Federated Identity and Single-Sign On

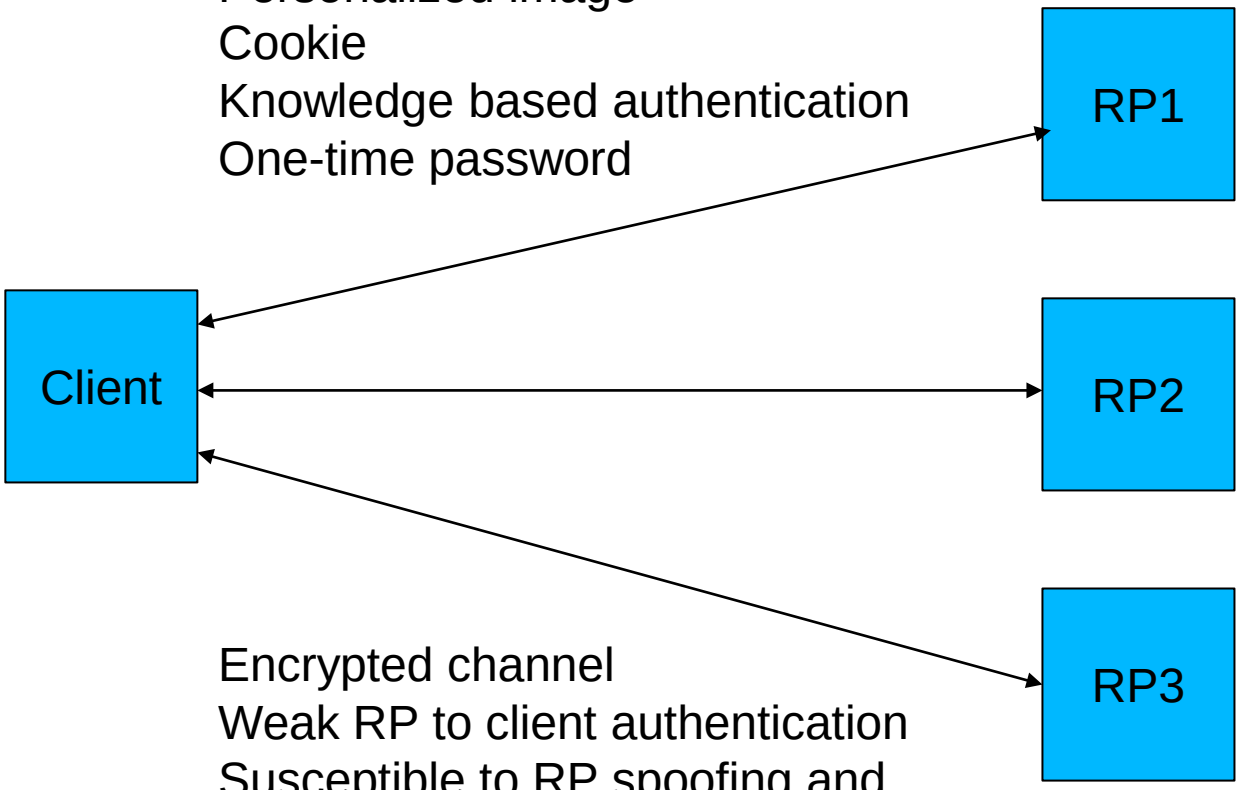
Prof. Ravi Sandhu
Executive Director and Endowed Chair

February 15, 2013

ravi.sandhu@utsa.edu
www.profsandhu.com

The Web Today

User ID, Password
+ maybe:
Personalized image
Cookie
Knowledge based authentication
One-time password



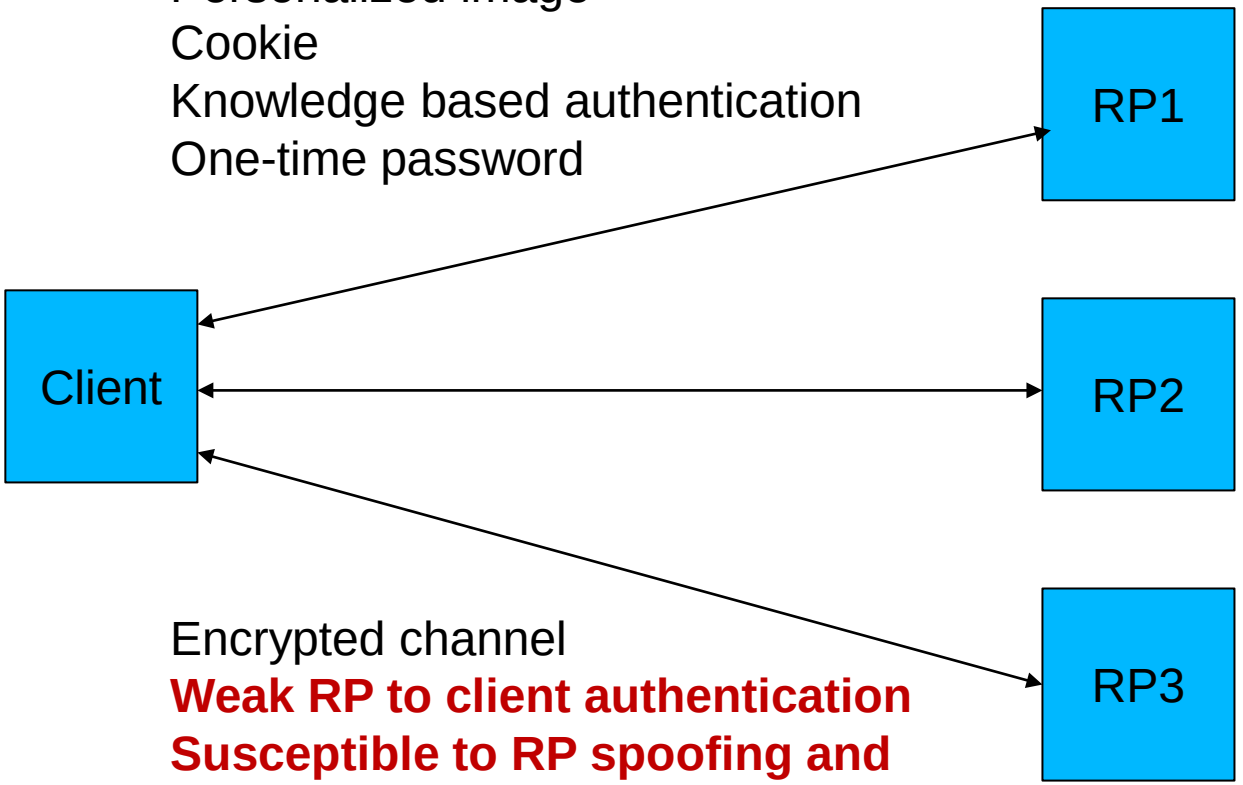
Relying Parties
(Service Providers)

