

# Virtualization + Cloud & Security

Mgr. Michael Grafnetter

Microsoft Services



# Agenda

- Virtualization Security Risks and Solutions
- Cloud Computing Security Risks
- Authentication in Cloud Applications



# Virtualization Security Risks and Solutions

Microsoft Services



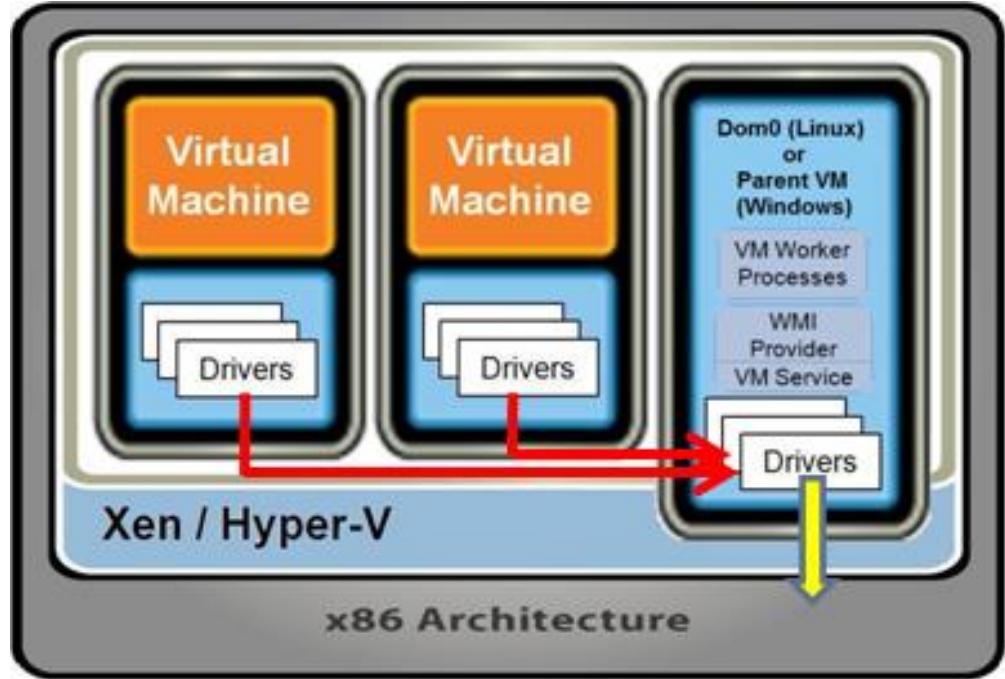
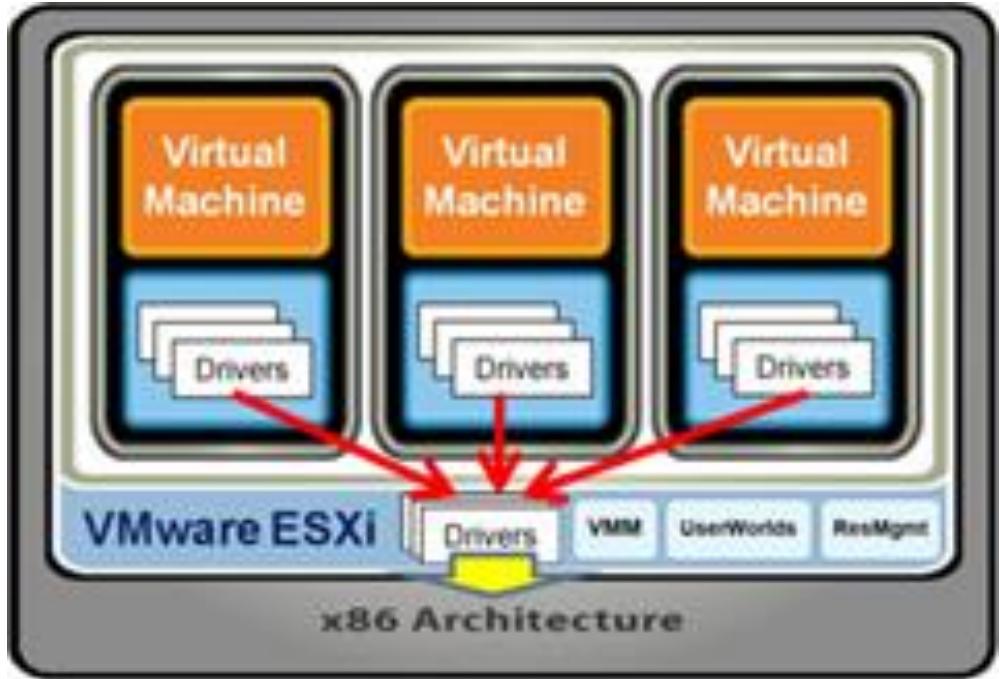
# Blue Pill Attack



# Blue Pill Attack

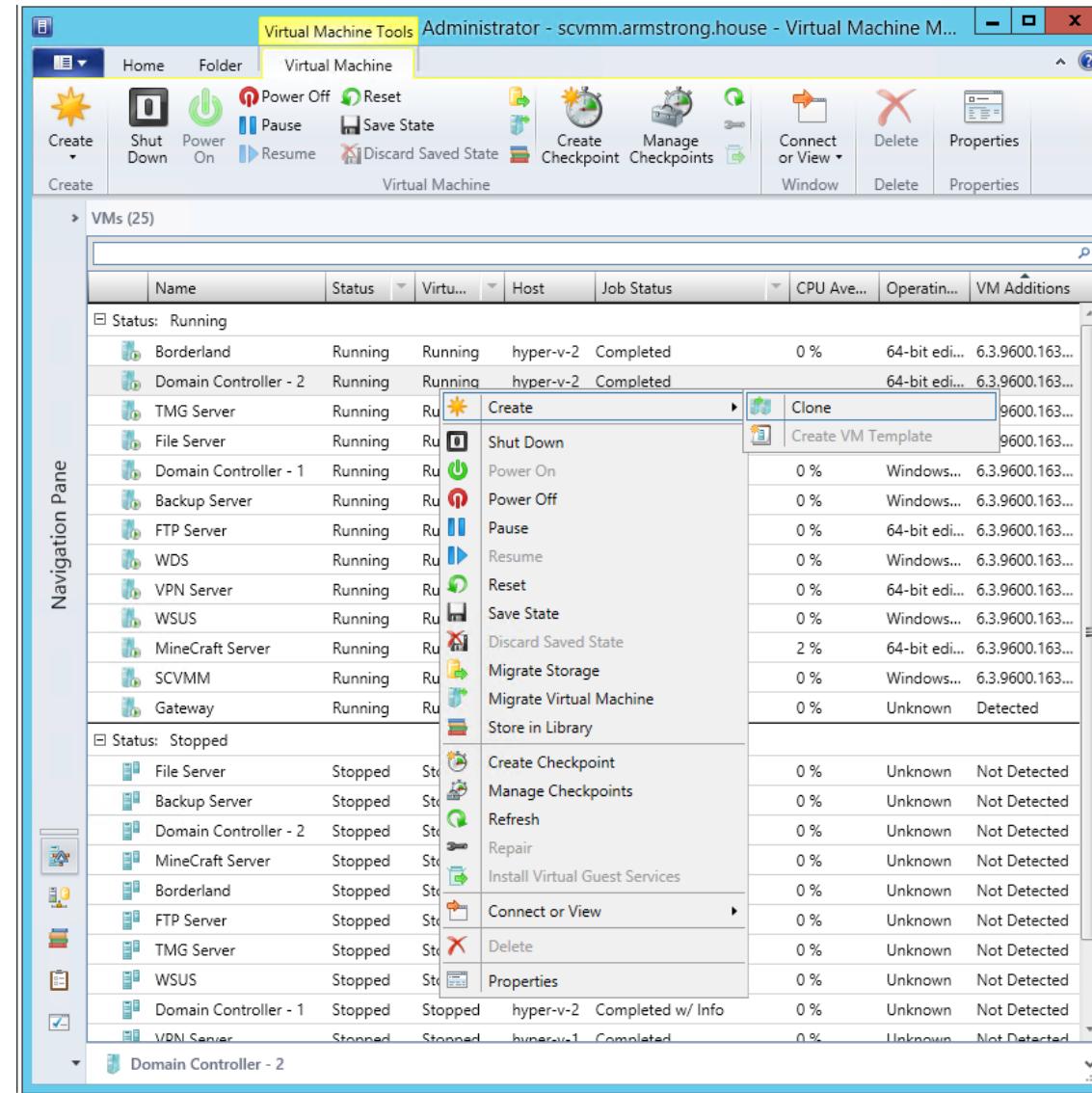
- Presented in 2006 by Joanna Rutkowska at Black Hat conference
- Traps running OS by starting a hypervisor and virtualizing the underlaying machine (needs right to run privileged instructions to achieve this)
- Could intercept nearly anything and send fake responses (hardware interrupts, requests for data, system time etc.)
- Detectable by timing attacks (Red Pill)
  - Trap-and-Emulate takes much longer than native instructions
  - External time sources (NTP) need to be used, because system time could be spoofed

# VMM Vulnerability



- By attacking a VMM, one could attack multiple servers at once

# Datacenter Management SW



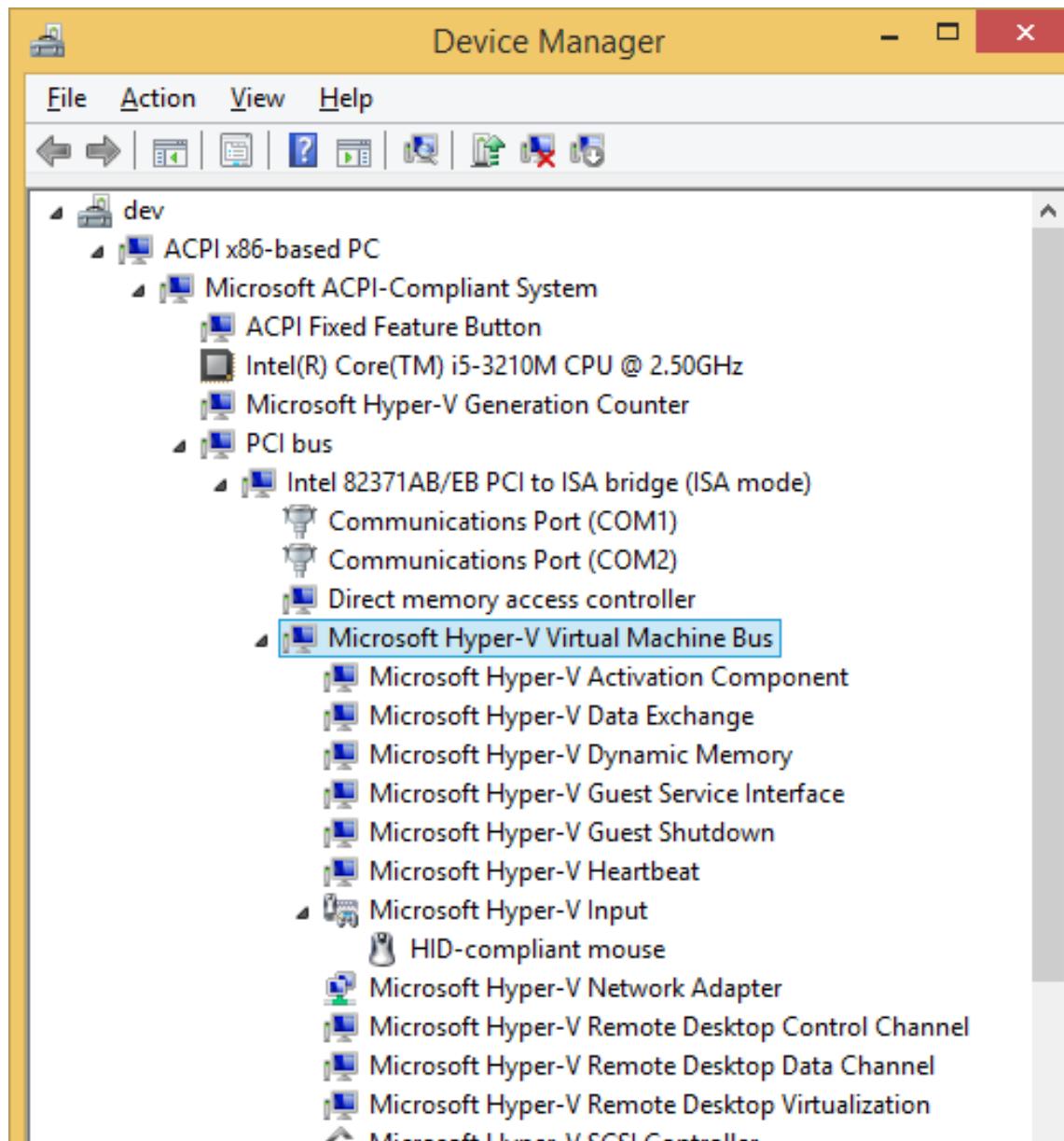
# Hypervisor Management + VM Bus

Management commands available using PowerShell or Web APIs

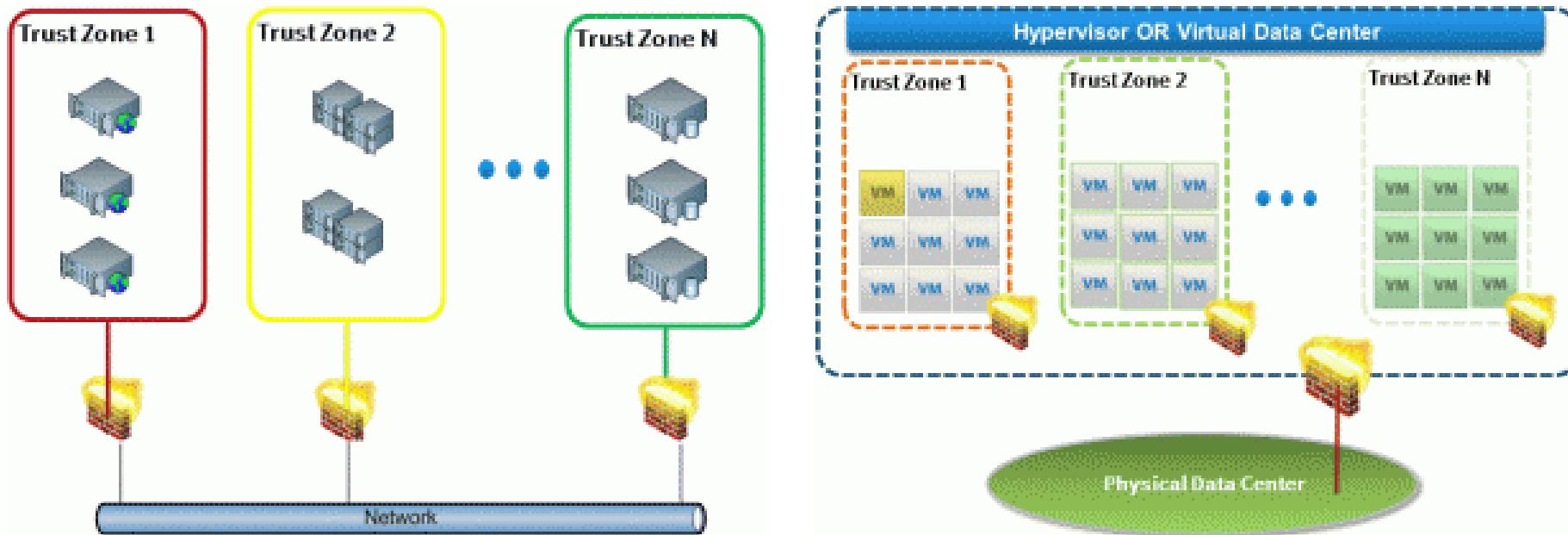
- Get-VM –Name \* | Stop-VM
- Get-VM –Name \* | Remove-VM
- Copy-VMGuestFile
- Invoke-VMScript –Type Bash
- ...



# VM Bus

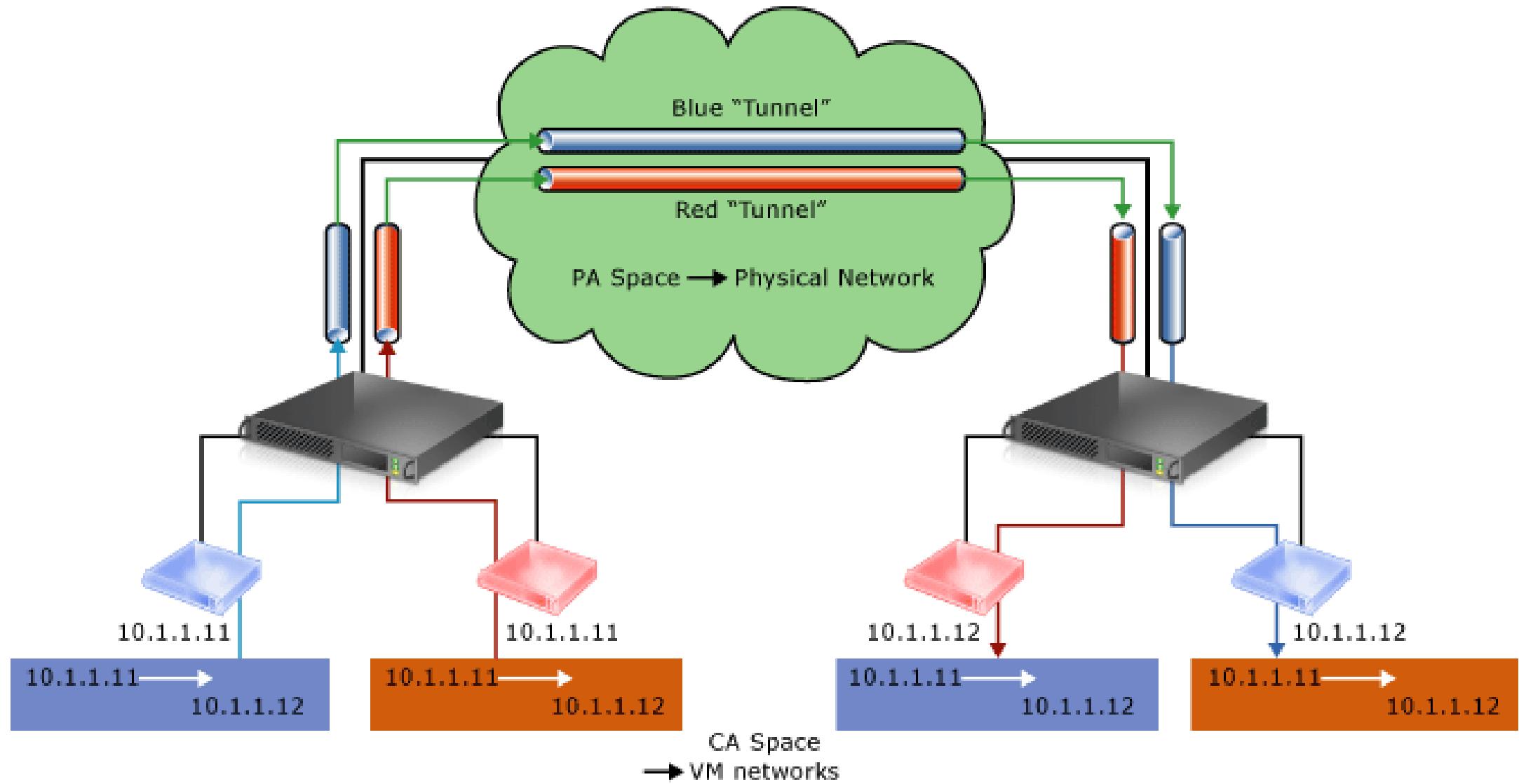


# Physical vs. Virtual Firewall

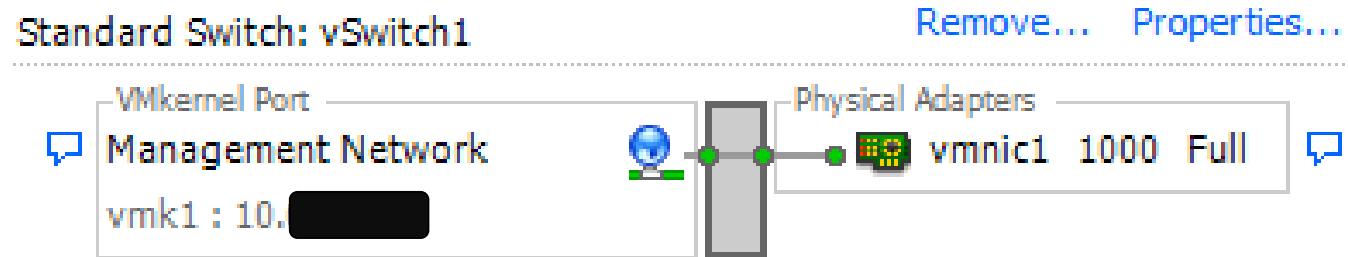
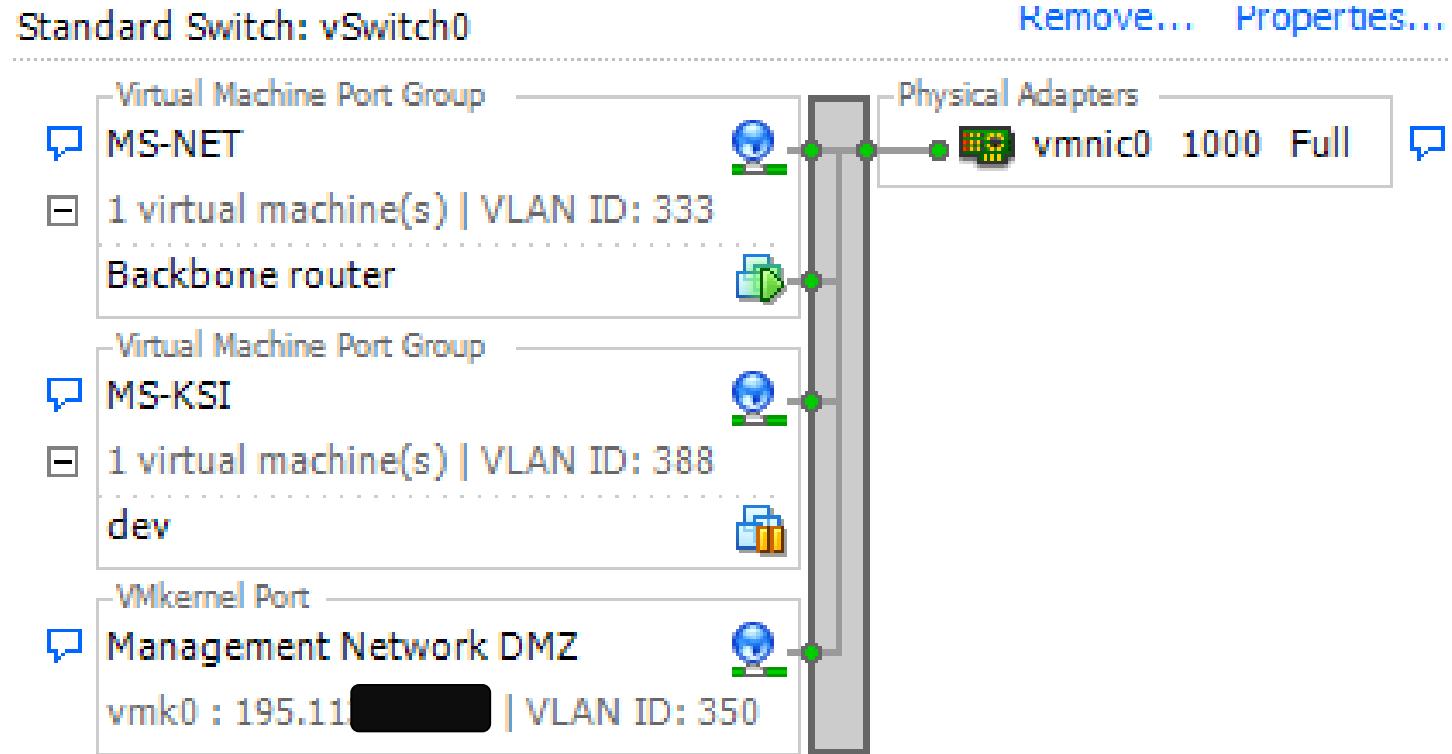


- With virtualization, servers from different Trust Zones usually share the same physical resources (memory, network card, etc.)

