



# Security and Identity Issues in Cross-Agency SOA

Philip Walston  
Senior Product Manager

[pwalston@layer7tech.com](mailto:pwalston@layer7tech.com)

May 2006



# Agenda and Theme

- Security and identity in SOA
- The challenges of security and identity
- What is federation about?
- Why federation of Web services is hard
- Breaking the problem down
- Tactical, standards-based solutions

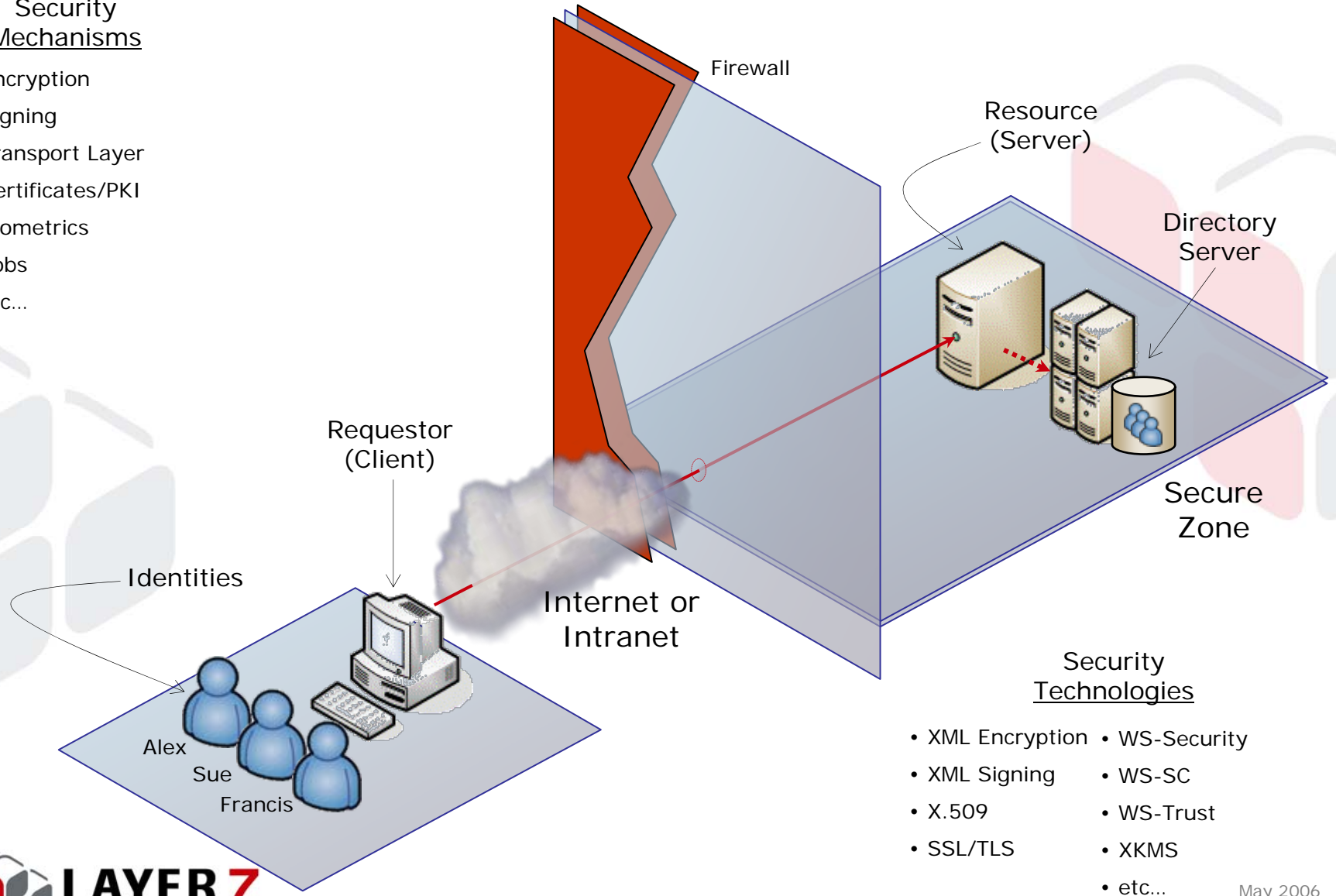
**Theme:** *A pragmatic approach to cross-agency SOA*

Security and federation for SOA is a complex problem, and the standards are still evolving. However, we can take a realistic look at what most services are being used for, we can build standards-compliant solutions today.

# Security in Cross-Domain Computing

## Security Mechanisms

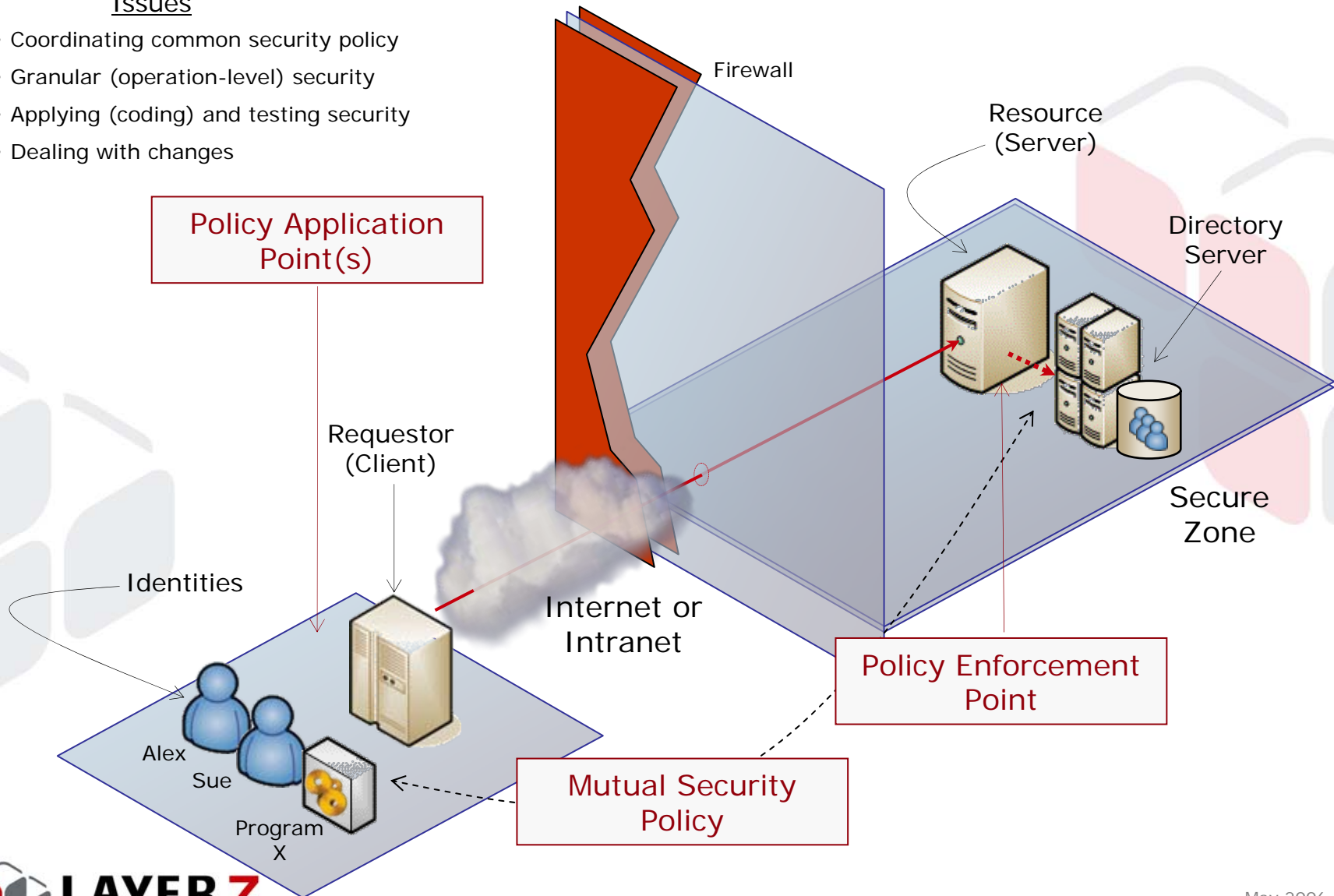
- Encryption
- Signing
- Transport Layer
- Certificates/PKI
- Biometrics
- Fobs
- etc...



