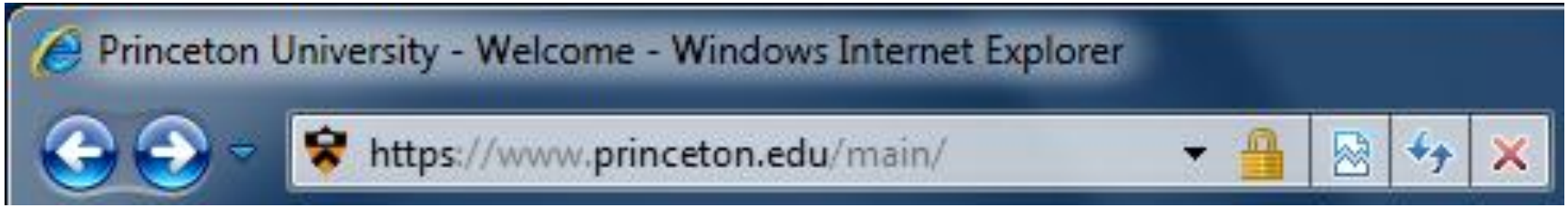
Online Trust and Digital Certificates: Tech Tutorial

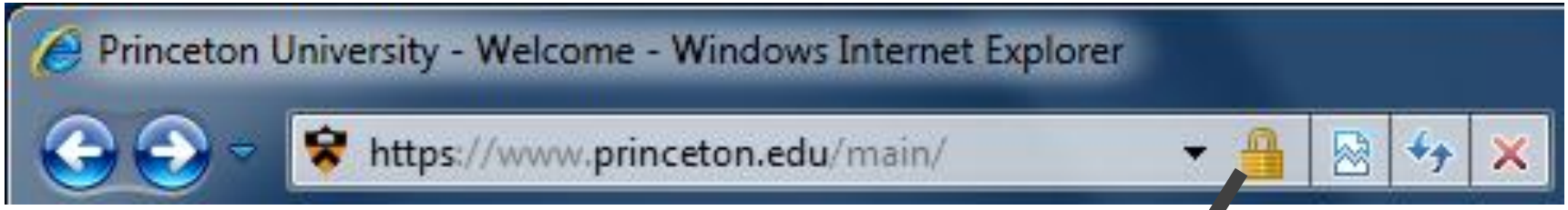
Edward W. Felten
Professor of Computer Science and Public Affairs
Princeton University


Princeton University - Welcome - Windows Internet Explorer
https://www.princeton.edu/main/


Princeton University - Welcome - Windows Internet Explorer
https://www.princeton.edu/main/


Send Money, Pay Online or Set Up a Merchant Account with PayPal - Windows Internet Explore
https://www.paypal.com/
PayPal, Inc. [US]


Princeton University - Welcome - Windows Internet Explorer
https://www.princeton.edu/main/



Secure connection means:

1. Protected channel to some server
2. Authentication of the server's identity

$$\forall\ 0 < x < pq: x^{(p-1)(q-1)} \bmod pq = 1$$

online identity: distinctive but anonymous

online identity: distinctive but anonymous

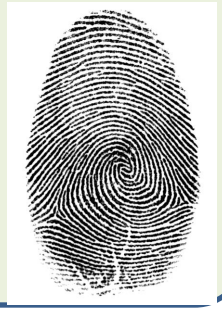
like a fingerprint

digital signature

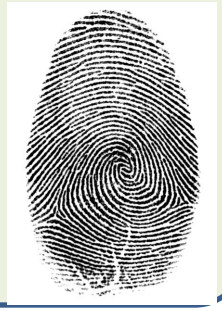
stamp document with your fingerprint

digital signature

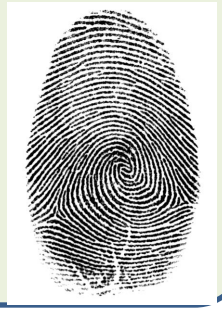
stamp document with your fingerprint



https://www.princeton.edu

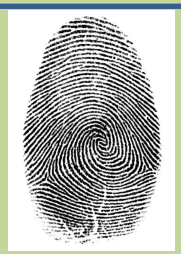


https://www.princeton.edu



Whose fingerprint is that?

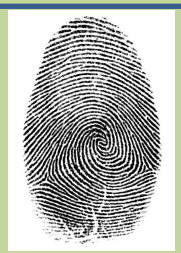
princeton.edu’s fingerprint:



Signed,

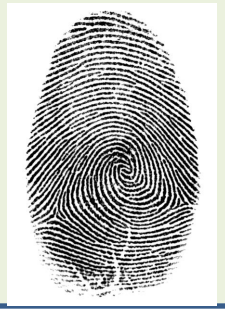
certificate (“cert”)

princeton.edu’s fingerprint:



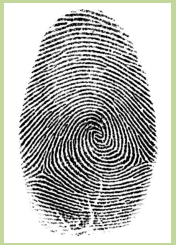
Signed,

https://www.princeton.edu



+

princeton.edu's fingerprint:



Signed,

Certificate Authority (“CA”)

Certificate Authority (“CA”)

issues / signs certificates

Certificate Authority (“CA”)