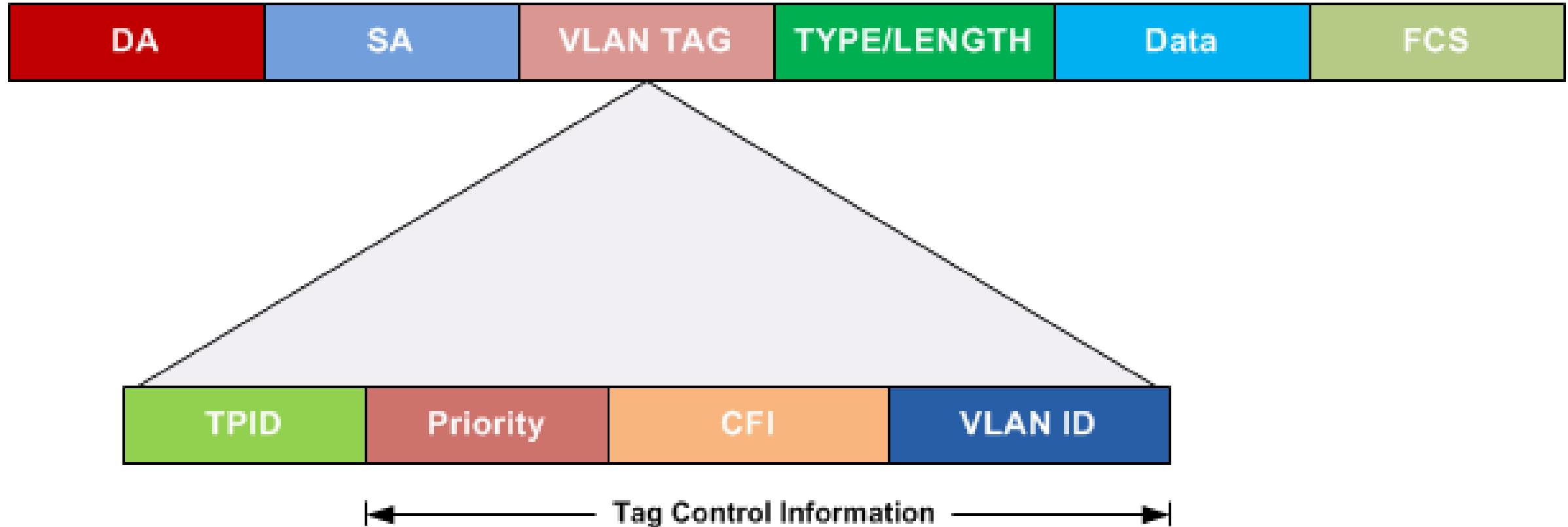
# Traffic Isolation



# Traffic Isolation – VLAN Tagging

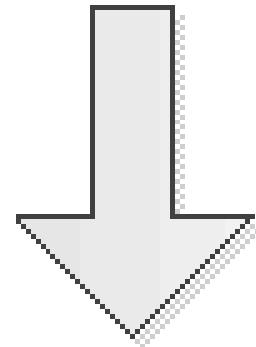


# Traffic Isolation – VLAN Tagging

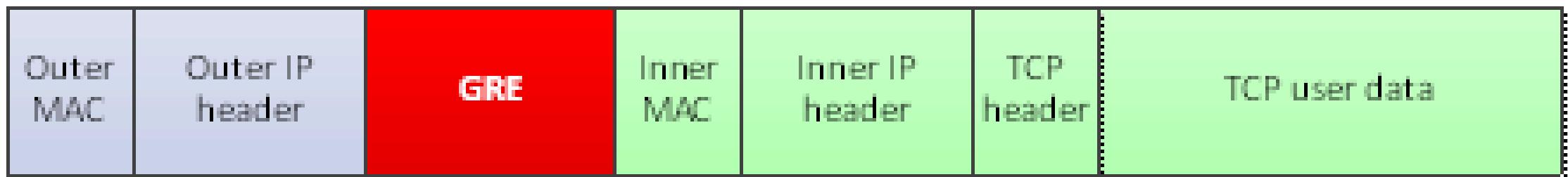


# Traffic Isolation - NVGRE

Original Packet



Packet with GRE encapsulation



# Traffic Monitoring

The screenshot shows the 'Network Adapter' settings for a virtual machine. The left pane lists various hardware components and management options. Under 'Management', the 'Name' is set to 'DEV'. The 'Integration Services' section indicates 'Some services offered'. The 'Checkpoints' section is set to 'Standard'. The 'Smart Paging File Location' is specified as 'C:\ProgramData\Microsoft\Win...' and the 'Automatic Start Action' is 'None'. The right pane displays detailed configuration for the network adapter. It includes sections for 'Enable router advertisement guard', 'Protected network' (with a checked checkbox), 'Port mirroring' (described as monitoring traffic by copying packets), and 'NIC Teaming'. A dropdown menu for 'Mirroring mode' is open, showing options: 'None' (selected), 'None', 'Destination', and 'Source'. Below the mirroring mode, there is a checkbox for enabling teaming in the guest OS. At the bottom, there are 'OK', 'Cancel', and 'Apply' buttons.

SCSI Controller

Network Adapter

- HV Wireless External
- Hardware Acceleration
- Advanced Features

COM 1

- None

COM 2

- None

Diskette Drive

- None

**Management**

Name: DEV

Integration Services: Some services offered

Checkpoints: Standard

Smart Paging File Location: C:\ProgramData\Microsoft\Win...

Automatic Start Action: None

Enable router advertisement guard

Protected network

Move this virtual machine to another cluster node if a network disconnection is detected.

Protected network

Port mirroring

Port mirroring allows the network traffic of a virtual machine to be monitored by copying incoming and outgoing packets and forwarding the copies to another virtual machine configured for monitoring.

Mirroring mode:

- None
- None
- Destination
- Source

NIC Teaming

You can establish NIC Teaming in the guest operating system to aggregate bandwidth and provide redundancy. This is useful if teaming is not configured in the management operating system.

Enable this network adapter to be part of a team in the guest operating system

When this option is cleared, a team created in the guest operating system will

OK Cancel Apply

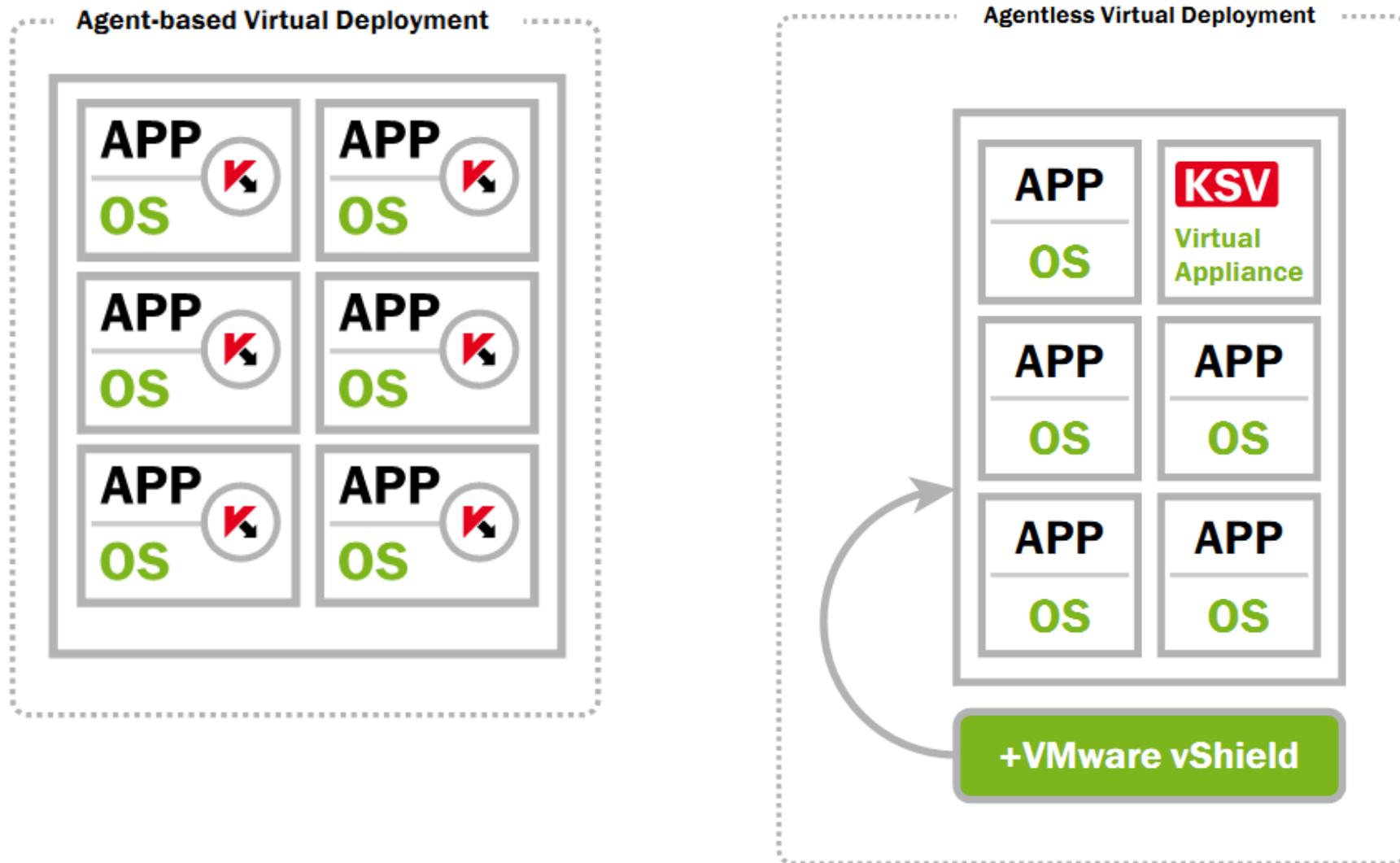
# Other risks of virtualization

- Introduction of yet another OS
- Reliance on traditional barriers
- Accelerated provisioning
- Security left to non-traditional security staff
- Audit scope creep

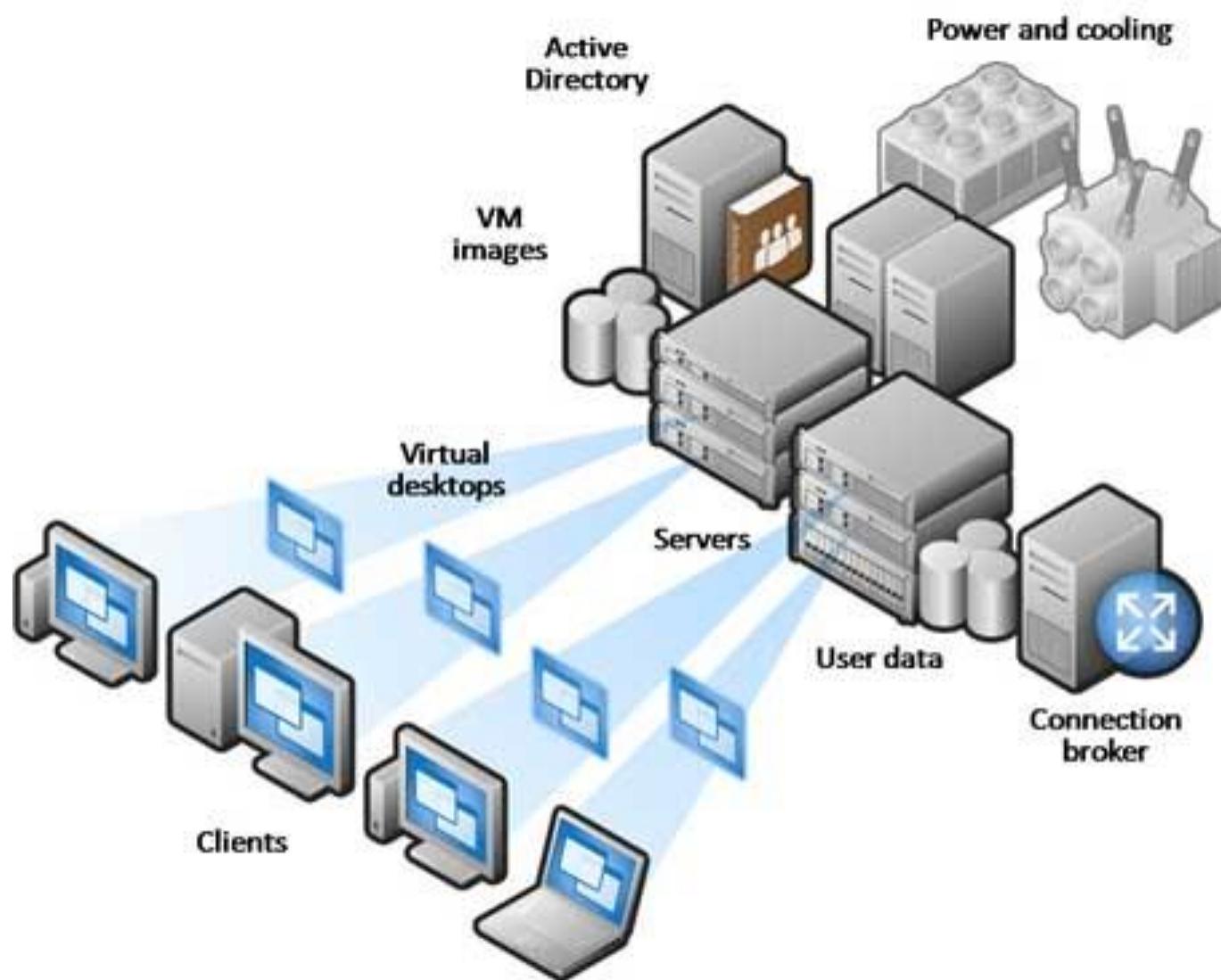
# Security Solutions

- Virtual Firewall
  - Live migration
  - Stretched clusters
- Agentless Antivirus
- Extensible Switches
- Mobile Virtualization Platform
- Virtual Desktop Infrastructure (VDI)

# Agentless AV



# Virtual Desktop Infrastructure



# Windows 10 Virtual Secure Mode: Motivation

```
Authentication Id : 0 ; 2594251 <00000000:002795cb>
Session          : Service from 0
User Name        : svc-SQLAnalysis
Domain          : ADSECLAB
SID              : S-1-5-21-1473643419-774954089-2222329127-1608

msv :
    10000000021 PwHash
        * Username : svc-SQLAnalysis
        * Domain  : ADSECLAB
        * NTLM     : 3c917b61c58c4cba165396aad7d140a2
        * SHA1     : f089edb437e1f455ac1ab65886ed51959df7dc30

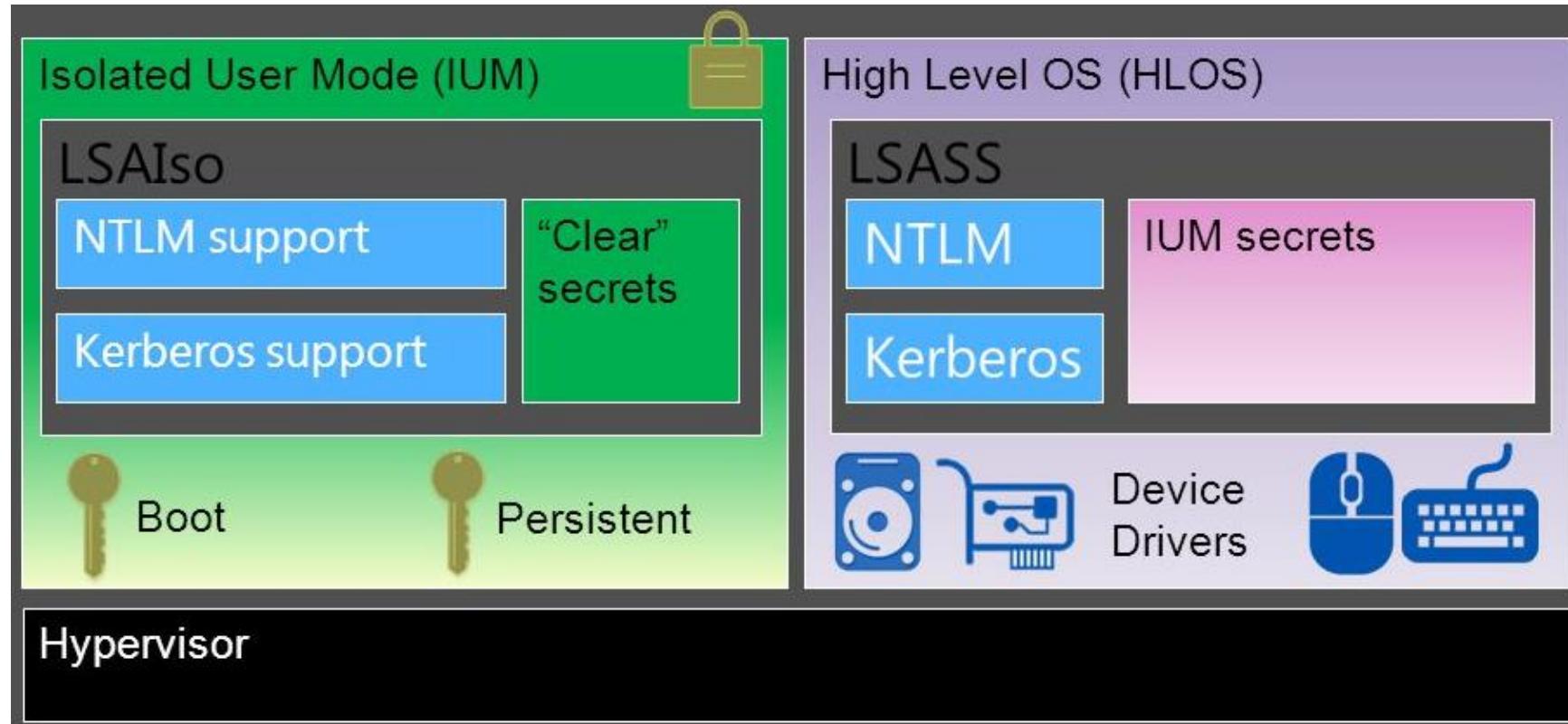
tspkg :
    * Username : svc-SQLAnalysis
    * Domain  : ADSECLAB
    * Password : ThisIsAnOKPassword99!

wdigest :
    * Username : svc-SQLAnalysis
    * Domain  : ADSECLAB
    * Password : ThisIsAnOKPassword99!

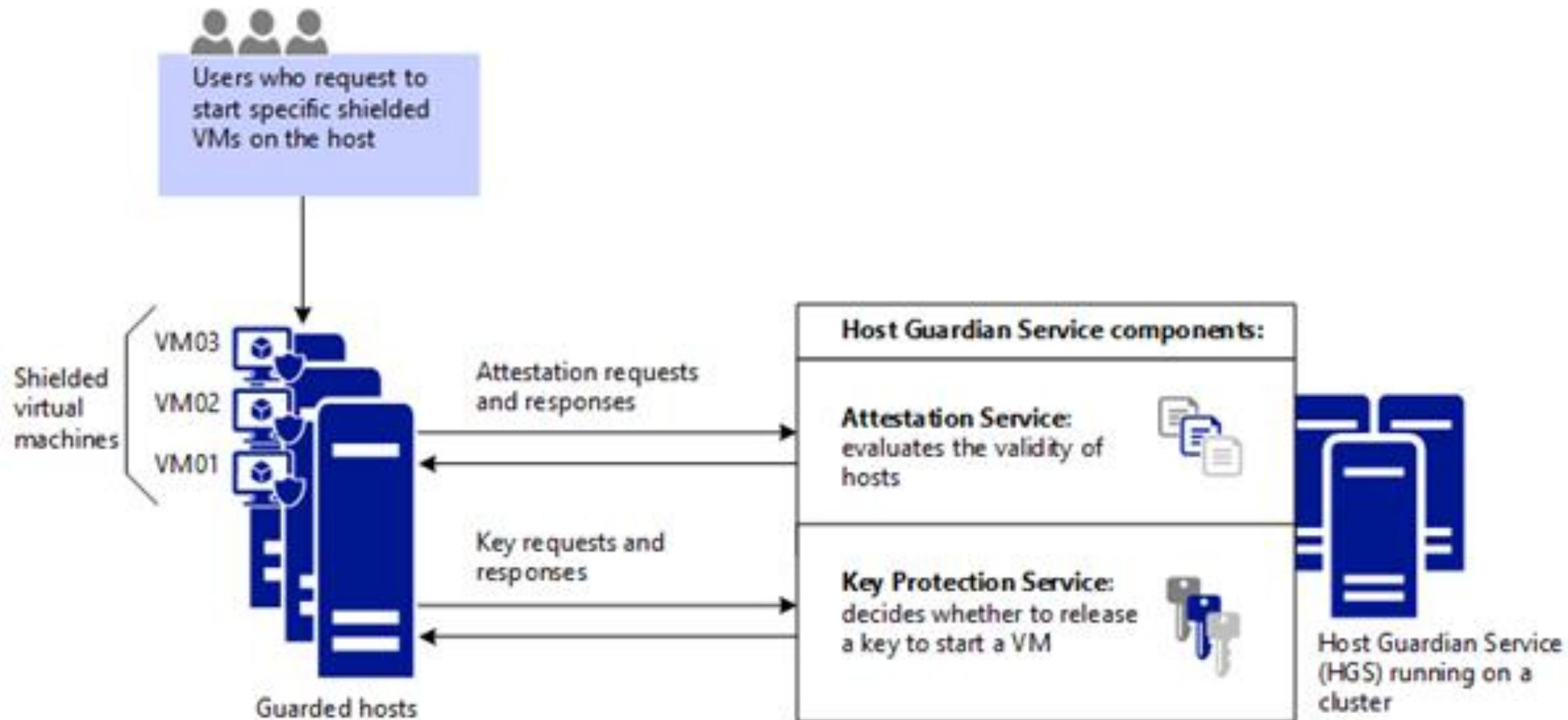
kerberos :
    * Username : svc-SQLAnalysis
    * Domain  : LAB.ADSECURITY.ORG
    * Password : ThisIsAnOKPassword99!

ssp :
credman :
```