# The Security Challenge of Cross-Agency SOA

## Issues

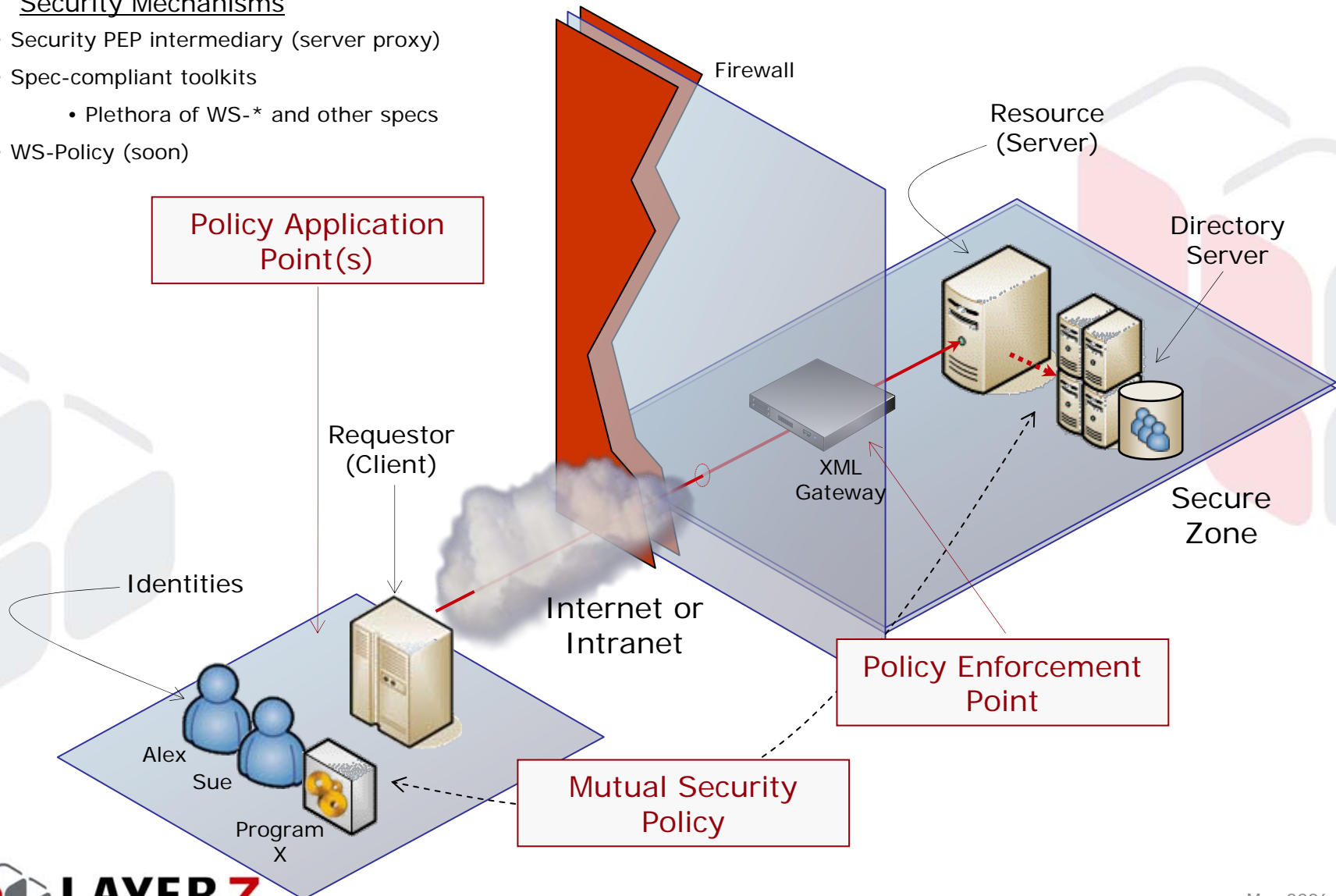
- Coordinating common security policy
- Granular (operation-level) security
- Applying (coding) and testing security
- Dealing with changes



# Tactical Strategy

## Security Mechanisms

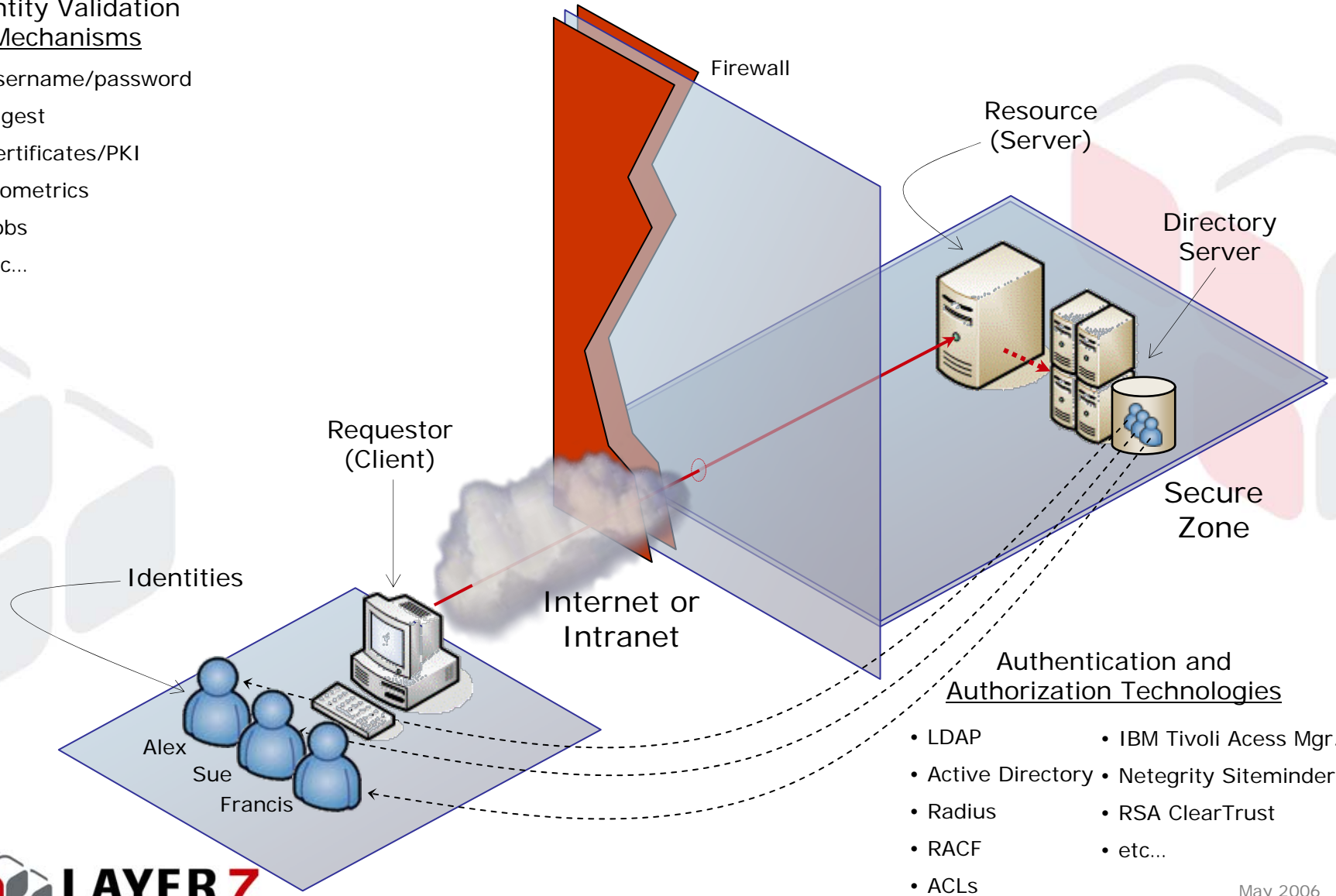
- Security PEP intermediary (server proxy)
- Spec-compliant toolkits
  - Plethora of WS-\* and other specs
- WS-Policy (soon)



