Microsoft

Virtualization + Cloud & Security

Mgr. Michael Grafnetter

Microsoft Services

Agenda

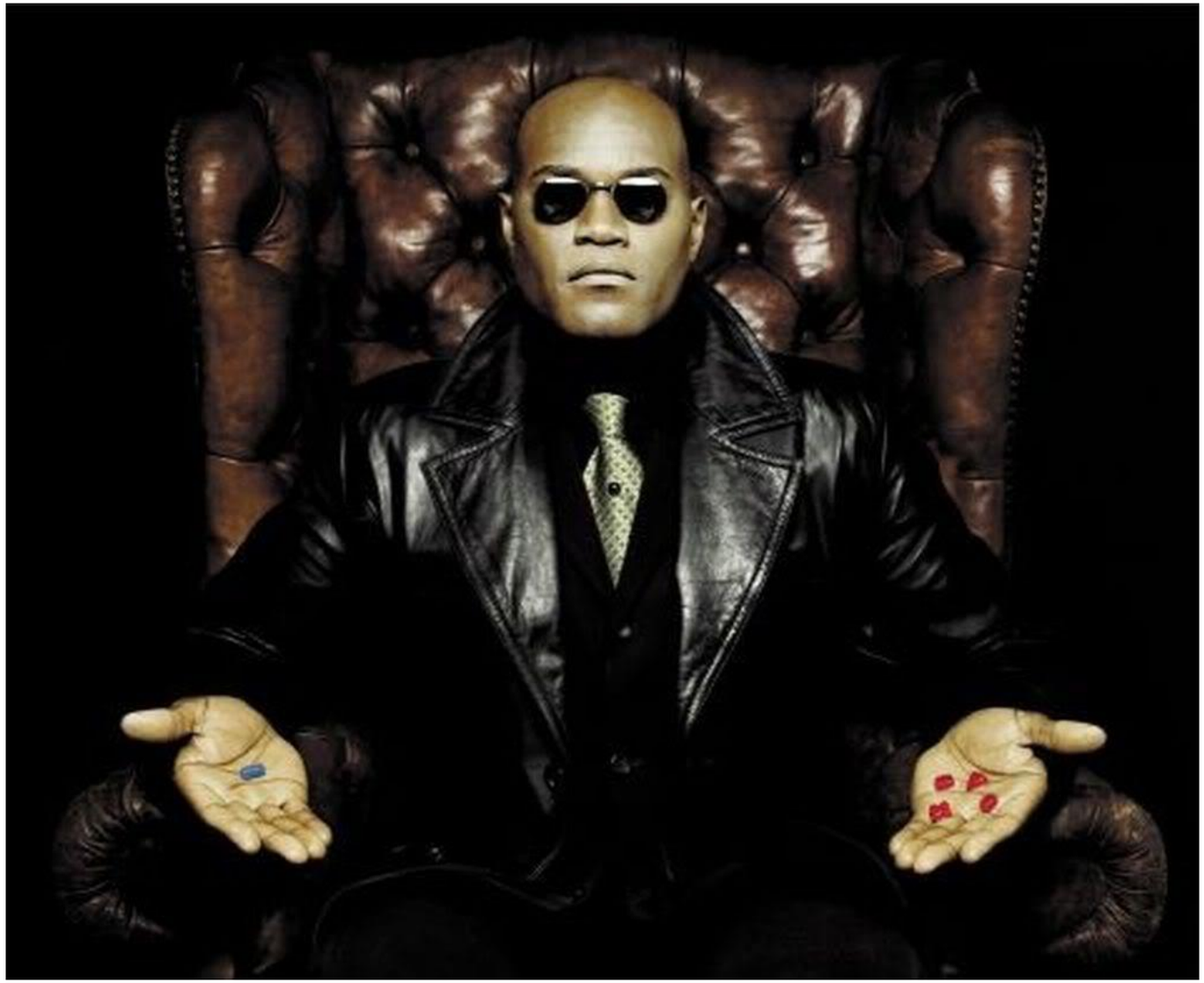
- Virtualization Security Risks and Solutions
- Cloud Computing Security Risks
- Authentication in Cloud Applications

