Online Trust and Digital Certificates: The Policy Landscape

Stephen Schultze
Associate Director
Center for Information Technology Policy, Princeton

The Stakeholders

browsers and operating system vendors

certificate authorities

sites (“subscribers”)

end-users (“relying parties”)

Browsers and OS Vendors

desktop

android

palm webOS™

BlackBerry

symbian
NOKIA OS

mobile

Certificate Authorities

public

private

Sites (“Subscribers”)

PayPal

Gmail by Google

Bank of America

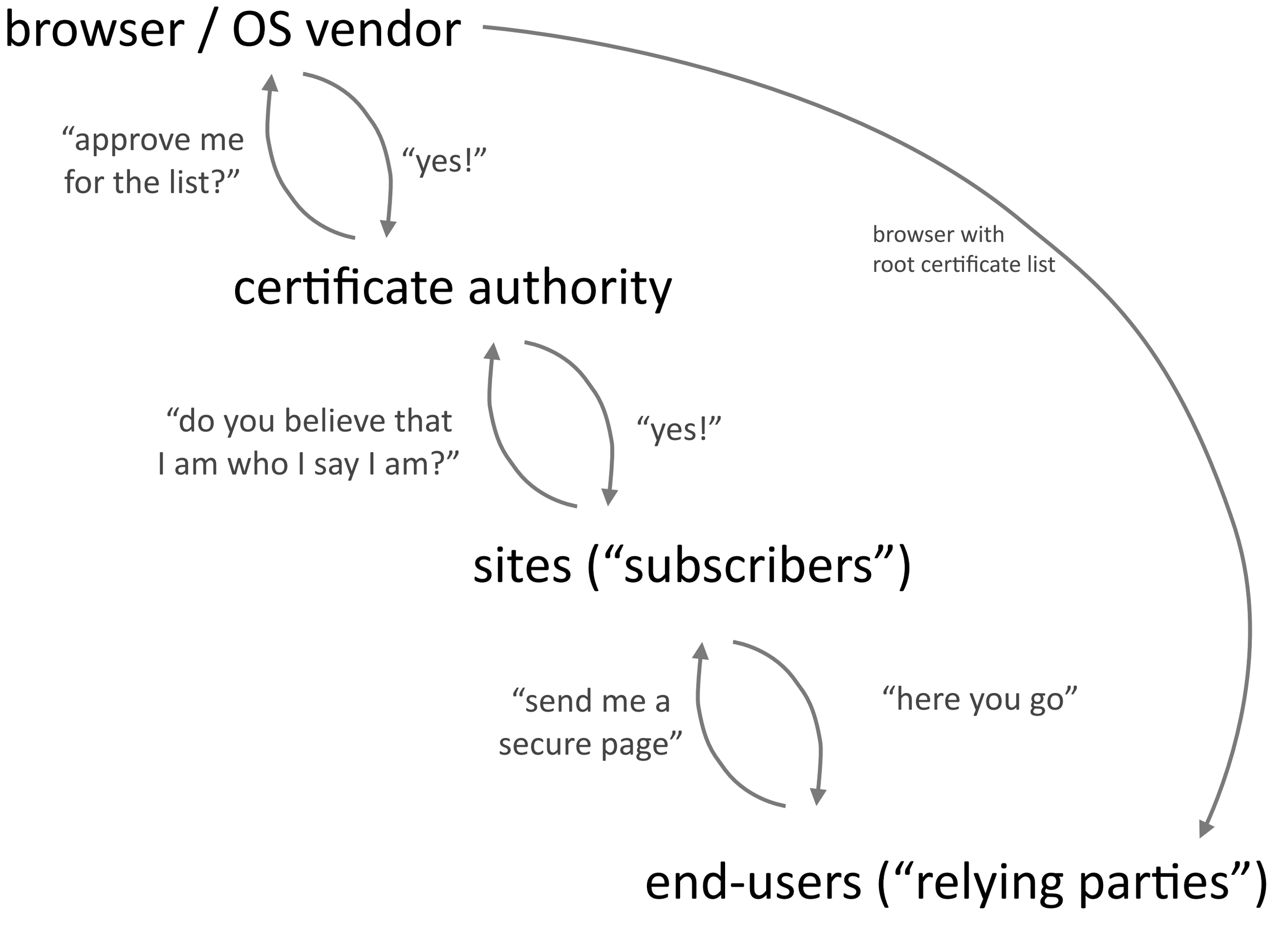
amazon.com

BlueCross BlueShield Association

USA.gov Government Made Easy

End-Users (“Relying Parties”)

You.