# Identity in Cross-Domain Computing

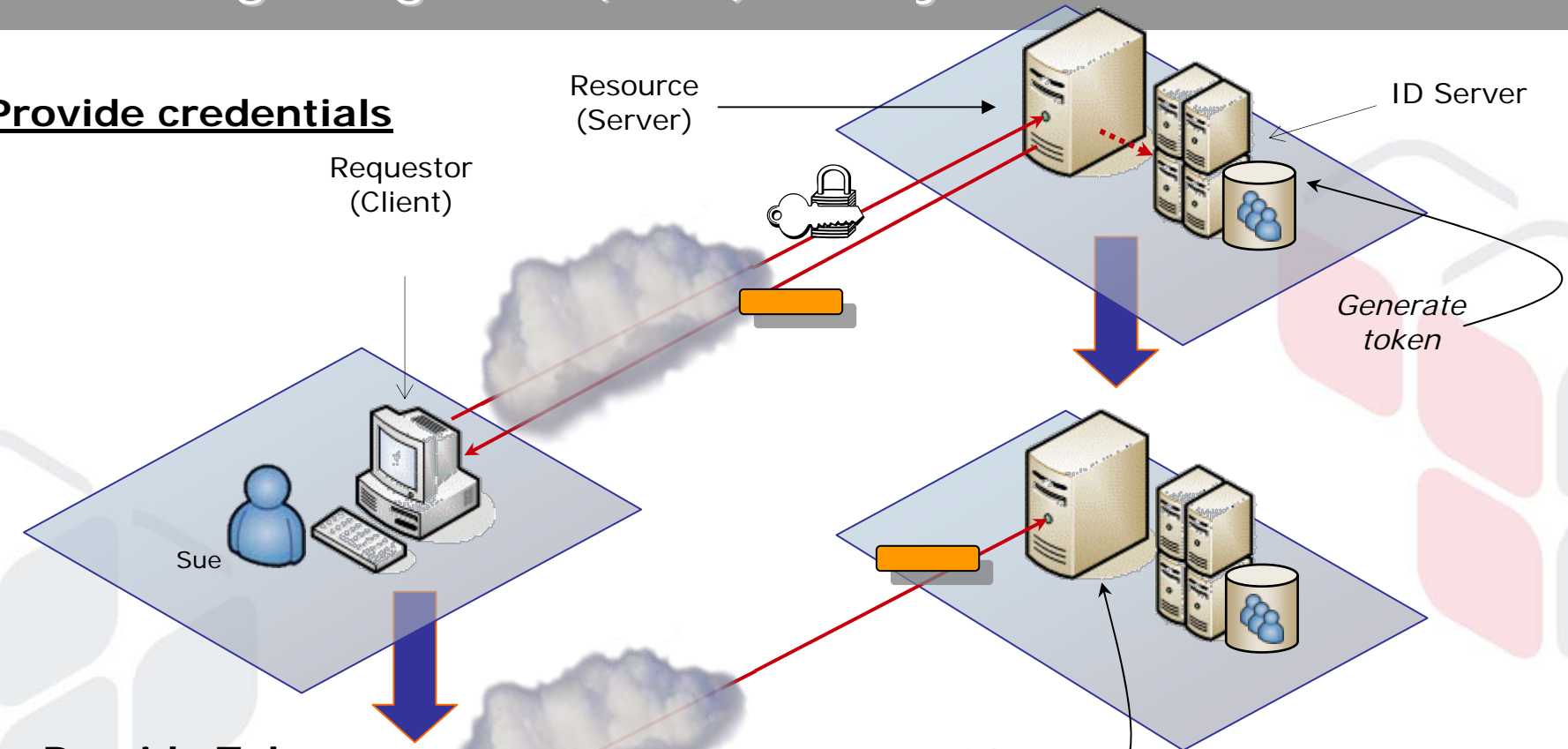
## Identity Validation Mechanisms

- Username/password
- Digest
- Certificates/PKI
- Biometrics
- Fobs
- etc...