# Windows 10 Virtual Secure Mode



# Shielded VMs





# Cloud Computing Security Risks

Microsoft Services



# Who has access to our data?



# Azure Datacenter Security

- 24 hour monitored  
**PHYSICAL SECURITY**

- Centralized  
**MONITORING AND ALERTS**

- Update  
**MANAGEMENT**

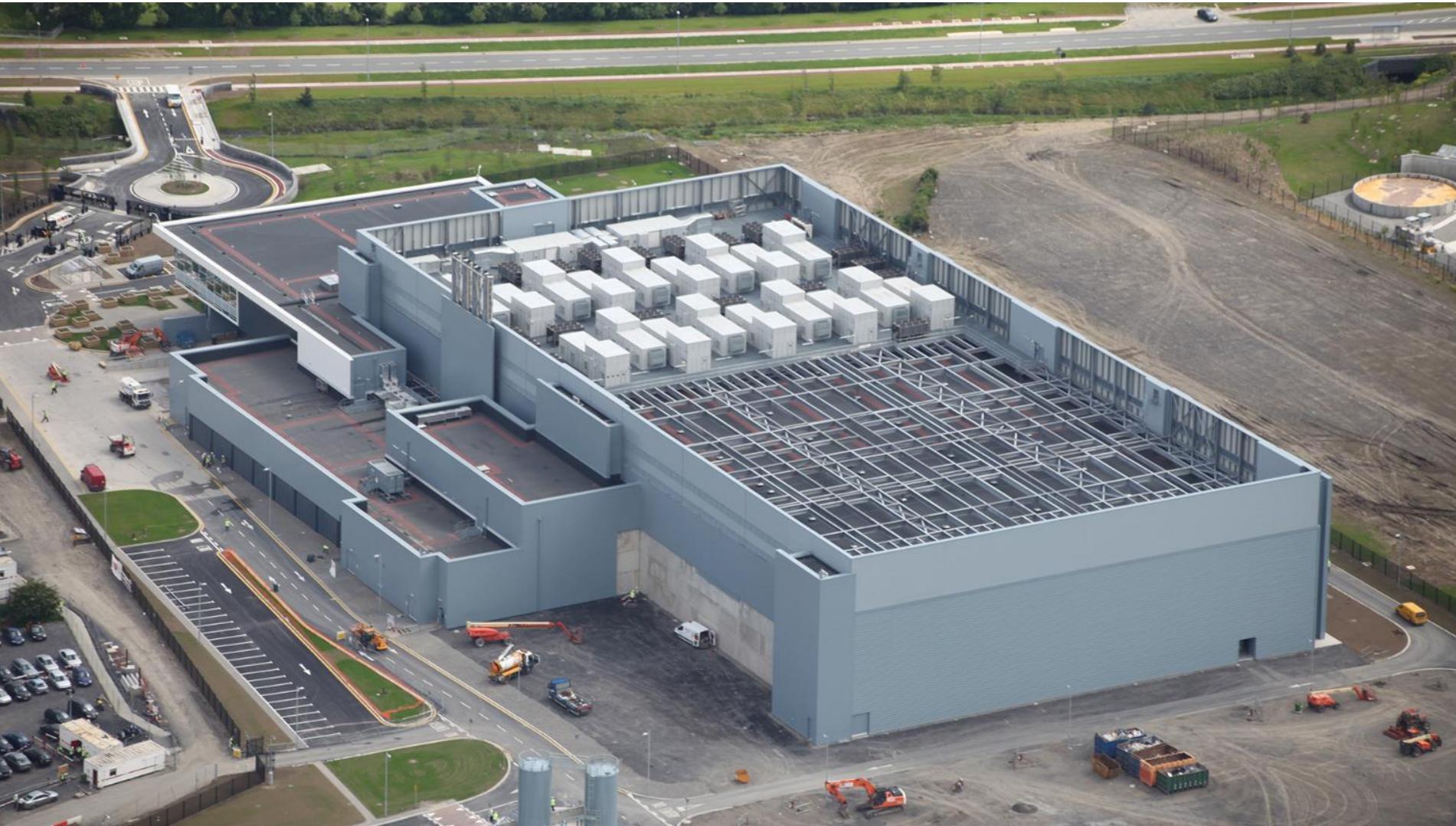


- Anti-Virus/Anti-Malware  
**PROTECTION**

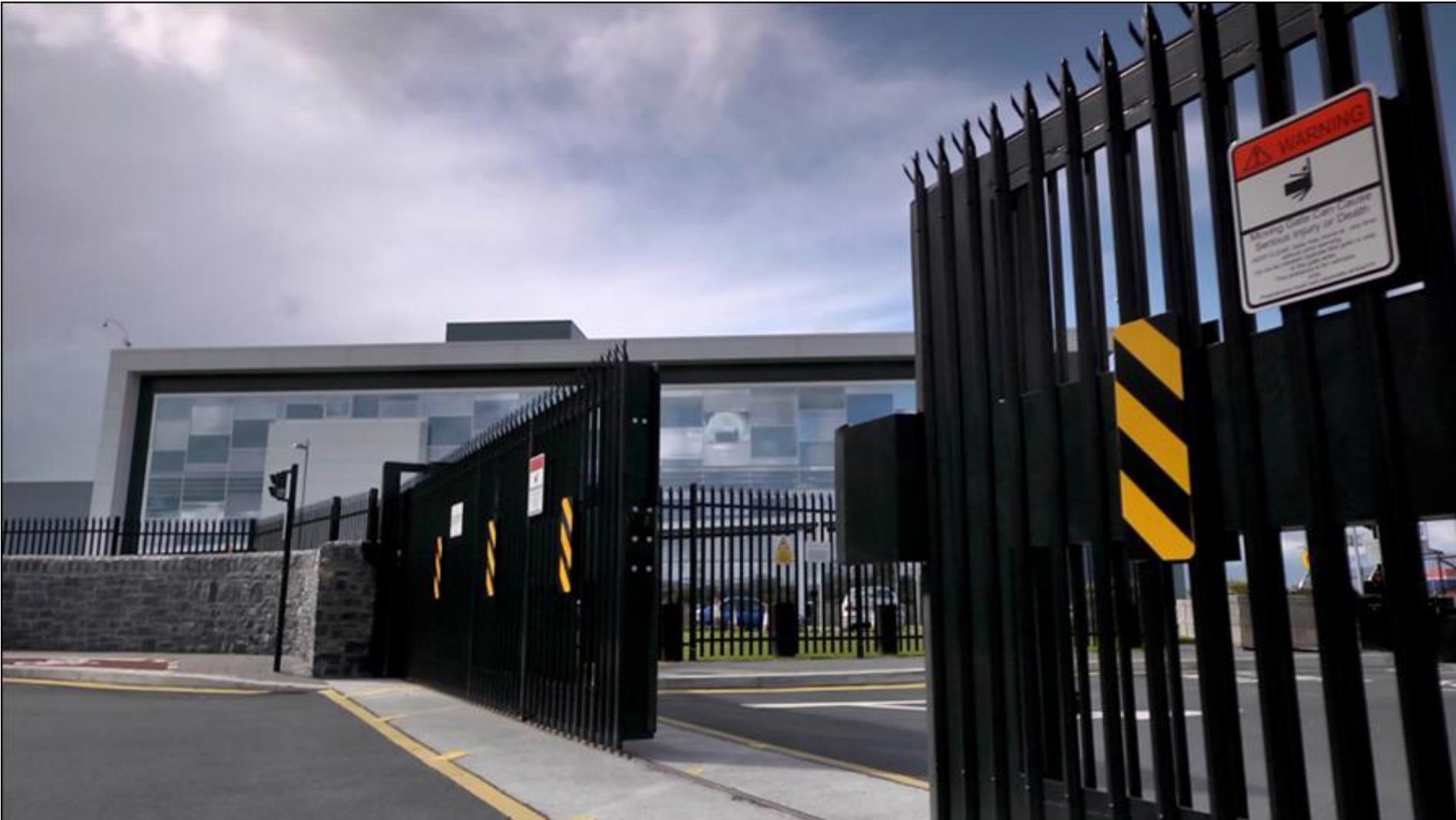
- Penetration **TESTING**

- DDoS **DEFENSE**

# Physical Security



# Physical Security



# Physical Security



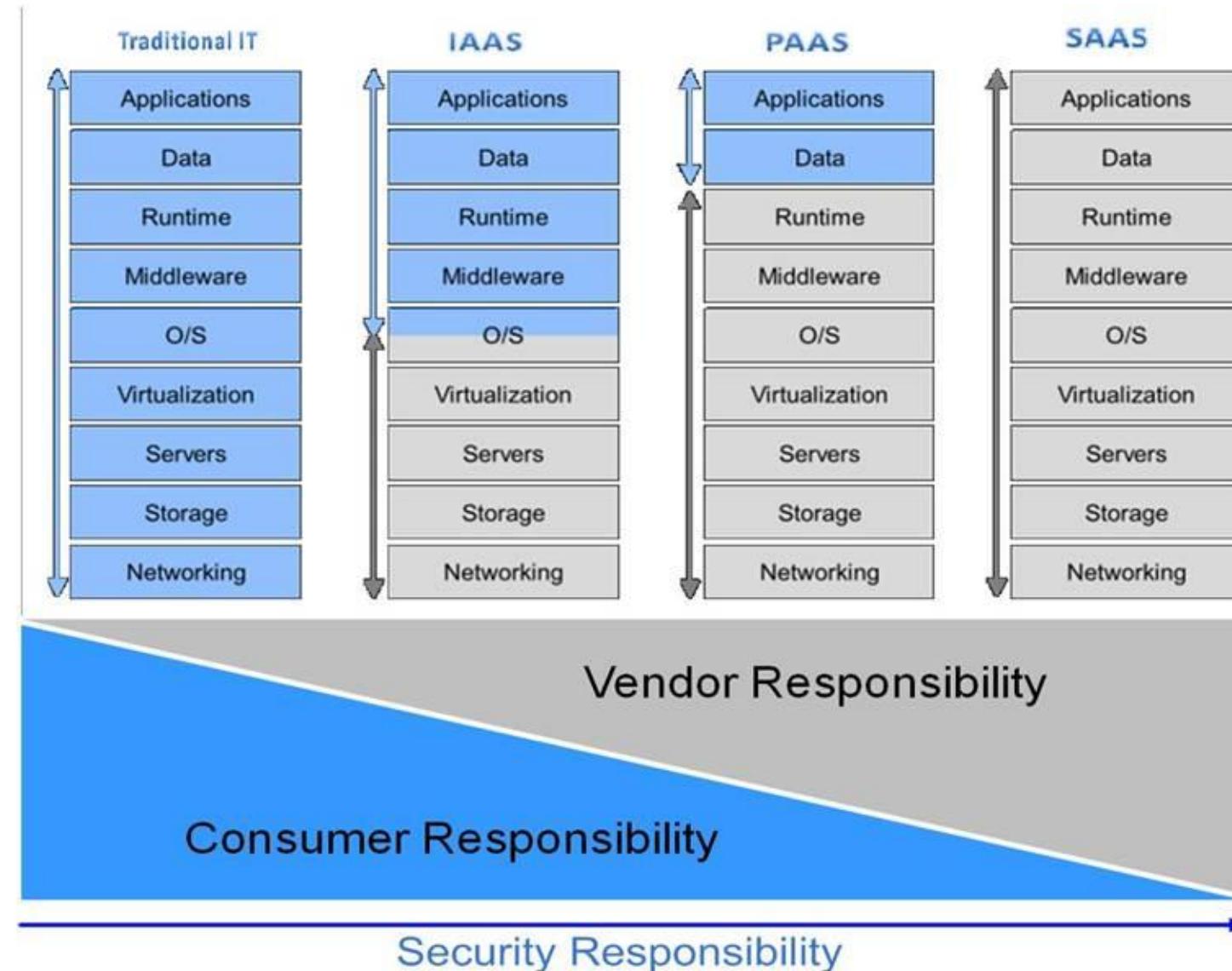
# Physical Security



# Hard Disk Crushers



# Shared Responsibility



# Custom Penetration Testing

**Penetration Test Approval Form**

**Client Testing Request**

---

**Request Details**

Azure portal login email

Subscription id  
 00000000-0000-0000-0000-000000000000

Contact name

Contact email address

Contact phone number

test being performed by third party  
 test end date  
 09/21/2016

Requested end date  
 09/28/2016

Detailed description of test

Listing of IP addresses and bNG names from where the tests will originate

---

**Tested Resources**

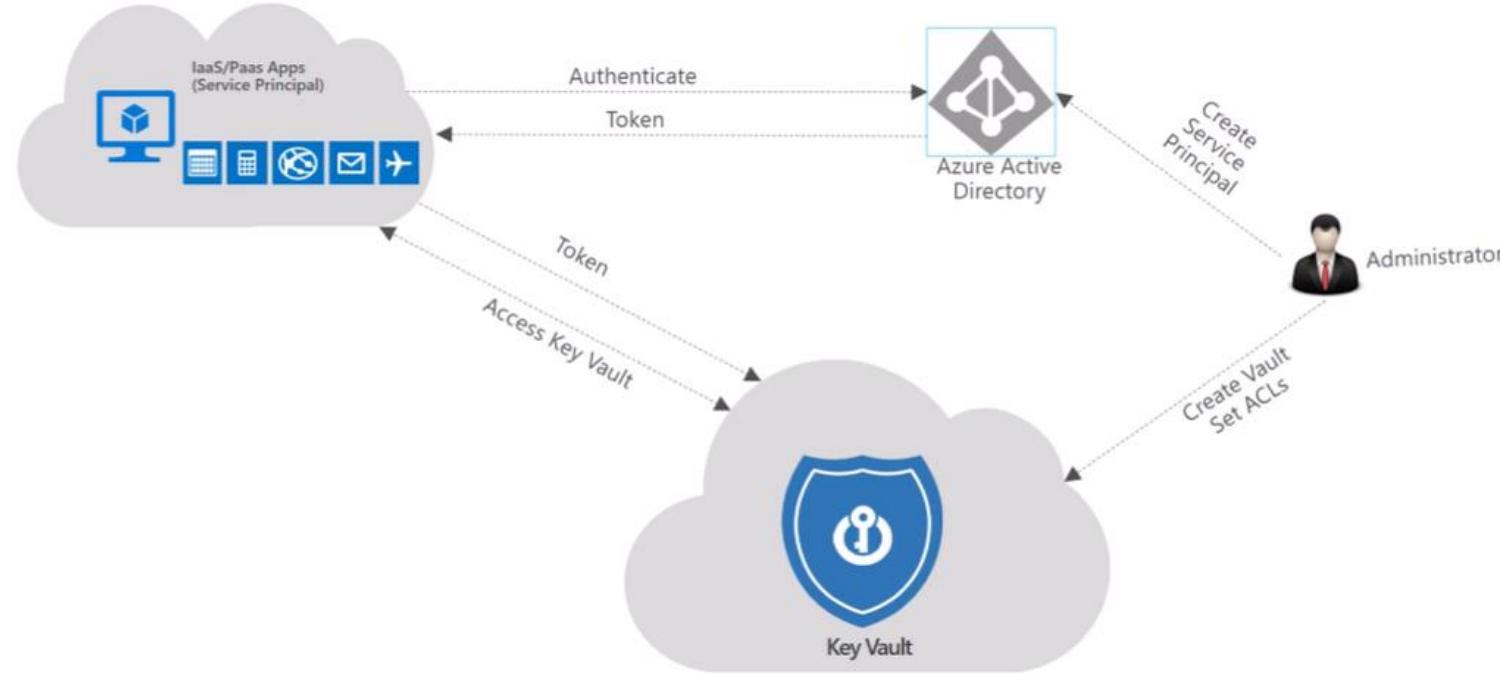
Resource type	Azure bNG name of resource	Description of test performed on resource	Tooling or utilities to be used on resource
Web	<input type="text"/>	<input type="text"/>	<input type="text"/>
<b>Add Resource</b>			

---

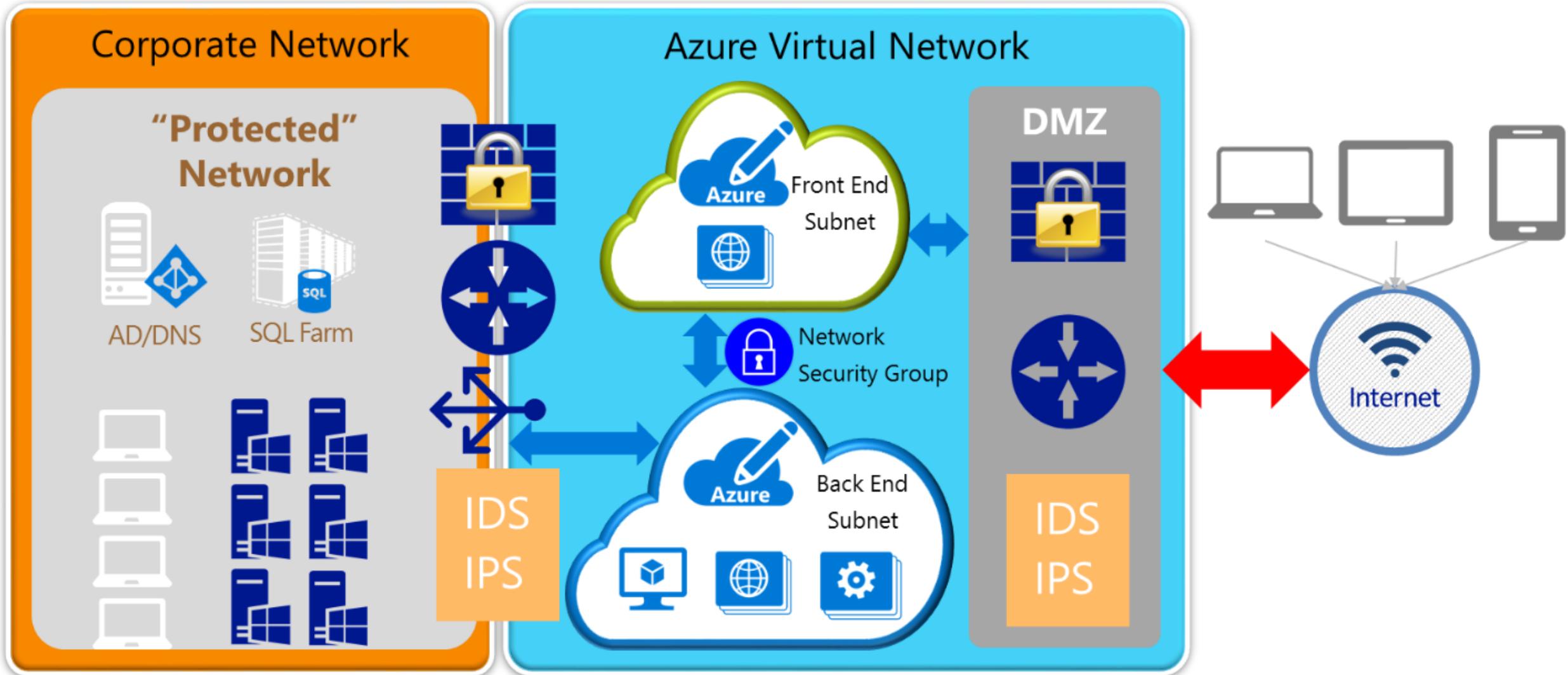
test only includes the standard tests described  
 agree the terms and conditions  
 not perform any of the prohibited tests

**Submit Request**

# Azure Key Vault



# Hybrid Network Topology



# Shadow IT – Anyone can use DropBox, GitHub,etc.

The screenshot shows a web-based dashboard titled "Cloud App Discovery". At the top, there's a navigation bar with links for "Dashboard", "Logout", and user information. Below the title, it says "last 30 days • business cloud apps •". A breadcrumb trail shows "dashboard > apps". On the left, there's a circular donut chart labeled "categories" with a legend listing 15 categories: Mail, Content Management, Collaboration, Developer Services, Social, Security, Project Management, Marketing, CRM, Telecommunications, Finance, HR, Productivity, E-commerce, and IT Infrastructure. The chart segments are colored blue, green, yellow, and grey. To the right of the chart is a 4x6 grid of application icons. The icons include Office 365 Exchange Online, Office 365 SharePoint Online, Dropbox, msdn, AddThis, New Relic, Symantec Trust Center, Orgatec, DigiCert, Yammer, GlobalLogic, Enterprise Security Center, Sogou, bazaarvoice, GitHub, Amazon Web Services (AWS), Cloudflare, Imaginsoft, Salesforce, Drupa, intuit, SurveyMonkey, sf, CodePen, and several other partially visible icons like a red 'a', a blue 'G', a pink 'm', a blue 'box', a blue 'n', and a blue 'Q'.

# Regulatory compliance - EU



CDSA



CSA CCM



ENISA IAF



EU Model Clauses



ISO/IEC 27001



ISO/IEC 27018



MPAA



PCI-DSS



SHARED ASSESSMENTS



SOC 1



SOC 2



SOC 3

# Regulatory compliance – Czech Republic

- Zákon č. 101/2000 Sb., o ochraně osobních údajů  
(Písemné vyjádření předsedy ÚOOÚ)
- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti...  
(přes ISO 27001)
- Zákon č. 365/2000 Sb., o informačních systémech veřejné správy  
(přes ISO 27001)
- Smluvní dodatek pro subjekty podléhající regulaci ČNB

# General Data Protection Regulation

- Approved by the EU Parliament in **April 2016**.
- Designed to harmonize data privacy laws across Europe.
- Direct effect in EU member states & local implementation measures.
- Enforcement date: **25 May 2018**.
- Replaces the Data Protection Directive 95/46/EC.



# Key changes addressed in the GDPR

## Personal privacy

Individuals have the right to:

- Access their personal data
- Correct errors in their personal data
- Erase their personal data
- Object to processing of their personal data
- Export personal data

## Controls and notifications

Organizations will need to:

- Protect personal data using appropriate security
- Notify authorities of personal data breaches
- Obtain appropriate consents for processing data
- Keep records detailing data processing

## Transparent policies

Organizations are required to:

- Provide clear notice of data collection
- Outline processing purposes and use cases
- Define data retention and deletion policies

## IT and training

Organizations will need to:

- Train privacy personnel & employees
- Audit and update data policies
- Employ a Data Protection Officer (if required)
- Create & manage compliant vendor contracts

# Penalties under GDPR

## Article 83: General conditions for imposing administrative fines.

€20,000,000 or 4% of total worldwide annual turnover in the preceding financial year (whichever is higher).

### Articles

e.g.

5: Principles relating to the processing of personal data

6: Lawfulness of processing

7: Conditions for consent

9: Processing special categories of personal data (i.e. sensitive personal data)

12 – 22: Data subject rights

44 – 49: Transfers to third countries

58: Supervisory Authorities

€10,000,000 or 2% of total worldwide annual turnover in the preceding financial year (whichever is greater).

### Articles

e.g.

8: Child's consent

25: Data protection by design and by default

26: Joint controllers

27: Representatives of controllers not established in EU

26 – 29 and 30: Processing

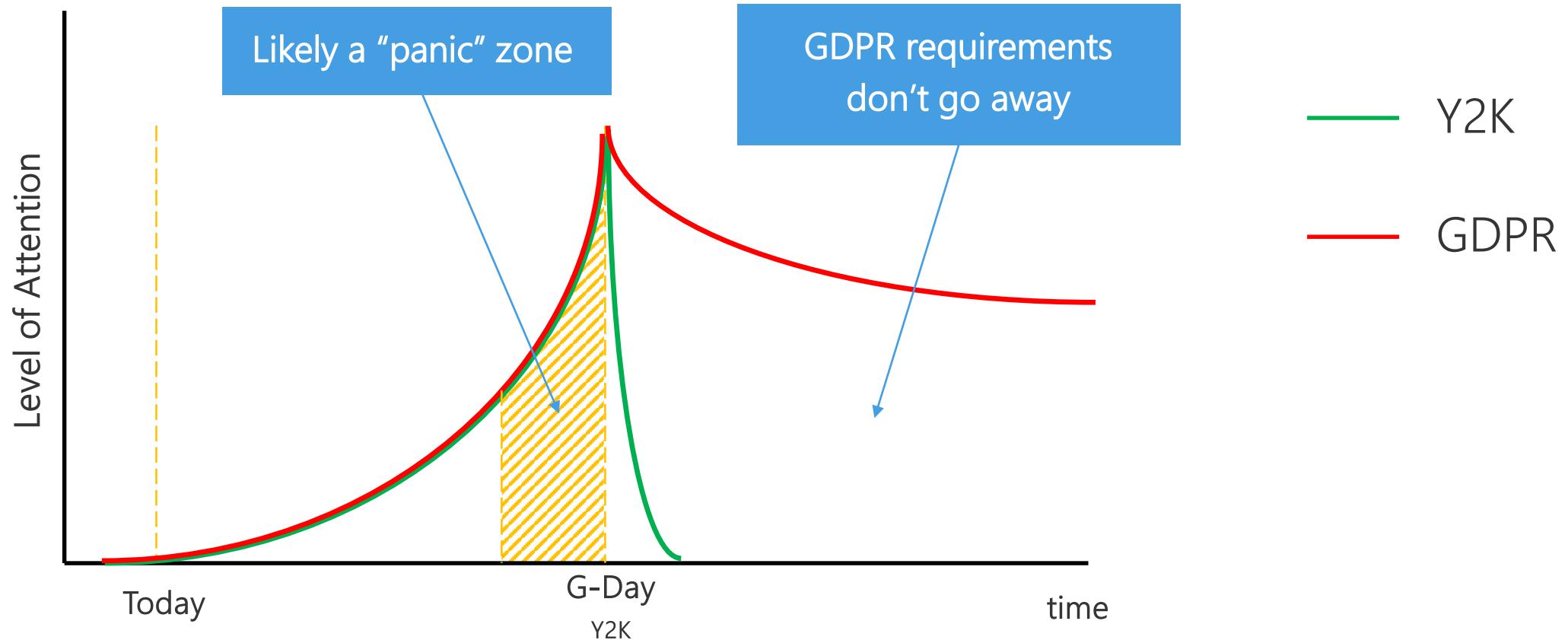
33 & 34: Notification of breaches

35 & 35: Data protection impact assessment & prior consultation

37 – 39: DPOs

# GDPR & Year 2000 – similar, not identical

26 million EU organizations effected



# Other Cloud Risks

- Unclear data location
- Data segregation
- Lack of investigative support
- Disaster recovery
- Long-term viability, vendor lock-in



# Authentication in Cloud Applications

Microsoft Services



# Authentication

- Basic Concepts
  - Two-factor authentication
  - OTPs
- Identity Federation
  - OAuth
  - OpenID
  - OpenID Connect
  - SAML
  - RADIUS Proxy
  - Identity Bridges

# Multi-Factor Authentication



# One-time Passwords

- HMAC-based One-time Password (HOTP)
- Time-based One-time Password (TOTP)
- Out-of-Band TANs
  - Pre-generated (POTP)
  - SMS
  - Push Notifications

# TOTP

$HMAC(K, C) :=$   
 $SHA1(K \oplus 0x5C5C... \| SHA1(K \oplus 0x3636... \| C))$

$HOTP(K, C) :=$   
 $Truncate(HMAC(K,C)) \& 0x7FFFFFFF$

K – Secret Key

C – Counter/Clock

# Problem: Lost Device

- Recovery Questions

What is the maiden name of your mother?



