In Root we Trust

Pavan Chander
Lisa Bui

OWASP Toronto: Feb 20, 2019

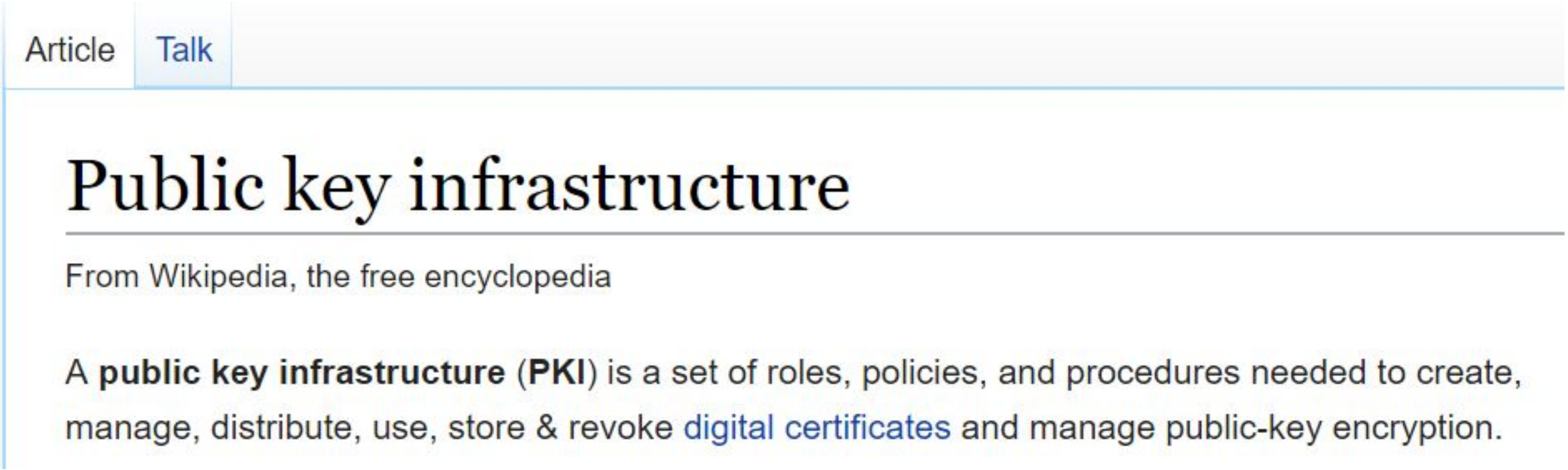
Who are we?

Pavan Chander
pchander@deloitte.ca

Pavan is a Manager with Deloitte’s Cyber Risk Advisory practice and has led WebTrust assurance engagements of both public and enterprise CAs. He has also been an official witness to several root key generation ceremonies both in Canada and internationally.

Lisa Bui
libui@deloitte.ca

Lisa is a consultant in Deloitte’s Risk Advisory practice. Her specialties include trust considerations of Public Key Infrastructure, Cyber Security, Enterprise Risk, and Third Party Service Auditor Reporting.

