Online Trust and Digital Certificates: Tech Tutorial

Edward W. Felten
Professor of Computer Science and Public Affairs
Princeton University
Secure connection means:

1. Protected channel to some server
2. Authentication of the server’s identity
∀ 0 < x < pq: x^{(p-1)(q-1)} \mod 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
Whose fingerprint is that?

https://www.princeton.edu
princeton.edu’s fingerprint:

Signed,
certificate ("cert")

princeton.edu’s fingerprint:
Signed,
Signed,

https://www.princeton.edu

princeton.edu’s fingerprint:
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?
<table>
<thead>
<tr>
<th>Issued To</th>
<th>Issued By</th>
<th>Friendly Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA Certificate Services</td>
<td>AAA Certificate Services</td>
<td>C·O·M·O·D·O</td>
</tr>
<tr>
<td>ABA.ECOM Root CA</td>
<td>ABA.ECOM Root CA</td>
<td>DST (ABA.ECOM) CA</td>
</tr>
<tr>
<td>AC Raíz Certicâmara S.A.</td>
<td>AC Raíz Certicâmara S.A.</td>
<td>AC Raíz Certicâmara S.A.</td>
</tr>
<tr>
<td>AC RAIZ DINE</td>
<td>AC RAIZ DINE</td>
<td>DIRECCION GENERAL DE LA...</td>
</tr>
<tr>
<td>AC RAIZ FNMT-RCM</td>
<td>AC RAIZ FNMT-RCM</td>
<td>AC RAIZ FNMT-RCM</td>
</tr>
<tr>
<td>ACEDICOM Root</td>
<td>ACEDICOM Root</td>
<td>EDICOM</td>
</tr>
<tr>
<td>A-CERT ADVANCED</td>
<td>A-CERT ADVANCED</td>
<td>A-CERT ADVANCED</td>
</tr>
<tr>
<td>ACNLB</td>
<td>ACNLB</td>
<td>NLB Nova Ljubljanska Banka</td>
</tr>
</tbody>
</table>

Learn more about [certificates](#)
Treat this fingerprint as if it were my own

Signed,
“domain validation” cert

“extended validation” cert
“domain validation” cert

“extended validation” cert

green
“domain validation” cert

“extended validation” cert

green
true name