- E-Mail Verification



- POTP

- In-Person Verification (used in enterprise environments, but not usable with cloud services)

# Application-Specific Passwords

Some protocols (or their implementations) like SSH, SFTP or IMAP do not support 2FA

The screenshot shows the GitHub user interface for managing SSH keys. On the left, a sidebar menu lists various account settings: Profile, Account settings, Emails, Notification center, Billing, Payment history, **SSH keys**, Security, Applications, Repositories, and Organizations. The 'SSH keys' option is currently selected. The main content area is titled 'SSH Keys' and contains the following information:

Need help? Check out our guide to [generating SSH keys](#) or troubleshoot [common SSH Problems](#)

**SSH Keys**

Add SSH key

This is a list of SSH keys associated with your account. Remove any keys that you do not recognize.

Key	Name	Key Fingerprint	Last Used	Action
●	info@brennaobrien.com	a0:56:bc:a0:ef:06:39:d6:03:cc:9a:7a:0e:d8:92:5c	Added 2 years ago — Last used on April 28, 2014	Delete
●	test server	4a:dd:4b:0a:c5:20:55:8c:1a:3c:ac:14:c5:b7:63:04	Added a year ago — Last used on March 20, 2014	Delete
●	hackeryou SSH	93:89:a8:46:ef:46:1b:99:7a:fe:66:c0:ba:28:1c:c9	Added 6 months ago — Last used on April 07, 2014	Delete



# Claims-Based Identity

Microsoft Services



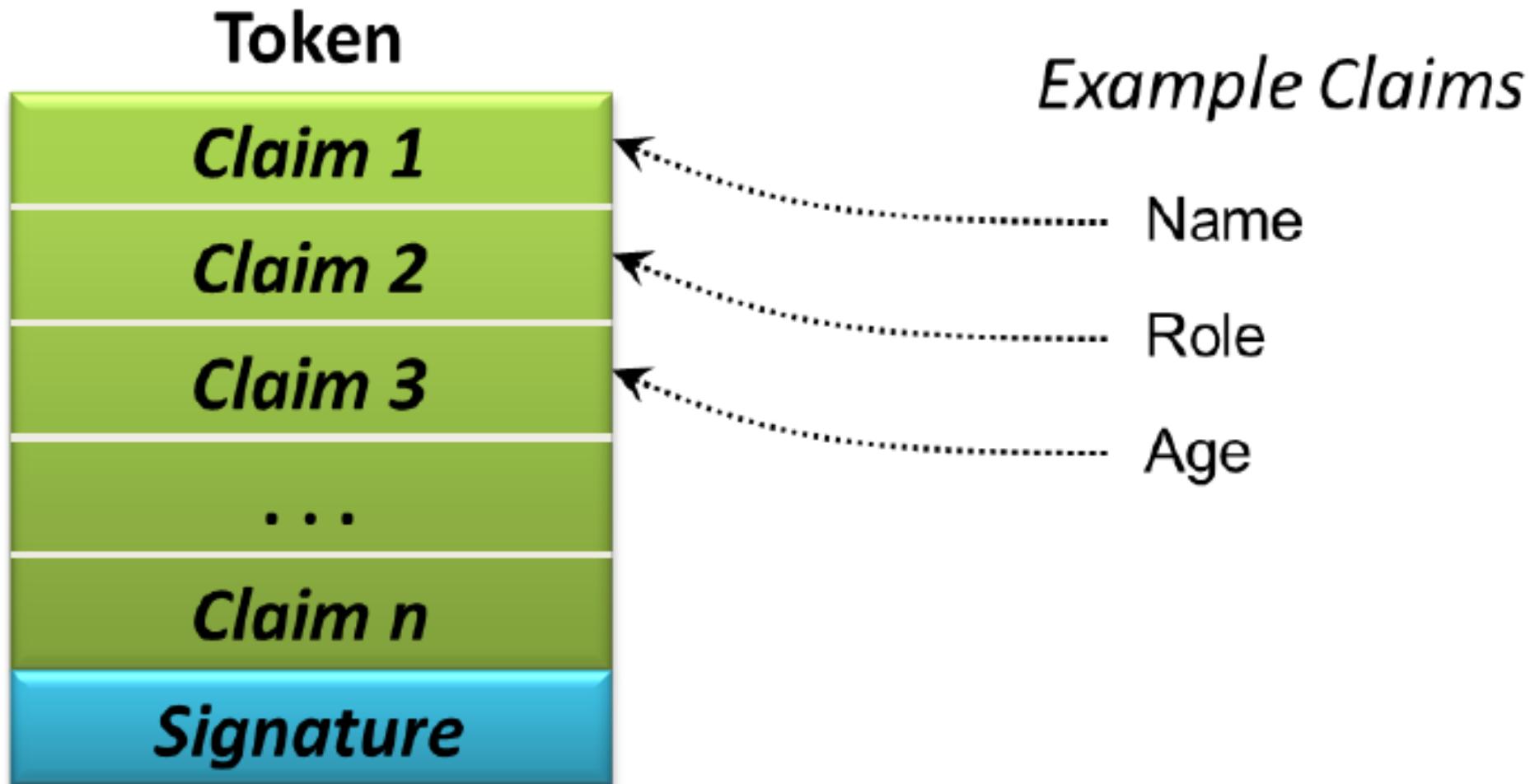
# Most Common Technologies

- OAuth
- OpenID
- OpenID Connect
- SAML
- WS-\*
- JWT
- SWT

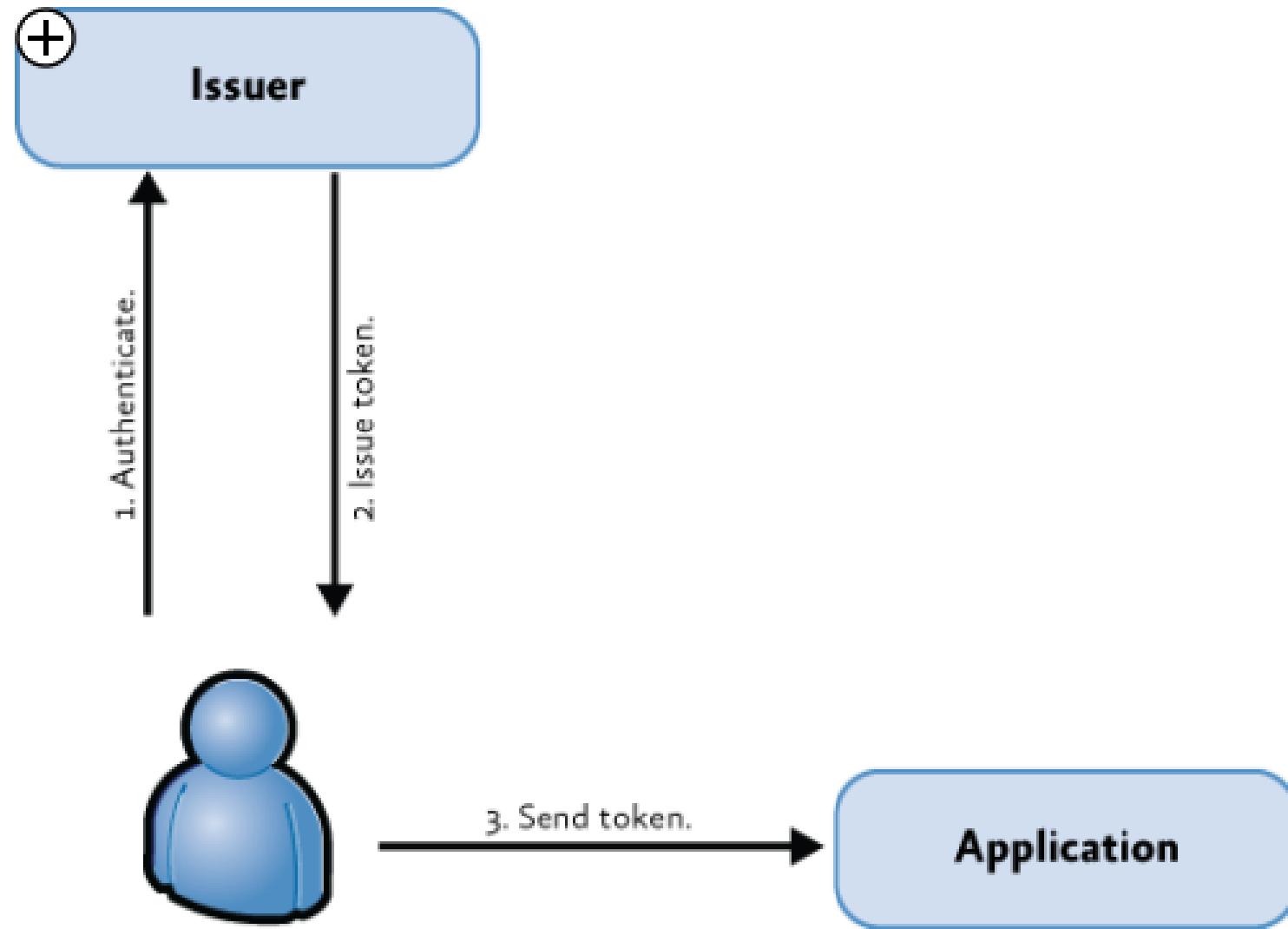
# Claims-based Identity

- First Name: John
- Last Name: Doe
- Login: John
- Mail: john@doe.com
- Role: User
- Role: Administrator

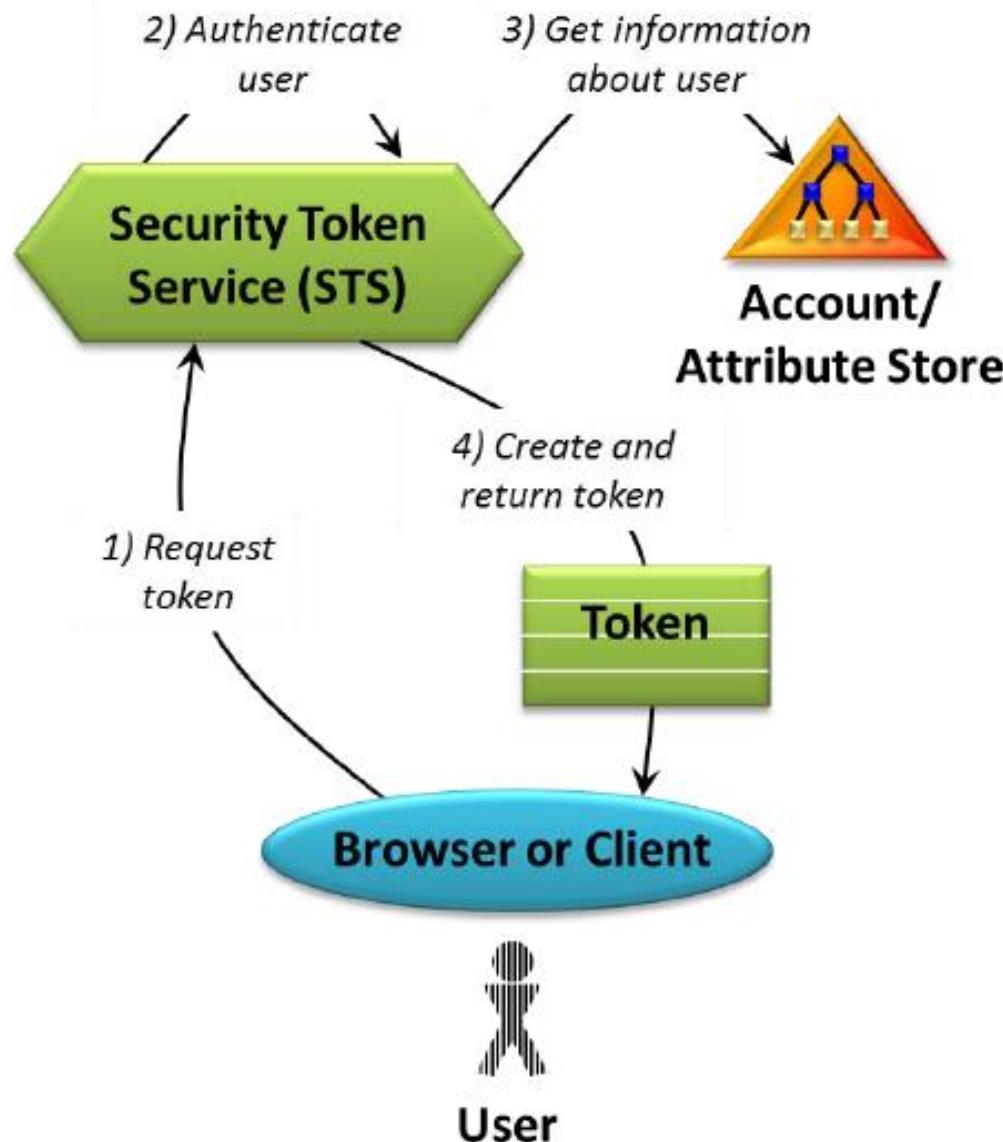
# Tokens



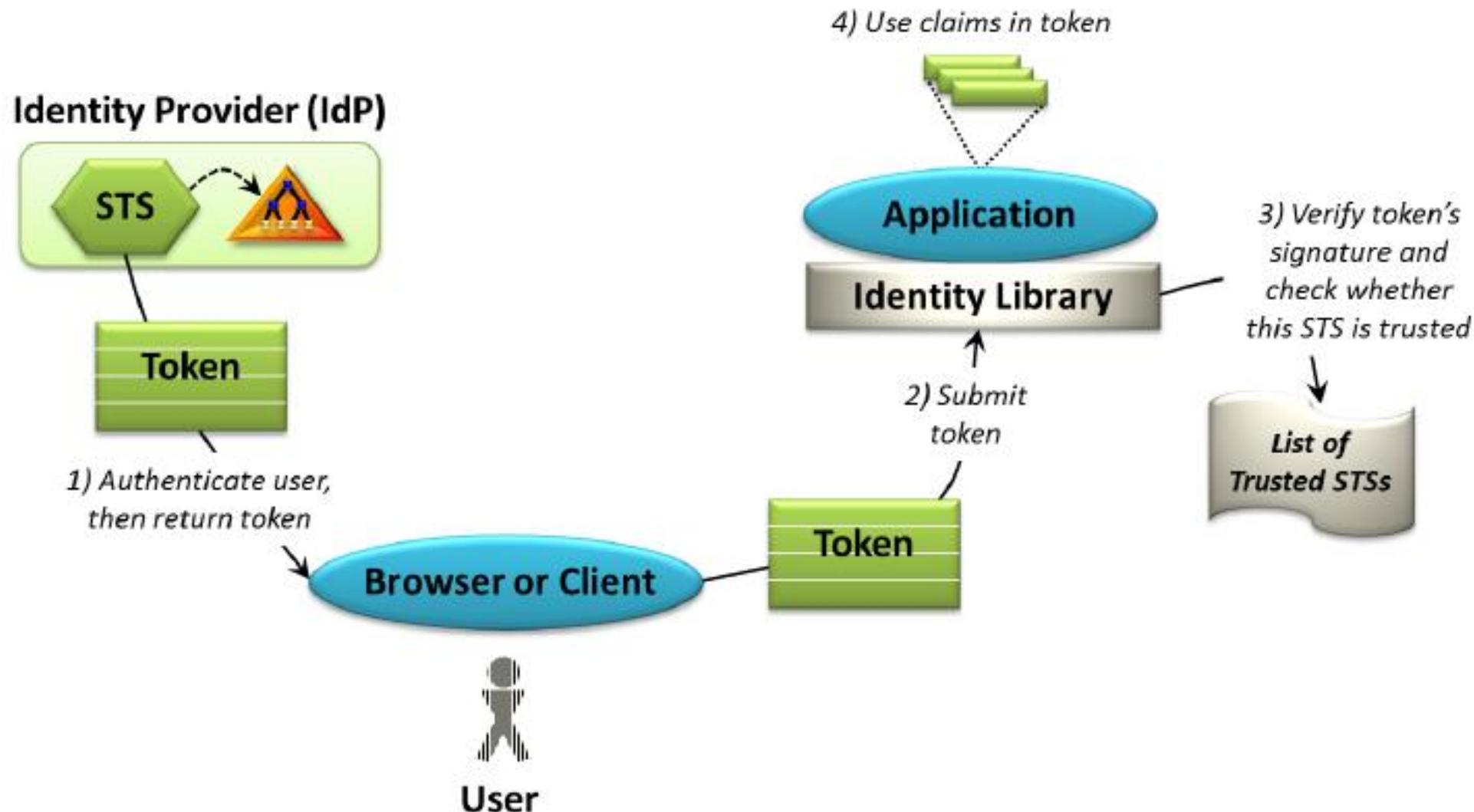
# Basic Communication Pattern



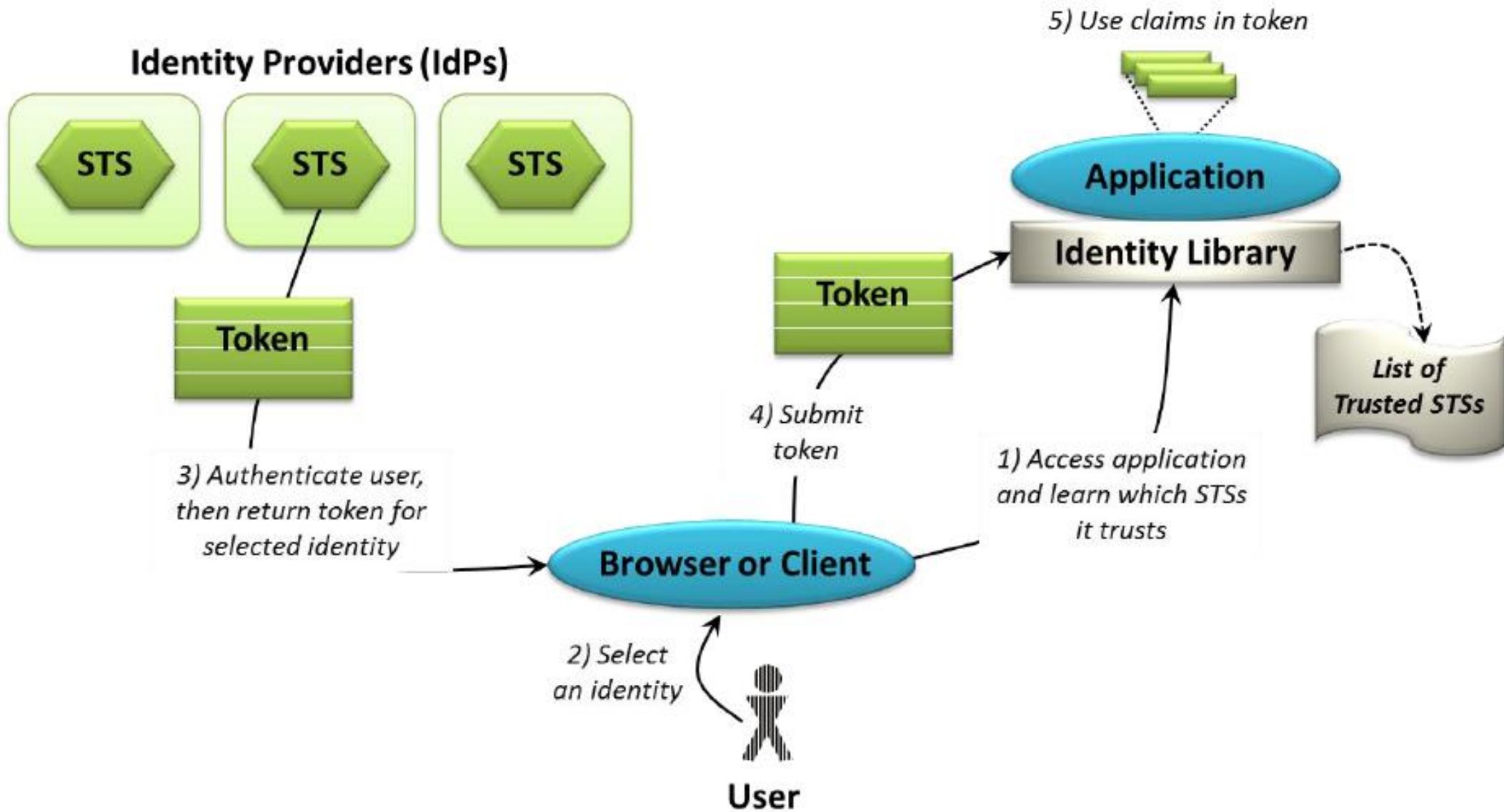
# Token Issuance



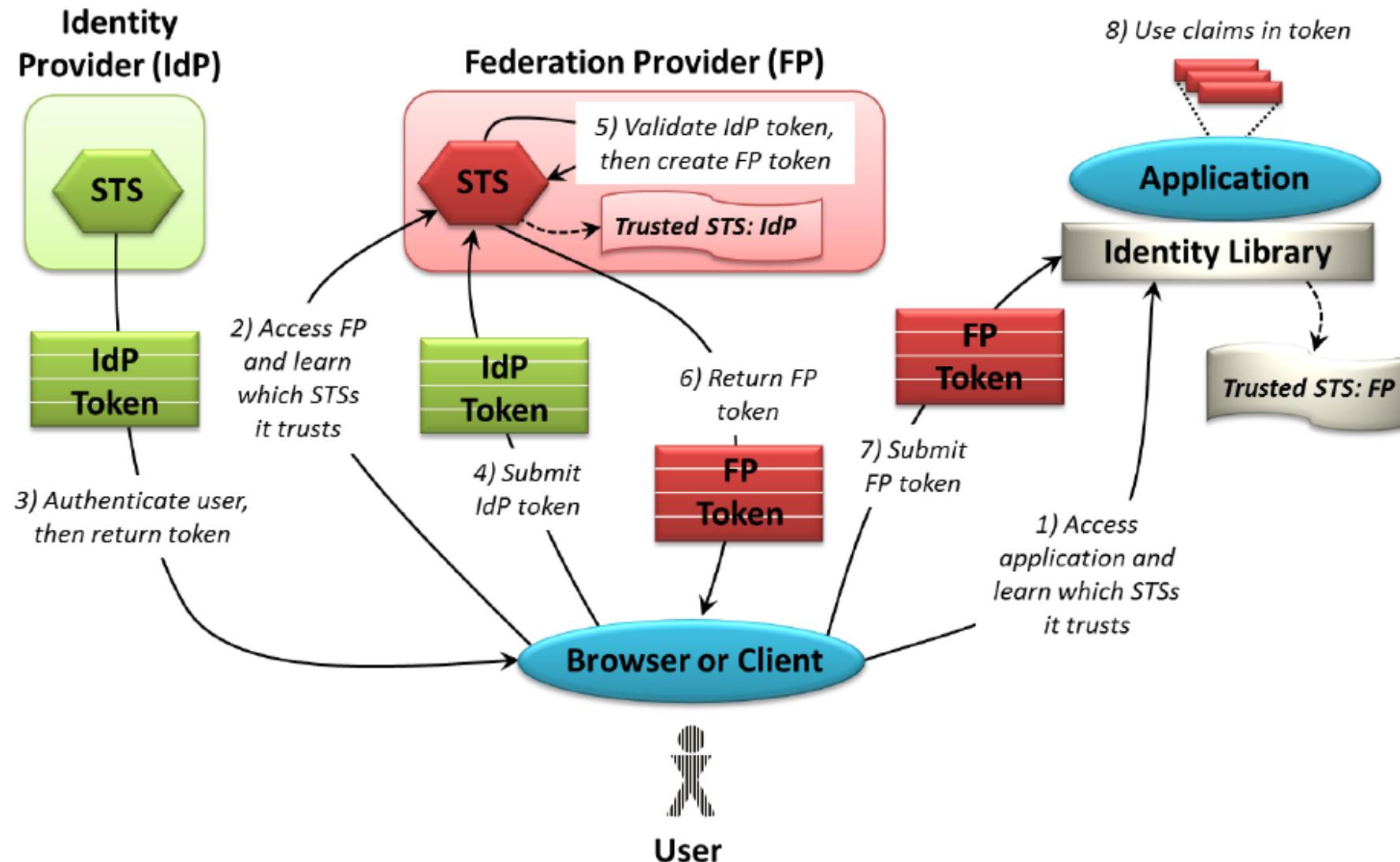
# Identity Providers and Identity Libraries