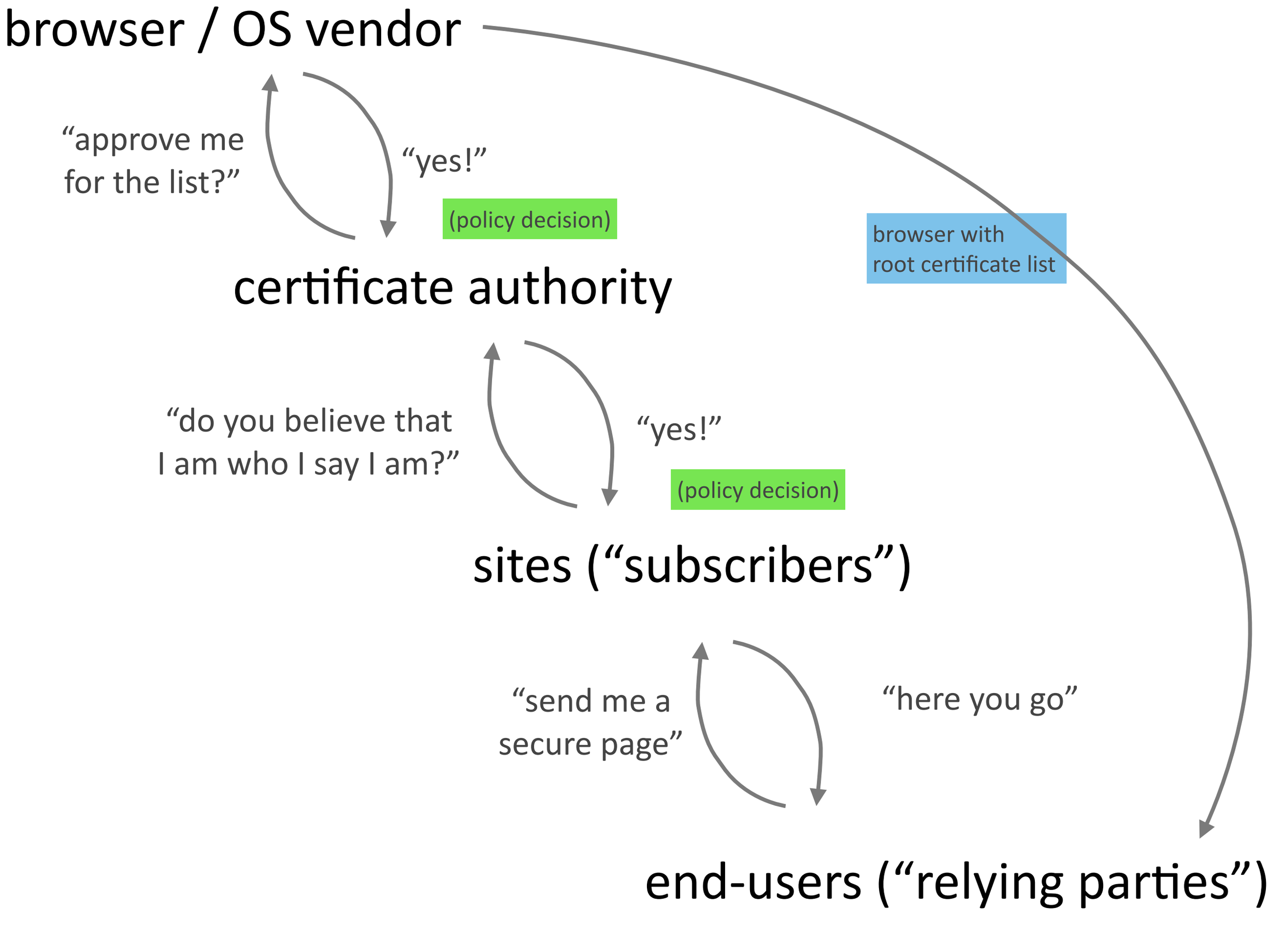

browser / OS vendor
"approve me for the list?"
"yes!"
browser with root certificate list
certificate authority
"do you believe that I am who I say I am?"
"yes!"
sites ("subscribers")
"send me a secure page"
"here you go"
end-users ("relying parties")

Why should users trust the system?

they know the CA

- or -

they believe that the overall process is trustworthy


browser / OS vendor
“approve me for the list?”
“yes!”
(policy decision)
browser with root certificate list
certificate authority
“do you believe that I am who I say I am?”
“yes!”
(policy decision)
sites (“subscribers”)
“send me a secure page”
“here you go”
end-users (“relying parties”)

Policy Decision Points

CA approval by browser

Site approval by CA

Where Policy Lives

auditor schemes

certificate authority policies

browser / os policies

standards bodies

Auditor Standards

WebTrust (CPA)

ETSI

ANSI

CA/Browser Forum

CA Policies

Certification Practice Statement

Certificate Policy

Subscriber Agreement

Browser / OS Policies

We reserve the right to not include a particular CA certificate [...] with CAs that

- knowingly issue certificates without the knowledge of the entities whose information is referenced in the certificates; or
- knowingly issue certificates that appear to be intended for fraudulent use.

