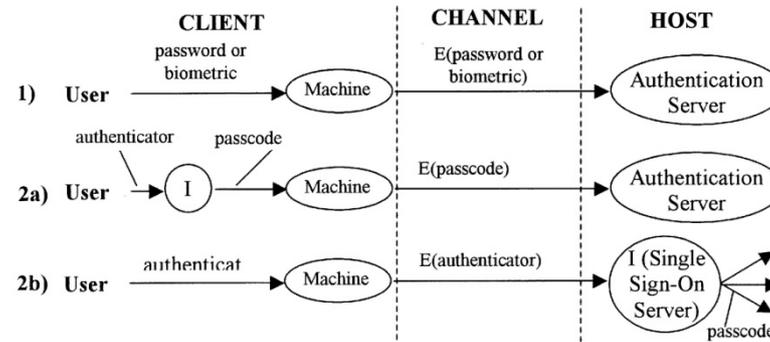# The Quest for Single-Sign On

Prof. Ravi Sandhu
Executive Director and Endowed Chair
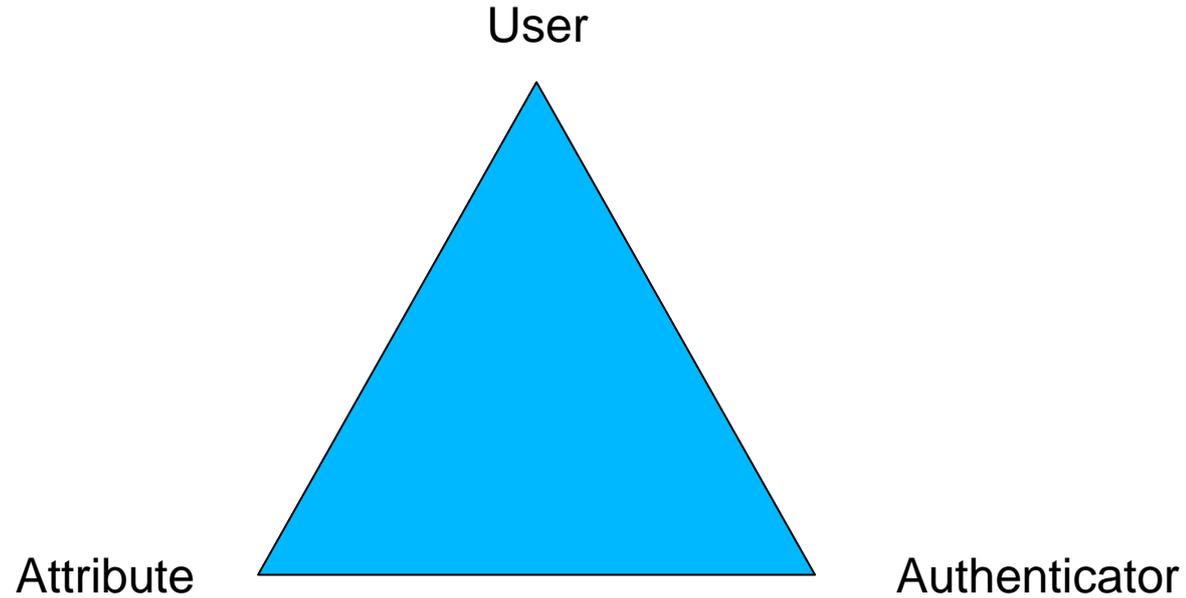
February 8, 2013