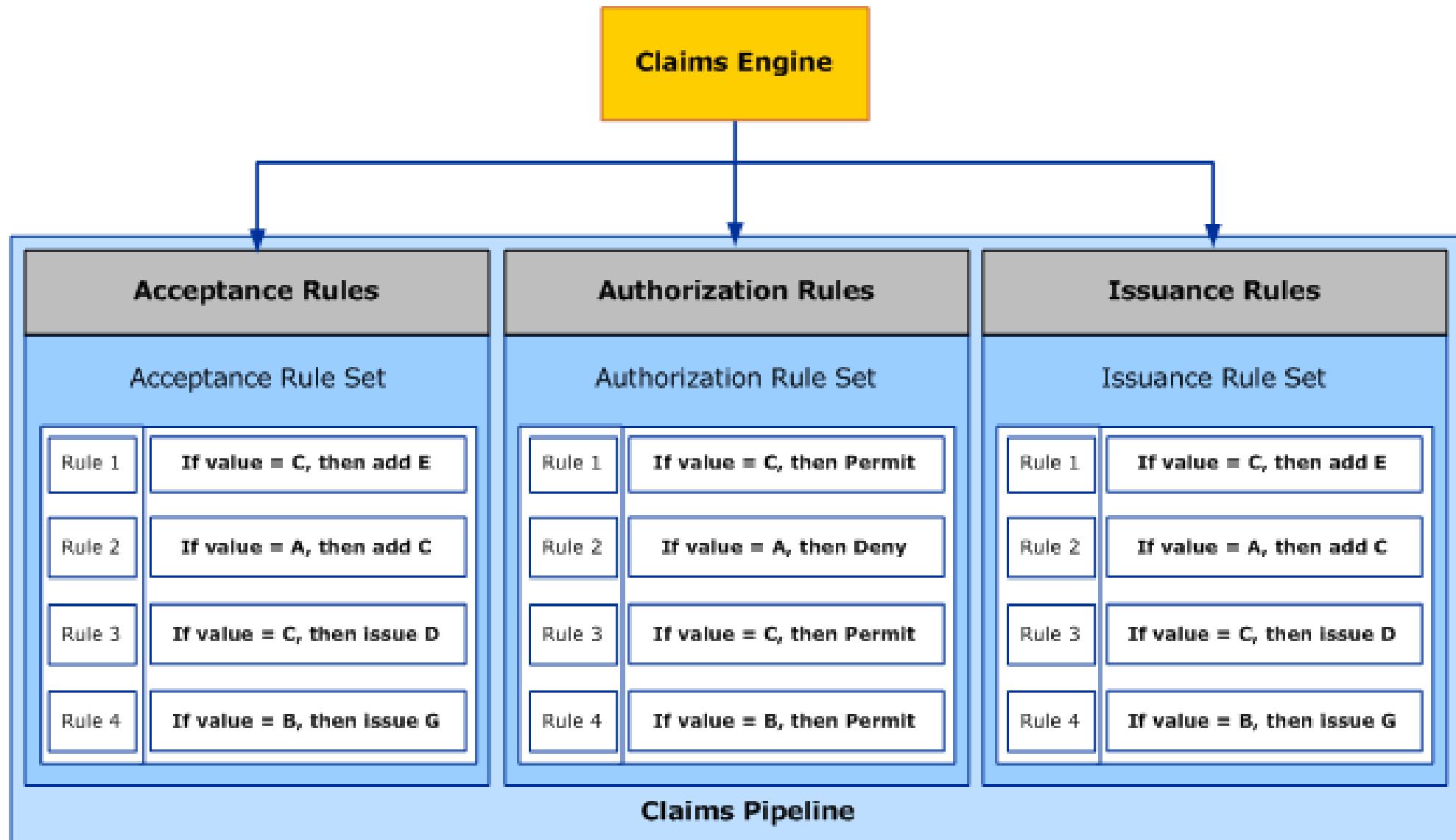
# Multiple Identity Providers



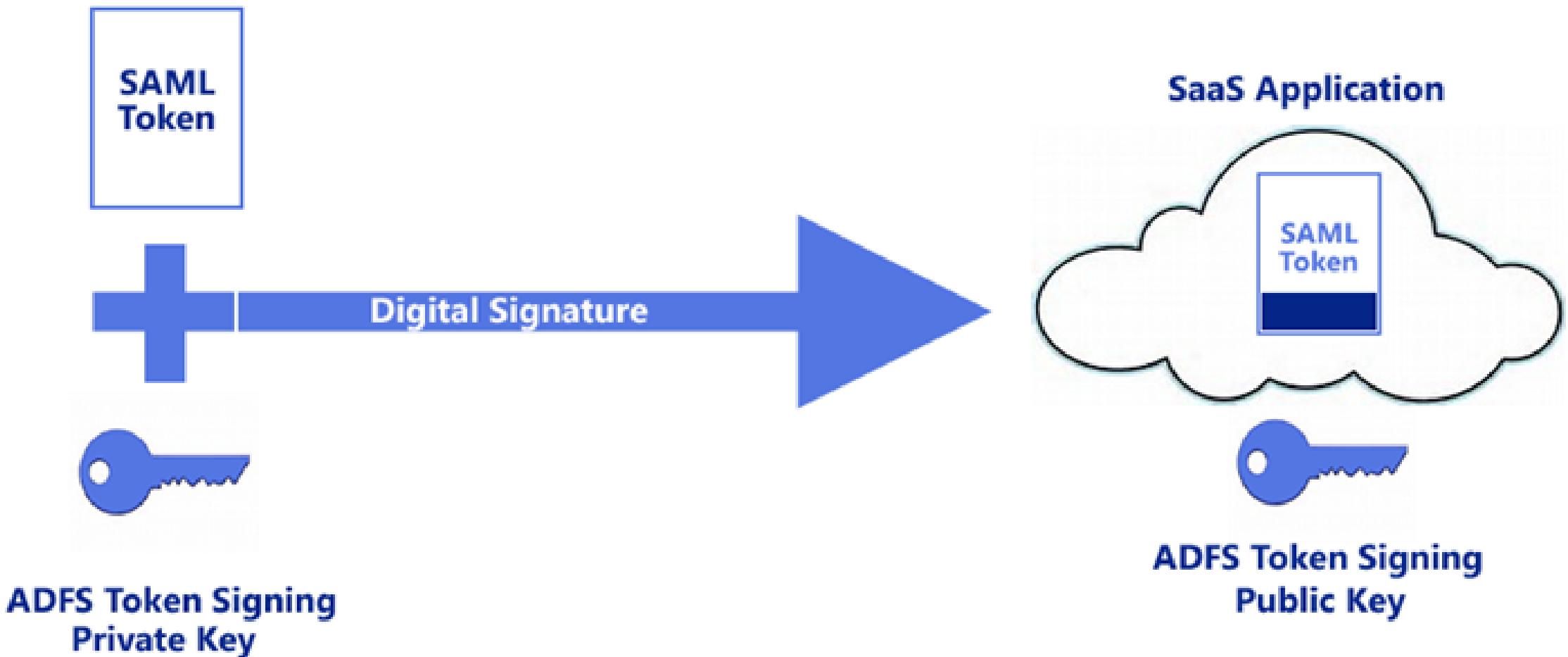
# Identity Federation



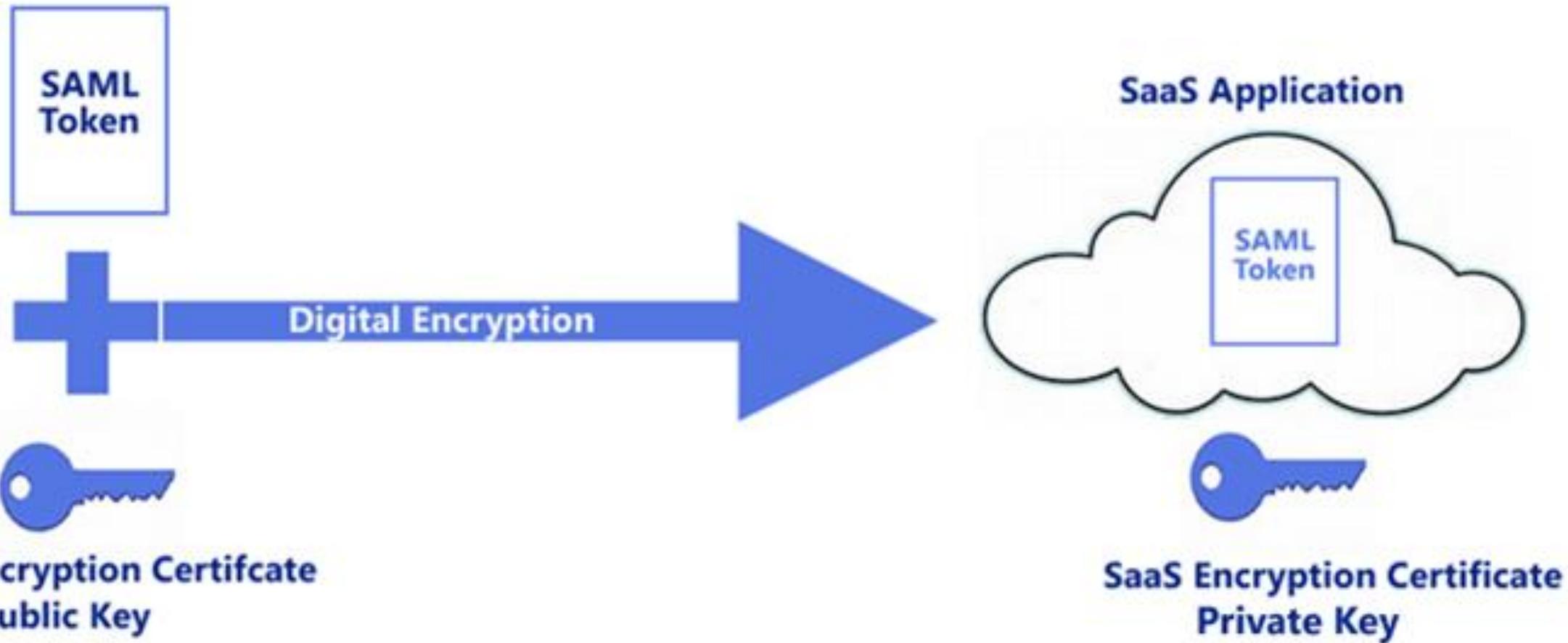
# Claims Rule Engine



# Token Digital Signature



# Token Encryption



# Shibboleth

The screenshot shows a login form for the Central Authentication Service (CAS) at the University of科威特 (UK). The header features the university's crest and the text "CAS - Centrální autentizační služba UK". The main message on the page reads: "Stránka vyžaduje přihlášení pomocí Centrální autentizační služby UK!" (The page requires authentication using the Central Authentication Service). The login form includes fields for "Přihlašovací jméno:" (Username) and "Heslo:" (Password), both currently empty. There is also a checkbox labeled "Upozornit před přihlášením k jiné aplikaci." (Notify before logging in to another application). Below the form is a red button labeled "Přihlásit" (Log in). To the right of the form, there is explanatory text about using the university ID or faculty email as the username, and a note about setting the keyboard layout correctly. At the bottom, there are links for "English" and "Czech".

**CAS - Centrální autentizační služba UK**

Stránka vyžaduje přihlášení pomocí Centrální autentizační služby UK!

**Centrální autentizační služba UK**

Přihlašovací jméno:

Heslo:

Upozornit před přihlášením k jiné aplikaci.

Přihlásit

Jako přihlašovací jméno zadejte své osobní číslo, které najdete pod fotografií na průkazu UK. Můžete také použít fakultní přihlašovací jméno spolu s doménou (např. novak@fakulta.cuni.cz).

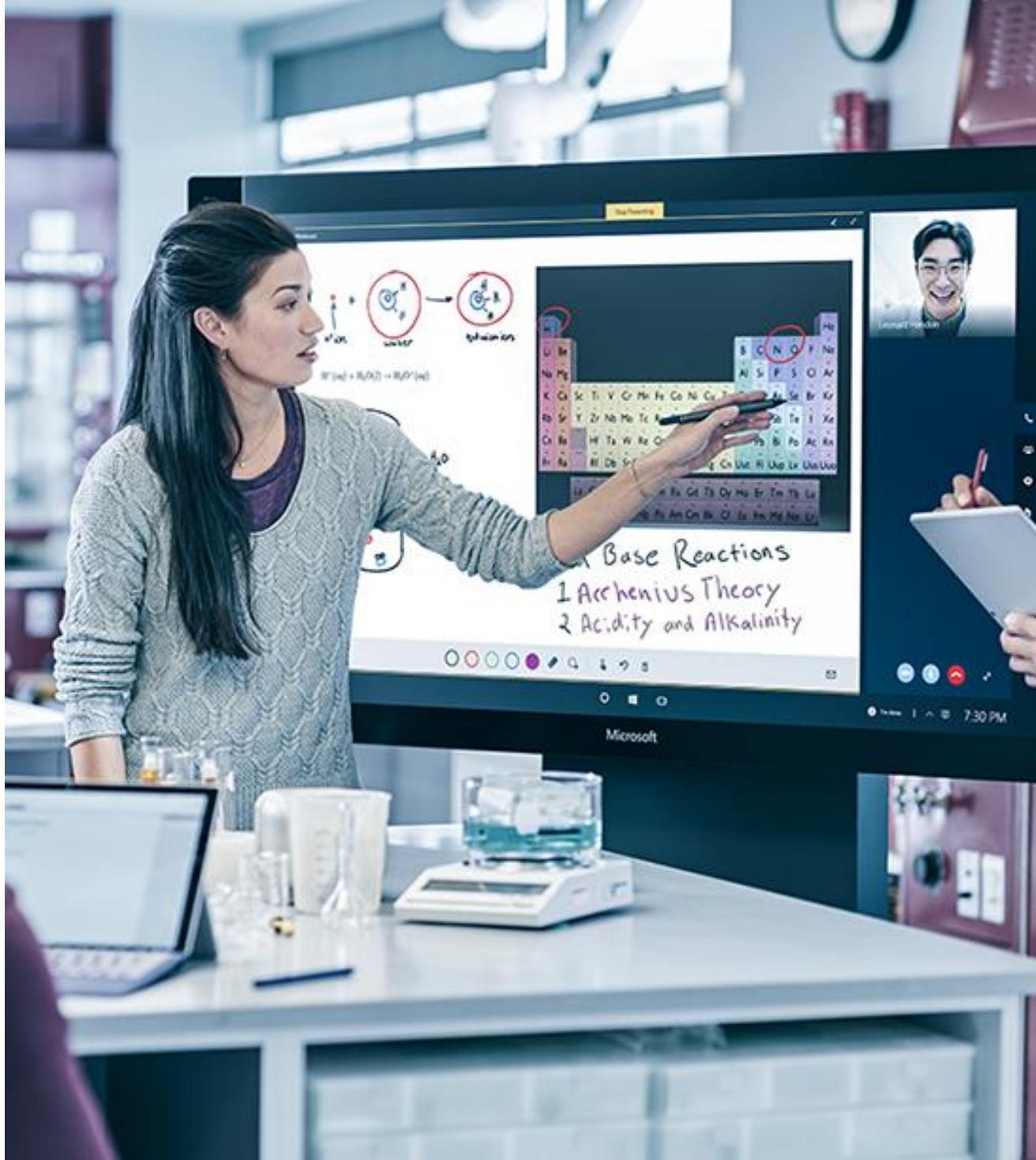
Při zadání hesla dbejte na správné nastavení klávesnice (jazyková verze, malá-velká písmena, prohození Z a Y).

**Z bezpečnostních důvodů se po ukončení práce odhlašte a zavřete okno prohlížeče!**

[English](#) [Czech](#)

- SAML-based federation portal
- Open Source

# Demo





# SAML

Microsoft Services



# SAML

- Security Assertion Markup Language
- Similar to OpenID, but targeted to the enterprise
- XML-based
- Supports Single sign-on
- Requires mutual trust between IdP and SP
- Multiple bindings, not just HTTP
- Supports Identity provider initiated authentication

# Underlying Standards

- Extensible Markup Language (XML)
- XML Schema (XSD)
- XML Signature
- XML Encryption
- Hypertext Transfer Protocol (HTTP)
- Simple Object Access Protocol (SOAP)

# SAML Versions

- SAML 1.0 - 2002
- SAML 1.1 - 2003
- SAML 2.0 - 2005
  - Incompatible with SAML 1.x
  - Renamed XML namespaces, elements and attributes
  - New bindings
  - New protocols

# Parts of SAML Specification

- SAML Core (Assertions + Protocols)
- SAML Bindings
- SAML Profiles (e.g. Web Browser SSO Profile)  
    Assertions + Protocols + Bindings

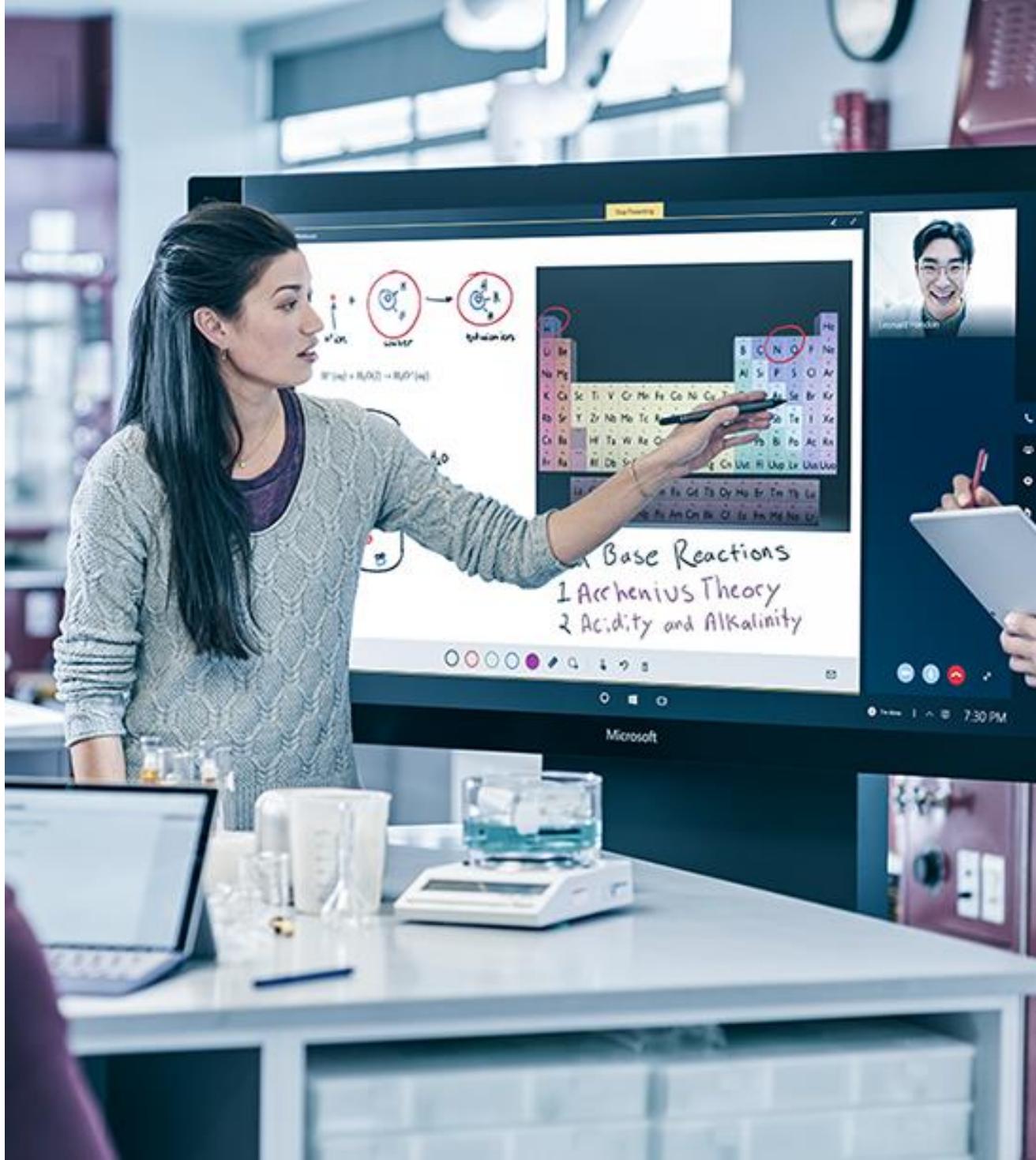
# SAML Assertions

```
<saml:Assertion ID="_3c39bc0fe7b13769cab2f6f45eba801b1245264310738"  
    IssueInstant="2009-06-17T18:45:10.738Z" Version="2.0">  
    <saml:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">  
        https://www.salesforce.com  
    </saml:Issuer>
```

Assertion A was issued at time t by issuer R  
regarding subject S provided conditions C are valid.

