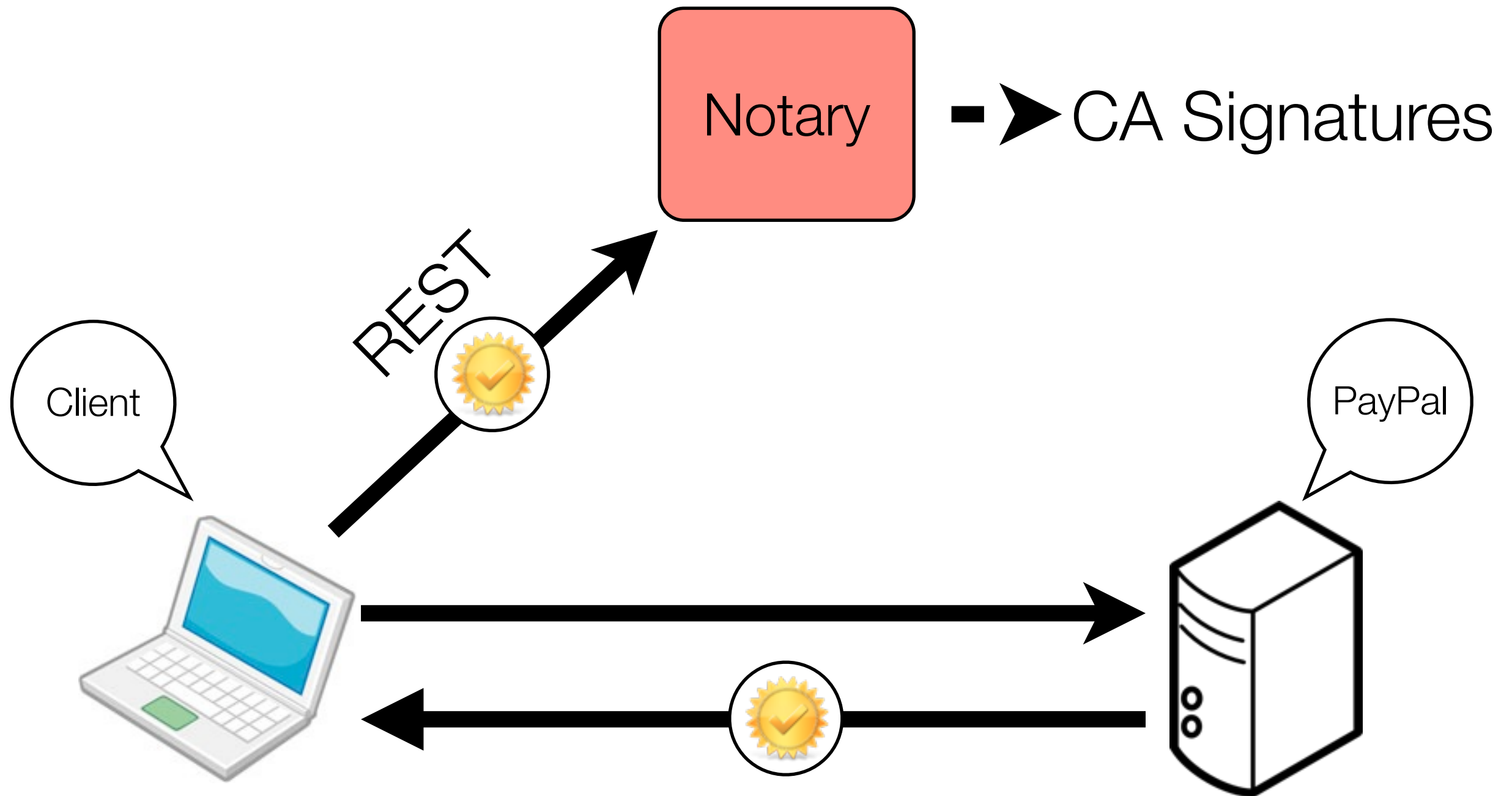
Convergence: Extensible for the future.



