A new Security Stack for modern Applications

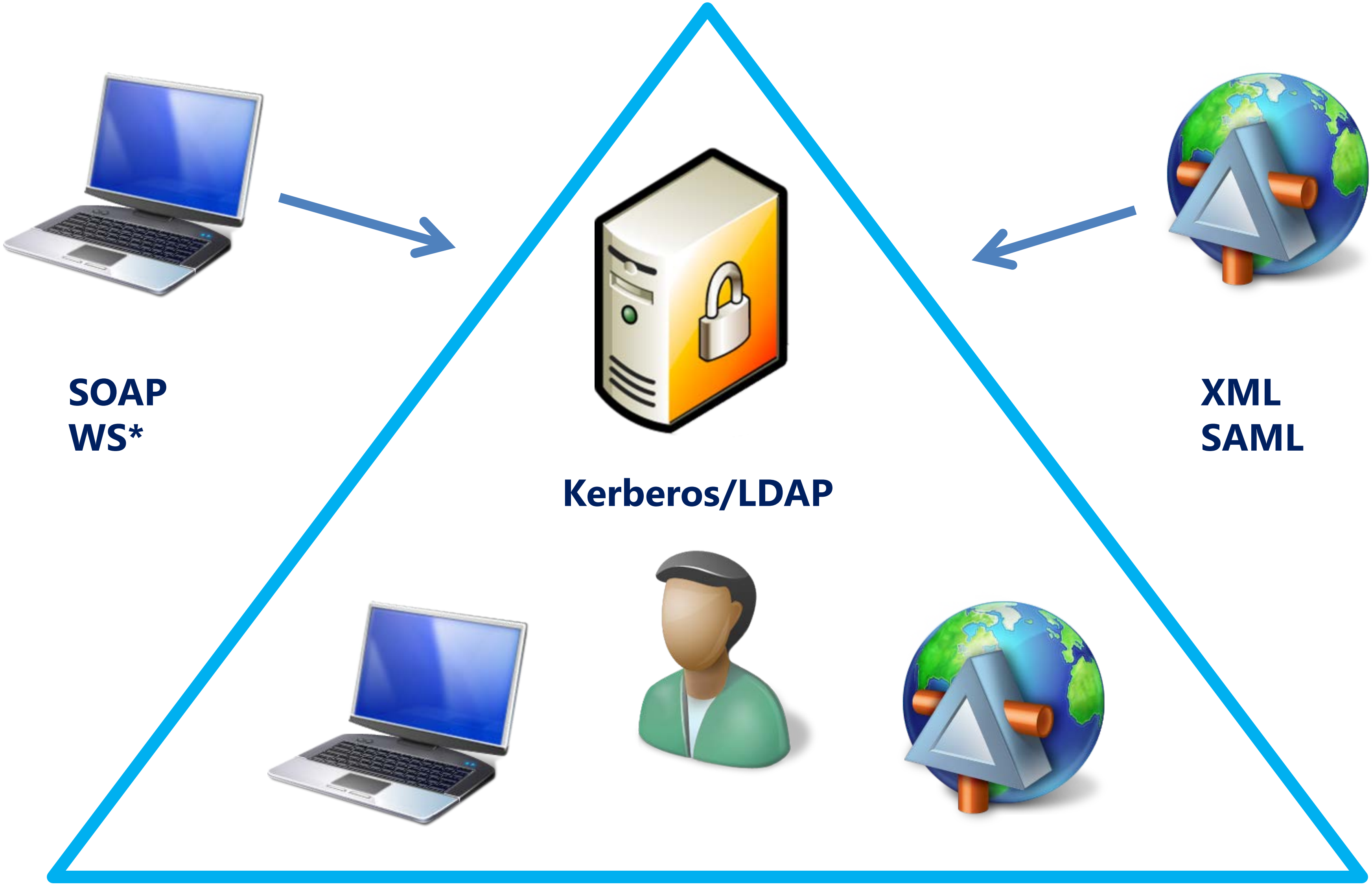
Dominick Baier

http://leastprivilege.com

@leastprivilege

pluralsight
hardcore developer training

Enterprise Security



SOAP
WS*

XML
SAML

Kerberos/LDAP

The mobile Revolution

No SOAP