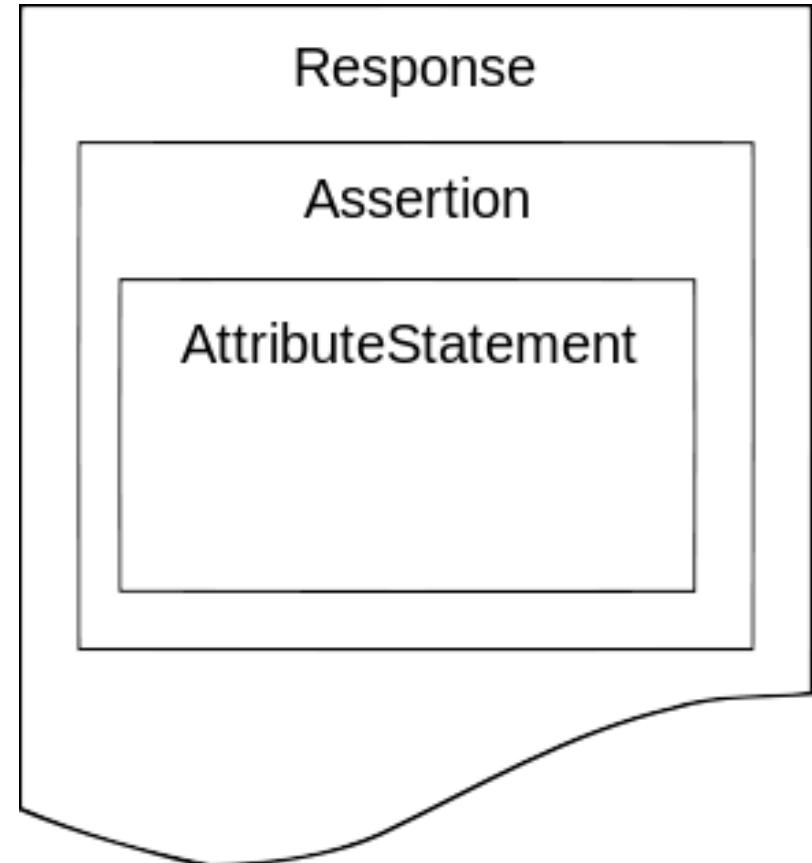
- Authentication statements
- Attribute statements
- Authorization decision statements

# Demo



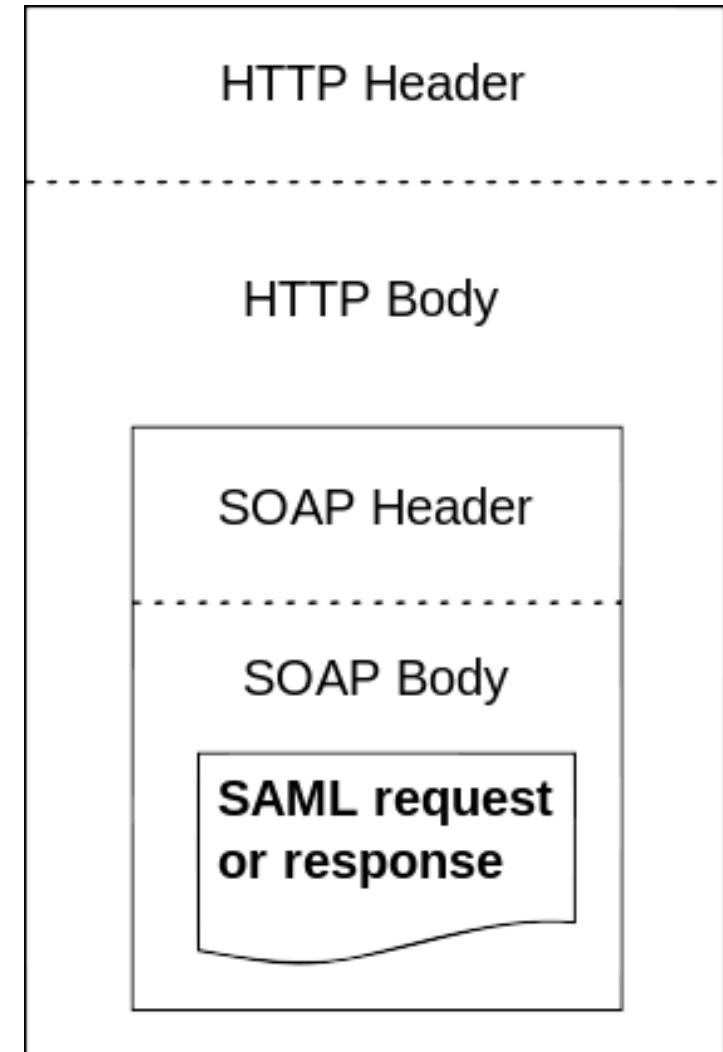
# SAML Protocols

- Assertion Query and Request Protocol
- Authentication Request Protocol
- Artifact Resolution Protocol
- Name Identifier Management Protocol
- Single Logout Protocol
- Name Identifier Mapping Protocol



# SAML Bindings

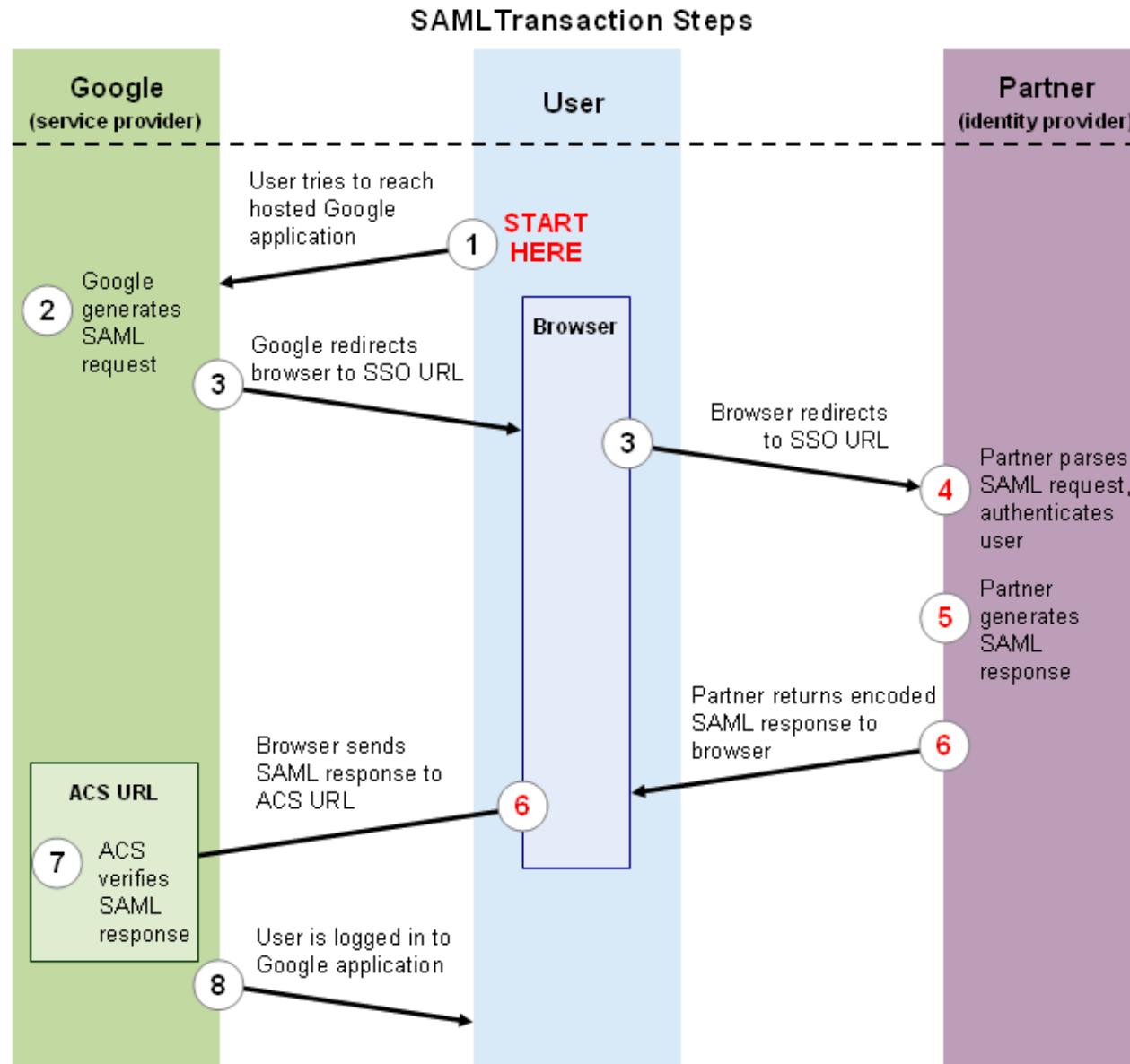
- SAML SOAP Binding
- Reverse SOAP (PAOS) Binding
- HTTP Redirect (GET) Binding
- HTTP POST Binding
- HTTP Artifact Binding
- SAML URI Binding



# SAML Profiles

- SSO Profiles
  - Web Browser SSO Profile
  - Enhanced Client or Proxy (ECP) Profile
  - Identity Provider Discovery Profile
  - Single Logout Profile
  - Name Identifier Management Profile
- Artifact Resolution Profile
- Assertion Query/Request Profile
- Name Identifier Mapping Profile
- SAML Attribute Profiles

# SAML (Google Apps)



# SAML Response Example

```
<saml:Assertion
  ID="b07b804c-7c29-ea16-7300-4f3d6f7928ac"  Version="2.0"
  IssueInstant="2004-12-05T09:22:05">
  <saml:Issuer>https://idp.example.org/SAML2</saml:Issuer>
  <ds:Signature>...</ds:Signature>
  ...
  <saml:Conditions
    NotBefore="2004-12-05T09:17:05"  NotOnOrAfter="2004-12-05T09:27:05">
  </saml:Conditions>
  <saml:AttributeStatement>
    <saml:Attribute x500:Encoding="LDAP" Name="urn:oid:1.3.6.1.4.1.5923.1.1.1"
      FriendlyName="eduPersonAffiliation">
      <saml:AttributeValue xsi:type="xs:string">member</saml:AttributeValue>
      <saml:AttributeValue xsi:type="xs:string">staff</saml:AttributeValue>
    </saml:Attribute>
  </saml:AttributeStatement>
</saml:Assertion>
```

# SAML Sign-In Protocol



WS-\*

Microsoft Services



# Web Services

- Web services are a standardized set of specifications used to build applications and services
- Web services typically:
  - Transmit data as XML
  - Use SOAP to define the XML message format
  - Use WSDL to define valid SOAP messages
  - Use UDDI to describe available Web services

# The WS\* Architecture

- WS\* was designed from the outset to be modular – allowing applications to be built using only the specifications they require
- There are various specifications in WS\*, some key ones are:
  - **WS-Security**
  - **WS-Trust**
  - **WS-Federation**

# WS-Trust

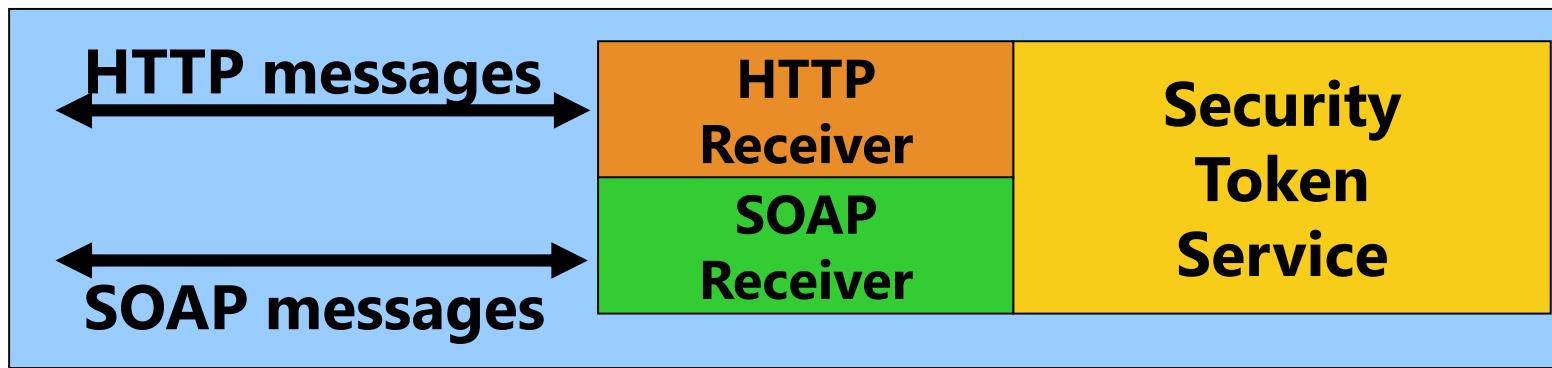
- OASIS Standard from 2007
- Deals with the issuing, validating, and renewal of security tokens
- Defines the concept of the Security Token Service
- Defines formats of messages used to request security tokens (RST) and respond to those requests (RSTR)
- Defines mechanisms for key exchange

# Demo



# WS-Federation

- OASIS Standard from 2006, drafted by IBM, Microsoft, RSA,...
- Uses SAML Tokens
- Based on WS-Security, WS-Trust and other WS-\* standards
- Supports automatic metadata discovery and certificate roll-over
- Defines common claims
- Two profiles of the model defined
  - Passive – for web browser clients
  - Active – SOAP clients



# WS-Federation SignIn

<https://sts.cloudready.ms/adfs/ls/?wa=wsignin1.0&wtrealm=https%3a%2f%2fclaim-sweb.cloudready.ms&wctx=rm%3d0%26id%3dpas-sive%26ru%3d%252f&wct=2014-10-21T22%3a15%3a42Z>

Let's break-out these parameters:

- **Wa=signin1.0:** This tells the ADFS server to invoke a login for the user.
- **Wtrealm:** This tells ADFS what application I was trying to get to. This has to match the identifier of one of the relying party trusts listed in ADFS.
- **Wctx:** This is some session data that the application wants sent back to it after the user authenticates.
- **wct:** This is the exact time I tried to gain access to the application.

# Communication

#	Result	Protocol	Host
1	302	HTTPS	claimsweb.cloudready.ms
2	200	HTTPS	sts.cloudready.ms
3	200	HTTPS	sts.cloudready.ms
4	200	HTTPS	claimsweb.cloudready.ms

# Federated SSO: Communication

#	Result	Protocol	Host
1	302	HTTPS	claimsweb.cloudready.ms
2	200	HTTPS	sts.cloudready.ms
3	302	HTTPS	sts.cloudready.ms
5	200	HTTPS	corp.sts.microsoft.com
6	200	HTTPS	sts.cloudready.ms
7	200	HTTPS	claimsweb.cloudready.ms

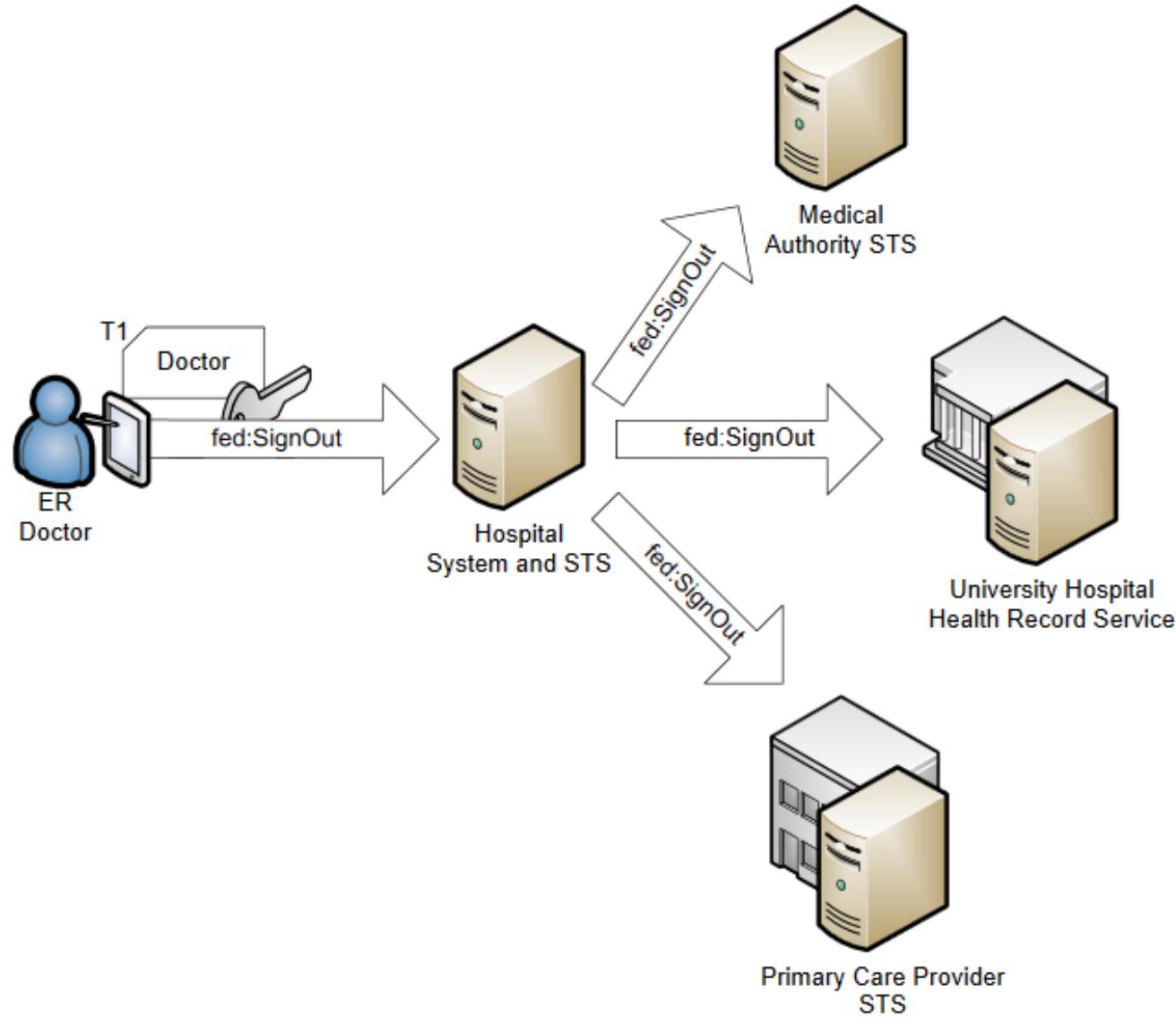
# Federated SSO: Claims

WELCOME CLAIMSWEB!



Issued Identity			
Claim Type	Claim Value	Issuer	OriginalIssuer
<a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress</a>	dgreg@microsoft.com	<a href="http://sts.cloudready.ms/adfs/service/trust">http://sts.cloudready.ms/adfs/service/trust</a>	<a href="http://corp.sts.microsoft.com">http://corp.sts.microsoft.com</a>
<a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn</a>	dgreg@microsoft.com	<a href="http://sts.cloudready.ms/adfs/service/trust">http://sts.cloudready.ms/adfs/service/trust</a>	<a href="http://corp.sts.microsoft.com">http://corp.sts.microsoft.com</a>
<a href="http://schemas.xmlsoap.org/claims/group">http://schemas.xmlsoap.org/claims/group</a>	Redmond\Corp Users	<a href="http://sts.cloudready.ms/adfs/service/trust">http://sts.cloudready.ms/adfs/service/trust</a>	<a href="http://corp.sts.microsoft.com">http://corp.sts.microsoft.com</a>
<a href="http://schemas.xmlsoap.org/claims/group">http://schemas.xmlsoap.org/claims/group</a>	NORTHAMERICA\CloudReadyUsers	<a href="http://sts.cloudready.ms/adfs/service/trust">http://sts.cloudready.ms/adfs/service/trust</a>	<a href="http://corp.sts.microsoft.com">http://corp.sts.microsoft.com</a>
<a href="http://schemas.microsoft.com/ws/2008/06/identity/claims/authenticationmethod/password">http://schemas.microsoft.com/ws/2008/06/identity/claims/authenticationmethod/password</a>	<a href="http://schemas.microsoft.com/ws/2008/06/identity/authenticationmethod/password">http://schemas.microsoft.com/ws/2008/06/identity/authenticationmethod/password</a>	<a href="http://sts.cloudready.ms/adfs/service/trust">http://sts.cloudready.ms/adfs/service/trust</a>	<a href="http://sts.cloudready.ms/adfs/service/trust">http://sts.cloudready.ms/adfs/service/trust</a>
<a href="http://schemas.microsoft.com/ws/2008/06/identity/claims/authenticationinstant">http://schemas.microsoft.com/ws/2008/06/identity/claims/authenticationinstant</a>	2014-08-25T03:06:51.345Z	<a href="http://sts.cloudready.ms/adfs/service/trust">http://sts.cloudready.ms/adfs/service/trust</a>	<a href="http://sts.cloudready.ms/adfs/service/trust">http://sts.cloudready.ms/adfs/service/trust</a>

# Single SignOut



# FederationMetadata

- Entity (STS) ID
- Token signing certificates
- WS-Federation endpoint URL
- SAML protocol endpoint URL
- ...

# Demo





# Simple Web Token

Microsoft Services



# Simple Web Token (SWT)

- Proposed by Microsoft in 2009?
- Much simpler than SAML
- Tokens can only be symmetric signed by a shared secret using the HMAC algorithm.

# SWT Sample

Issuer=issuer.example.com&  
ExpiresOn=1262304000&  
com.example.group=gold&  
over18=true&  
HMACSHA256=  
AT55%2B2jLQeuigpg0xm%2Fvn7tjpSGXBUfFe0UXb0%2F9opE%3D



# JSON Web Token

Microsoft Services



# JSON Web Token

- Defined in IETF RFC7519 from May 2015
- Inspired by SWT
- Based on
  - JSON Web Signature (JWS, RFC7515)
  - JSON Web Encryption (JWE, RFC7516)
- Very compact
- Can use different encryption schemes

# Token Structure

Header: { typ: 'JWT', alg: 'HS256' }

Payload/Claims:

{

  user: john,

  admin: true,

  exp: 8.10.2016, 15:27

}

Signature

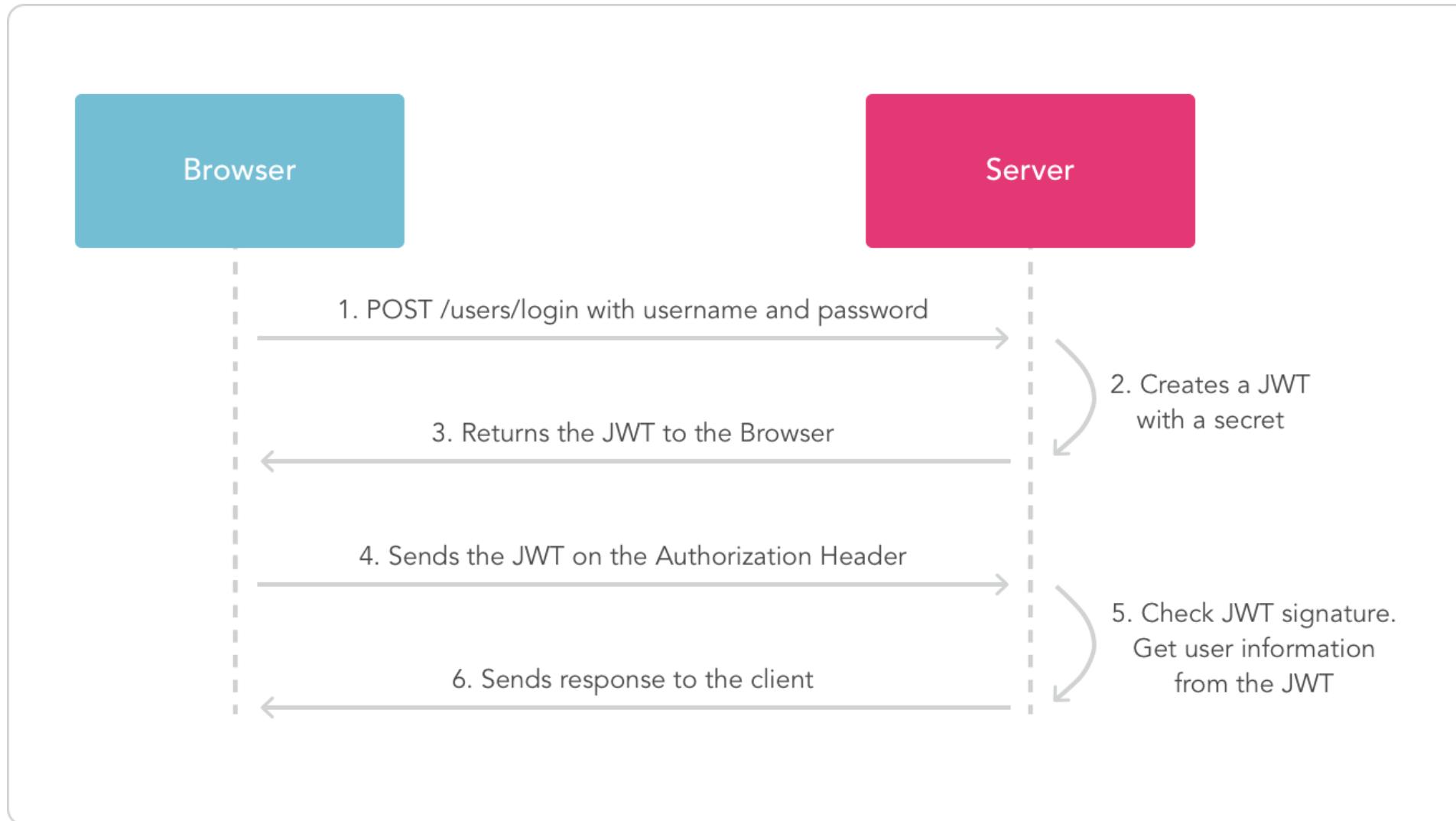
=> BASE64

# Encoded and Signed Token

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9 .  
eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4  
gRG9lIiwiaXNTb2NpYWwiOnRydWV9 .  
4pcPyMD09o1PSyXnrXCjTwXyr4BsezdI1AVTmud2fU4

---

# Communication



# Raw HTTP Sample

HTTP/1.1 200 OK

Cache-Control: no-cache, no-store

Pragma: no-cache

Content-Length: 1103

Content-Type: application/json; charset=utf-8

Expires: -1

Server: Microsoft-IIS/7.5

Request-id: 8d44e415-caa7-4a67-90f6-1f20a679285b

X-Content-Type-Options: nosniff

X-Powered-By: ARR/2.5

X-Powered-By: ASP.NET

Date: Thu, 08 Aug 2013 17:42:18 GMT

{"token\_type":"Bearer","access\_token":"eyJ...w","expires\_in":43200,"not\_before":1375983748,"expires\_on":1376026948,"resource":"https://graph.windows.net"}