Encrypted channel
Weak RP to client authentication
Susceptible to RP spoofing and
man-in-the-middle

The Web Today

Relying Parties
(Service Providers)

User ID, Password
+ maybe:
Personalized image
Cookie
Knowledge based authentication
One-time password



Private Key
Public Key

Private Key
Public Key

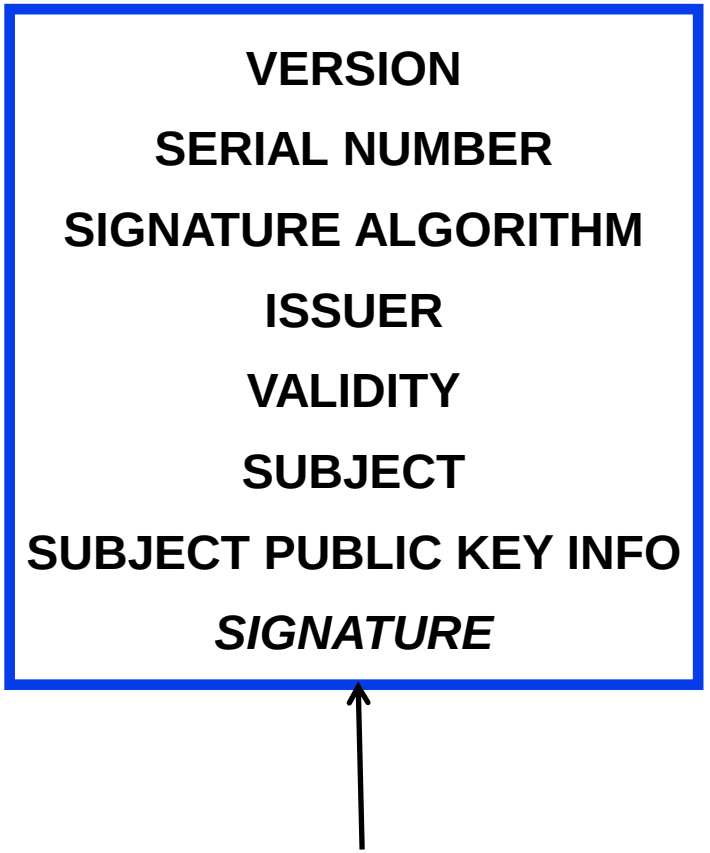
Private Key
Public Key

Encrypted channel
Weak RP to client authentication
Susceptible to RP spoofing and man-in-the-middle

Signature: done by Private Key, Verified by Public Key
Encryption: done by Public Key, Decrypted by Private Key