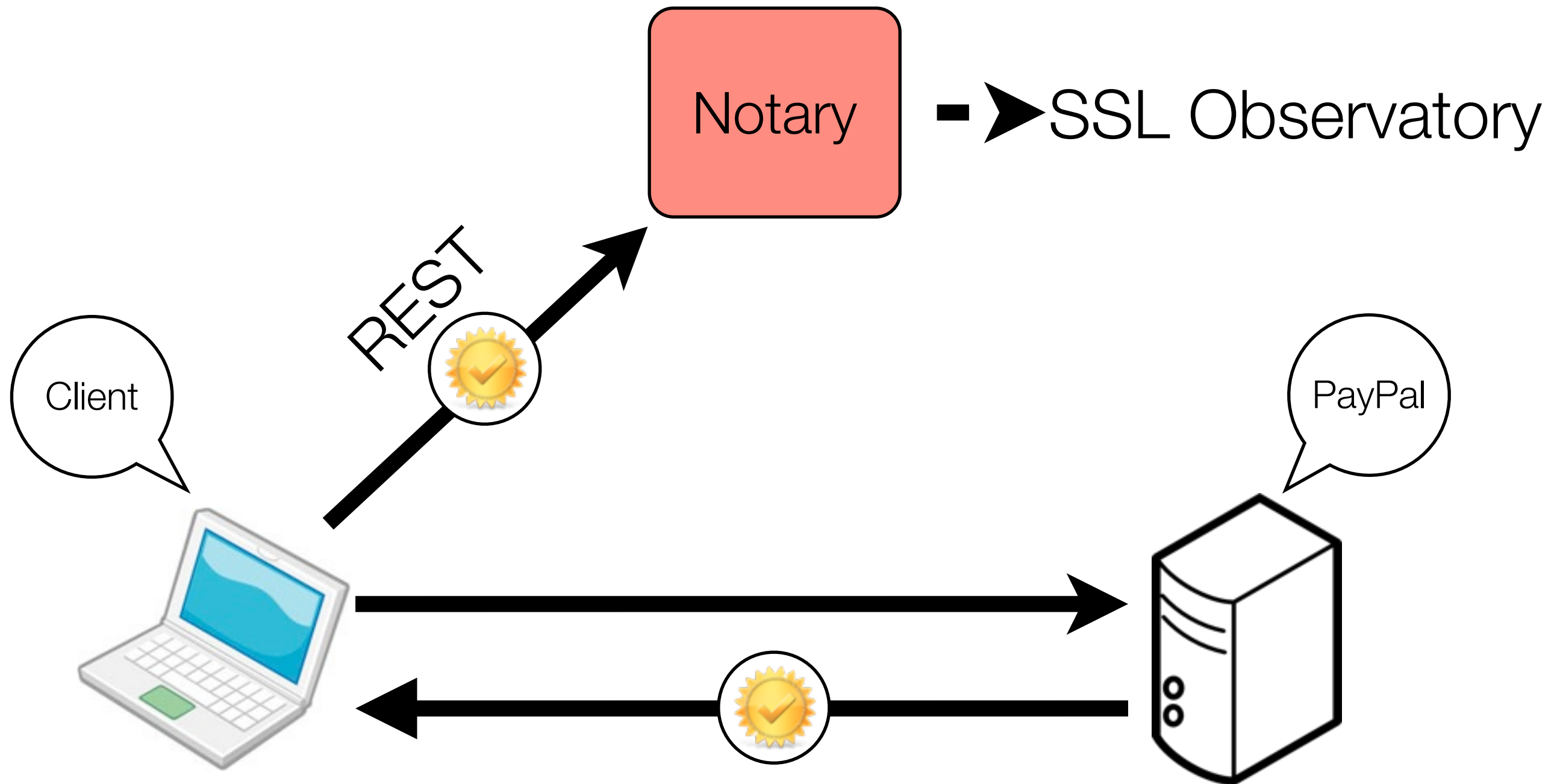
Convergence: Extensible for the future.



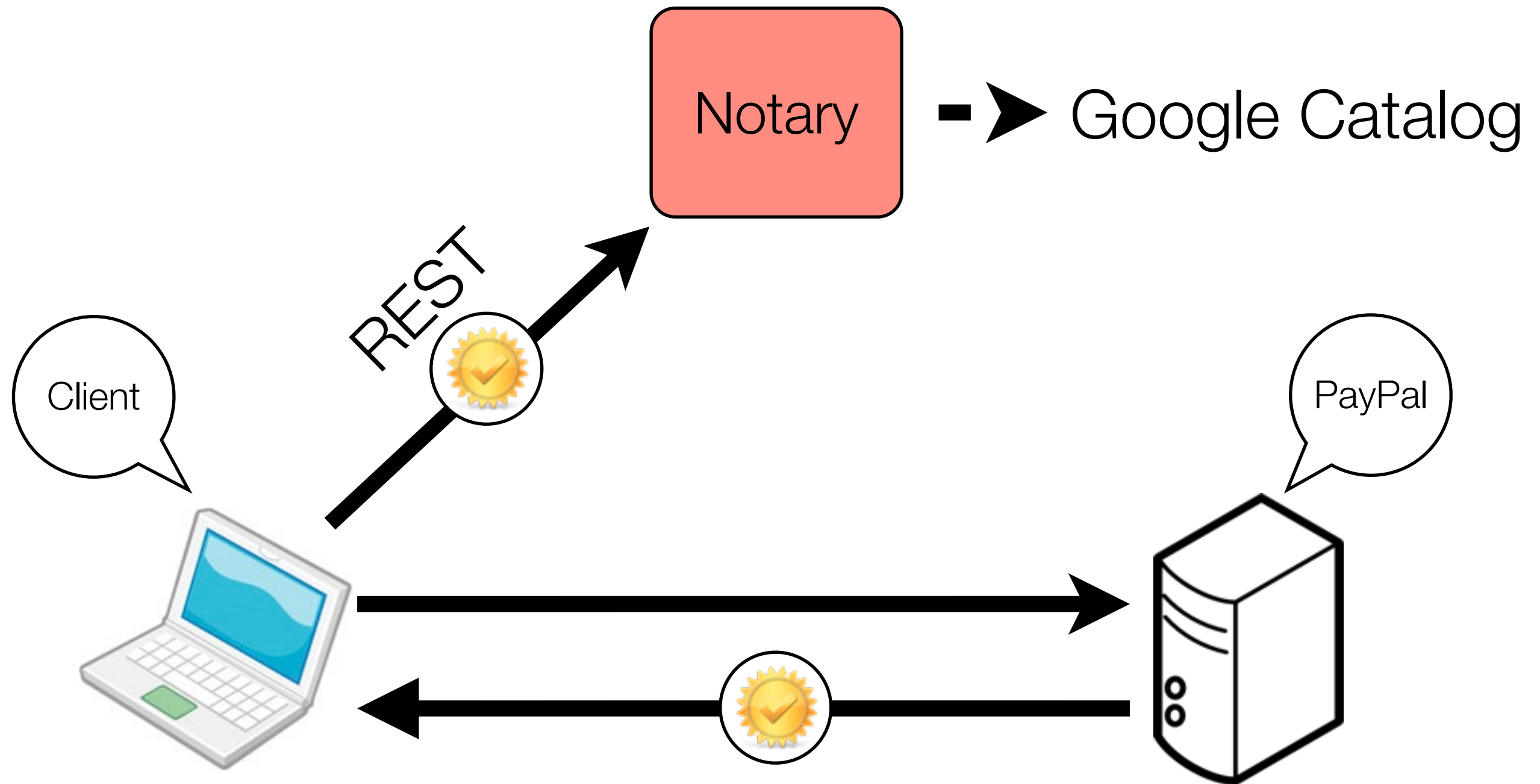
Convergence: Extensible for the future.