No SAML
No WS*

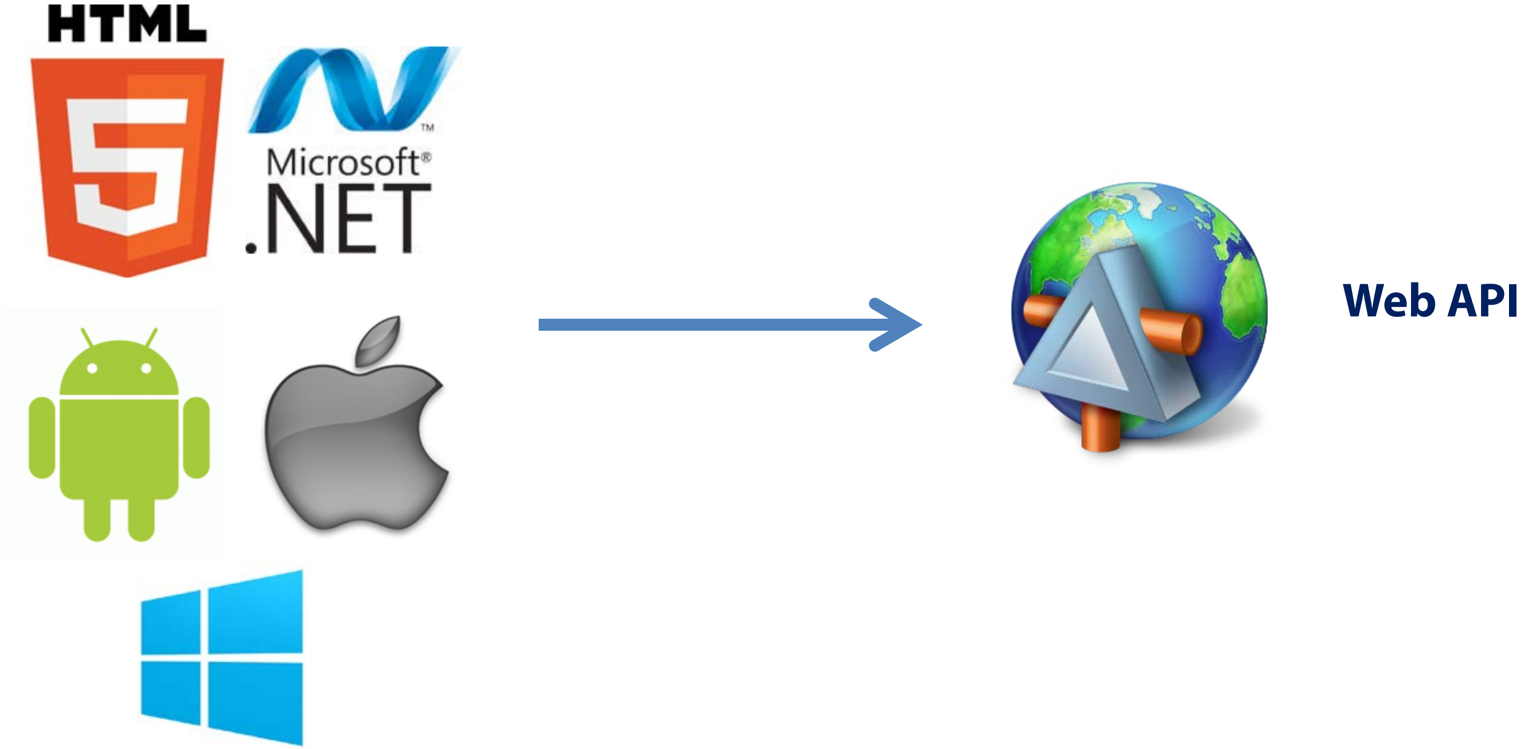
HTTP
JSON

Scenario 1: Mobile Enterprise Apps

AT&T 3G
9:42 AM
SMS
Text
Tuesday
9
Calendar
Photos
Camera
YouTube
Stocks
280
Maps
73°
Weather
Clock
Calculator
Notes
Settings
iTunes
App Store
Phone
Mail
Safari
iPod