The Web Today

How to get a public key?
Digital Certificates

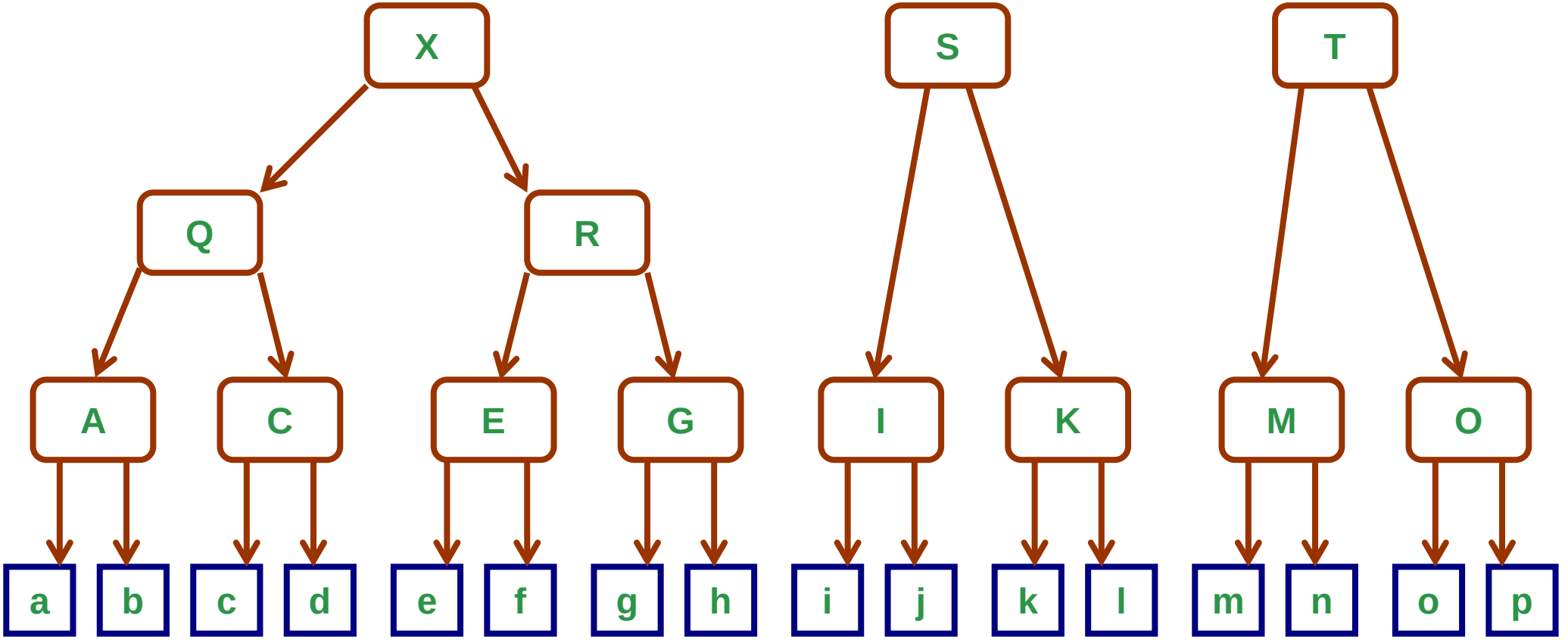


PKI: Public Key Infrastructure

Guarantees authentication and integrity
But how does one verify this signature
Need another Public Key

The Web Today

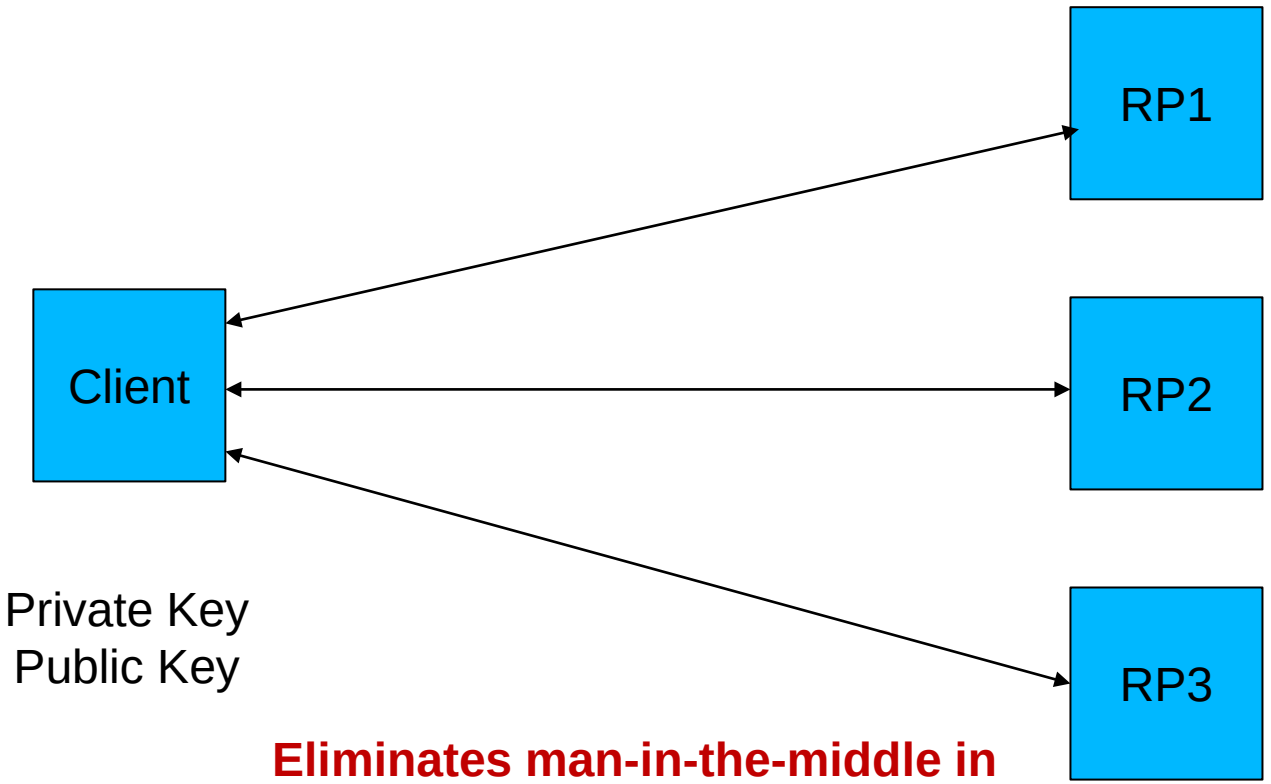
Root certificates are weakly protected in today's browsers



Multi-rooted Certificate Hierarchy

The PKI Vision (1980s Onwards)

Relying Parties
(Service Providers)