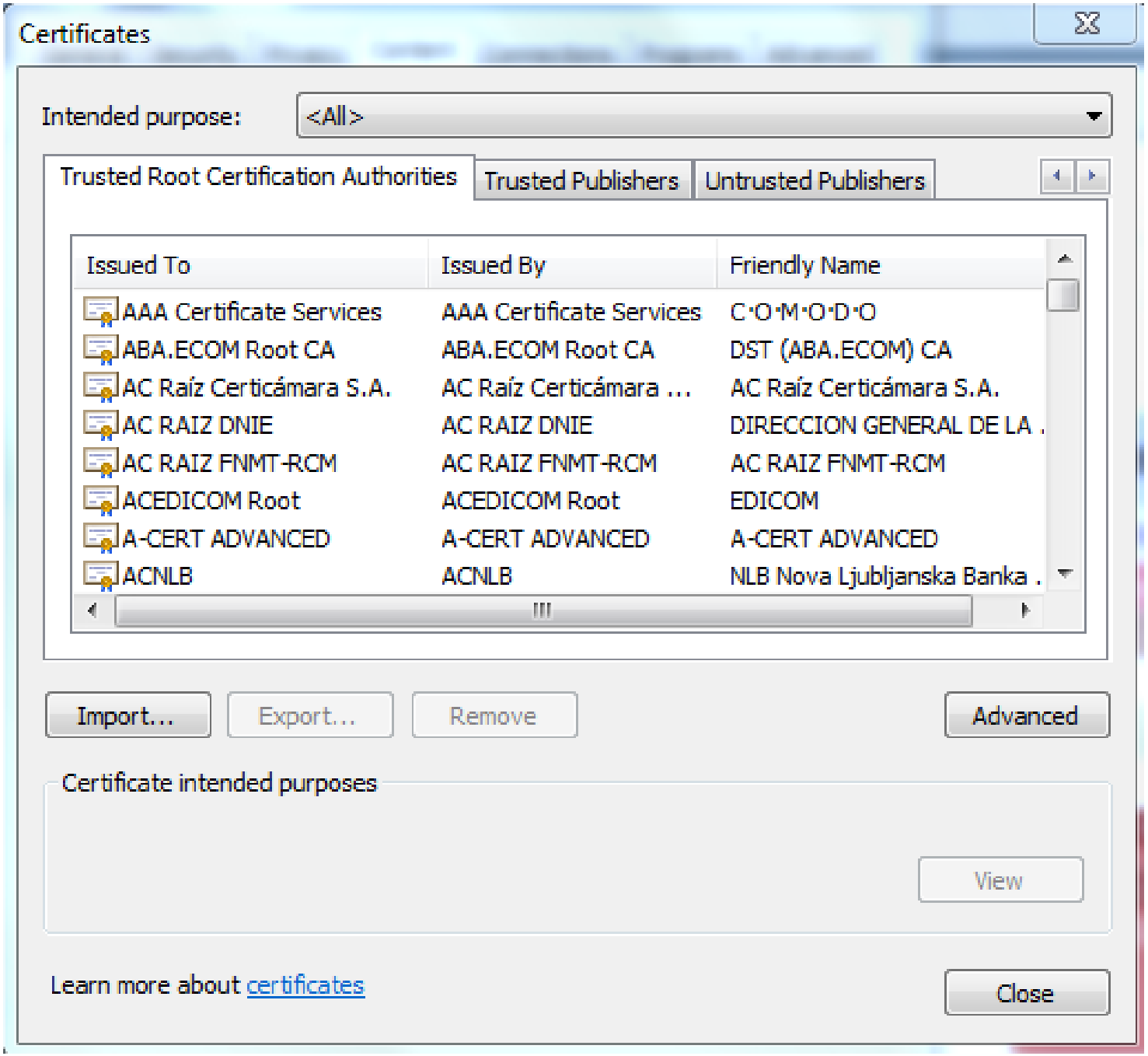
issues / signs certificates

based on due diligence

Is that really the CA's fingerprint?

Is that really the CA's fingerprint?

Do I trust the CA?


Certificates
Intended purpose:
<All>
Trusted Root Certification Authorities
Trusted Publishers
Untrusted Publishers
Issued To
Issued By
Friendly Name
AAA Certificate Services
AAA Certificate Services
C·O·M·O·D·O
ABA.ECOM Root CA
ABA.ECOM Root CA
DST (ABA.ECOM) CA
AC Raíz Certicámara S.A.
AC Raíz Certicámara ...
AC Raíz Certicámara S.A.
AC RAIZ DNIE
AC RAIZ DNIE
DIRECCION GENERAL DE LA .
AC RAIZ FNMT-RCM
AC RAIZ FNMT-RCM
AC RAIZ FNMT-RCM
ACEDICOM Root
ACEDICOM Root
EDICOM
A-CERT ADVANCED
A-CERT ADVANCED
A-CERT ADVANCED
ACNLB
ACNLB
NLB Nova Ljubljanska Banka .
Import...
Export...
Remove
Advanced
Certificate intended purposes
View
Learn more about certificates
Close

Treat this fingerprint
as if it were my own

Signed,


Princeton University - Welcome - Windows Internet Explorer
https://www.princeton.edu/main/


Send Money, Pay Online or Set Up a Merchant Account with PayPal - Windows Internet Explore
https://www.paypal.com/
PayPal, Inc. [US]

“domain validation” cert

“extended validation” cert

“domain validation” cert

“extended validation” cert

“domain validation” cert

“extended validation” cert