Microsoft

Virtualization Security Risks and Solutions

Microsoft Services

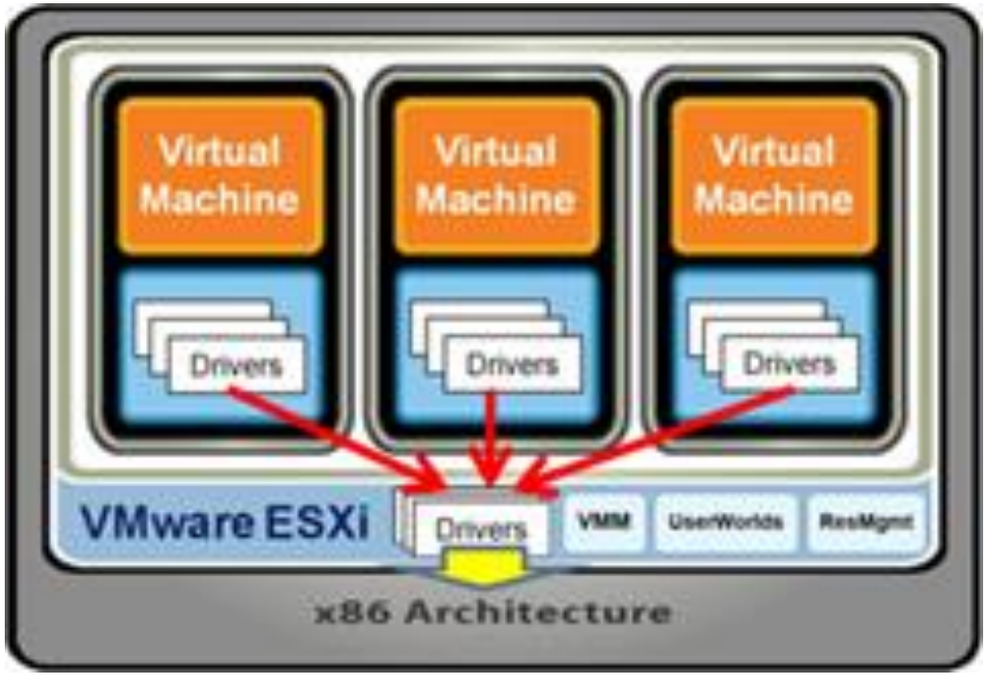
Blue Pill Attack

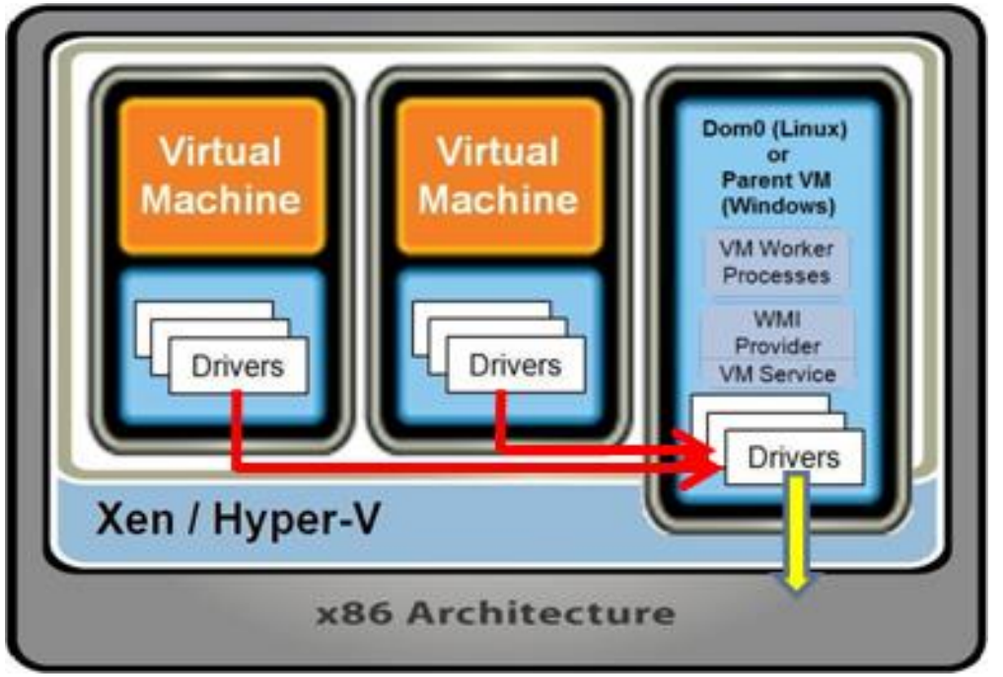