Private Key
Public Key

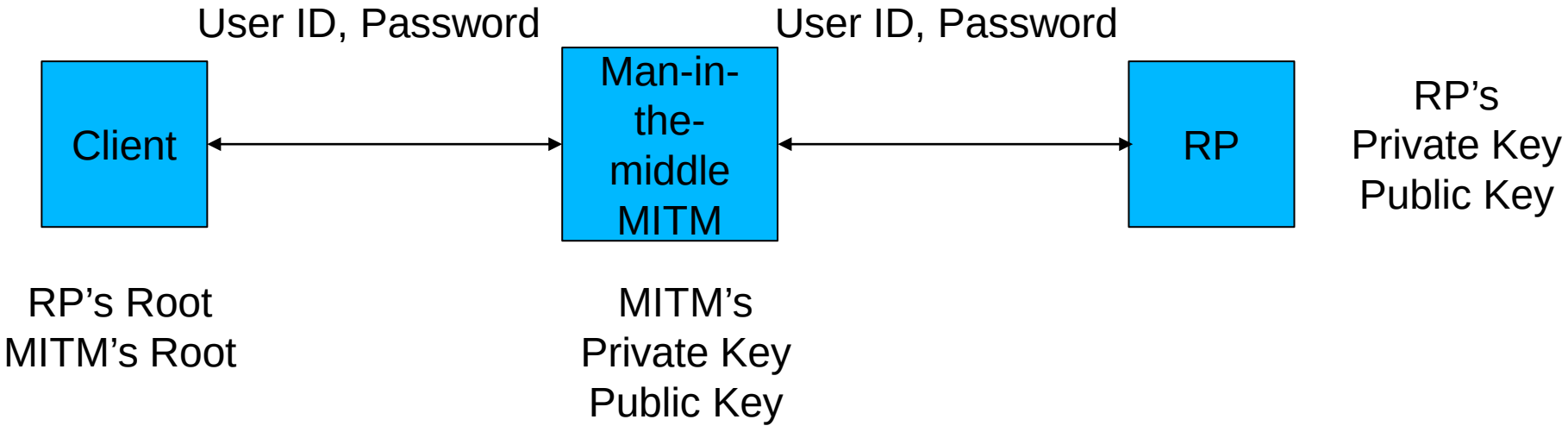
Private Key
Public Key

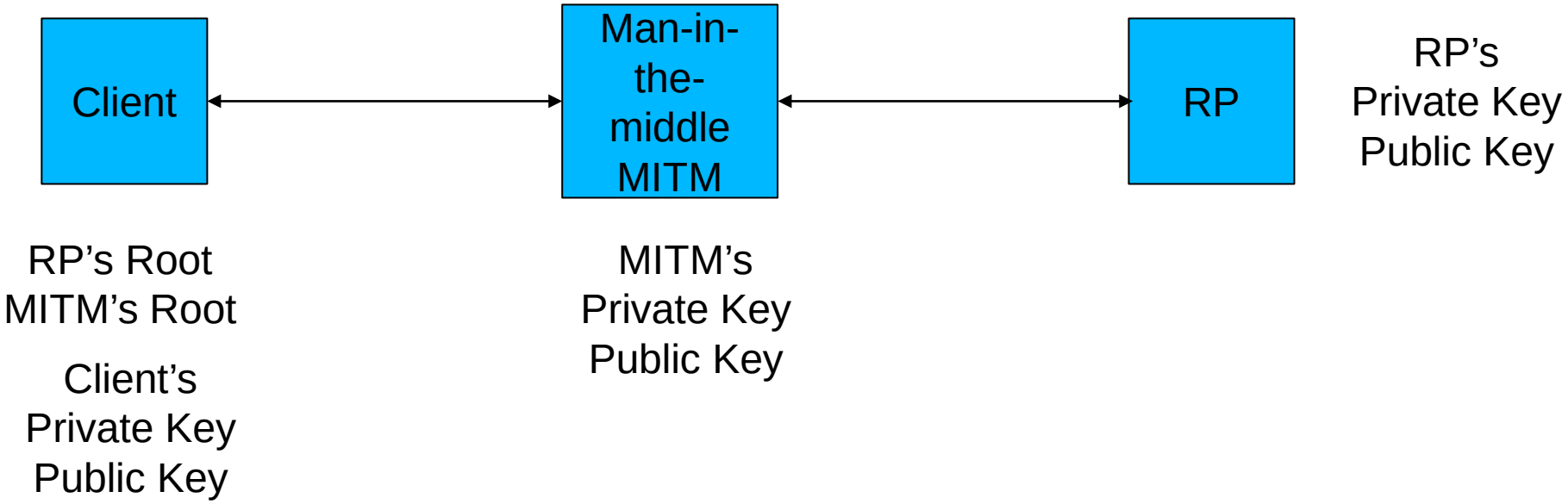
Private Key
Public Key

Private Key
Public Key

Eliminates man-in-the-middle in the network. Remains vulnerable to man-in-the-browser and man-in-the-PC