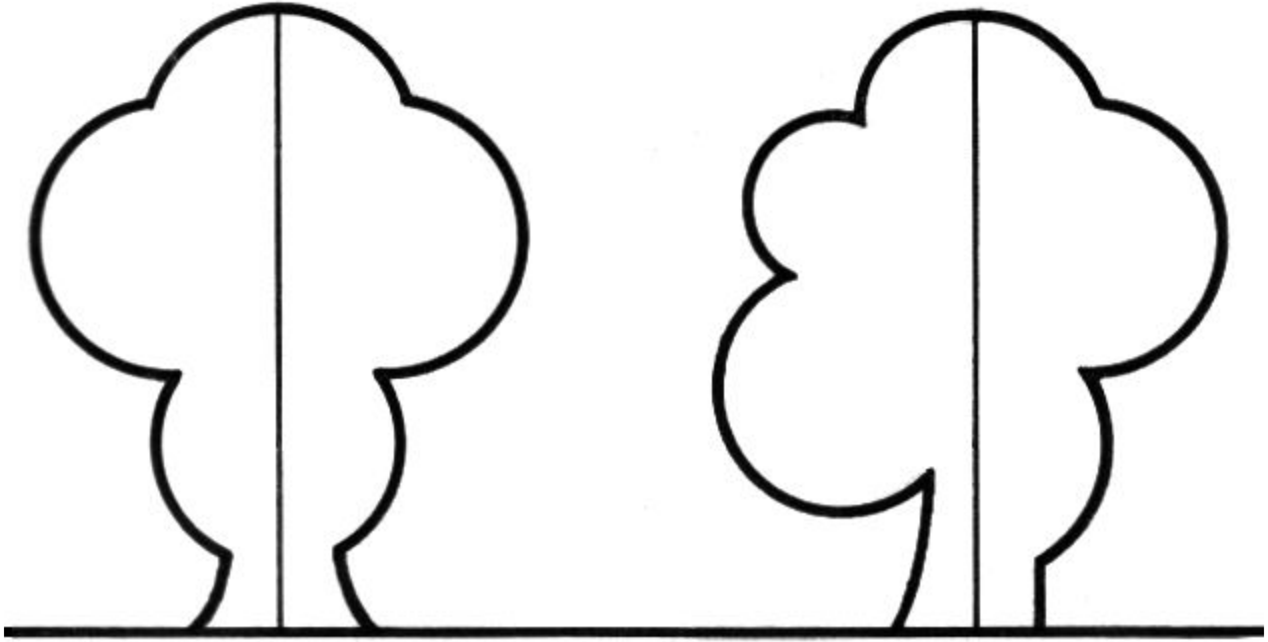


Public key infrastructure

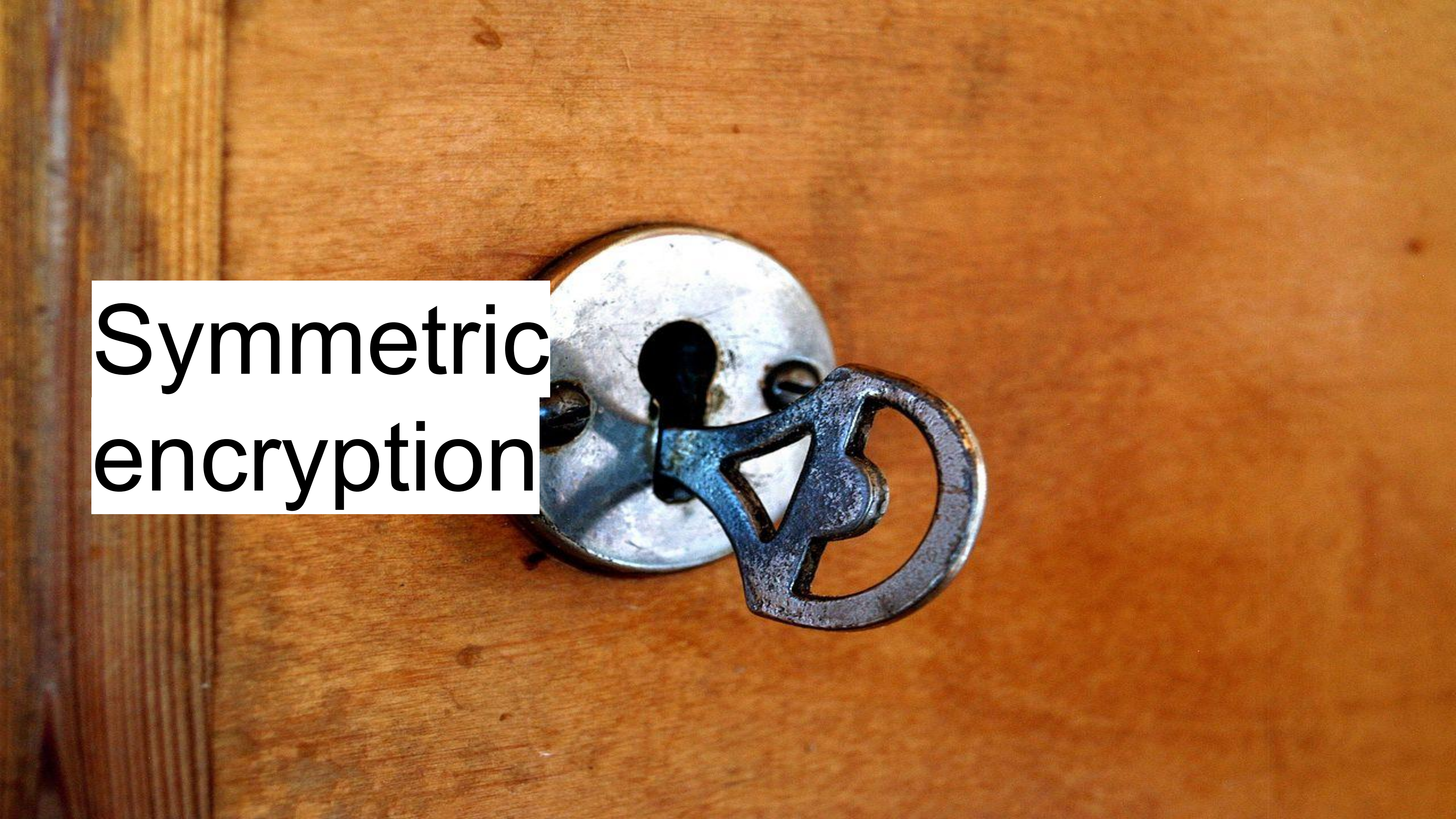
From Wikipedia, the free encyclopedia

A **public key infrastructure** (**PKI**) is a set of roles, policies, and procedures needed to create, manage, distribute, use, store & revoke digital certificates and manage public-key encryption.