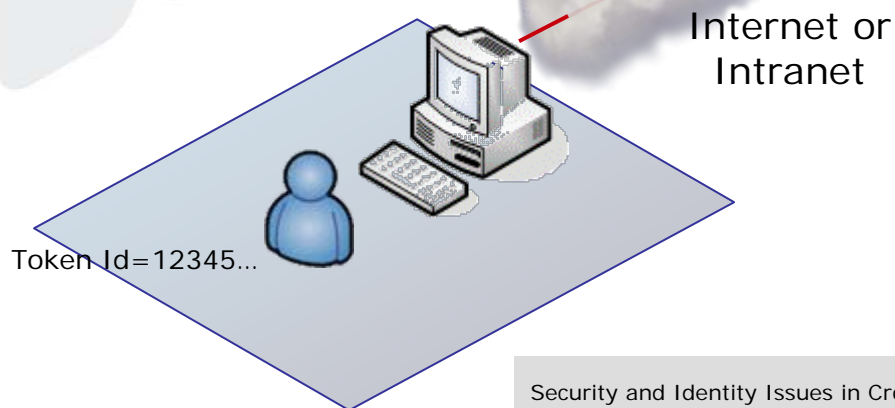


# What's Single Sign On (SSO) Really About?

## 1. Provide credentials



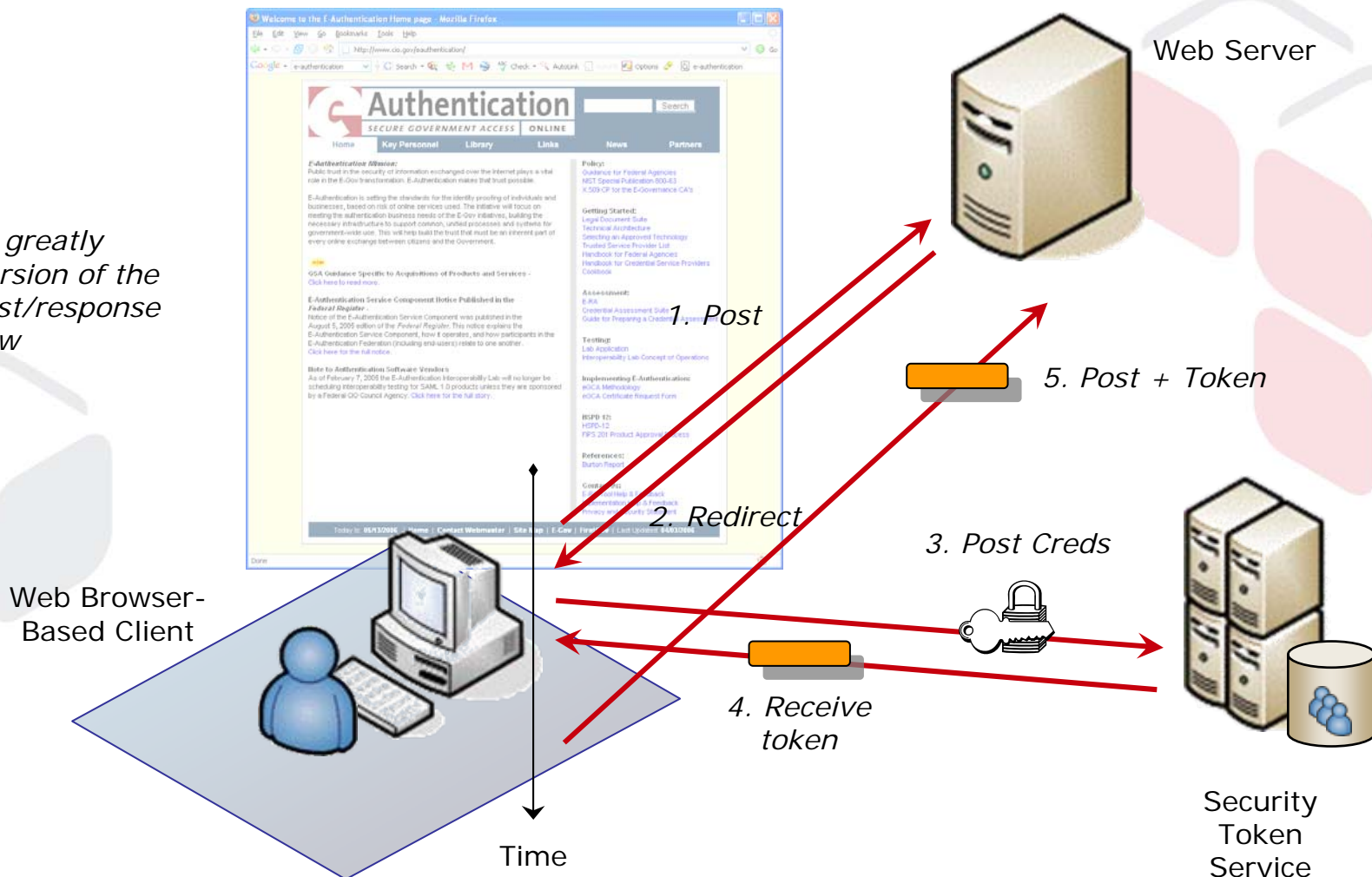
## 2.-n. Provide Token



# Why Does SSO Work for Browsers?

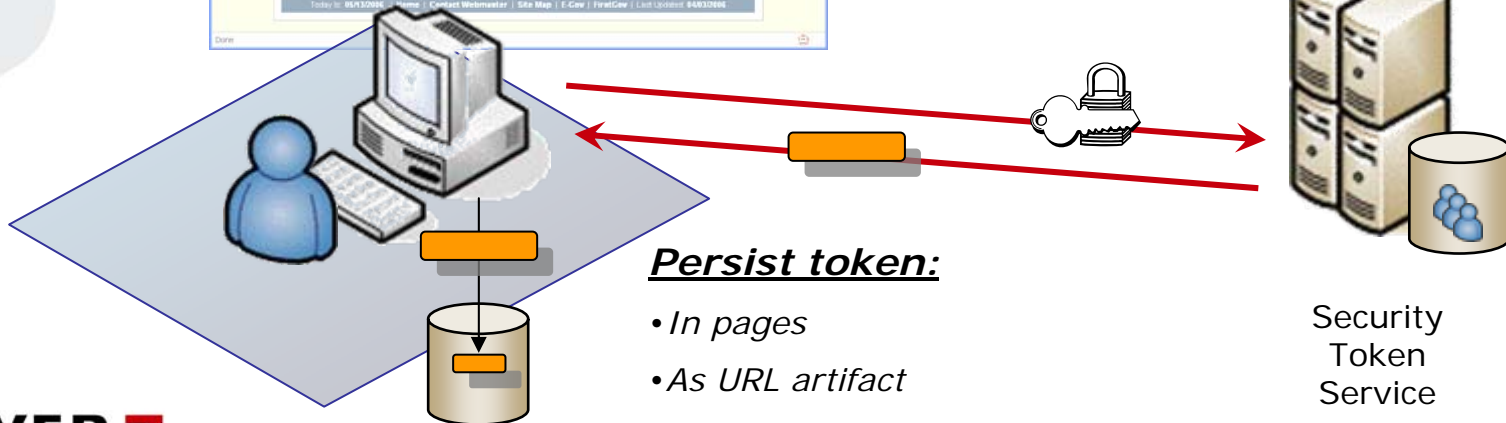
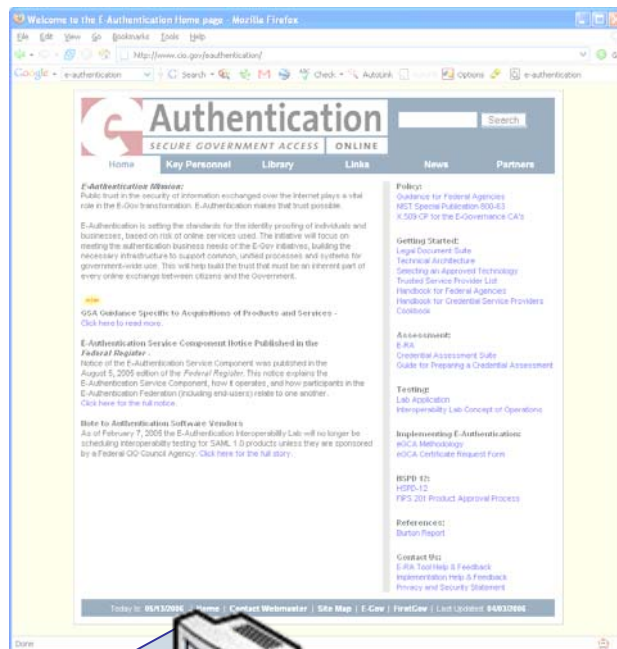
## 1. HTTP Redirects