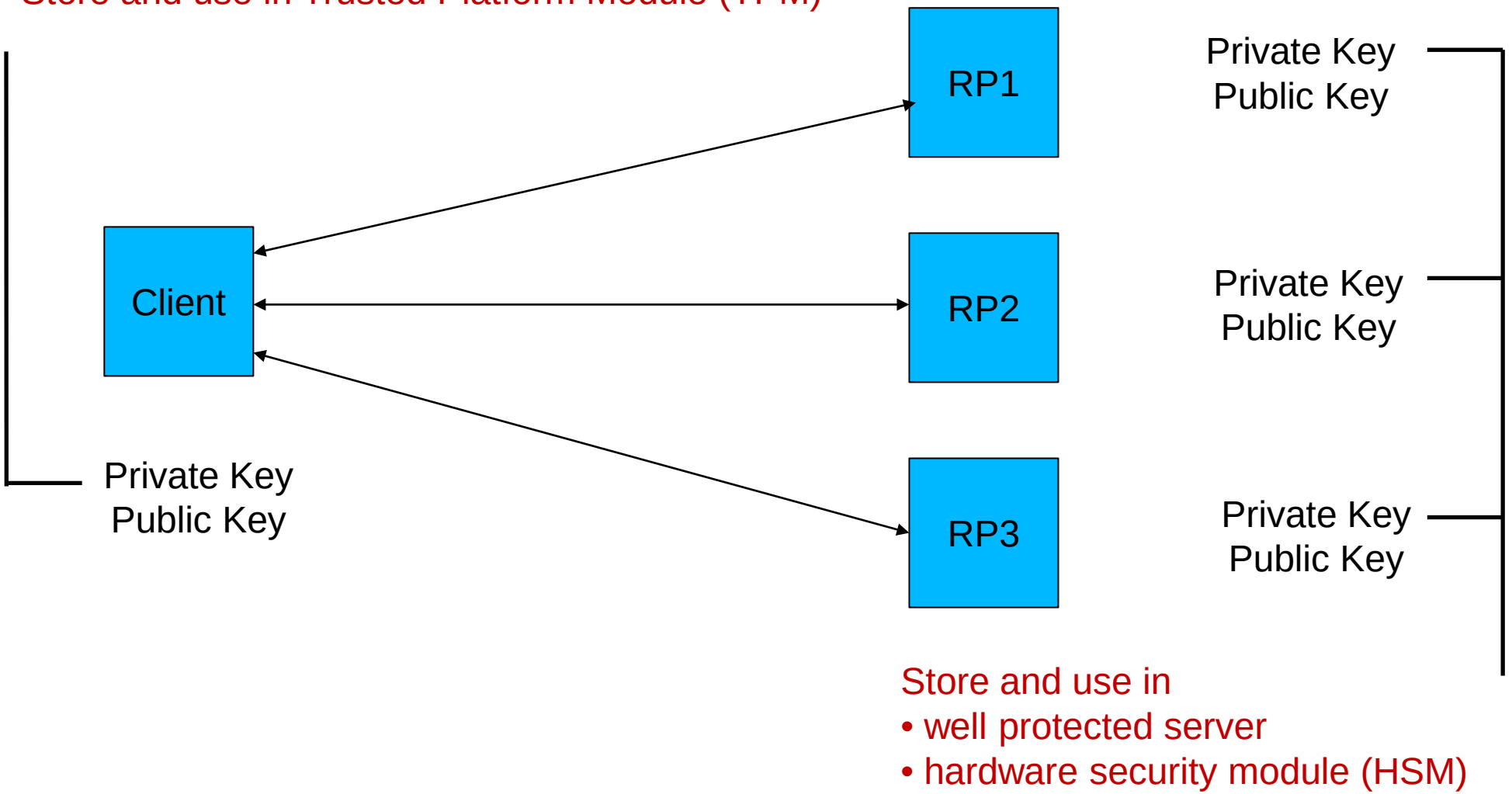
The PKI Vision (1980s Onwards)





The PKI Vision (1980s Onwards)

- Store as password protected and use in insecure PC
- Store and use in smartcard
- Store and use in Trusted Platform Module (TPM)



Store and use in
- well protected server
- hardware security module (HSM)

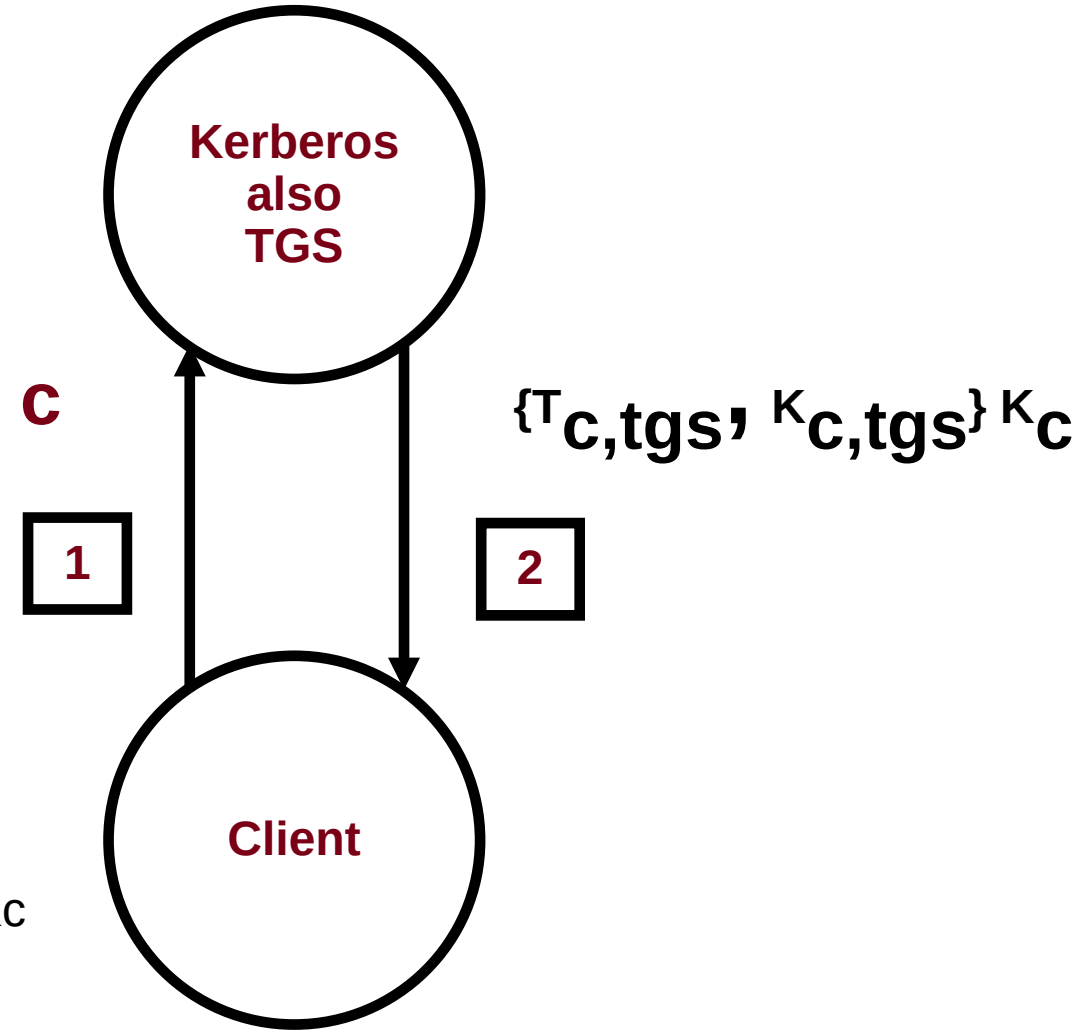
The PKI Vision (1980s Onwards)