ravi.sandhu@utsa.edu
www.profsandhu.com
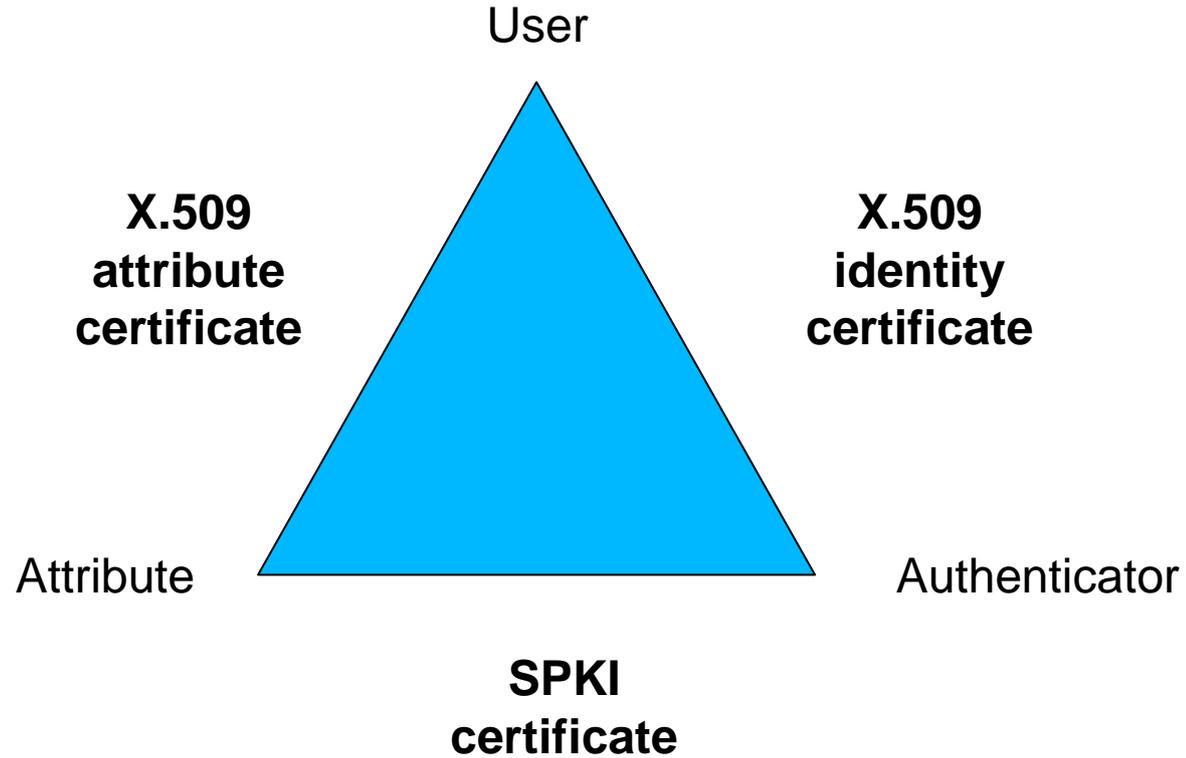
World-Leading Research with Real-World Impact!