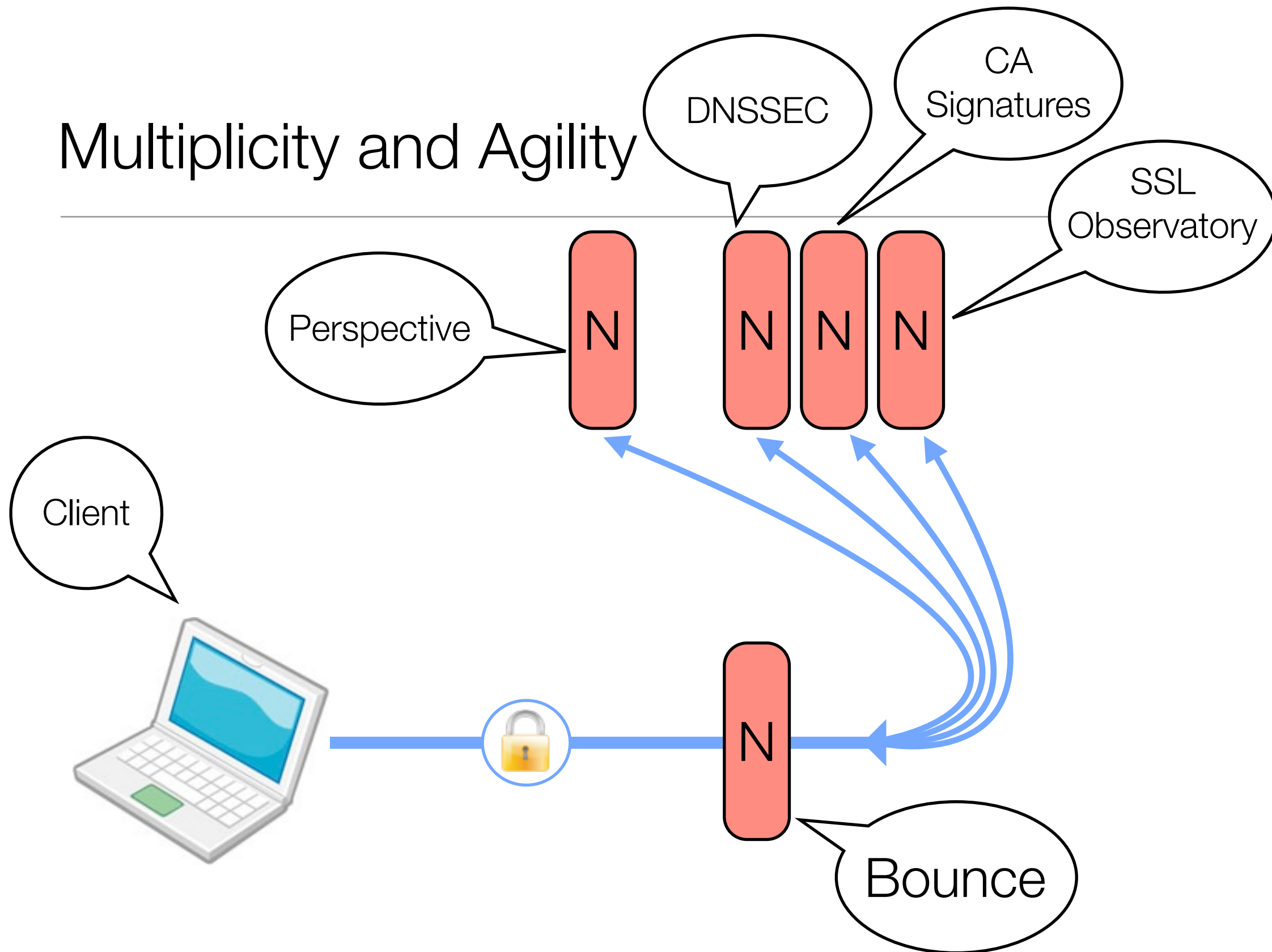
Convergence: Extensible for the future.