Blue Pill Attack

- 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

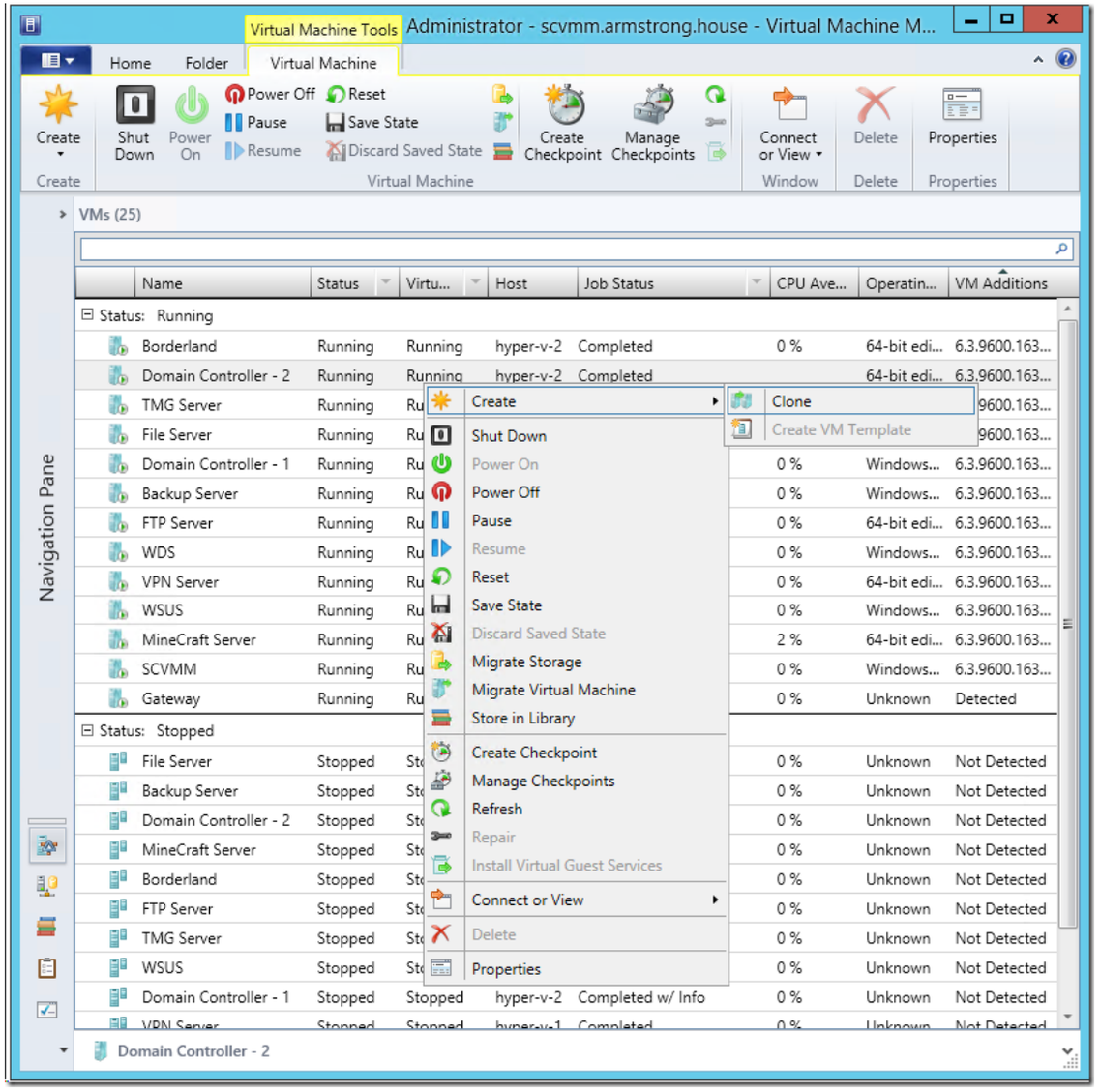
VMM Vulnerability





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