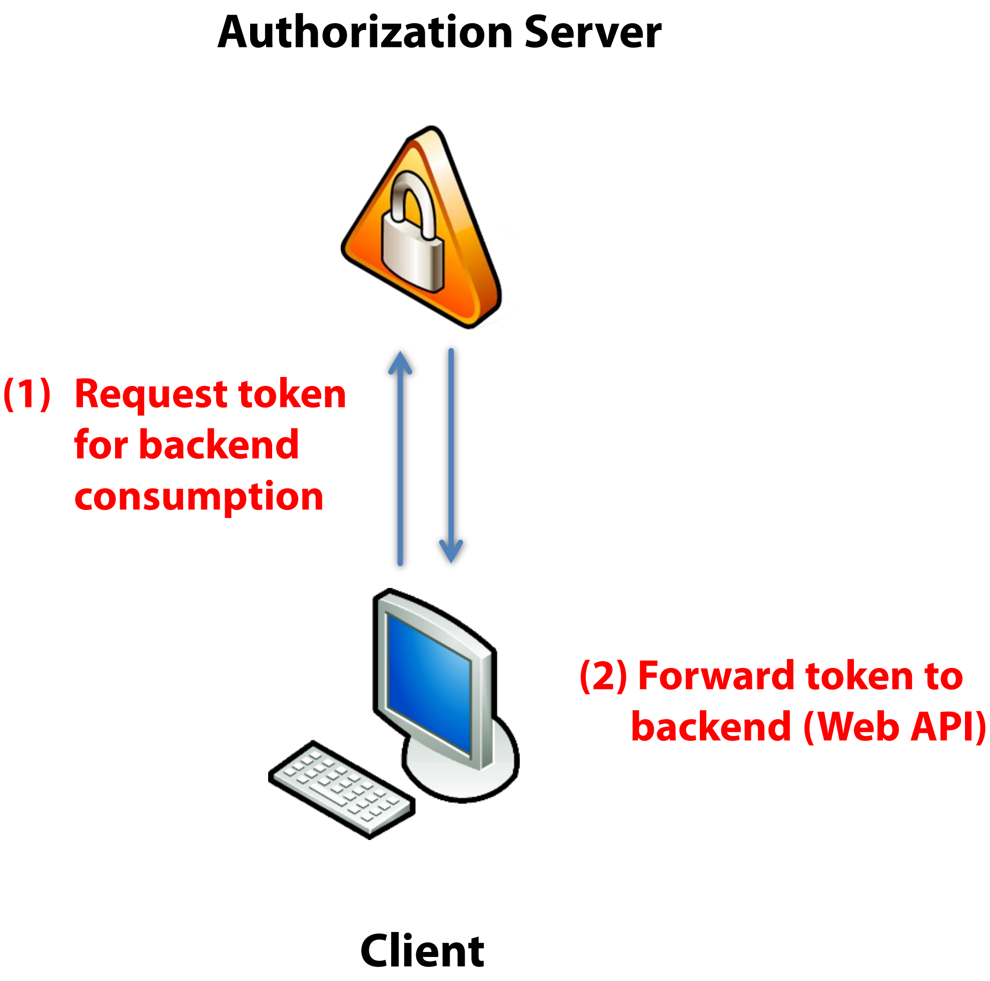
Scenario 2: Business to Customer

- Software vendors jump on the "apps bandwagon"
- Reach and cross-platform design becomes much more important