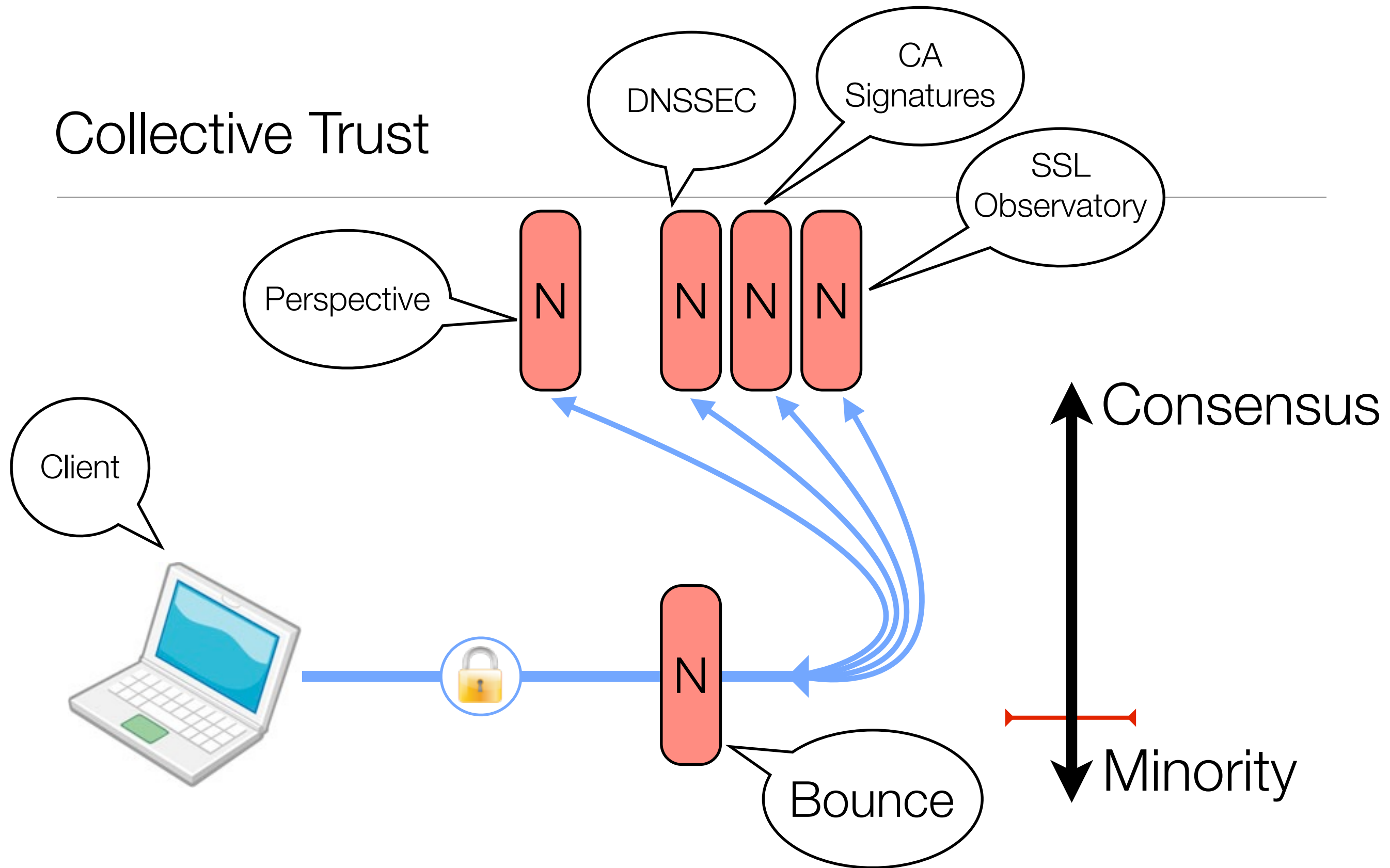
Convergence: Extensible for the future.