- One authenticator for each client
  - Protected by one or more additional factors
- Usable by every RP who trusts the client's root
- Built-in out-of-the box Single Sign-On (SSO)
- Massive expense by US DoD on Common Access Card

Kerberos SSO (1980's onward)

Symmetric Key Technology

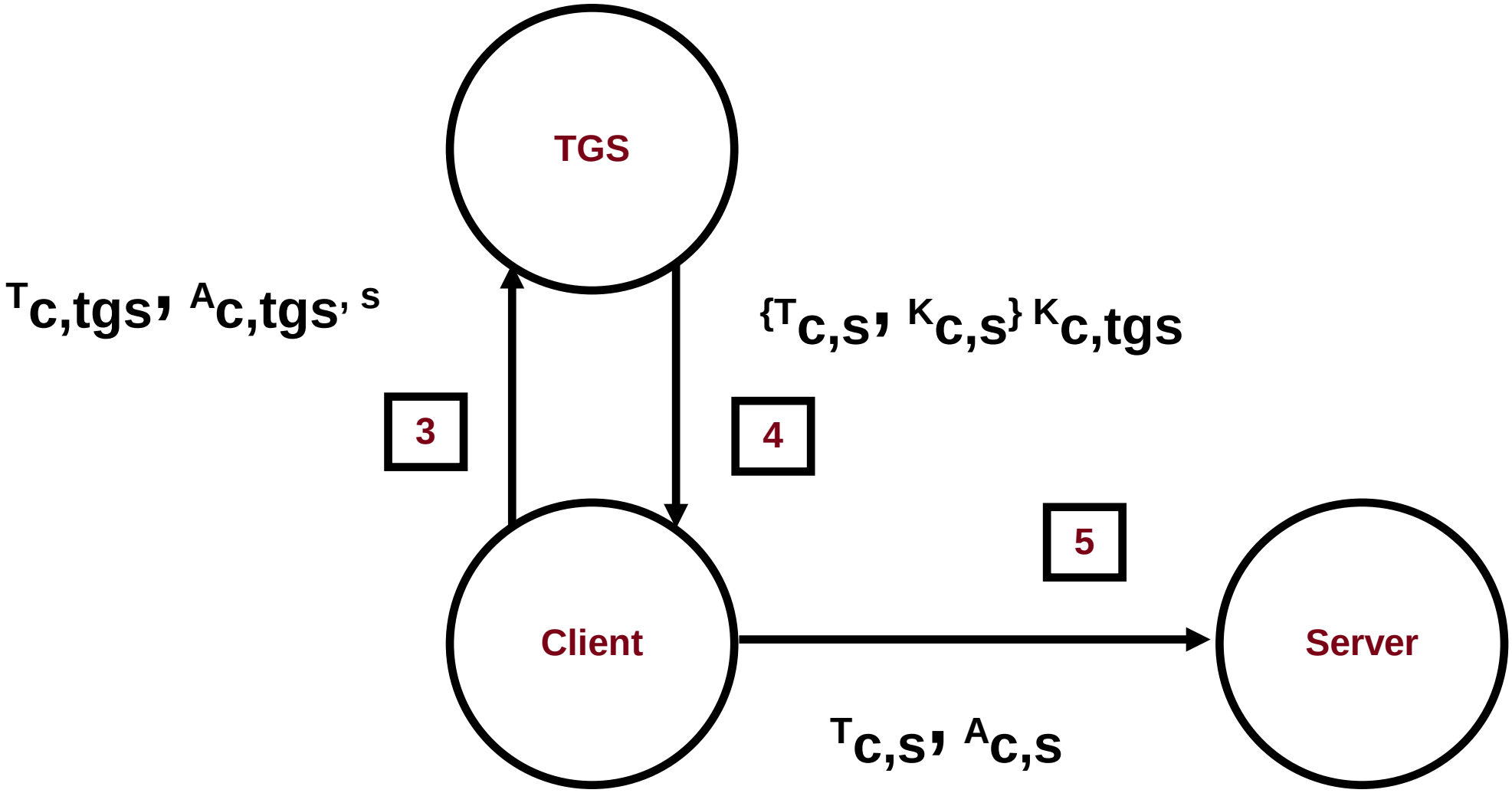
Stored client symmetric key Kc



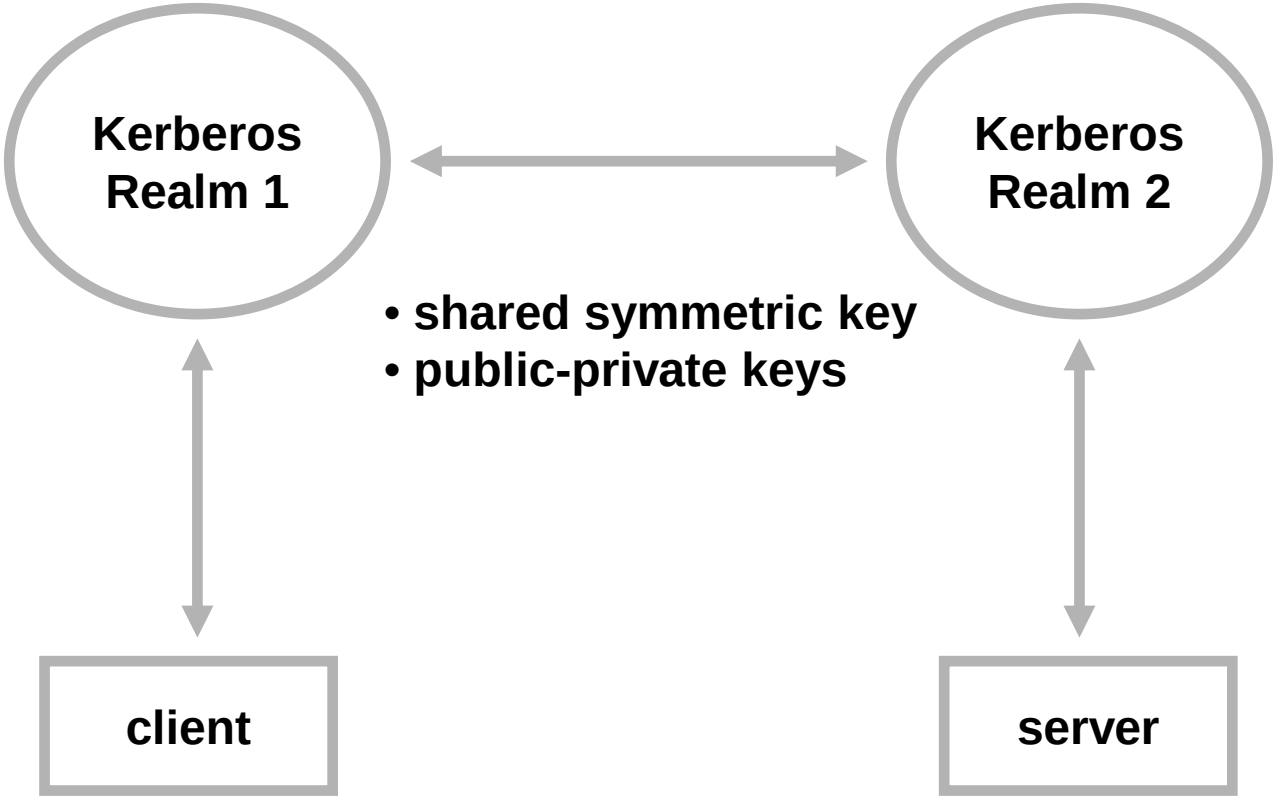