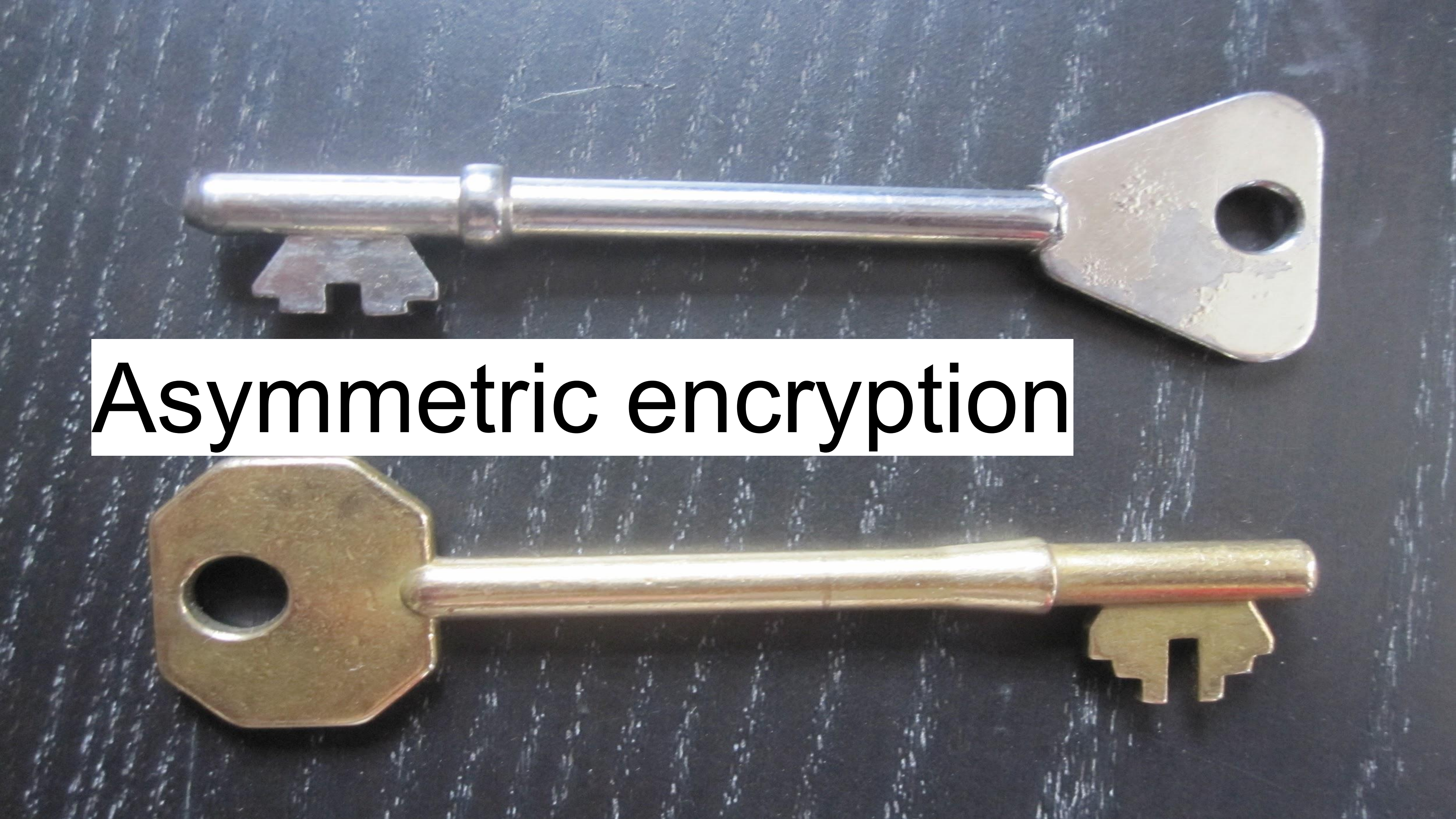
Let’s talk about encryption



SYMMETRIC
ASYMMETRIC

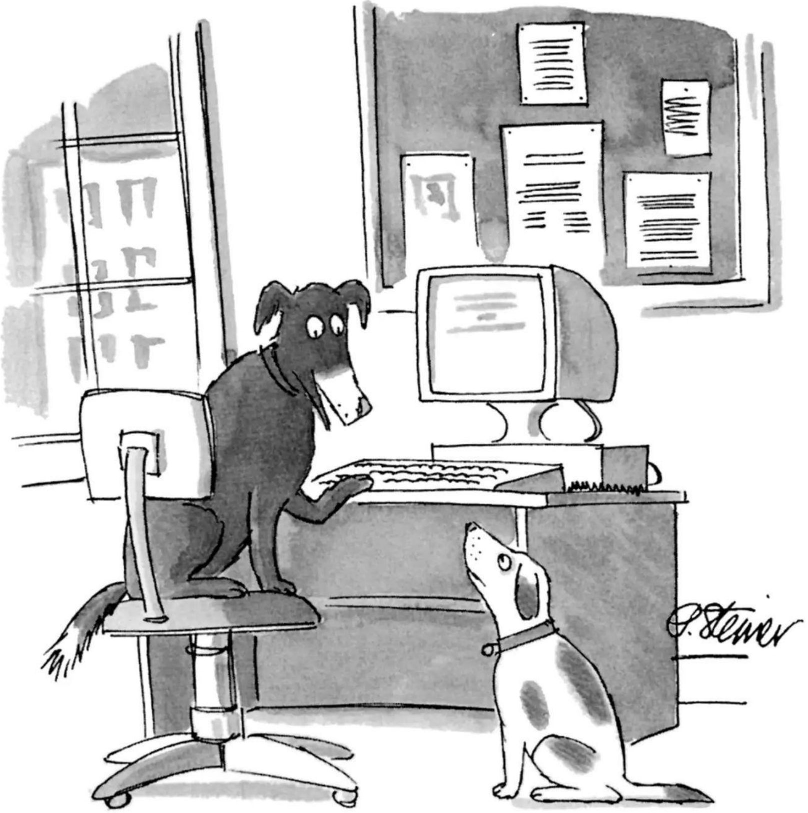


Symmetric encryption



