The goal of a public-key infrastructure (PKI) is to enable secure, convenient, and efficient discovery of public keys.

-- Radia Perlman, IEEE Network, Nov/Dec 1999

Rather say usage instead of discovery

Discovery may be the long term problem
Current problem is usage

In most cases public-key “discovery” is achieved by explicit transport of certificate chains
SSL for example
Public-key “discovery” as such is required only for non-interactive protocols (email) for
Public-key encryption
Public-key key agreement
**SERVER-SIDE SSL (OR 1-WAY) HANDSHAKE WITH RSA**

<table>
<thead>
<tr>
<th>Client</th>
<th>Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>ClientHello</td>
<td>ServerHello</td>
</tr>
</tbody>
</table>

Handshake Protocol

<table>
<thead>
<tr>
<th>ClientKeyExchange</th>
<th>ServerKeyExchange</th>
</tr>
</thead>
<tbody>
<tr>
<td>[ChangeCipherSpec]</td>
<td>[ChangeCipherSpec]</td>
</tr>
<tr>
<td>Finished</td>
<td>Finished</td>
</tr>
</tbody>
</table>

Application Data

**SINGLE ROOT CA MODEL**

**MULTIPLE ROOT CA’s MODEL**

**CLIENT-SIDE SSL (OR 2-WAY) HANDSHAKE WITH RSA**

<table>
<thead>
<tr>
<th>Client</th>
<th>Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>ClientHello</td>
<td>ServerHello</td>
</tr>
</tbody>
</table>

Handshake Protocol

<table>
<thead>
<tr>
<th>ClientKeyExchange</th>
<th>ServerKeyExchange</th>
</tr>
</thead>
<tbody>
<tr>
<td>CertificateRequest</td>
<td>Certificate</td>
</tr>
<tr>
<td>CertificateVerify</td>
<td>[ChangeCipherSpec]</td>
</tr>
<tr>
<td>Finished</td>
<td>Finished</td>
</tr>
</tbody>
</table>

Application Data

**MULTIPLE ROOT CA’s MODEL**

**ROOT CA PLUS INTERMEDIATE CA’s MODEL**
SECURE ELECTRONIC TRANSACTIONS (SET) CA HIERARCHY

- **Root**
  - **Brand**
  - **Brand**
  - **Brand**
  - **Geo-Political**
    - **Bank**
    - **Acquirer**
      - **Customer**
      - **Merchant**

MULTIPLE ROOT CA’s PLUS INTERMEDIATE CA’s MODEL

- **X**
  - **Q**
  - **R**
  - **A**, **C**, **E**, **G**, **I**, **K**, **M**, **O**

- **S**
  - **T**

- **Essentially the model on the web today**
- **Deployed in server-side SSL mode**
- **Client-side SSL mode yet to happen**

SERVER-SIDE SSL (OR 1-WAY) HANDSHAKE WITH RSA

---

**Client**
- **Handshake Protocol**
- **ClientHello**
- **ClientKeyExchange**
- **ChangeCipherSpec**
- **Finished**

**Server**
- **ServerHello**
- **ServerHelloDone**
- **Certificate**
- **ChangeCipherSpec**
- **Finished**

**Record Protocol**
- **Application Data**
SERVER-SIDE MASQUARADING

Bob
Web browser
Server-side SSL
www.host.com
Web server

CLIENT-SIDE SSL (OR 2-WAY)
HANDSHAKE WITH RSA

Handshake Protocol
Client
ClientHello
-------->
ServerHello
Certificate
CertificateRequest
<----------
ServerHelloDone
Certificate
ClientKeyExchange
CertificateVerify
[ChangeCipherSpec]
Finished
-------->
[ChangeCipherSpec]
<----------
Finished
Application Data
Application Data

MAN IN THE MIDDLE
MASQUARADING PREVENTED

Bob
Web browser
www.host.com
Web server

ATTRIBUTE-BASED CLIENT SIDE MASQUARADING

Joe@anywhere
Web browser
Client-side SSL
BIMM.com
Web server

Record Protocol
Application Data
Application Data

Record Protocol
Application Data
Application Data
ATTRIBUTE-BASED CLIENT SIDE MASQUARADING

Alice@SRPC
Web browser
SRPC

BIMM.com
Web server

Bob@PPC
Web browser
PPC

ATTRIBUTE-BASED CLIENT SIDE MASQUARADING

Alice@SRPC
Web browser
SRPC

BIMM.com
Web server

Bob@PPC
Web browser
PPC

ATTRIBUTE-BASED CLIENT SIDE MASQUARADING

Alice@SRPC
Web browser
SRPC

BIMM.com
Web server

Bob@PPC
Web browser
PPC

PKI AND TRUST

- Got to be very careful
- Not a game for amateurs
- Not many professionals as yet