*This is a greatly simplified version of the actual request/response flow*



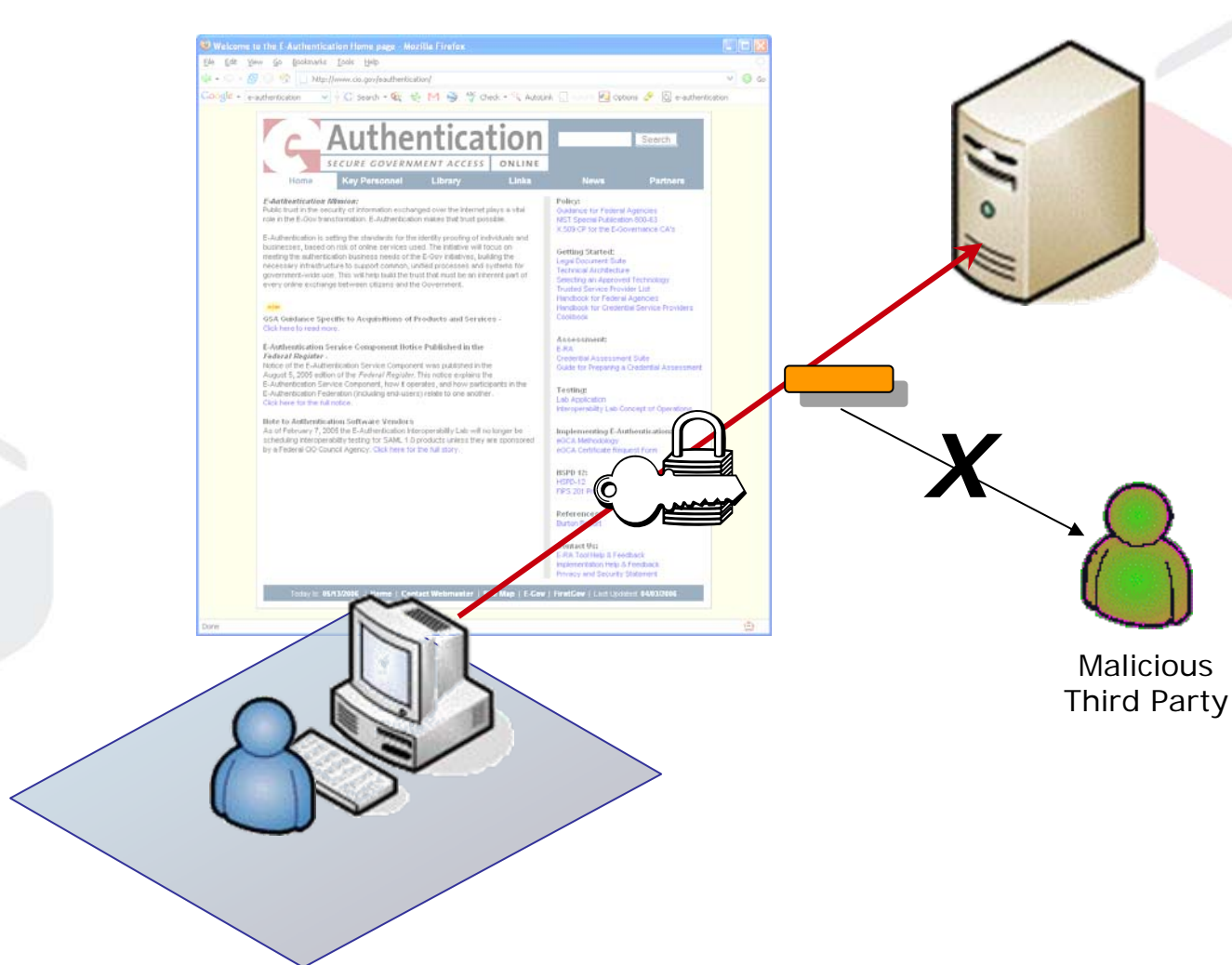
# Why Does SSO Work for Browsers?