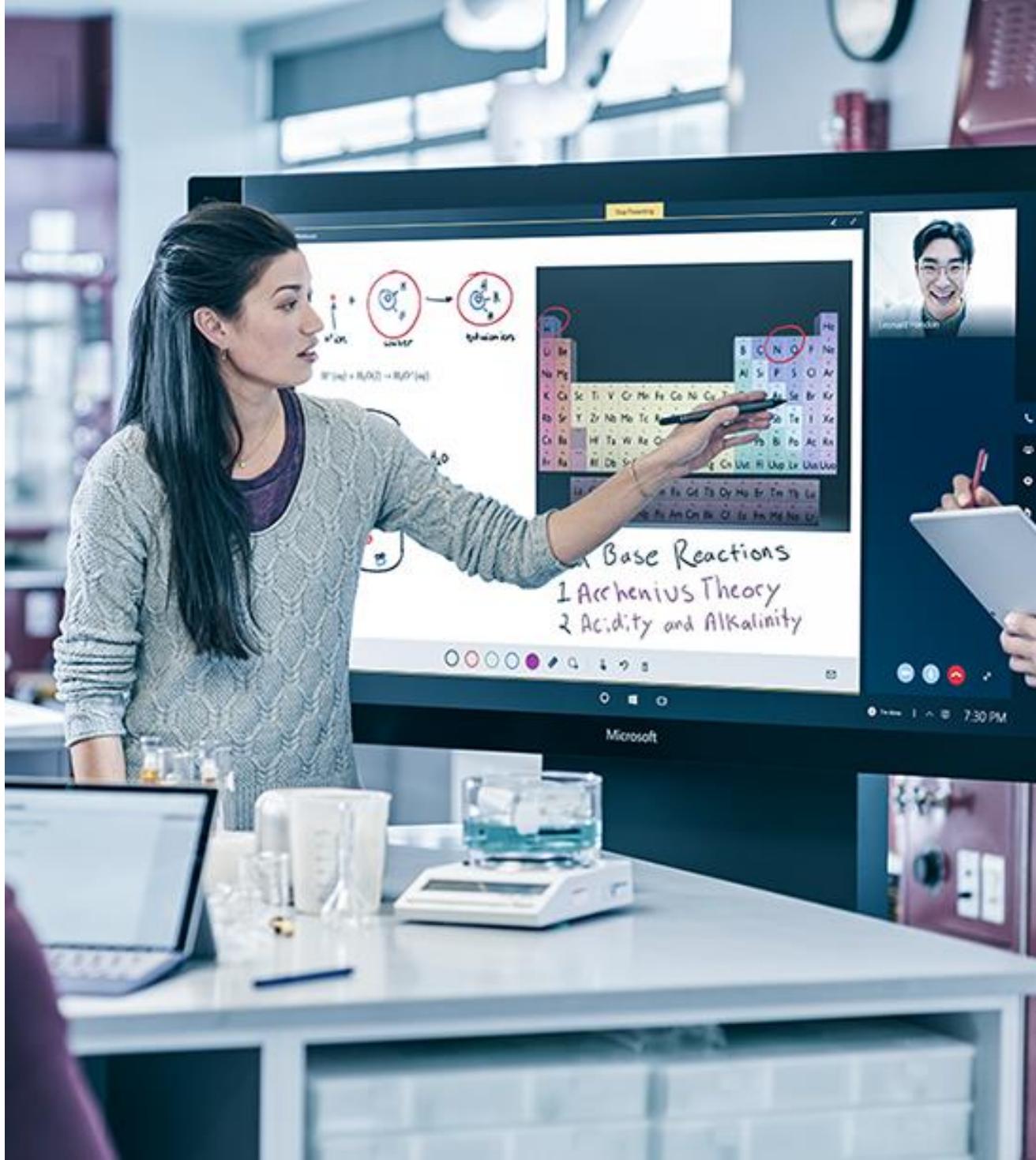
# JWT Response in Fiddler

The screenshot shows the Fiddler application interface with a captured response message. The response is displayed in a JSON viewer. The JSON structure includes the following fields:

- access\_token: ey30eXAiOiJKV1QLCjhbGciOiJSUzI1NiIsIng1dCI6IkSHVEZ2ZEstZnI0aEV1THdqchdBsk4...
- expires\_in: 43200
- expires\_on: 1376358323
- not\_before: 1376315123
- resource: https://graph.windows.net
- token\_type: Bearer

At the bottom of the JSON viewer, there are buttons for "Expand All" and "Collapse". A status message "JSON parsing completed." is also visible. Below the JSON viewer, the URL of the request is shown: "/mvdemo.onmicrosoft.com/oauth2/token?api-version=1.0".

# Demo





# OAuth

Microsoft Services

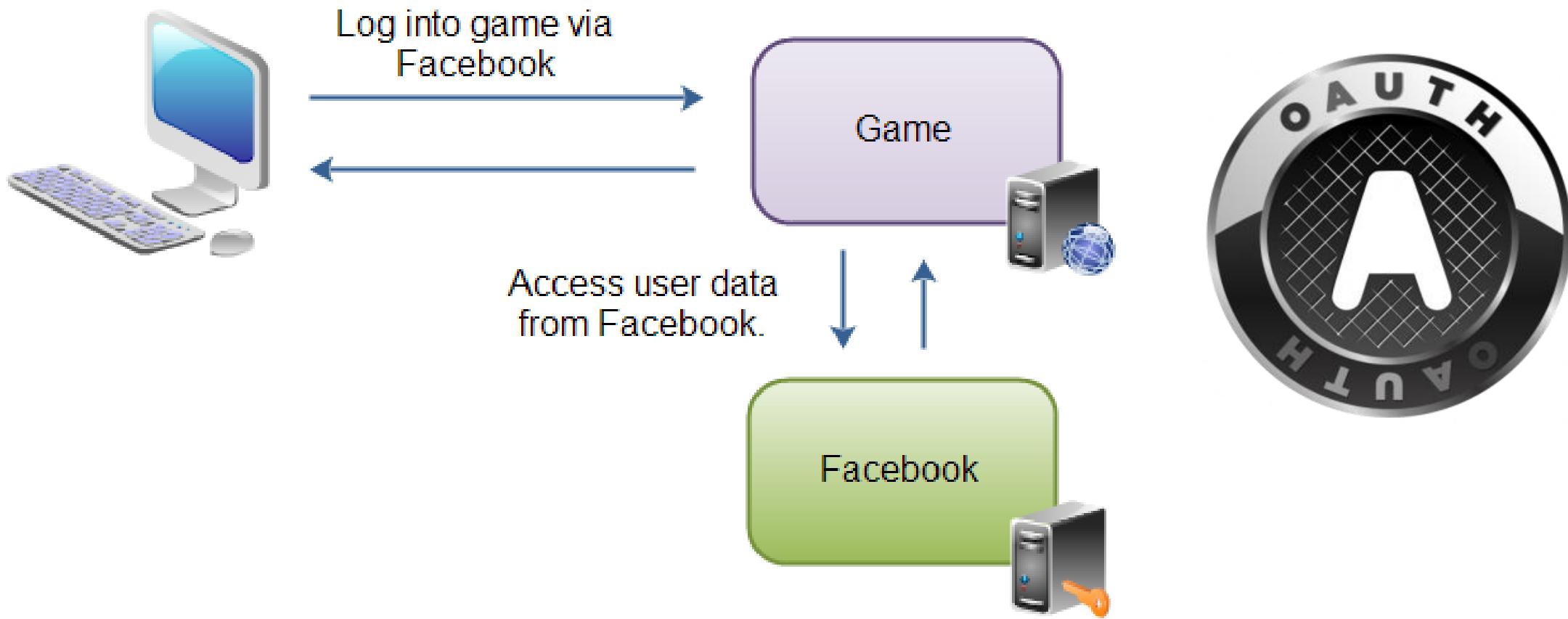


# OAuth



# OAuth

Used to delegate user authorization to a 3<sup>rd</sup>-party service provider



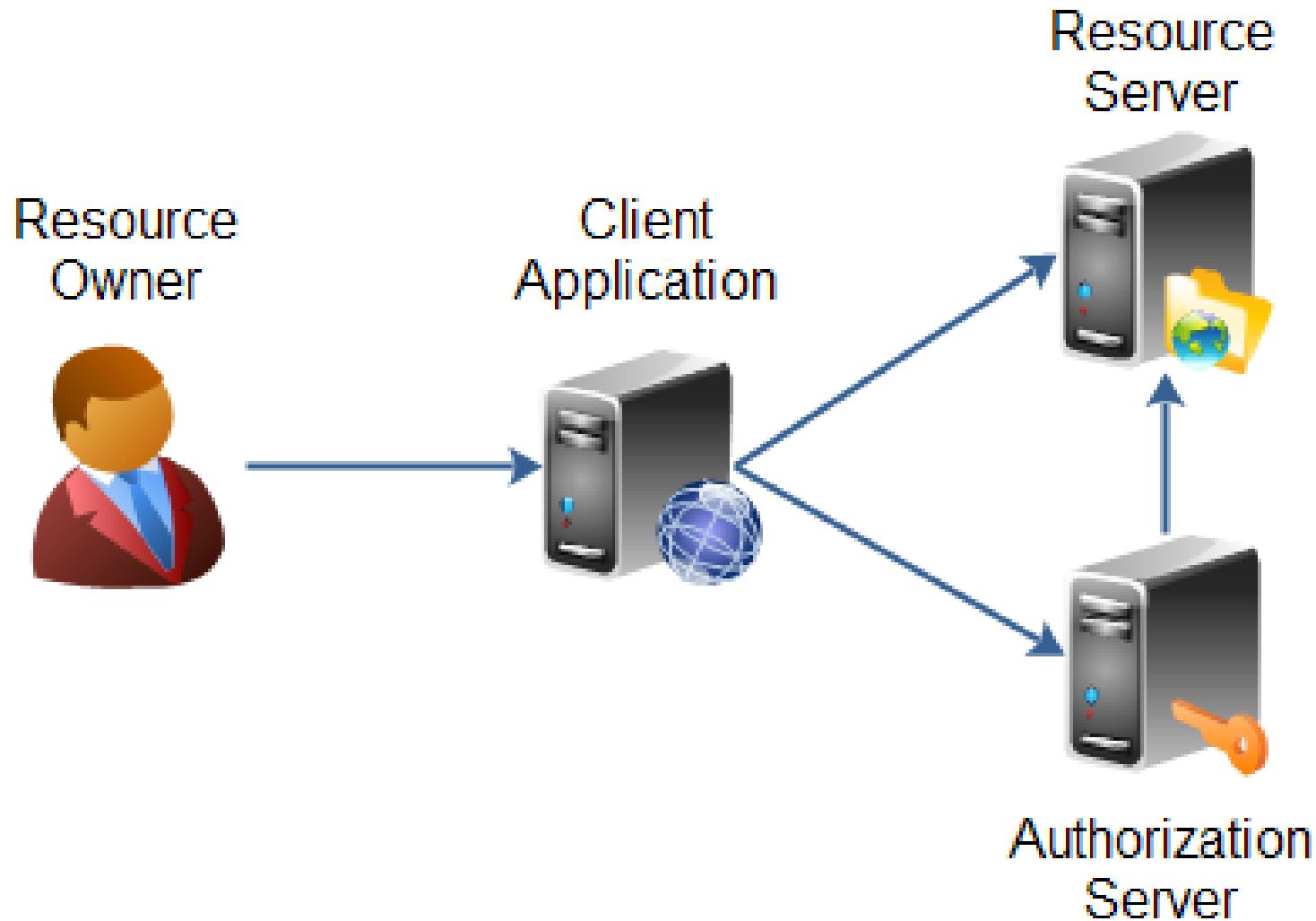
# History

- 2006 – Twitter missing delegation in OpenID
- 2007 – OAuth Core 1.0 (Twitter, Google,...)
- 2010 – OAuth 1.0 (IETF RFC 5849)
- 2012 – OAuth 2.0
  - Framework - RFC 6749
  - Bearer Token Usage - RFC 6750
  - Threat Model and Security Considerations - RFC 6819
  - ...

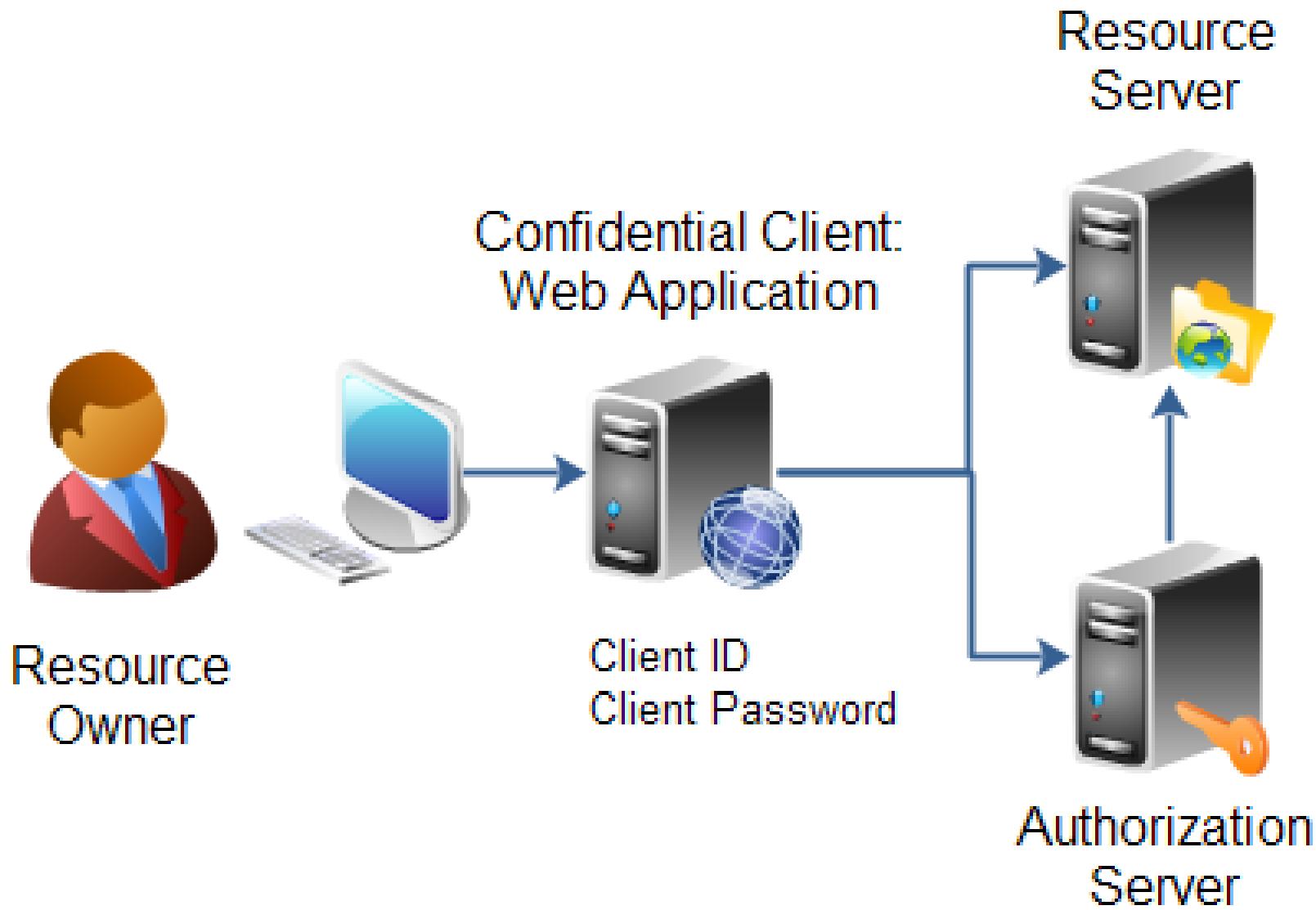
# OAuth 2.0

- Not backwards compatible with OAuth 1.0
- Framework -> Non-interoperability
- Authorization flows for web, desktop, mobile and TV applications
- Client types
  - Public
  - Confidential
- Client Profiles
  - Web Application
  - User Agent
  - Native

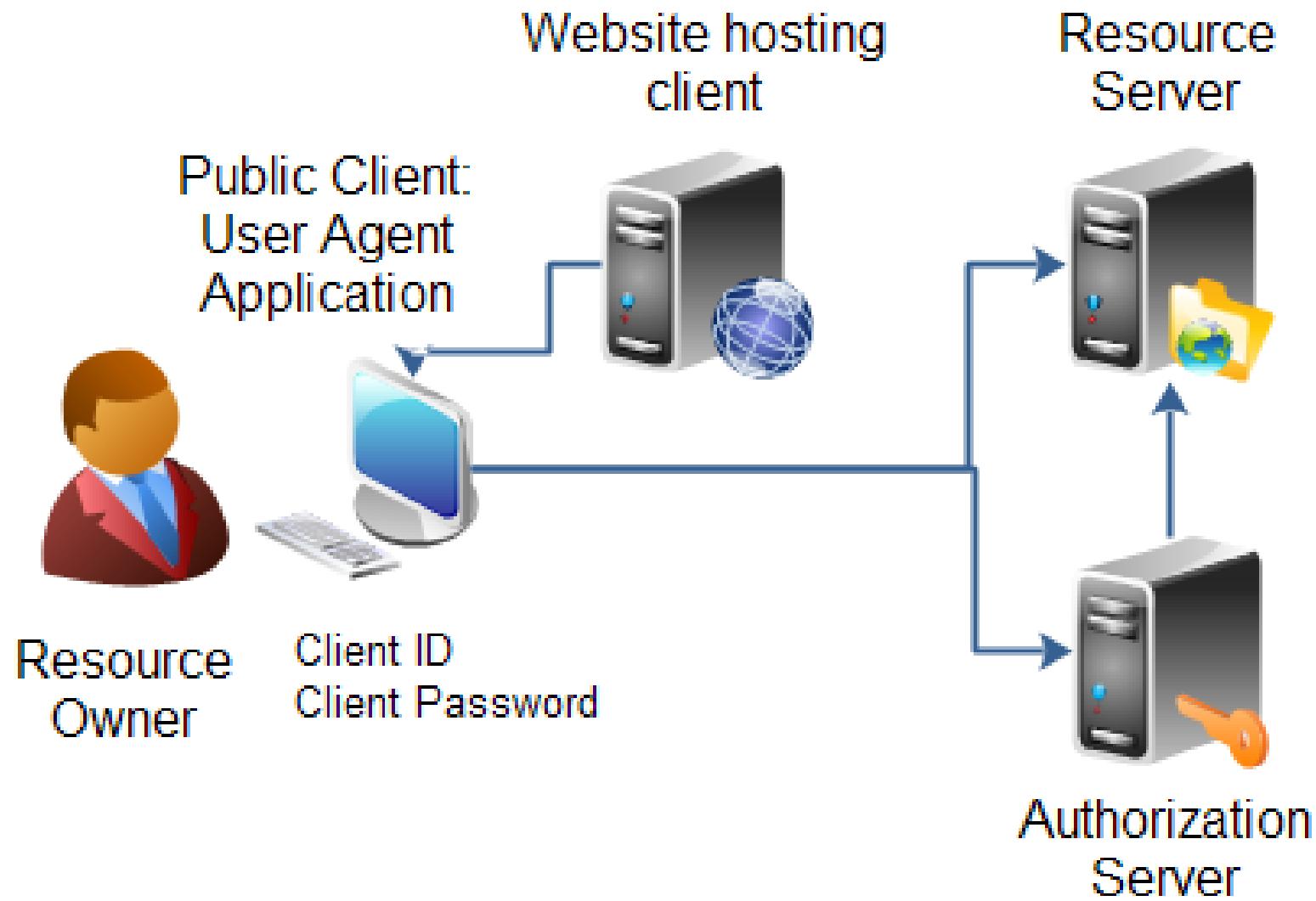
# User and application roles



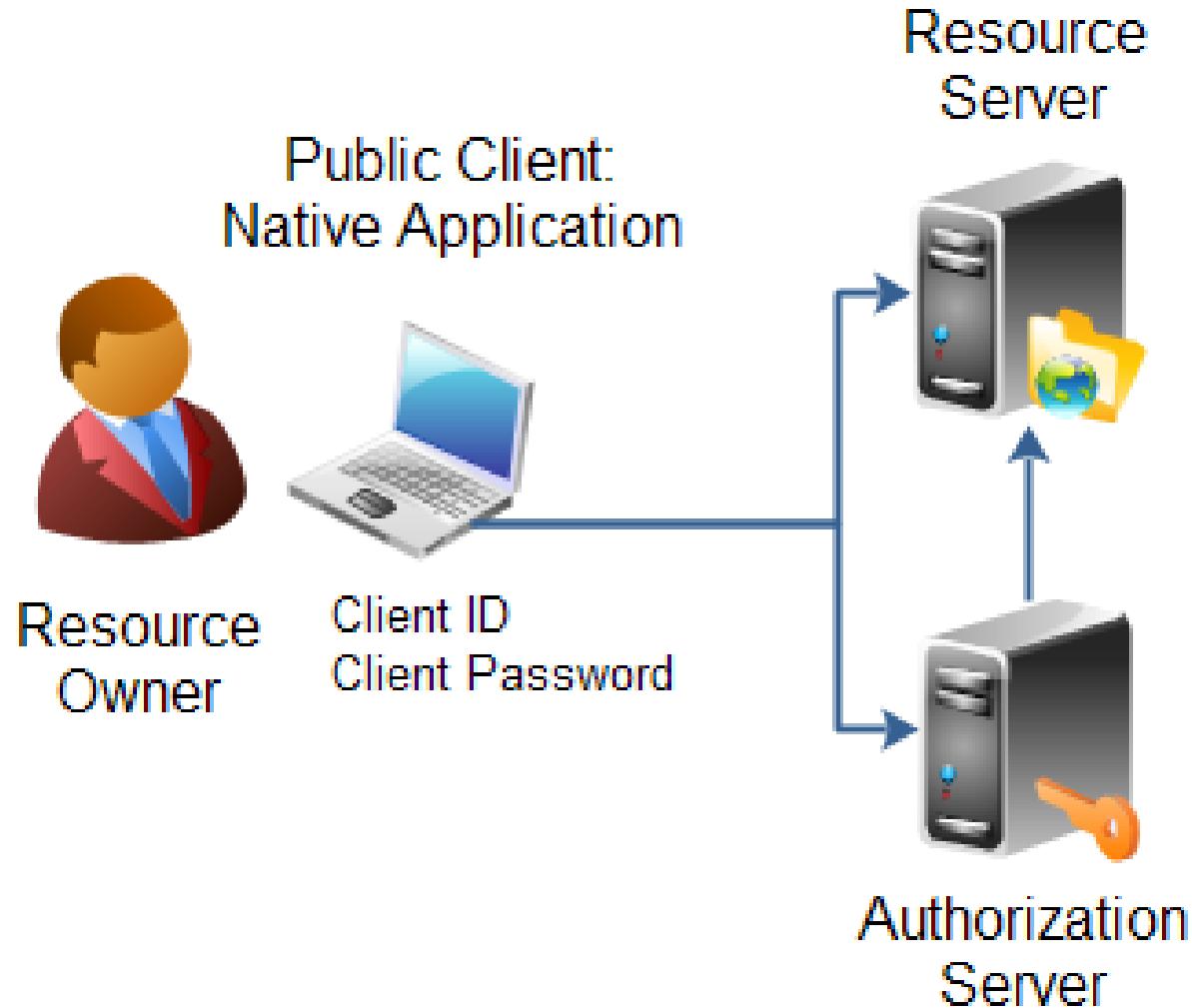
# Confidential client web application



# Client user agent application



# Client native application



# Application registration

- Client ID
- Client secret
- Redirect URI

The screenshot shows the Facebook App Dashboard for an application named "My Great App".

**Basic Info**

Display Name: [?]	My Great App
Namespace: [?]	
Contact Email: [?]	support@mygreatsite.com
App Domains: [?]	www.mygreatsite.com <input type="button" value="X"/>
Hosting URL: [?]	You have not generated a URL through one of our partners (Get one)
Sandbox Mode: [?]	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

**Select how your app integrates with Facebook**

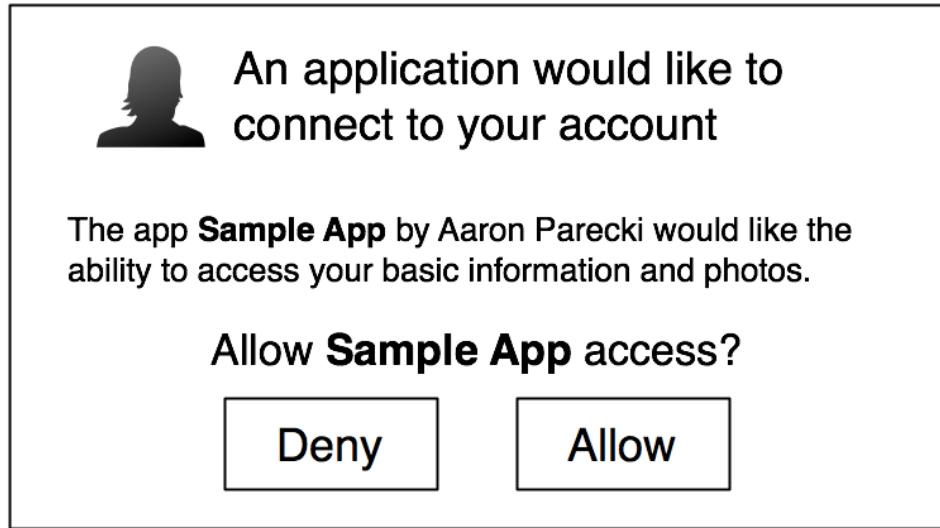
Website with Facebook Login

Site URL: [?]	http://www.mygreatsite.com/
---------------	-----------------------------

App on Facebook

Use my app inside Facebook.com.