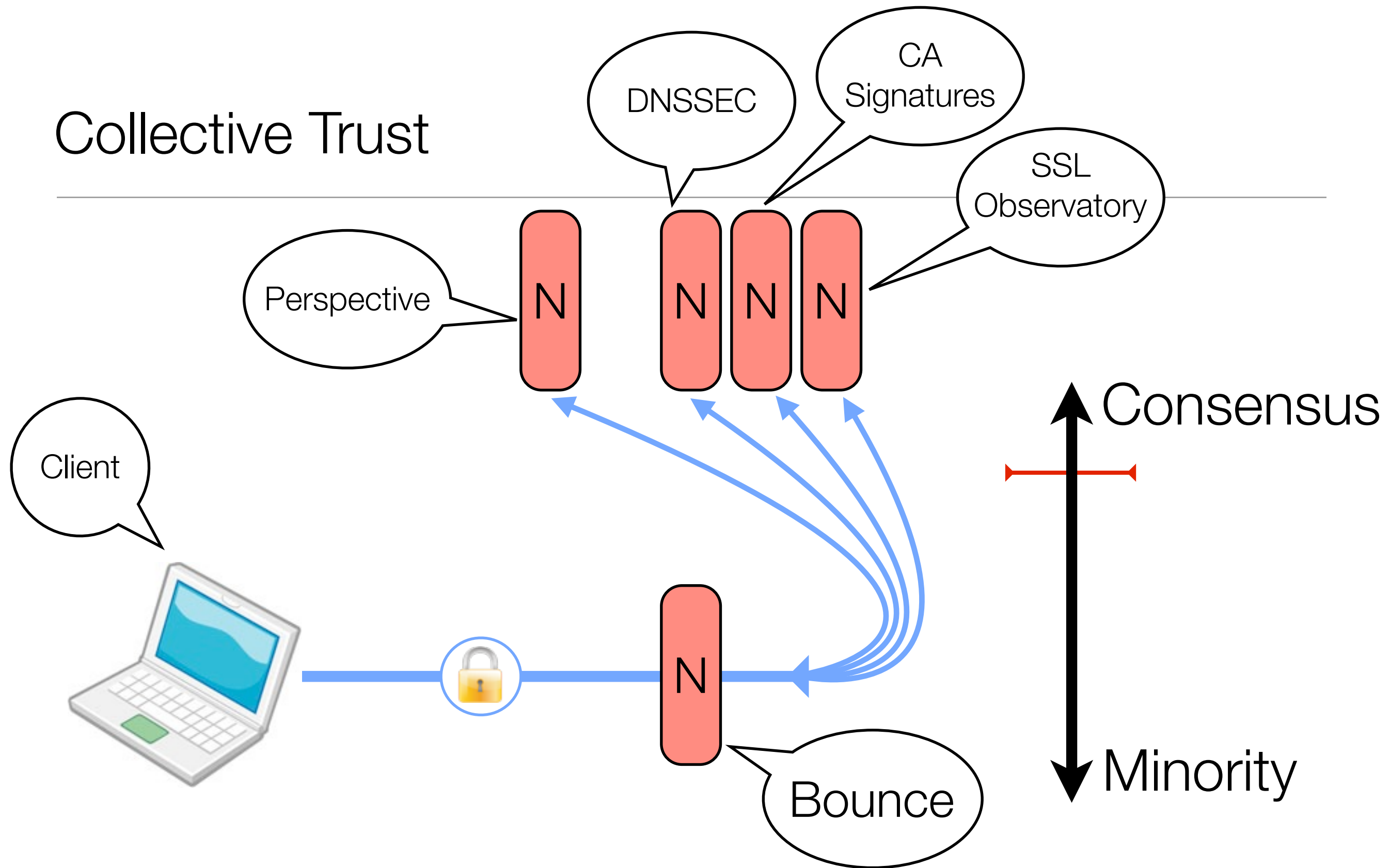
Multiplicity and Agility



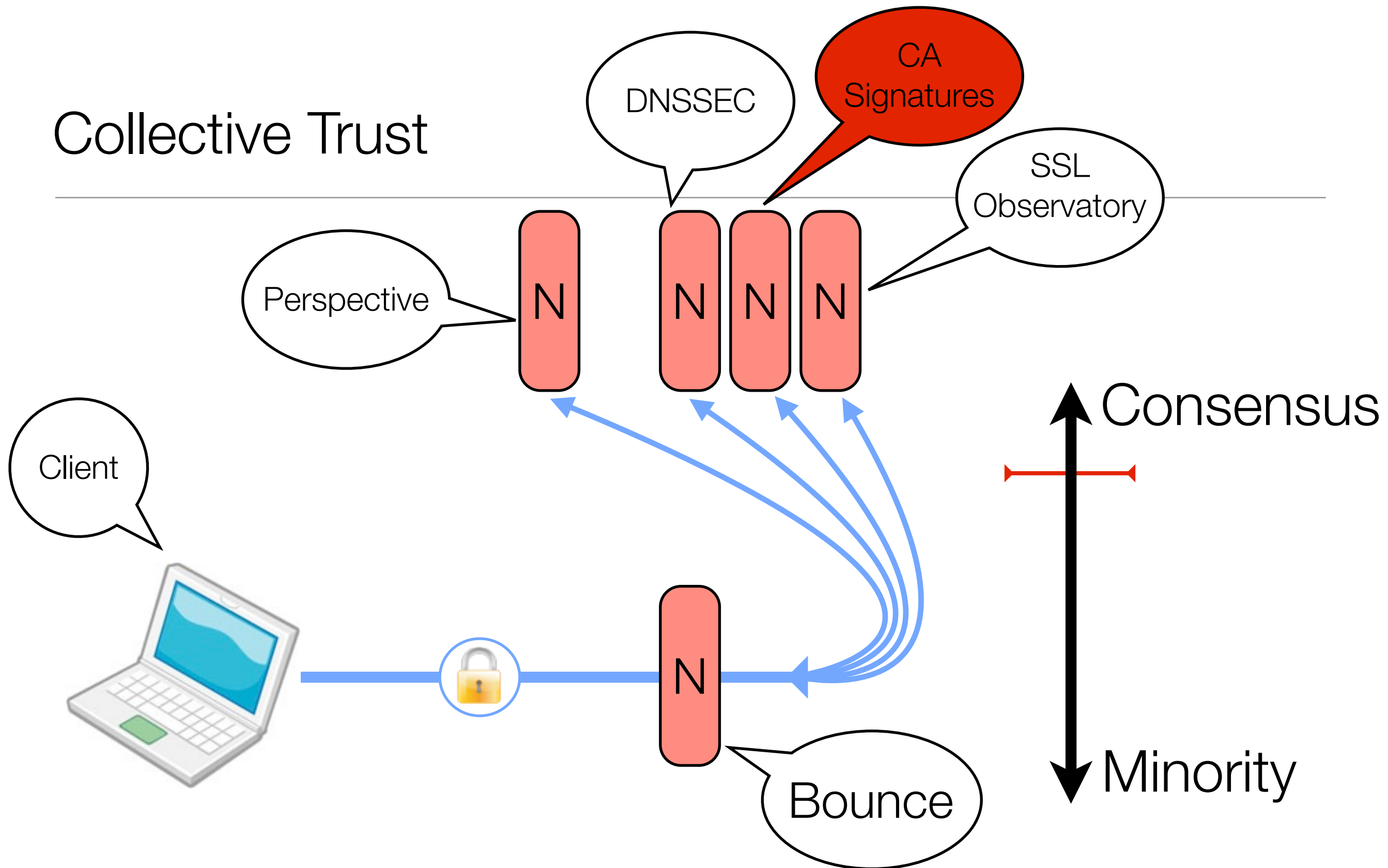
Collective Trust



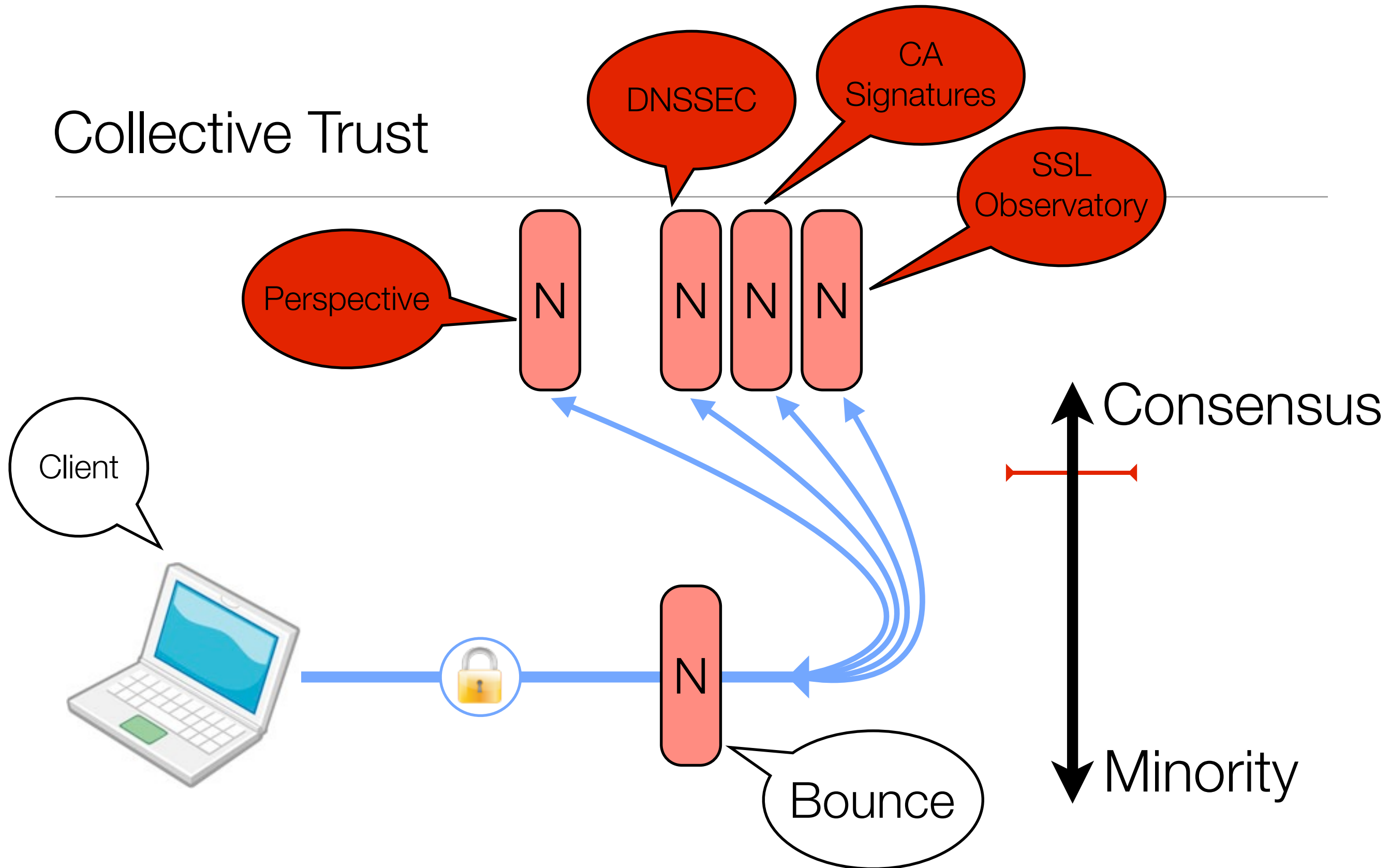
Collective Trust