## 2. A Client-side Persistence Model

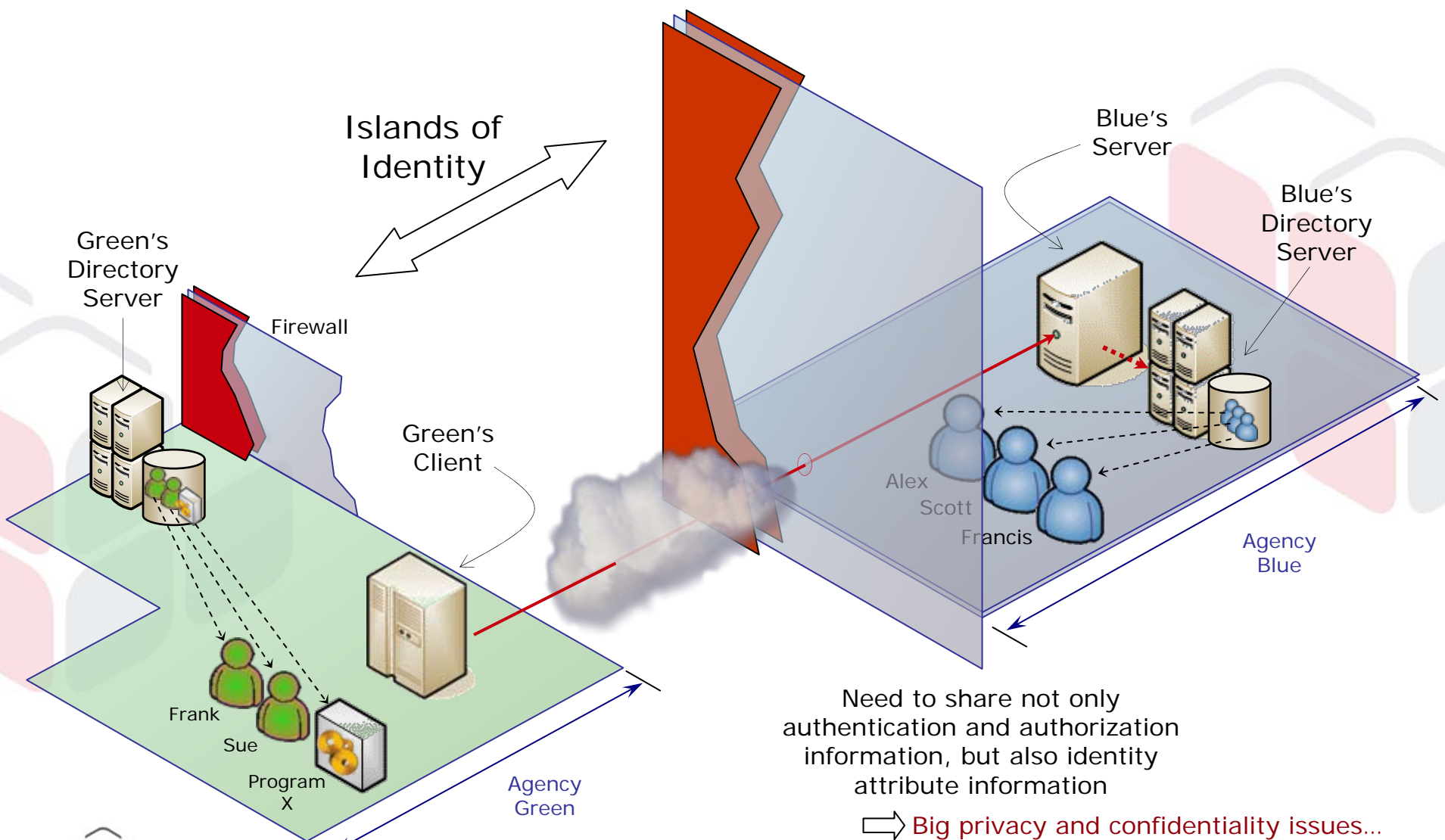


# Why Does SSO Work for Browsers?

## 3. SSL Protection of Tokens



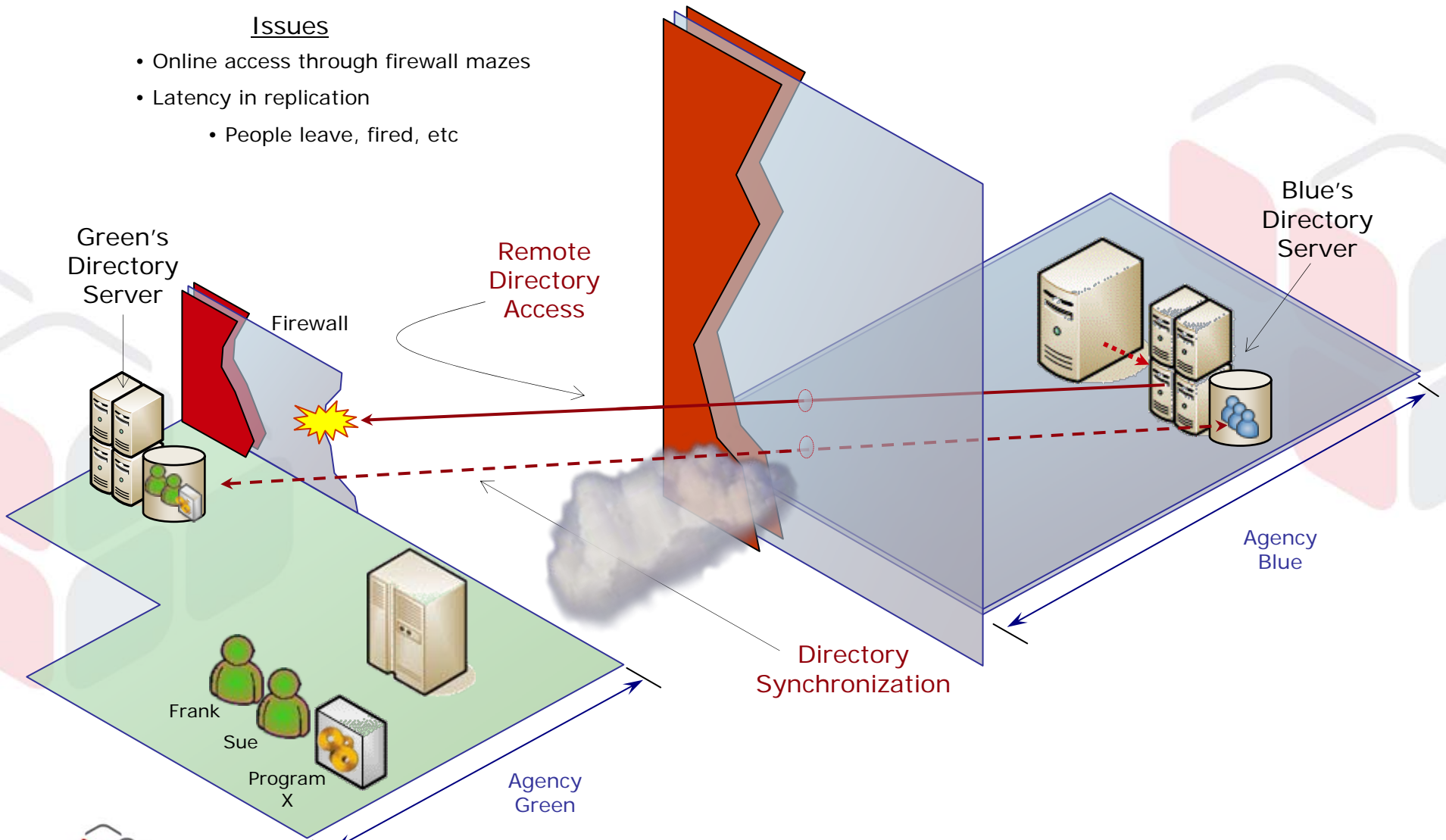
# The Identity Challenge of Cross-Agency SOA