Client password -> client symmetric key Kc

Kerberos SSO (1980's onward)

Symmetric Key Technology



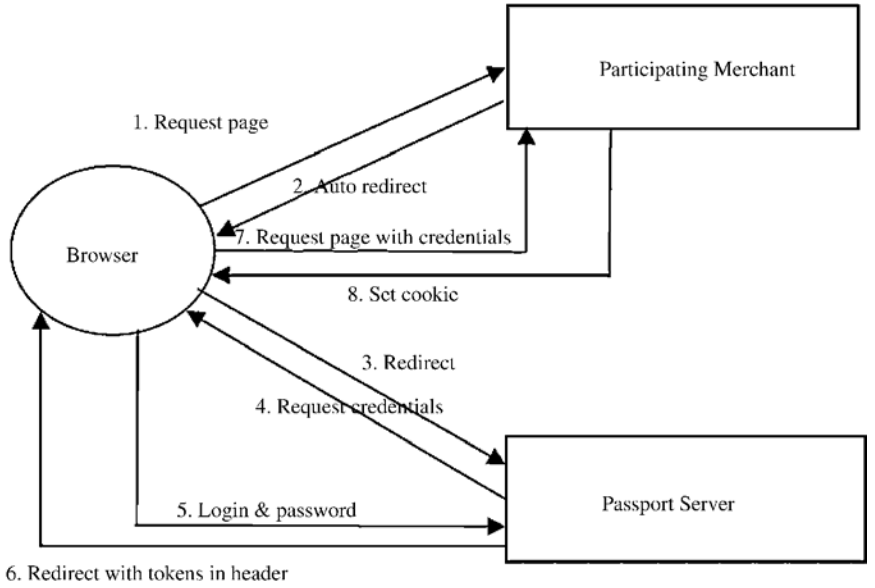
Kerberos SSO (1980's onward)



Kerberos SSO (1980's onward)

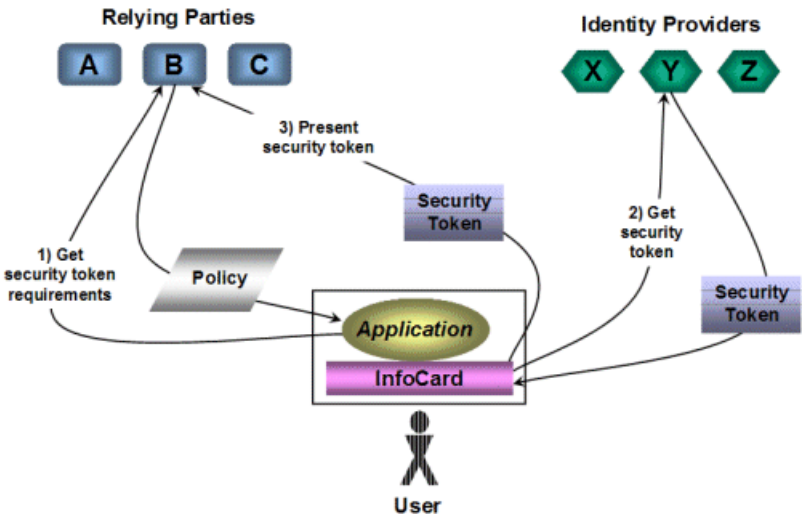
- Successful in Enterprise SSO
  - Scales to 10's or 100's of thousands of users
- Microsoft Active Directory login is based on Kerberos
- Inter-realm rarely deployed