Asymmetric encryption

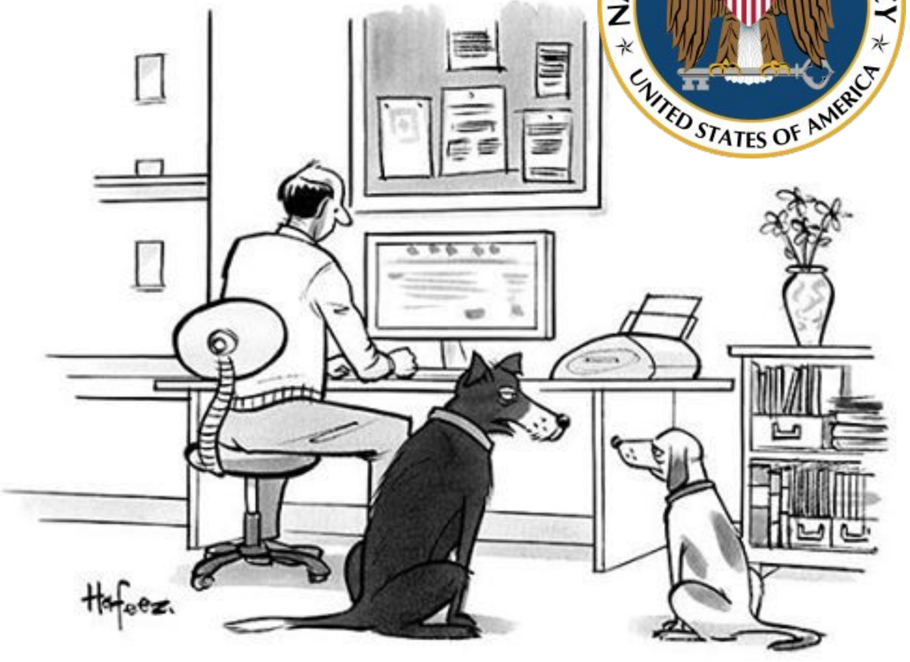
NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA



"On the Internet, nobody knows you're a dog."