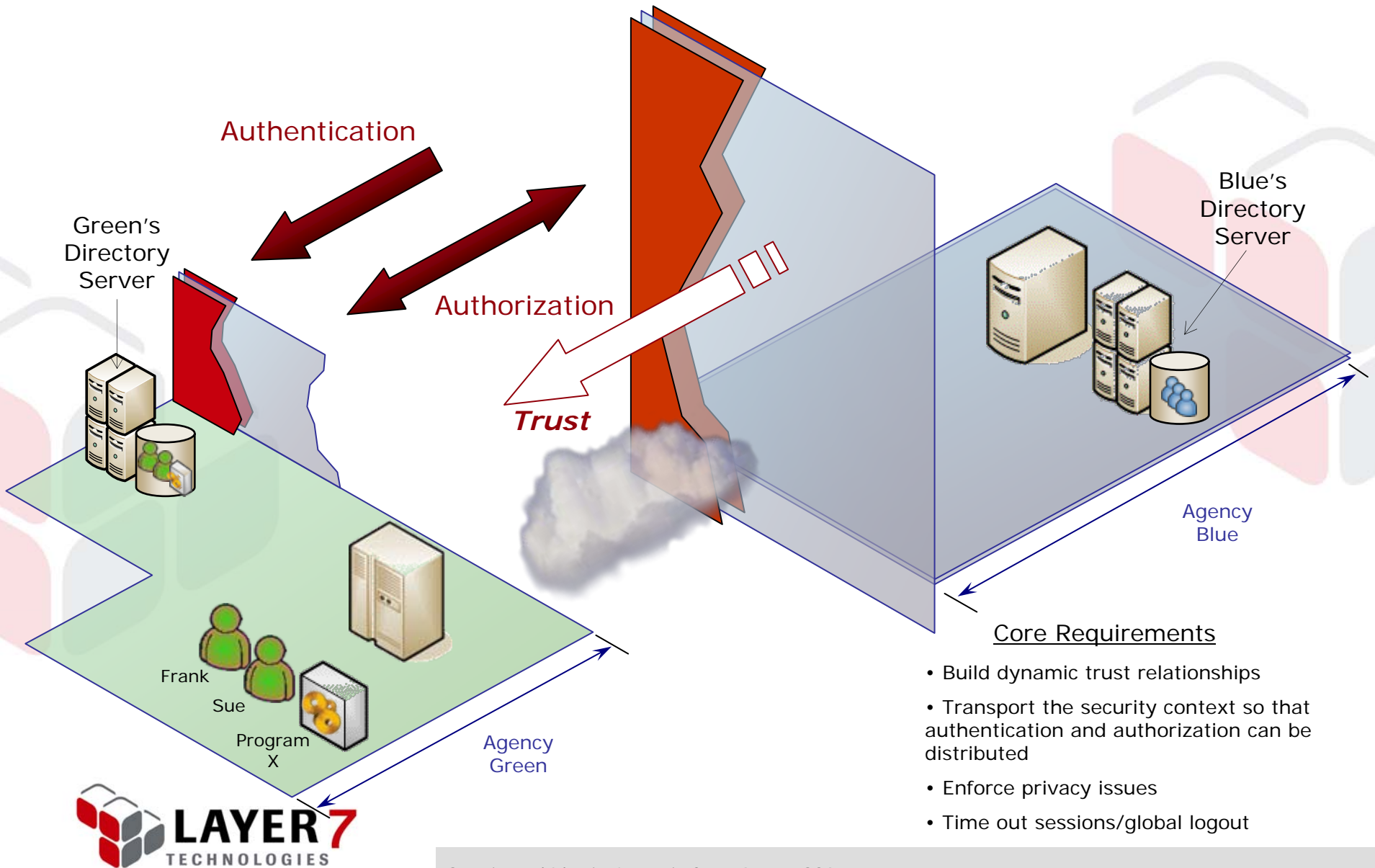
# What Hasn't Worked in the Past

## Issues

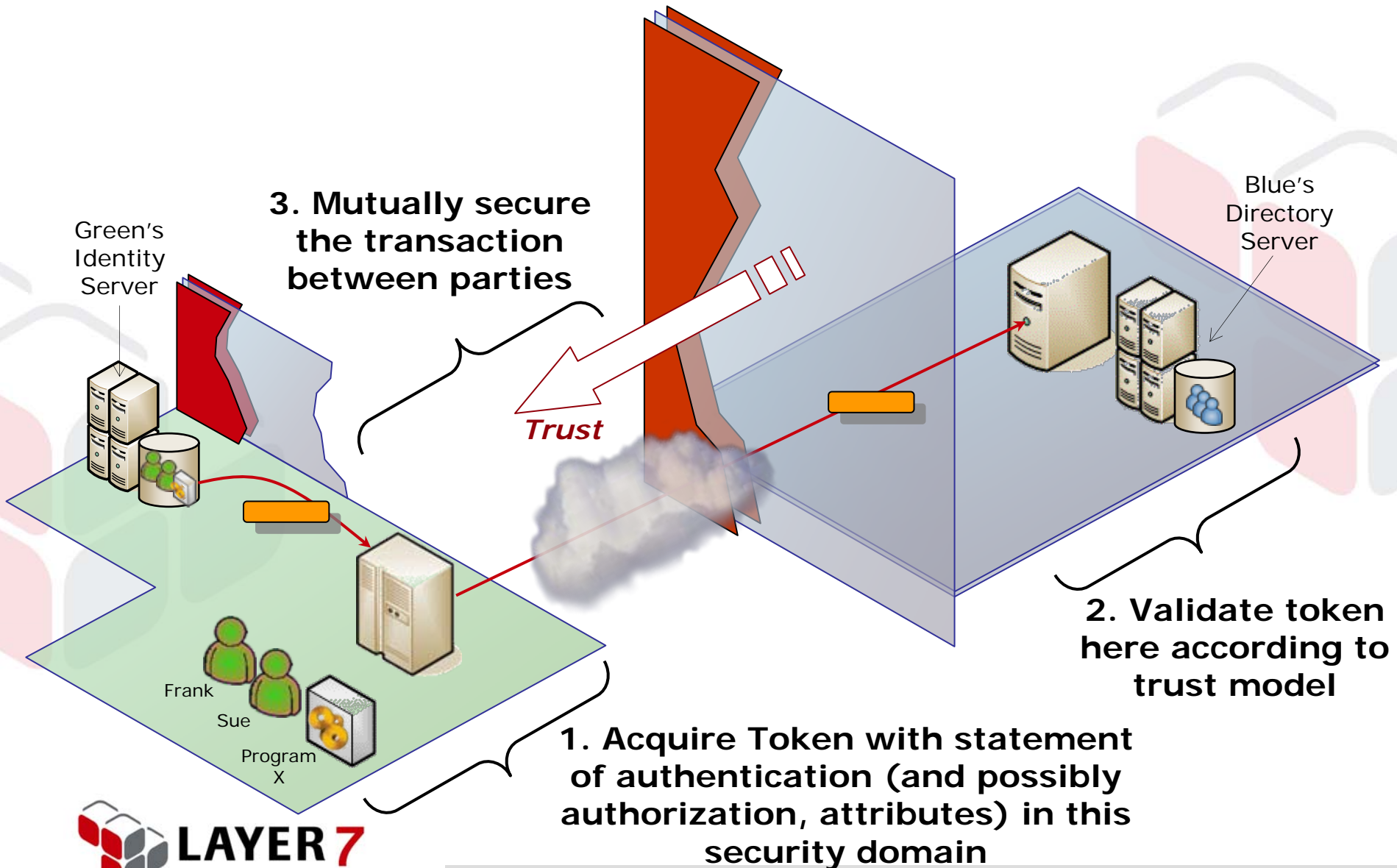
- Online access through firewall mazes
- Latency in replication
  - People leave, fired, etc



# What We Really Need is Effective *Separation of Concerns*



# The Mechanism



# Validation / Authorization Blurs the Concept of Identity



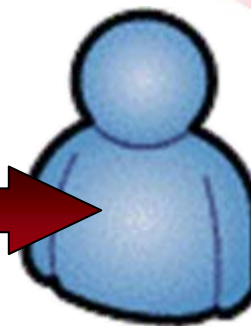
Conventional Identity  
(e.g. DN=CN=Phil Walston)



- Time of day
- Origin IP
- Attributes
- Remote authorization statements
- Different trust paths
- etc...