> Initial authentication
> Session establishment and maintenance to authentication server
> Authentication to multiple servers
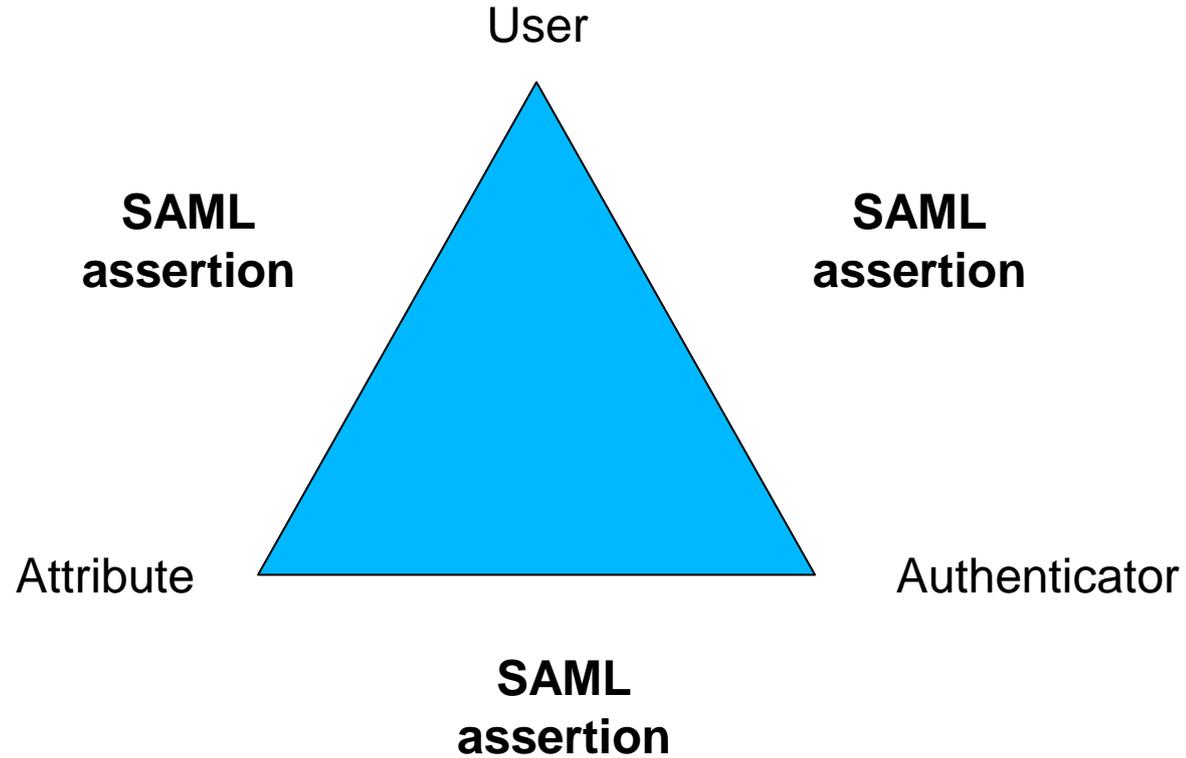> Session establishment and mantenance at multiple servers
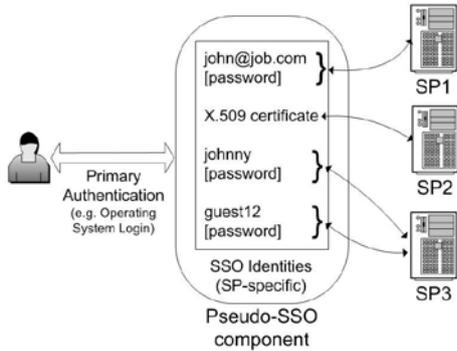> Single logout