Datacenter Management SW

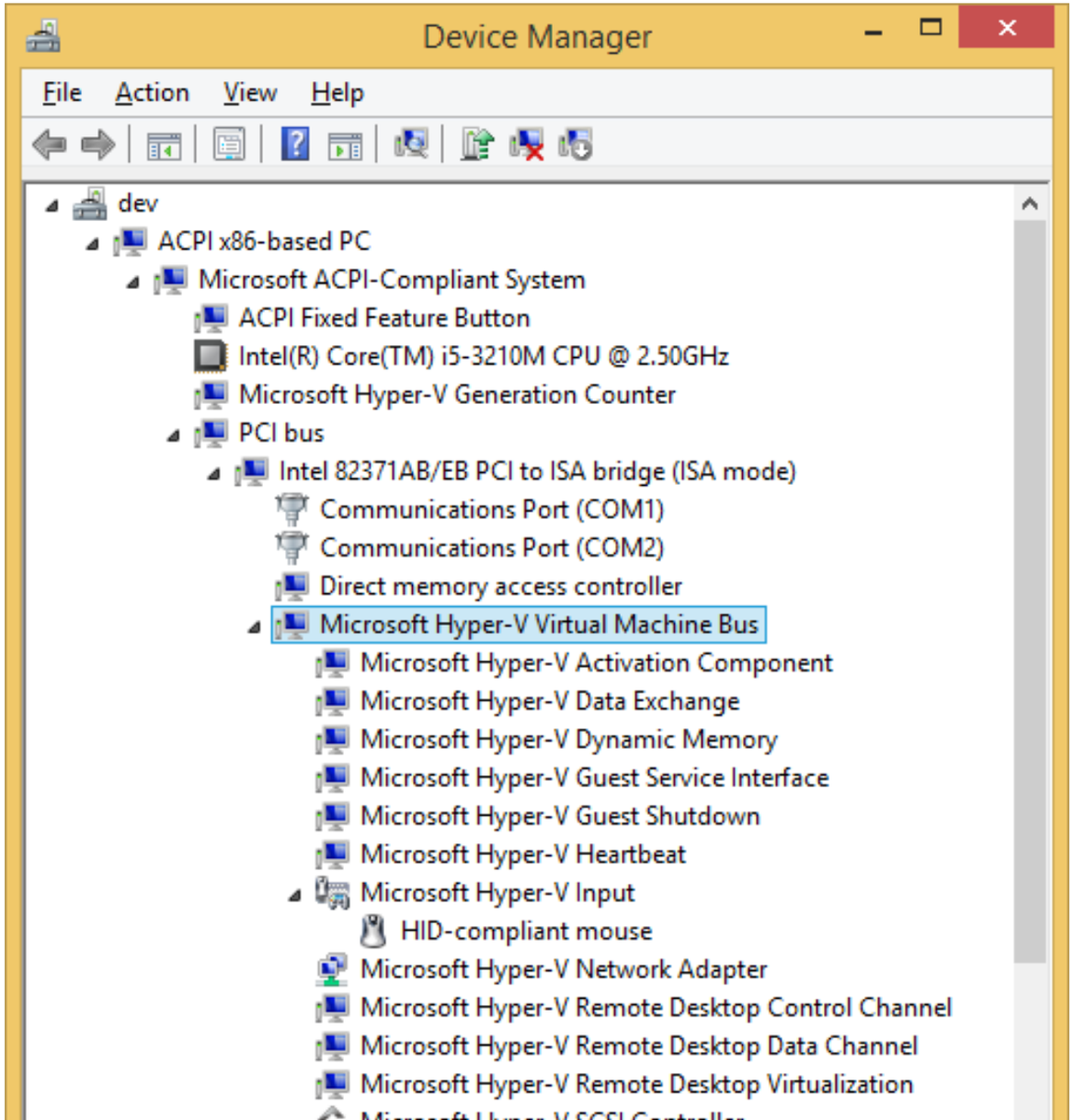


Hypervisor Management + VM Bus

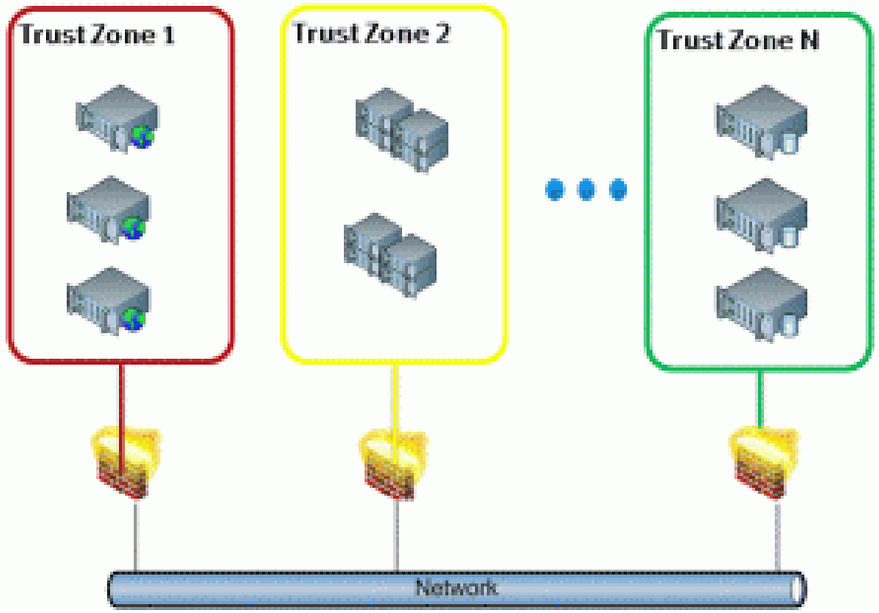
Management commands available