Web API

OAuth2



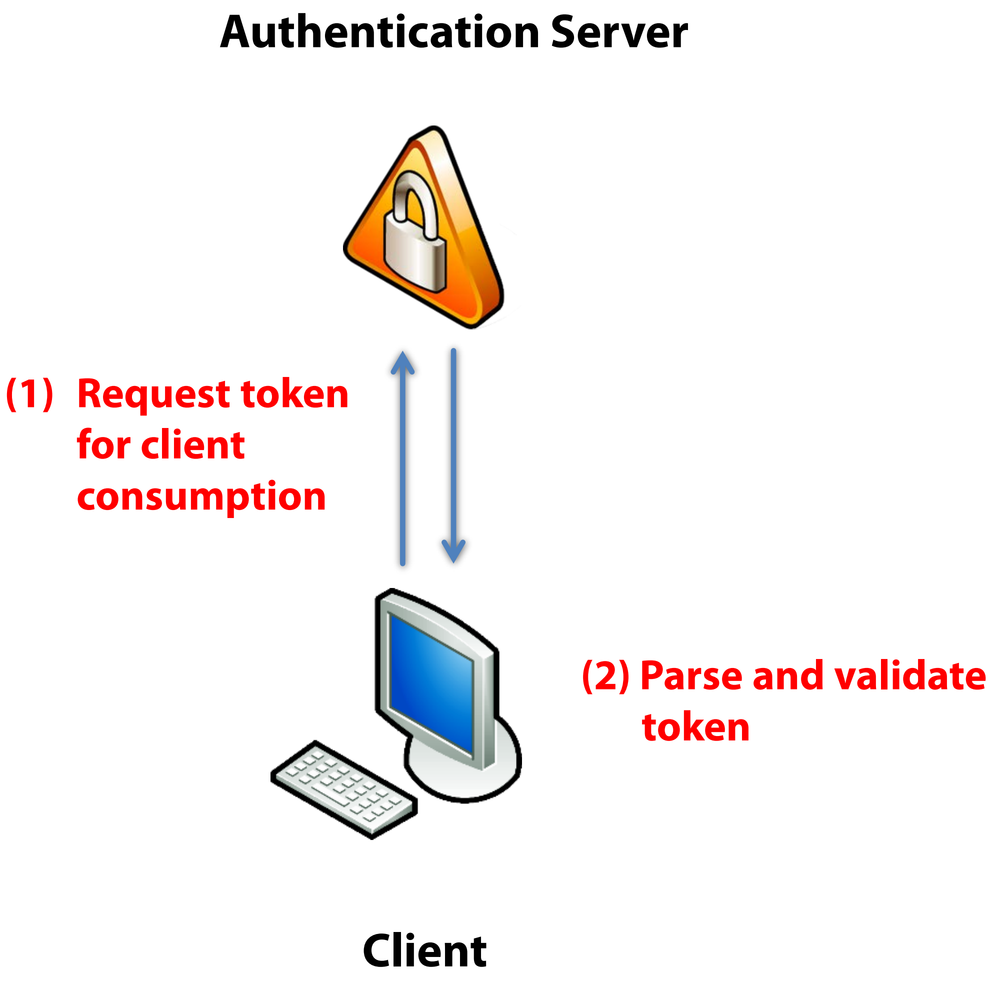
Authorization Server

(1) Request token for backend consumption

(2) Forward token to backend (Web API)

Client

OpenID Connect



Authentication Server

(1) Request token for client consumption

(2) Parse and validate token

Client

Summary

- **"Classic" security is intranet-only**
  - plus maybe special customer facing (web) applications in the DMZ
- **B2B federation using protocols like WS-Federation, SAML2p and WS-Trust**

- **Mobile devices are a game changer**
  - no "enterprise security" integration
  - less powerful
  - …but increasingly popular and business criticial
- **New "common denominator" technologies**
  - presentation (e.g. HTML5)
  - authentication & authorization