We will discuss SSO separately

User

Attribute   Authenticator

1990s

User

X.509
attribute
certificate

X.509
identity
certificate

Attribute

Authenticator

SPKI
certificate

2000s

User

SAML assertion
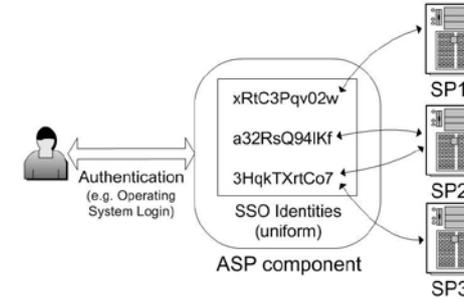
SAML assertion

Attribute

Authenticator
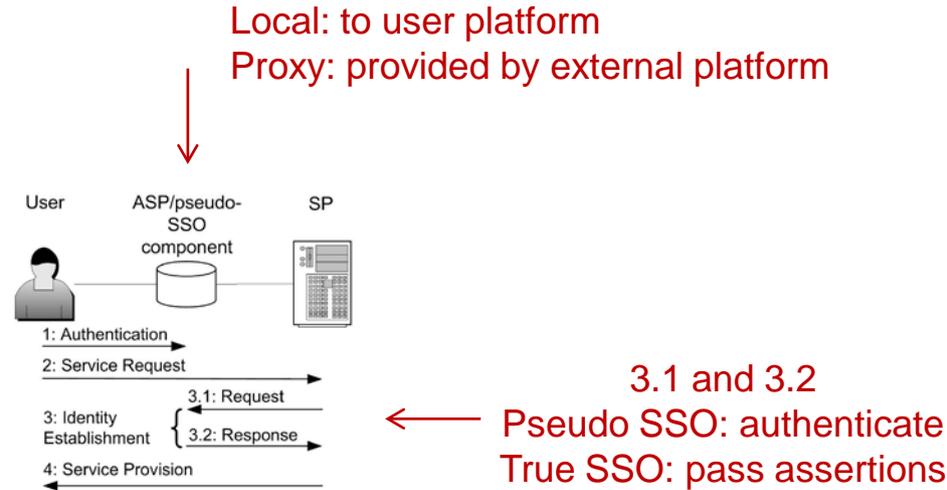
SAML assertion

Pseudo SSO
Identity to SP is n to 1

True SSO
Identity to SP is n to m

SSO: single sign on
SP: service provider (also called relying party)
ASP: authentication service provider

Taxonomy 2003

Local: to user platform
Proxy: provided by external platform

3.1 and 3.2
Pseudo SSO: authenticate
True SSO: pass assertions

- Local, Pseudo
- Proxy, Pseudo
- Local, True
- Proxy, True

World-Leading Research with Real-World Impact!

PKI (Public Key Infrastructure) does not fall neatly into this characterization

SP1

User Private Key

SP2

SP3
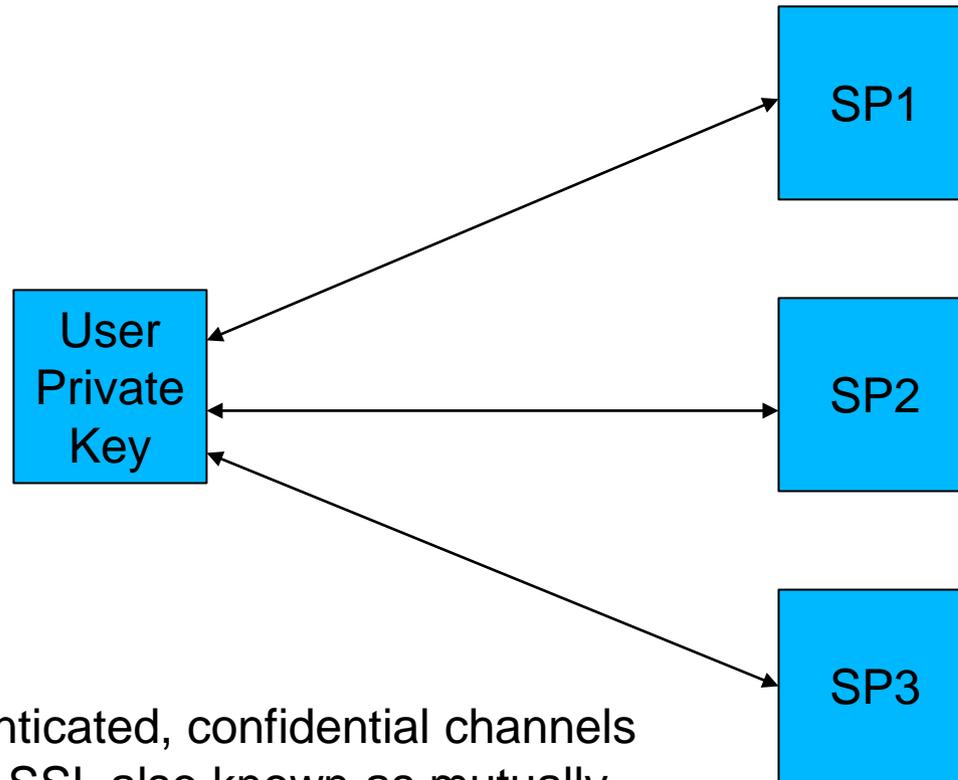
Authenticated, confidential channels
2-way SSL also known as mutually
authenticated SSL