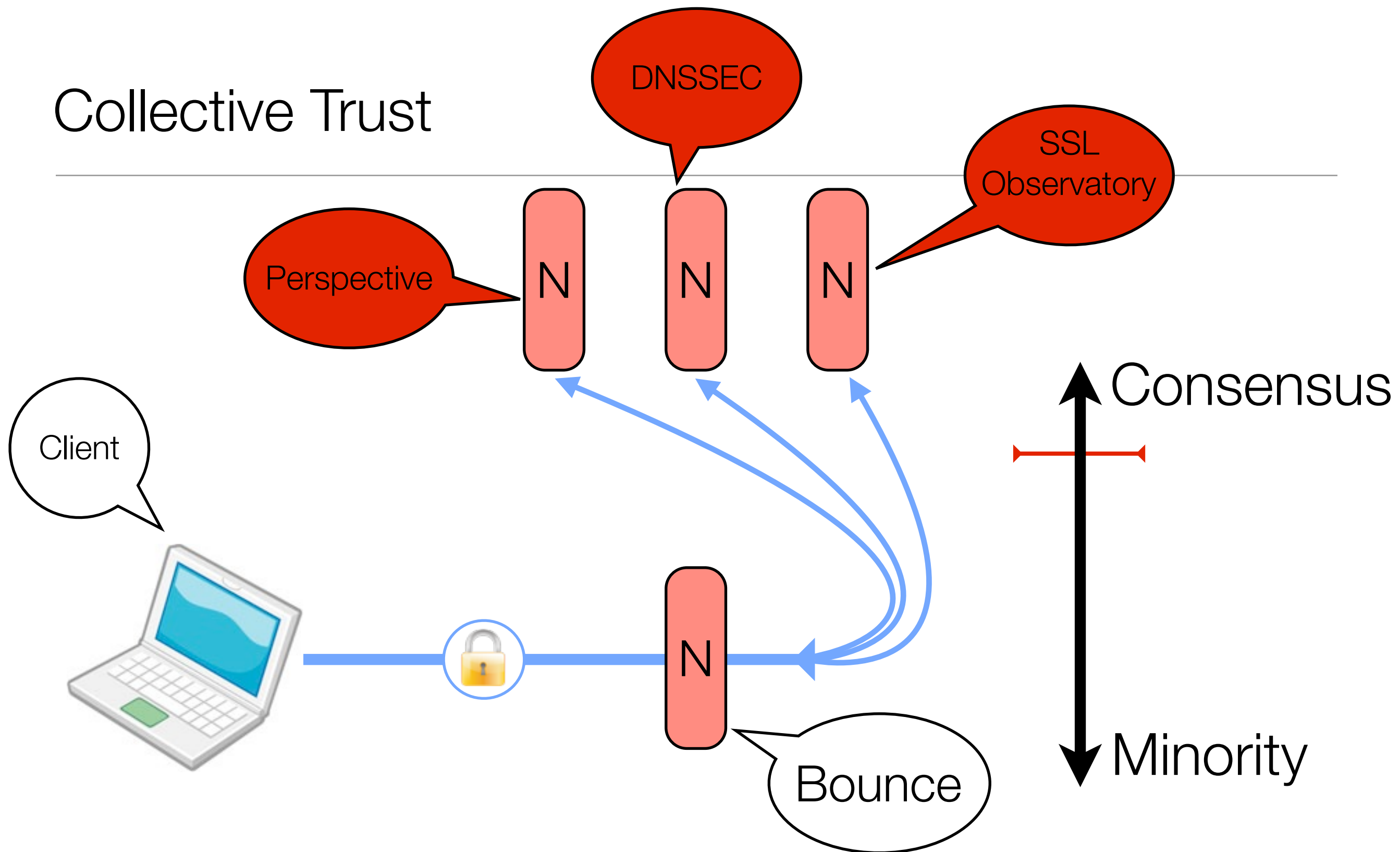
Collective Trust



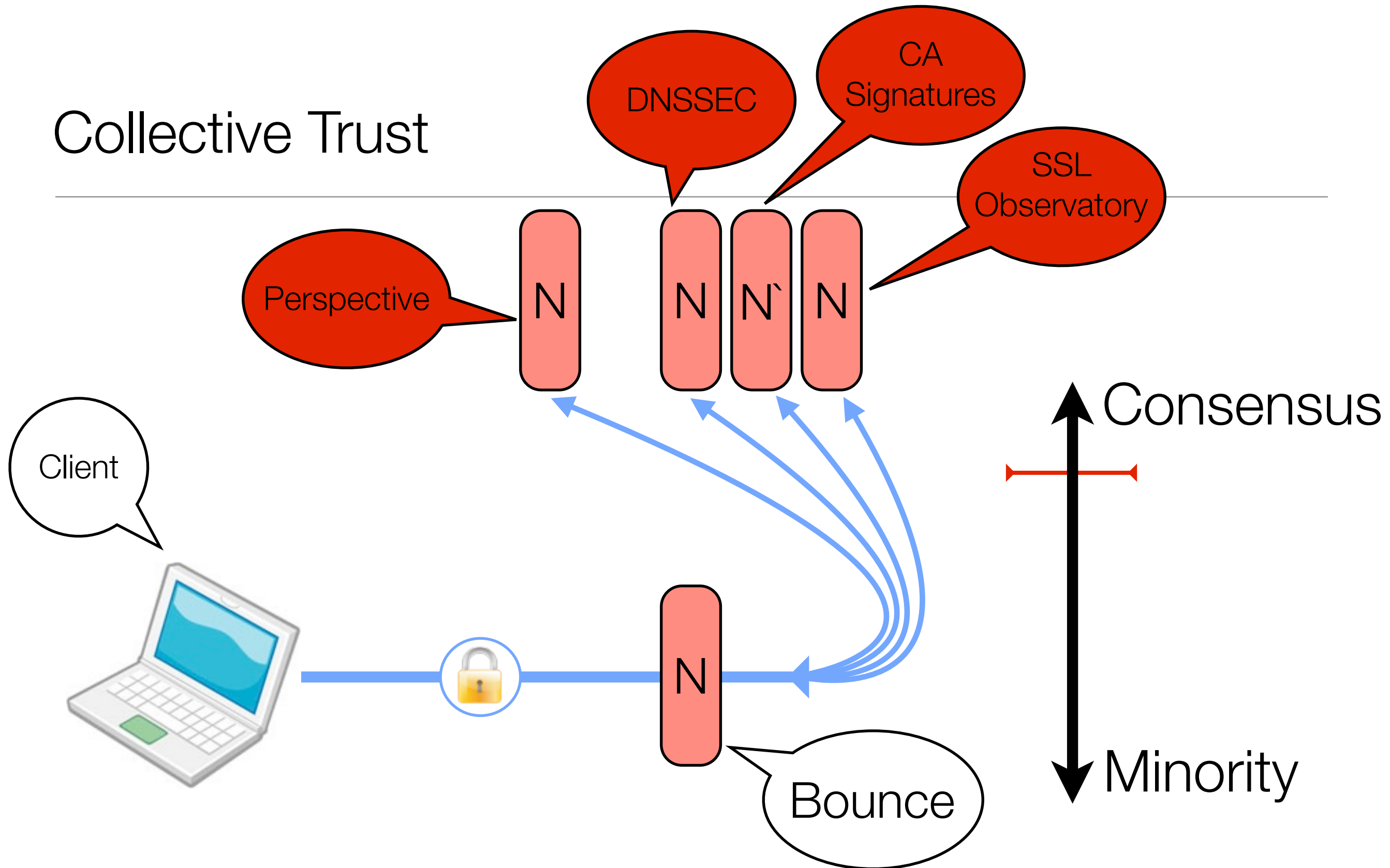
Collective Trust



Collective Trust



Collective Trust



Other Nice Things

Servers Do Nothing