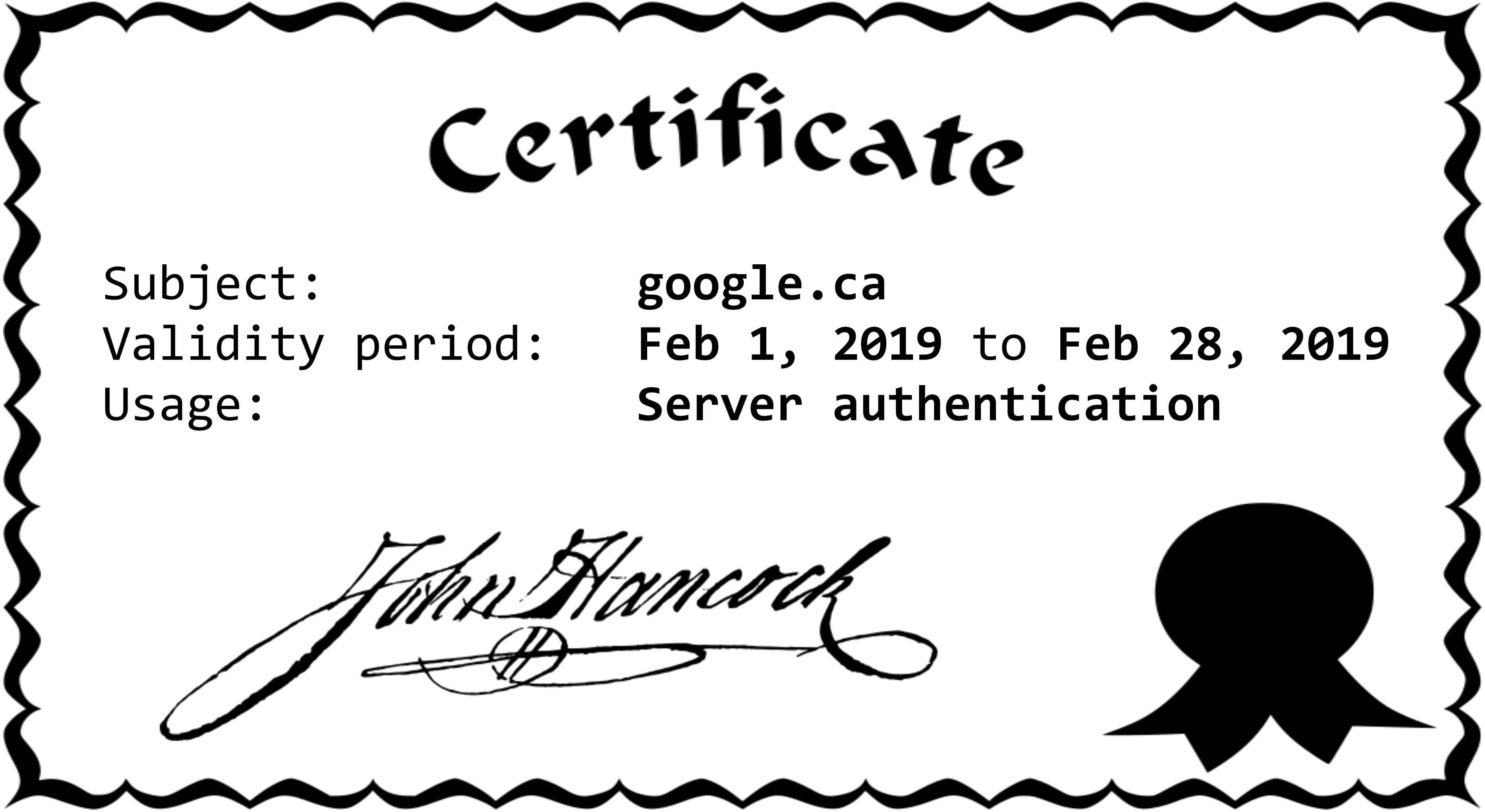
©The New Yorker Collection 1993 Peter Steiner
From cartoonbank.com. All rights reserved.