using PowerShell or Web APIs

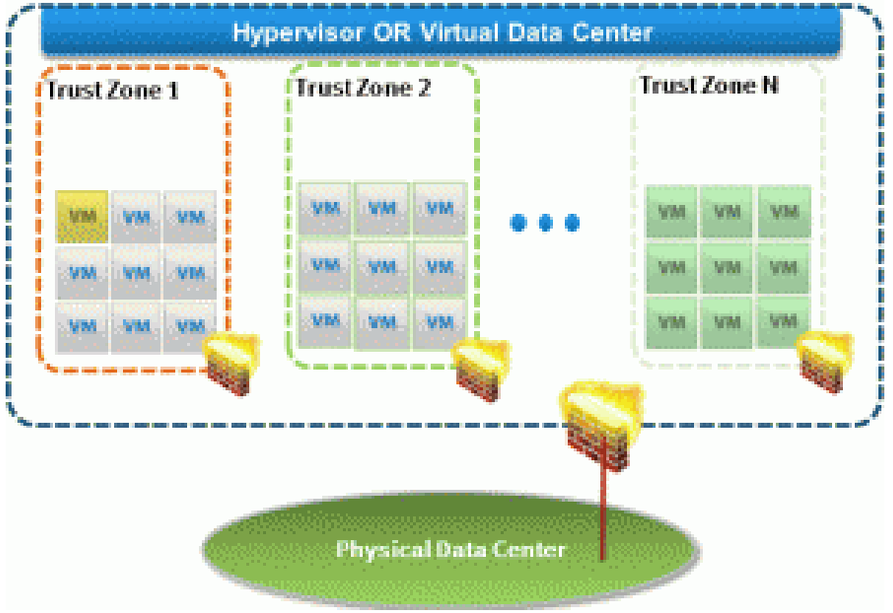
- Get-VM –Name * | Stop-VM
- Get-VM –Name * | Remove-VM
- Copy-VMGuestFile
- Invoke-VMScript –Type Bash
- …