# Confirmation



# Authorization Management

Authorized applications    Developer applications    **Revoke all**

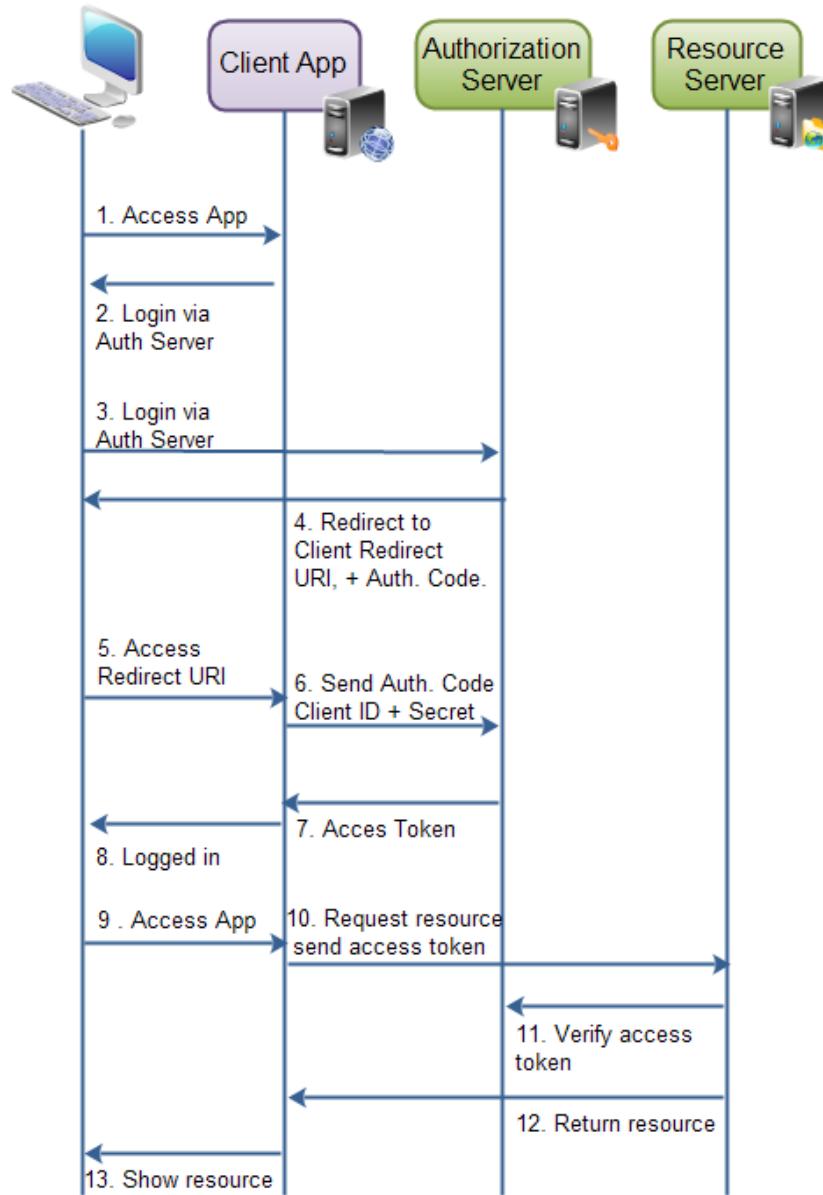
 You have granted the following applications access to your account. Read more about connecting with third-party applications at [GitHub Help](#).

4 Authorized applications		Sort ▾
	<b>Atom.io</b> Last used on Apr 5, 2015 · Owned by atom	<b>Revoke</b>
	<b>CodePen.io</b> Last used on Apr 22, 2015 · Owned by CodePen	<b>Revoke</b>
	<b>GitHub for Mac</b> Last used on May 5, 2015 · Owned by github	<b>Revoke</b>
	<b>Libraries.io</b> Last used on Apr 6, 2015 · Owned by librariesio	<b>Revoke</b>

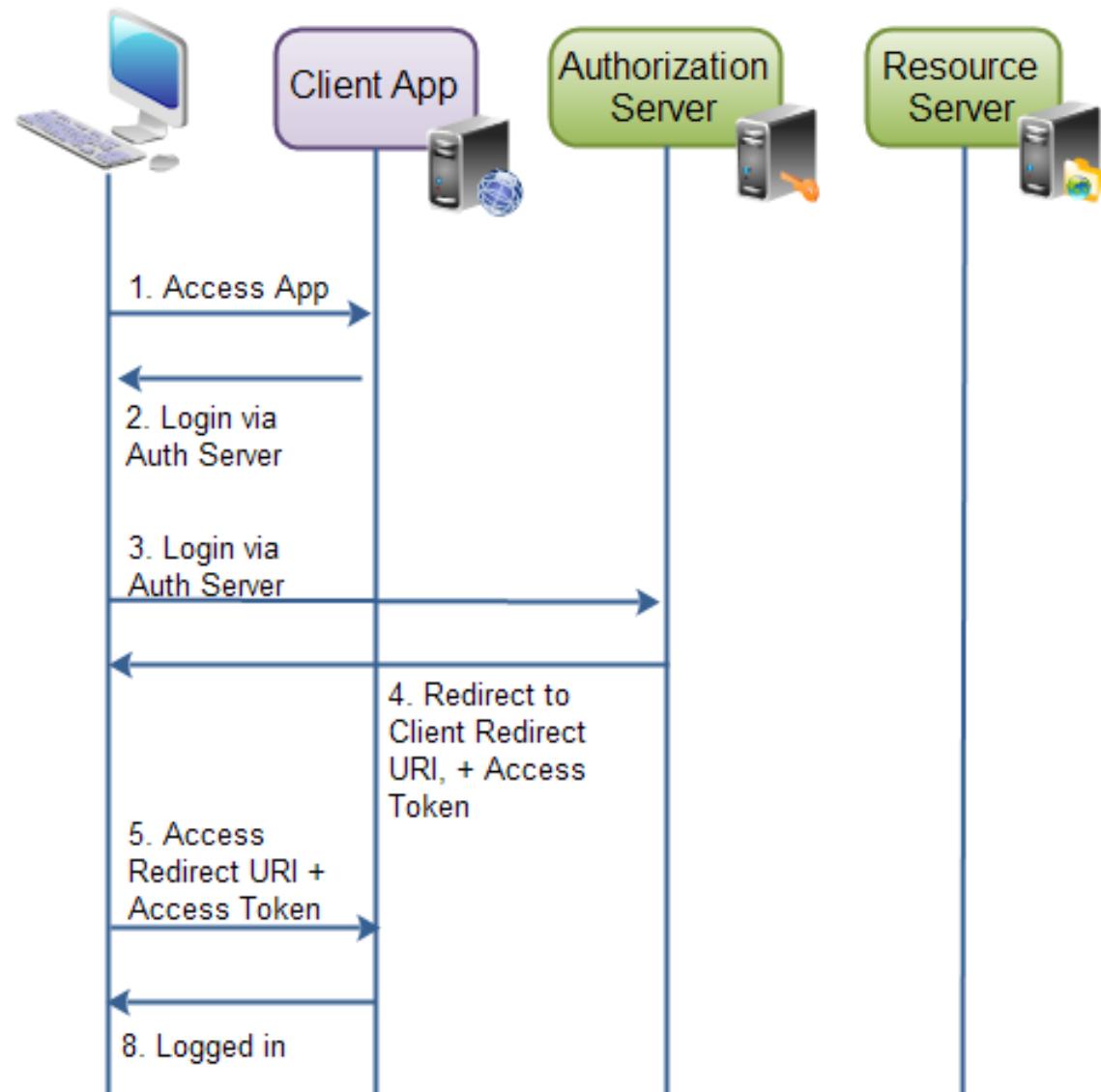
# Authorization Grant Methods

- Authorization Code
- Implicit
- Resource Owner Password Credentials
- Client Credentials

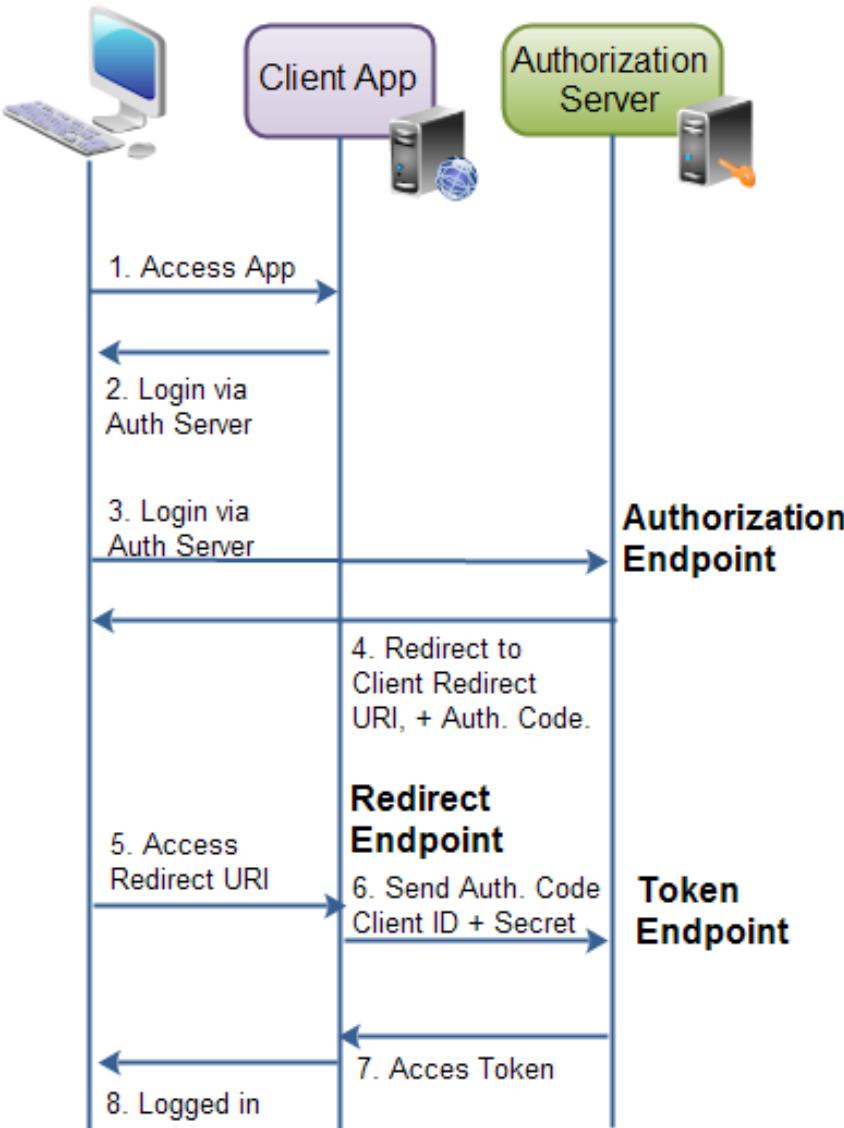
# Authorization Code



# Implicit Authorization Grant



# Endpoints



# Authorization Request

[https://sts.cloudready.ms/adfs/oauth2/authorize?re-](https://sts.cloudready.ms/adfs/oauth2/authorize?response_type=code&client_id=3fb2a37f-4ced-409c-937c-dddd776f4dfd&redirect_uri=https://www.davetestapp.com&resource=https://www.davetestapp.com)  
[sponse\\_type=code&client\\_id=3fb2a37f-4ced-409c-937c-dddd776f4dfd&redire](#)  
[ct\\_uri=https://www.davetestapp.com&resource=https://www.davetestapp.com](#)

Let's break down these parameters:

- **response\_type:** tells that ADFS server that I want to perform OAuth and get an authorization code in return.
- **client\_id:** The ID of the application I'm trying to get to.
- **Resource:** the URL/URI of the application I'm trying to get to.
- **redirect\_uri:** Tells ADFS who to POST the auth code back to

# Authorization Response

ms-app://s-1-15-2-1101140336-4090662585-1905587327-  
262951538-2732256205-1306401843-  
4235927180?code=AAAAAAAAAAAAAAA. lxt7fs590QgJA  
JqMtW9C8KN6tLE.SzhnV- R4lbKXj46nwlbFUm6SLnyryJNE72e  
g3797LwkSfFQsSNpr7E9sUlCYBH52xvLZDAbwwu7qXCMlqCuVciQ0j  
3P3-l3ep\_lOSJOD3LnwDnXb3MPM1UUNcGLxxVeJmeYhEr15Basdk  
WqGzTYrCJKf4jbVT0qb4HKEhpD2aQCDwqjeFF8mNwfne\_KL1Ve6Z  
TNwBWS41SauUnbCTM9qzx-MCDWKEPrLmRR14hCxIsaWfrHmiE  
Ybfl4JXyGcJvhUyffcl-UVwJsQSBjHGlbQXIwrba-ejvvZ6me3YC8CL  
oS2pvXAMzbppBfg8YAJbGzBPNplbkjM10A7OKifLT4yqQ

# Token Request – Authorization Code

HTTP POST

- code=<Authorization Code>
- redirect\_uri=https://www.davetestapp.com
- grant\_type=authorization\_code
- client\_id=3fb2a37f-4ced-409c-937c-dddd776f4fd"

# Token Response

```
{"access_token":"eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6ImPIUVExOS1fVGRuSzRqTlJvbn-JZYTF2a0pIWSJ9eyJhdWQiOiJodHRwczovL3d3dy5kYXZldGVzdGFwcC5jb20iLCJpc3MiOi-JodHRwOi8vc3RzMnzb3Vkcma
```

```
VhZHkubXMvYWRmcy9zZXJ2aWNlcyc90cnVzdClslmlhdCI6MTQwNzE3MjQ4OSwiZXhwI-joxNDA3MTc2MDg5LCJlbWFpbCI6ImRncmVnQG1pY3Jvc29mdC5jb20iLCJ1cG4iOijkZ3JIz0BjbG91ZHJ-IYWR5LmludGVybmFslwiYXV0a
```

```
F90aW1lljoiMjAxNC0wOC0wNFQxNzoxND00OC44NTZaliwiYXV0aG1IdGhvZCI6InVybjpvYXN-pczpuYW1lczp0YzpTQU1MOjluMDphYzpjbGFzc2VzOIBhc3N3b3JkUHJvdGVjdGVkVHJhbnNwb3J0liwid-mVyljoiMS4wliwiYXBwaWQ
```

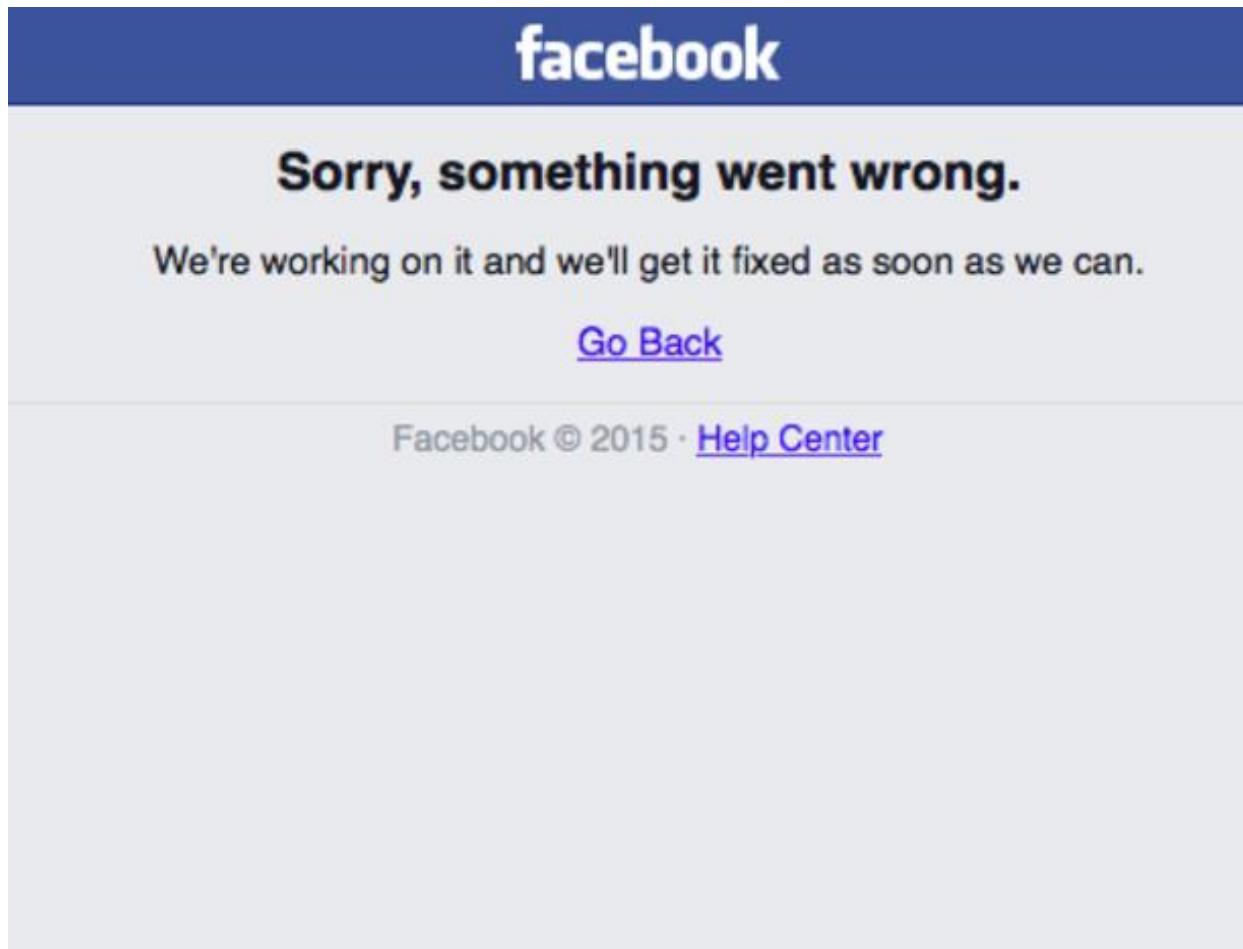
```
iOilzZmlyYTM3Zi00Y2VkLTQwOWMtOTM3Yy1kZGRkNzc2ZjRkZmQifQ.bkMvnIJaB6DRdyCiTLsxstPtqvGyd-cAmsXQjEumMjH4IN75jx2uCCLg44PU-aXSHZ6R-dOth1iqD-Lf-xy4SKw0O0Z5_oQhPn-3-H0DII3SxtDuR5vr-BObKVc-DT8HGxEHQqPPB5EyF_H21fJ_cqjz-dNyVXK_WoTbM1gQf44Lz5250NjFKjIA1M4sG8bjh-mjo-HZMhR3SwtixCNmQKqYai_8S5KZz1Srg1oIGprwRDbT-NVdzh7Qv0vg1RgaejF3i1J-kWmf2Zx_PVQflTAfzu01BUvAiQCOK7-V4RsduEOTSEI9SYVt2E8pvkUrmNdo-hVKVWopfOK3r0zXZwTYT4w","token_type":"bearer","expires_in":3600}
```

# Token Request – Password grant type

POST https://api.oauth2server.com/token

grant\_type=password&  
username=USERNAME&  
password=PASSWORD&  
client\_id=CLIENT\_ID

# DoS Risk



# DoS Risk

## You're Temporarily Blocked for 30 Days

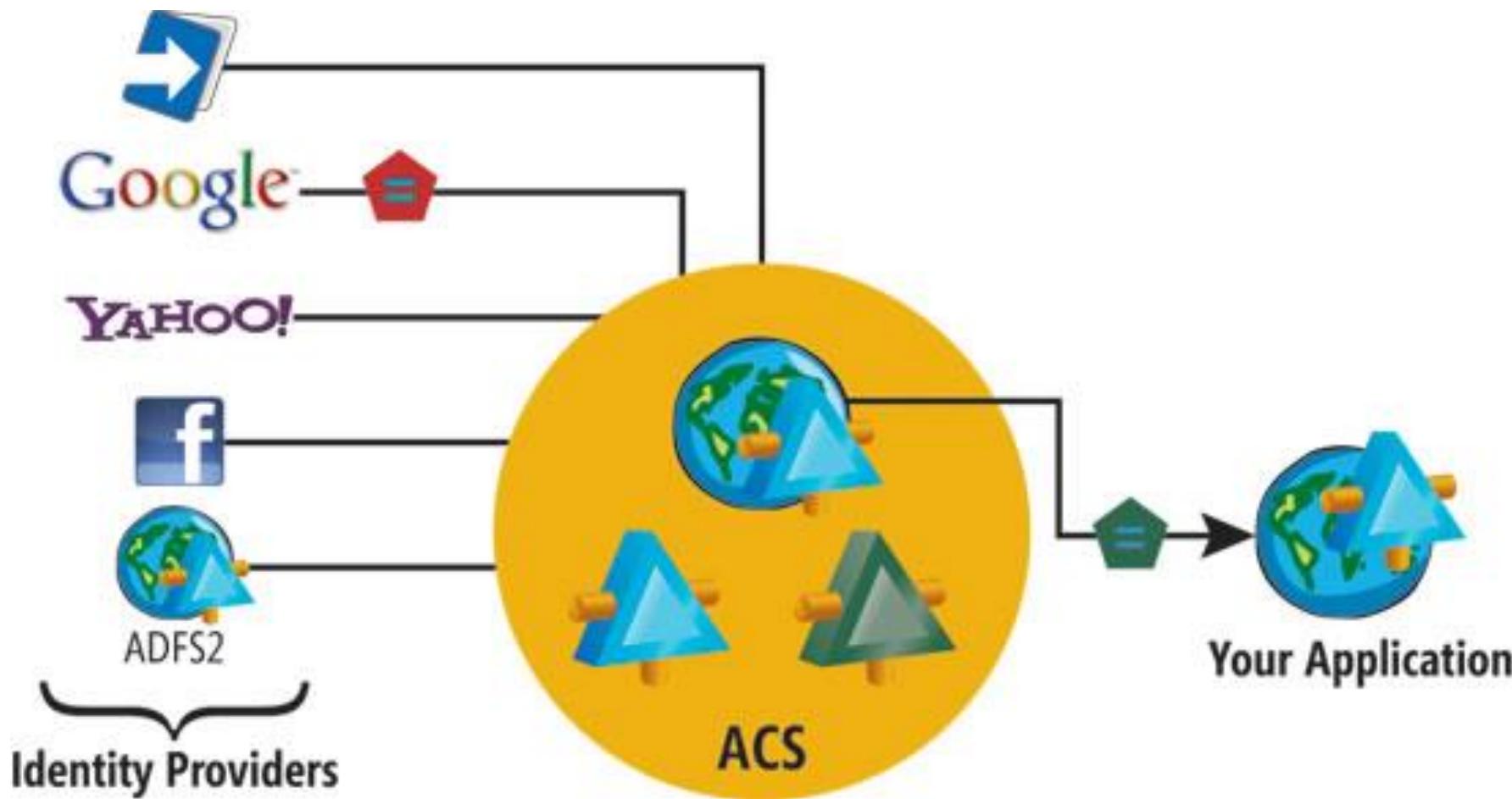
You've been temporarily blocked from using certain features because you violated Facebook's Terms. Please review the Community Standards to learn what's okay to share on Facebook.

This block will be lifted in 30 days, but if you continue to violate Facebook's Terms, your account could be permanently disabled.

[Facebook Community Standards](#)

下一页

# Identity Bridges



# Virtualization + Cloud & Security

Mgr. Michael Grafnetter

Microsoft Services