1993



"Remember when, on the Internet, nobody knew who you were?"

2019



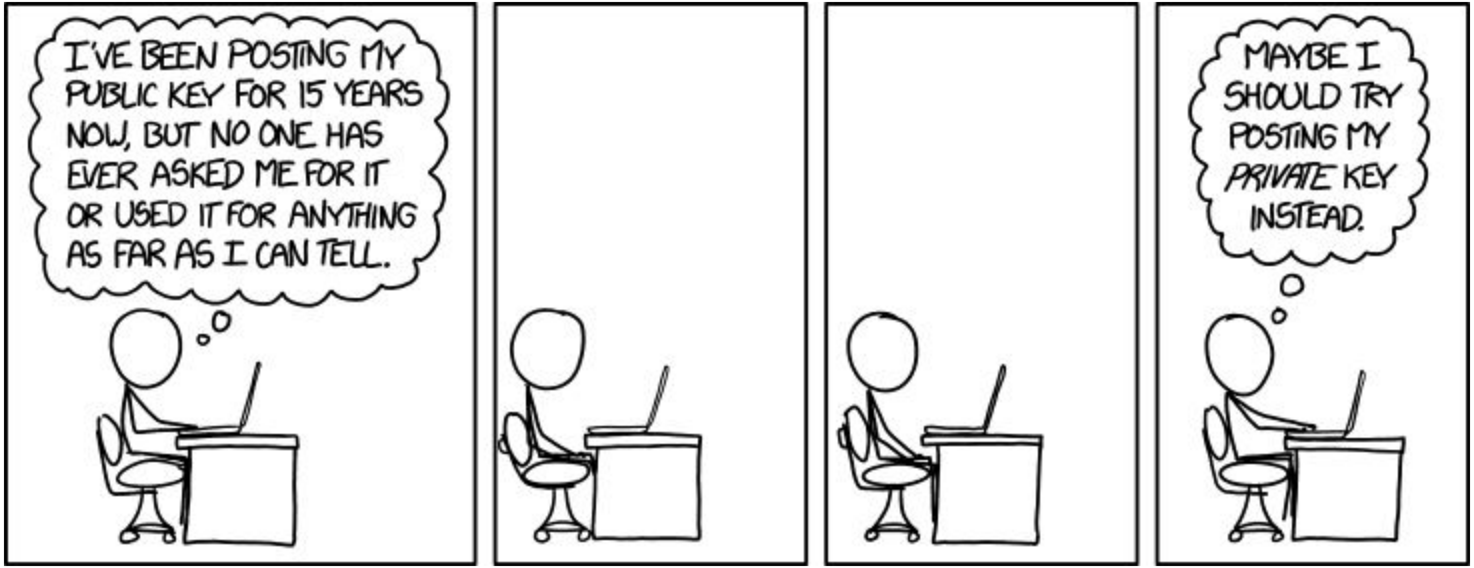
Certificate

Subject: **google.ca**

Validity period: **Feb 1, 2019** to **Feb 28, 2019**

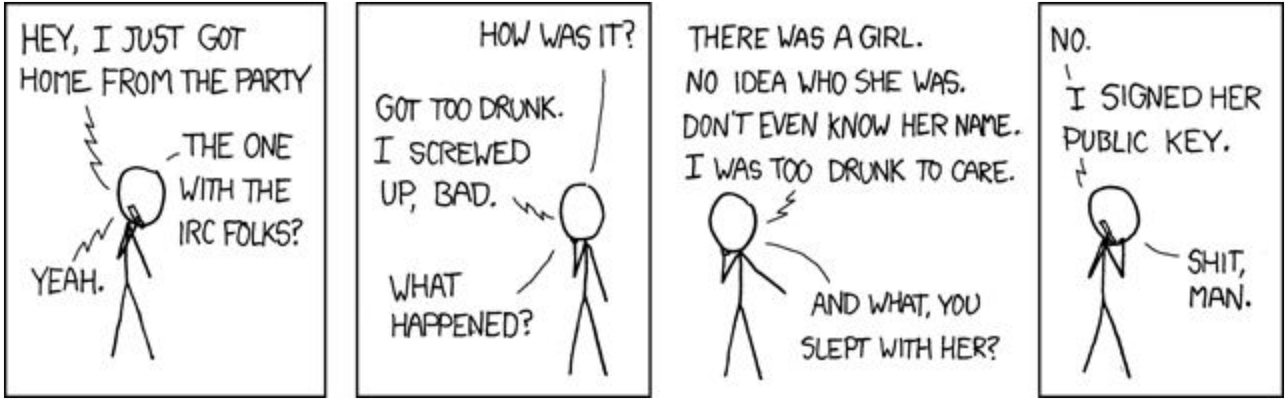
Usage: **Server authentication**

John Hancock


I'VE BEEN POSTING MY PUBLIC KEY FOR 15 YEARS NOW, BUT NO ONE HAS EVER ASKED ME FOR IT OR USED IT FOR ANYTHING AS FAR AS I CAN TELL.
MAYBE I SHOULD TRY POSTING MY *PRIVATE* KEY INSTEAD.

Certification Authorities

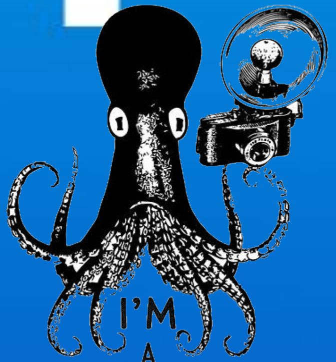
Amazon, Comodo, DigiCert, Entrust, GoDaddy, Google, ~~Symantec~~, VeriSign, and many more...


HEY, I JUST GOT HOME FROM THE PARTY
THE ONE WITH THE IRC FOLKS?
YEAH.
HOW WAS IT?
GOT TOO DRUNK. I SCREWED UP, BAD.
WHAT HAPPENED?
THERE WAS A GIRL. NO IDEA WHO SHE WAS. DON'T EVEN KNOW HER NAME. I WAS TOO DRUNK TO CARE.
AND WHAT, YOU SLEPT WITH HER?
NO.
I SIGNED HER PUBLIC KEY.
SHIT, MAN.