[F]or a certificate to be used for SSL-enabled servers, the CA takes reasonable measures to verify that the entity submitting the certificate signing request **has registered the domain(s) referenced in the certificate** or has been authorized by the domain registrant to act on the registrant's behalf;

[F]or certificates to be used for and marked as Extended Validation, the CA complies with Guidelines for the Issuance and Management of Extended Validation Certificates (as modified by the erratum published by the **CAB Forum**)

(mozilla certificate policy)
(under revision)

Browser / OS Policies

By "**competent party**" we mean a person or other entity who is authorized to perform audits according to the stated criteria (e.g., by the organization responsible for the criteria or by a relevant government agency) or for whom there is sufficient public information available to determine that the party is competent to judge the CA's conformance to the stated criteria. In the latter case the "public information" referred to should include information regarding the party's

- knowledge of CA-related technical issues such as public key cryptography and related standards;
- experience in performing security-related audits, evaluations, or risk analyses; and
- honesty and objectivity.

(mozilla certificate policy)
(under revision)

Standards Bodies

IETF

ICANN

NIST

browser / OS vendor

"approve me for the list?"

"yes!"

(because your **auditor** said so)

browser with root certificate list

certificate authority

"do you believe that I am who I say I am?"

"yes!"

(because I sent you an **email**)

sites ("subscribers")

"send me a secure page"

"here you go"

end-users ("relying parties")

browser / OS vendor

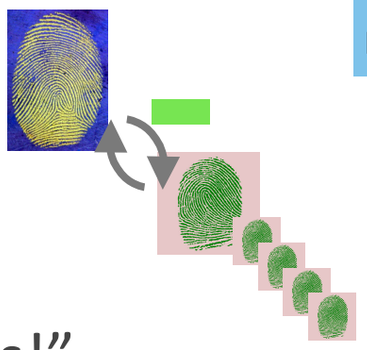
"approve me for the list?"

"yes!"

(because your **auditor** said so)

browser with root certificate list

certificate authority



"do you believe that I am who I say I am?"

"yes!"

(because I sent you an **email**)

sites ("subscribers")

"send me a secure page"

"here you go"

end-users ("relying parties")

Some Problems

Unconstrained Delegation

(delegation gives subordinate CAs “god-like” power)

No Excludability

(a site can’t say, “only trust one specific certificate authority for identifying me”)

Hundreds of CAs

(the “weakest link” problem)
(manageable load for vendors?)

Perfect Audits Aren’t Enough

(they don’t even include third-parties like subordinate CAs or RAs)

Bad Economic Incentives

("race to the bottom" for certificate authorities and auditors)

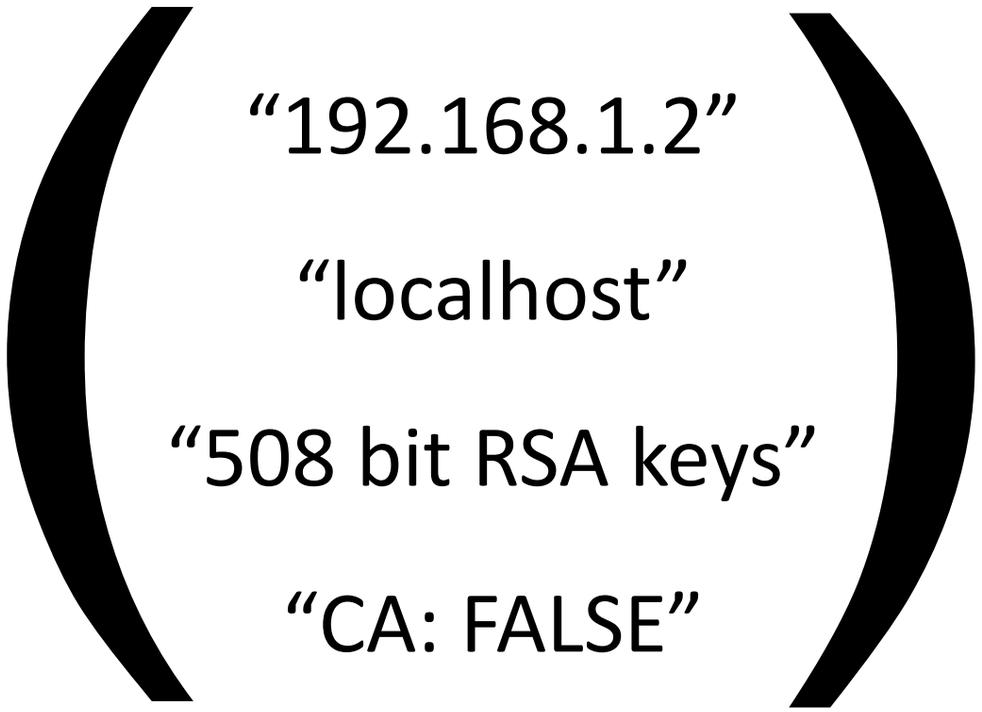
Vendors Don’t Drop CAs

(and they don’t have a “little stick” either)

Vendors Won’t Judge “Trustworthiness”

(only the process that the CA claims to follow)

Technical Bad Practices



* see Peter’s DEFCON slides

Jurisdiction is Complicated

(“whose law?”)

Hope

not many browsers/os’s

patches are possible

potential partial alternatives/ augmentations

#ethreats