Other Nice Things

!migrate internet

Other Nice Things

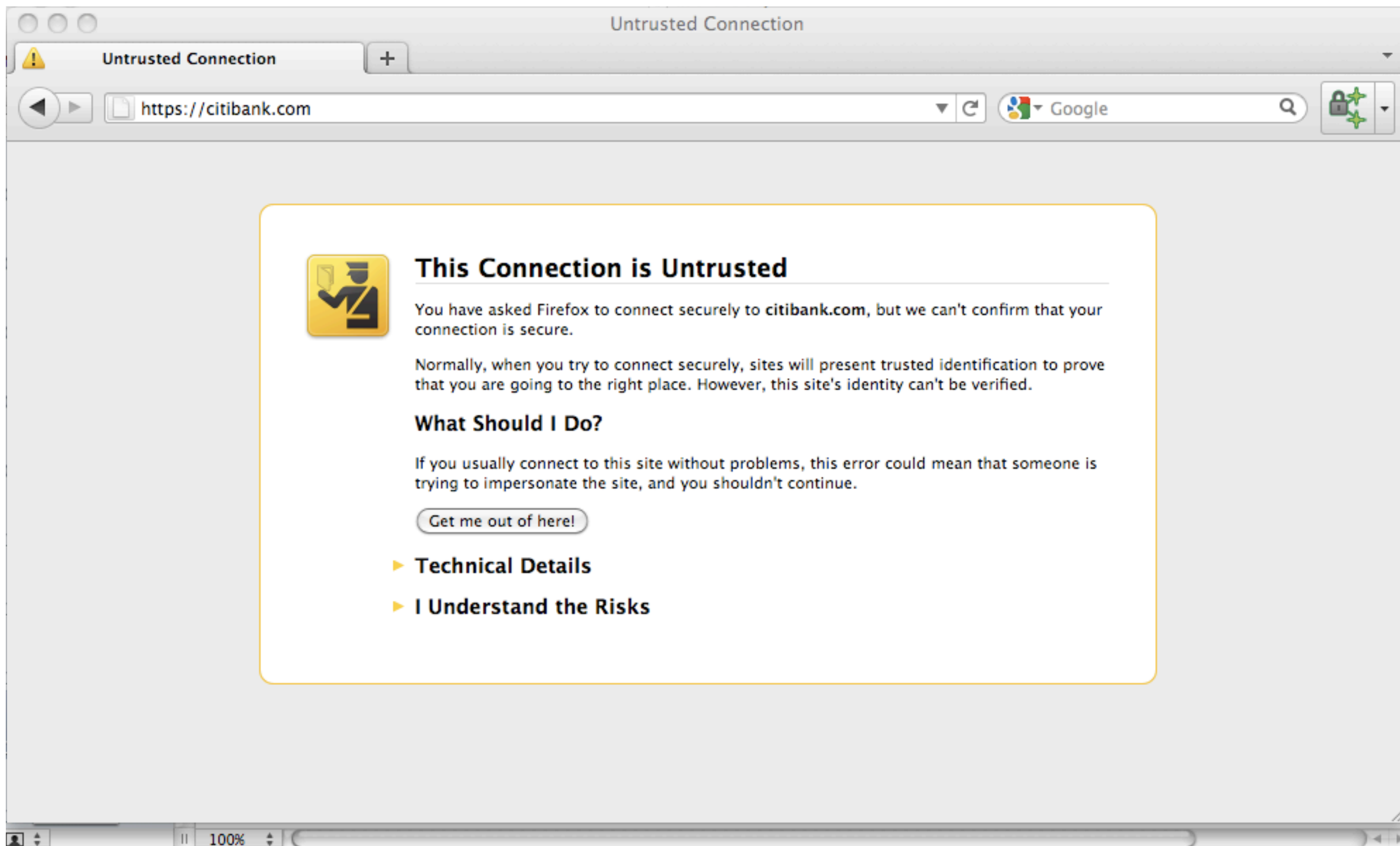
- (1) Implement Convergence in the four major browsers.
- (2) Be done.

Other Nice Things

no more self-signed certificate warnings

problems

“citibank problem”



captive portals

<http://convergence.io>

Leave with this:

Who do I have to trust?

...and for how long?

A prescribed set of people,
forever.