How to Become a NOTARY

A Simple, 5-Step Plan

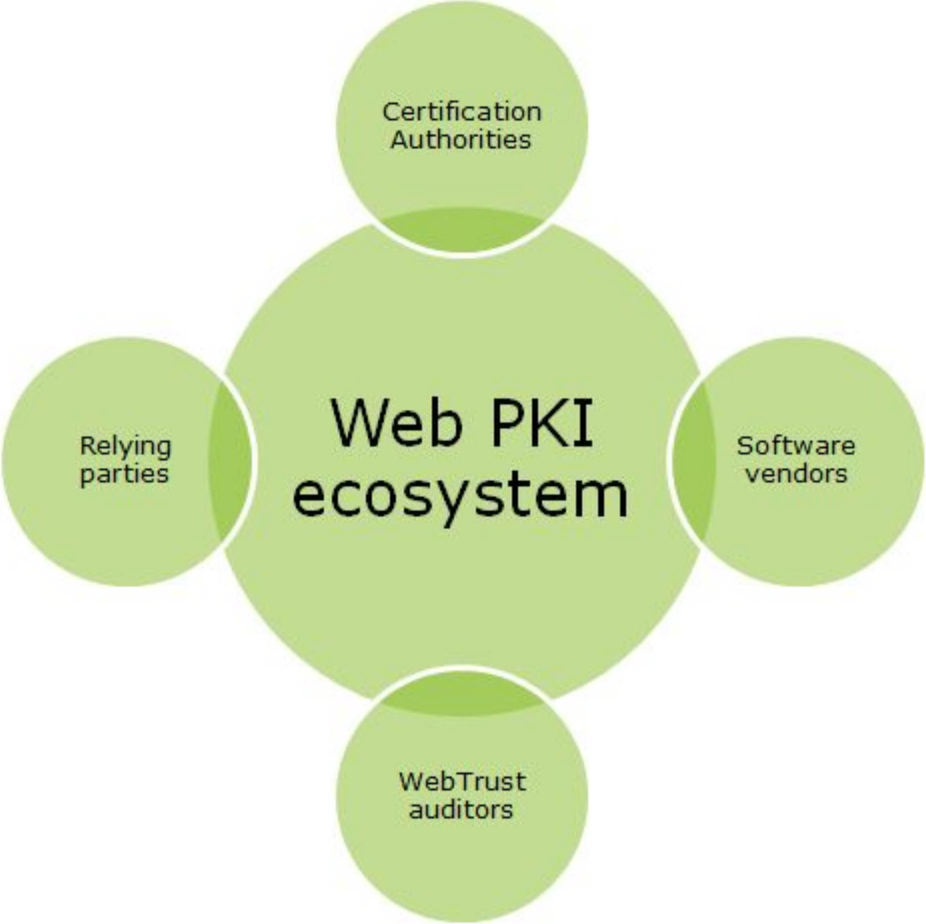
TRUST ME



I'M A ~~PHOTOGRAPHER~~

CERTIFICATION AUTHORITY

Deloitte.
pwc
KPMG
EY
Grant Thornton
BDO



Industry: CA/Browser Forum

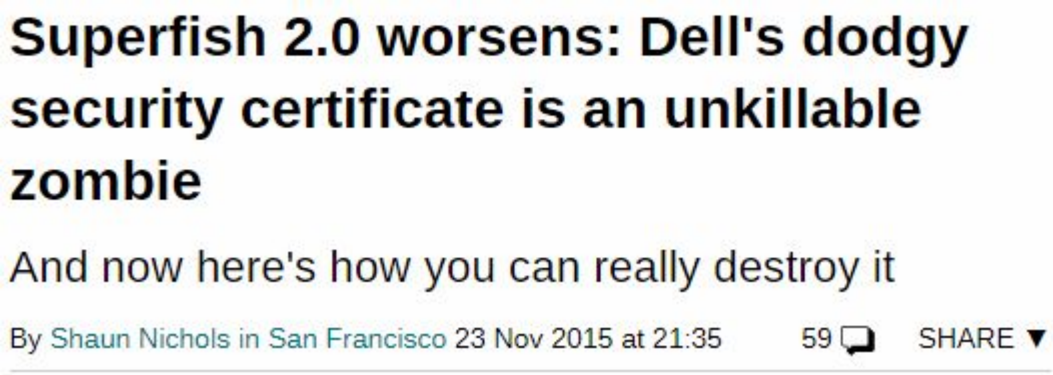
- Certification Authorities
- Browser/OS vendors
  (e.g. Apple, Google, Microsoft, Mozilla)

Auditors: CPA Canada WebTrust/PKI Assurance Taskforce

- CPA Canada members
- Audit firms

Other things...

- Publicly trusted vs Enterprise
- Other use cases
  - Client authentication: **VPN**
  - Code signing: **Airplanes, Windows Updates**
  - Email
  - V2X

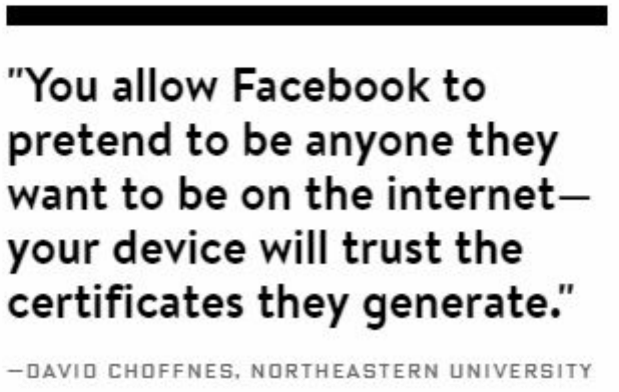


Superfish 2.0 worsens: Dell's dodgy security certificate is an unkillable zombie

And now here's how you can really destroy it

By Shaun Nichols in San Francisco 23 Nov 2015 at 21:35

facebook
research



"You allow Facebook to pretend to be anyone they want to be on the internet—your device will trust the certificates they generate."

—DAVID CHOFFNES, NORTHEASTERN UNIVERSITY

Microsoft trust store

Governments of…

- Australia
- Brazil
- Finland
- France
- Hong Kong
- Hungary
- India
- Japan
- Korea
- Lithuania
- Macao
- Portugal
- Saudi Arabia
- Slovenia
- South Africa
- Spain
- Sweden
- Taiwan
- The Netherlands
- Tunisia
- Turkey
- Uruguay

...plus many private sector companies from around the world

Takeaways...

- https://cabforum.org/
- http://www.webtrust.org/
- https://wiki.mozilla.org/CA
- https://groups.google.com/forum/#!forum/mozilla.dev.security.policy
- https://crt.sh/?cablint=1+week

KEEP
CALM
AND
SING
KUMBAYA