Microsoft SSO (1990's)



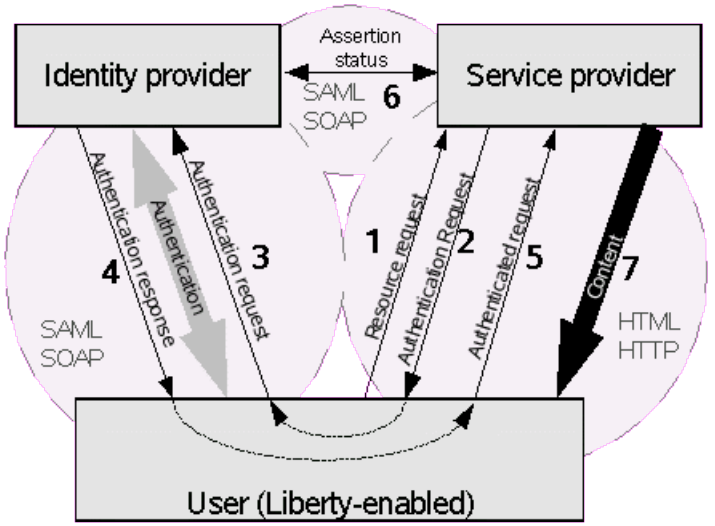
Failed

Microsoft Infocard Identity Ecosystem (2000's)



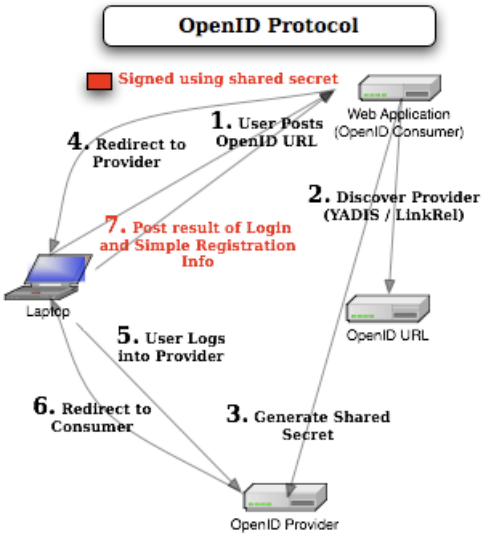
Failed

Liberty Alliance (2000's)

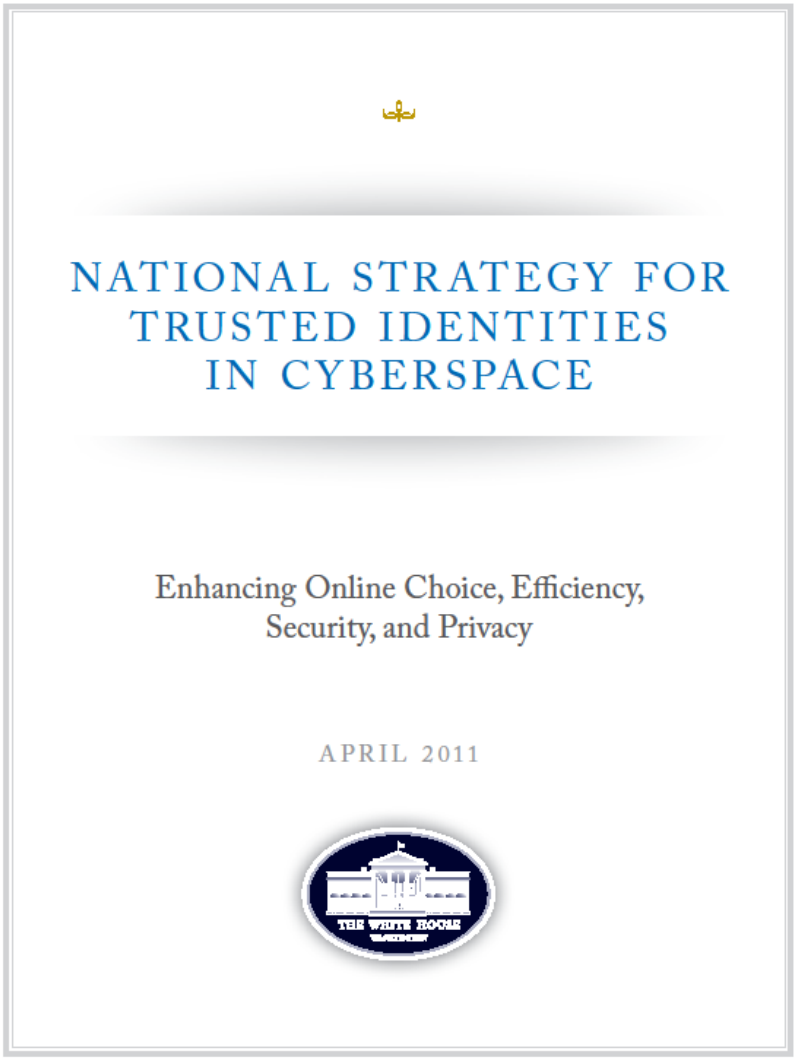


Failed

OpenID (2000's)



Failing


NATIONAL STRATEGY FOR
TRUSTED IDENTITIES
IN CYBERSPACE
Enhancing Online Choice, Efficiency,
Security, and Privacy
APRIL 2011
THE WHITE HOUSE