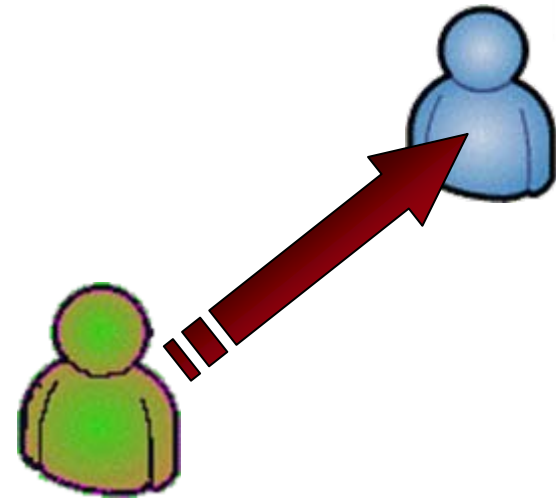


## Ephemeral identity



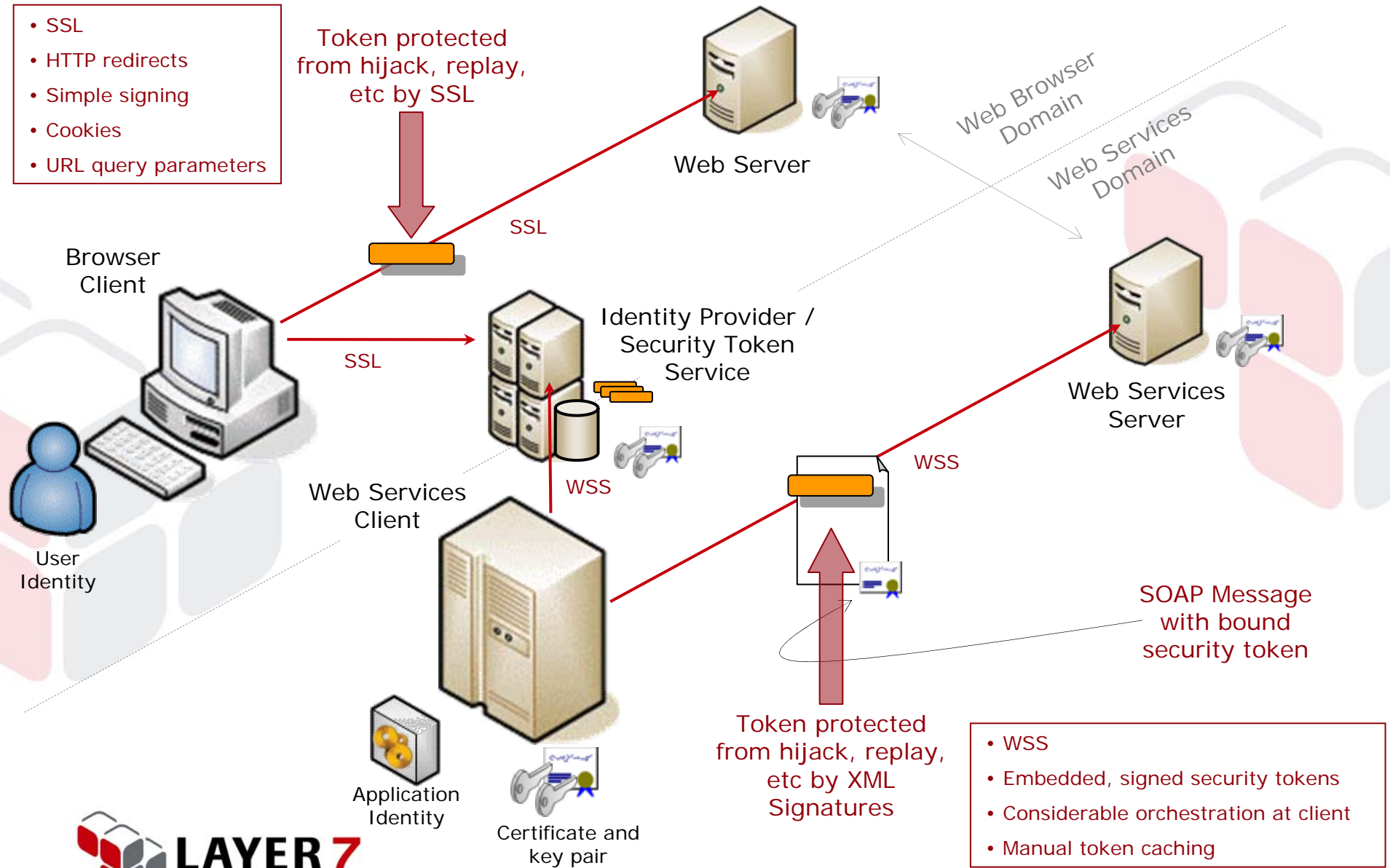
# Issue – Identity Mapping

- Fan in
  - E.g. to service account
- Map to local existing account
  - E.g. `phil.walston` -> `pwalston`
- Map to role
  - E.g. `TrustedAdministrator`
- Etc...

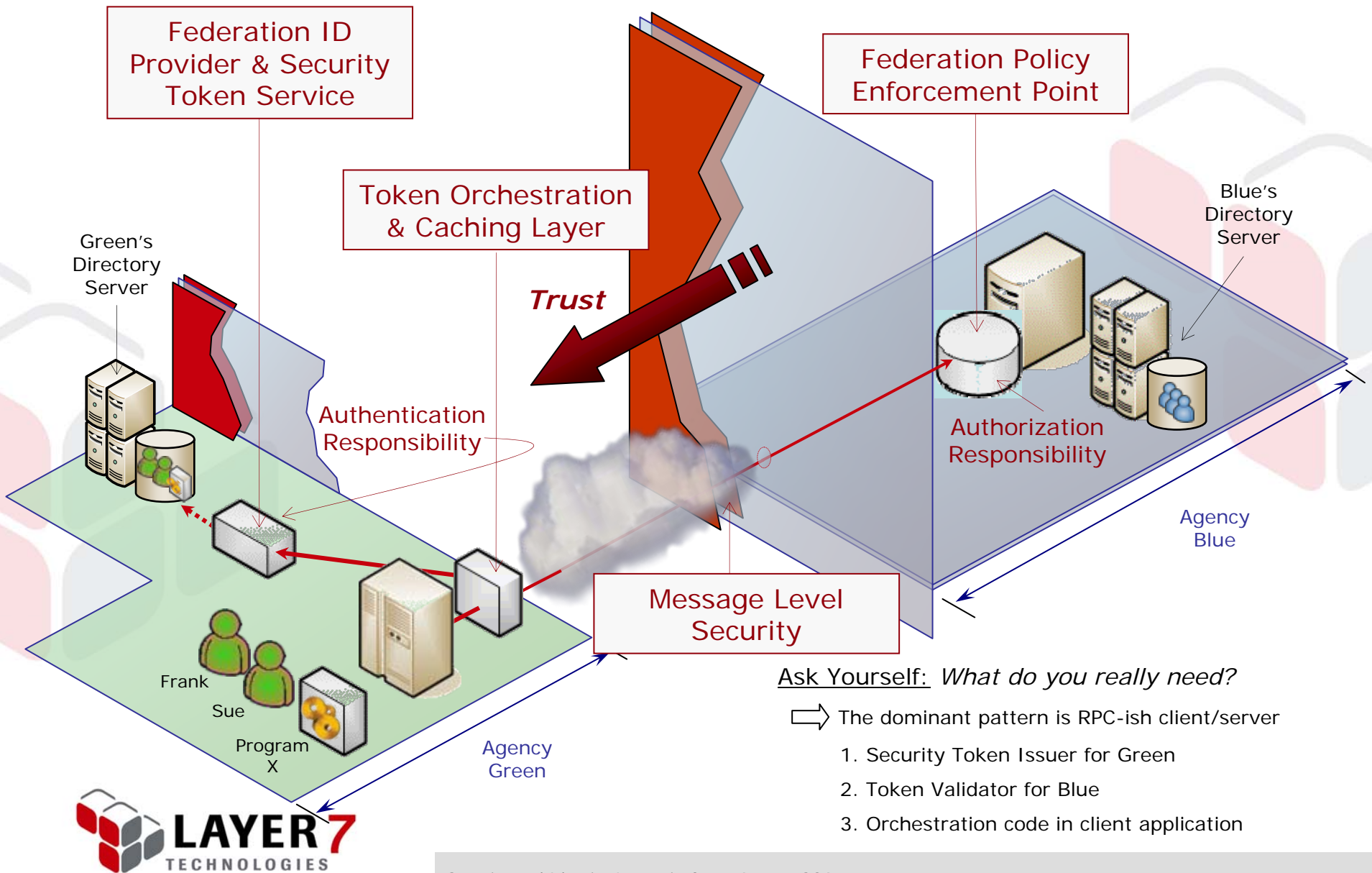


# Why is Federation/SSO of Web Services So Hard?

- SSL
- HTTP redirects
- Simple signing
- Cookies
- URL query parameters



# Tactical Strategy



# The Standards and Specifications Landscape

## ▪ Security

- Existing / emerging W3C and OASIS
  - ◆ SSL/TLS, XML Crypto/Sig, WSS, WS-SecureConversation, WS-SecurityPolicy ....

## ▪ Identity

- WS-Federation (Focus on technology)
  - ◆ IBM, Microsoft, BEA, RSA, Verisign
  - ◆ SAML, SSL/TLS, WSS, WS-Trust, WS-Policy, WS-MetadataExchange
- Liberty Alliance (Focus on business problem)
  - ◆ Consortium of over 150 companies
  - ◆ SAML, SSL/TLS, WSS
- Government
  - ◆ E-Authentication

# Conclusions

- Federation is simply SSO between different security domains
- The new issue for secure cross-agency (federated) SOA is resolving security and trust models for remote entities
- Security and federation for Web services have roots in distributed computing model, but are much more complicated
  - ◆ Variable security model
  - ◆ No automatic orchestration of client (redirects)
  - ◆ No formal client-side persistence model
- This all leads to much more independent clients and servers, different security mechanisms, and much more complex logistics
- Implementing secure federated Web services is extremely complex, and current support in application servers is very limited
- Third-party infrastructure, however, does exist to provide drop-in security and federation for Web services

For further information:

**Philip Walston**

Layer 7 Technologies

1501 – 700 West Georgia St.

Vancouver, BC

Canada

(800) 681-9377

[pwalston@layer7tech.com](mailto:pwalston@layer7tech.com)

<http://www.layer7tech.com>



May 2006