VM Bus


Device Manager
File
Action
View
Help
dev
ACPI x86-based PC
Microsoft ACPI-Compliant System
ACPI Fixed Feature Button
Intel(R) Core(TM) i5-3210M CPU @ 2.50GHz
Microsoft Hyper-V Generation Counter
PCI bus
Intel 82371AB/EB PCI to ISA bridge (ISA mode)
Communications Port (COM1)
Communications Port (COM2)
Direct memory access controller
Microsoft Hyper-V Virtual Machine Bus
Microsoft Hyper-V Activation Component
Microsoft Hyper-V Data Exchange
Microsoft Hyper-V Dynamic Memory
Microsoft Hyper-V Guest Service Interface
Microsoft Hyper-V Guest Shutdown
Microsoft Hyper-V Heartbeat
Microsoft Hyper-V Input
HID-compliant mouse
Microsoft Hyper-V Network Adapter
Microsoft Hyper-V Remote Desktop Control Channel
Microsoft Hyper-V Remote Desktop Data Channel
Microsoft Hyper-V Remote Desktop Virtualization

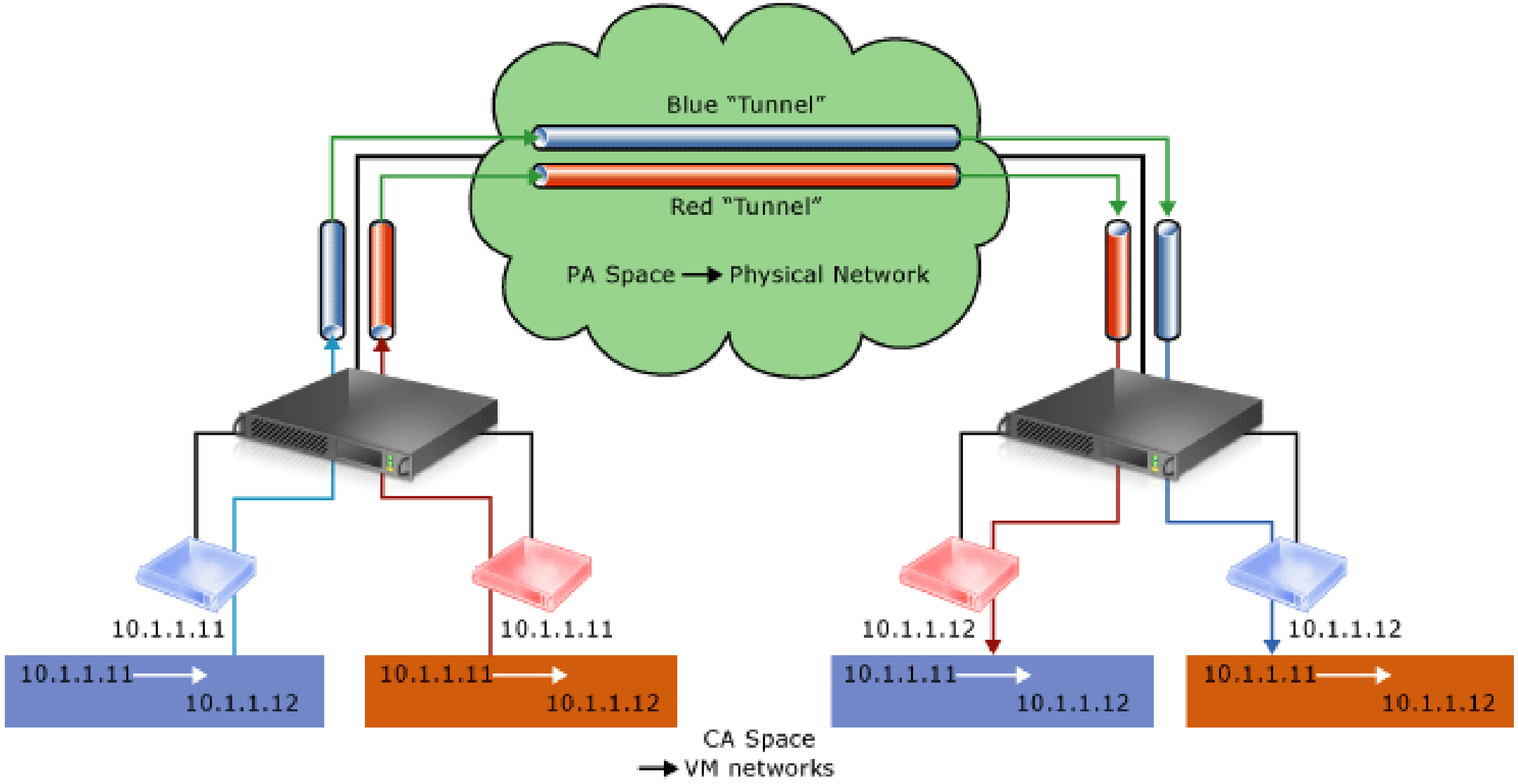
Physical vs. Virtual Firewall



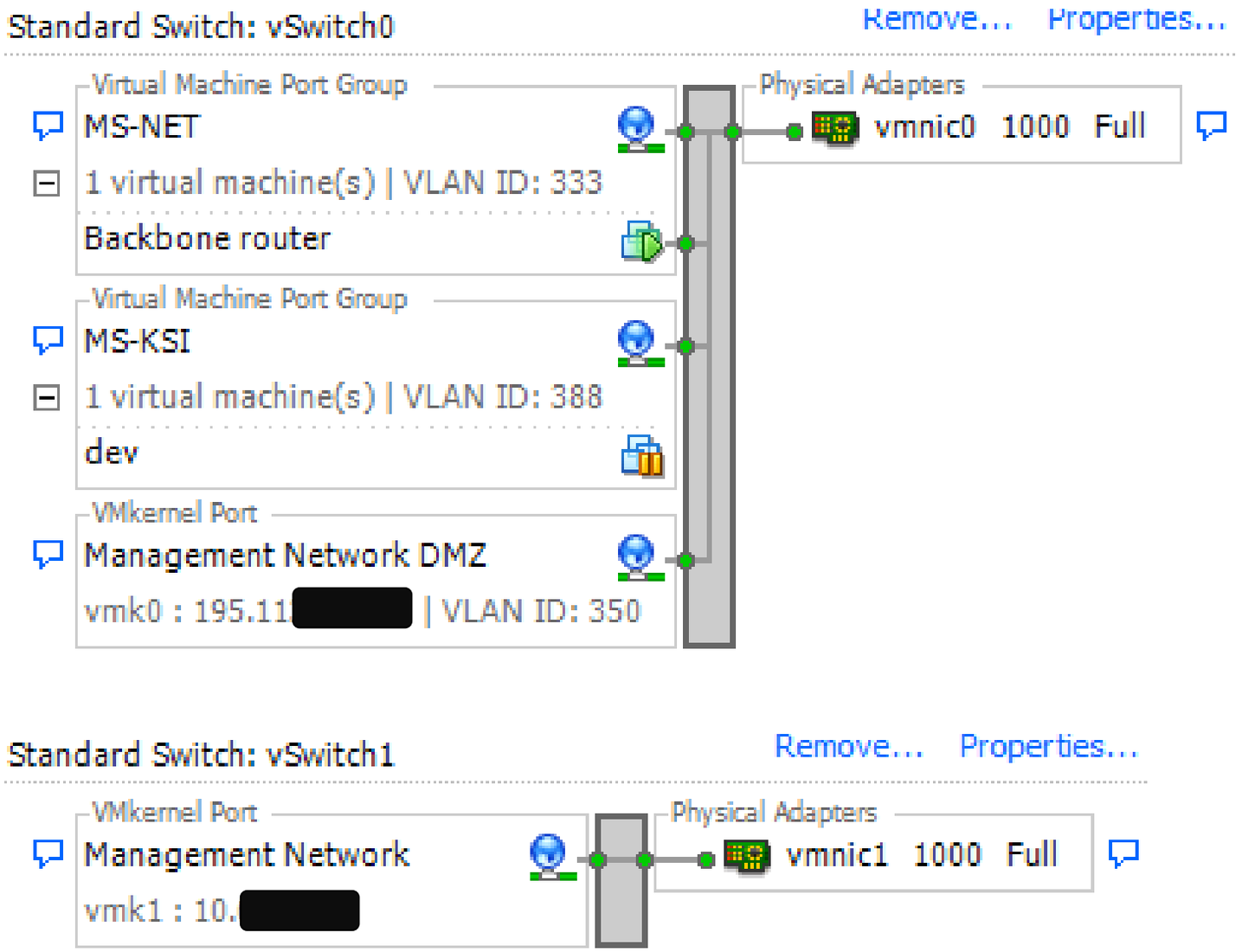


- With virtualization, servers from different Trust Zones usually share the same physical resources (memory, network card, etc.)

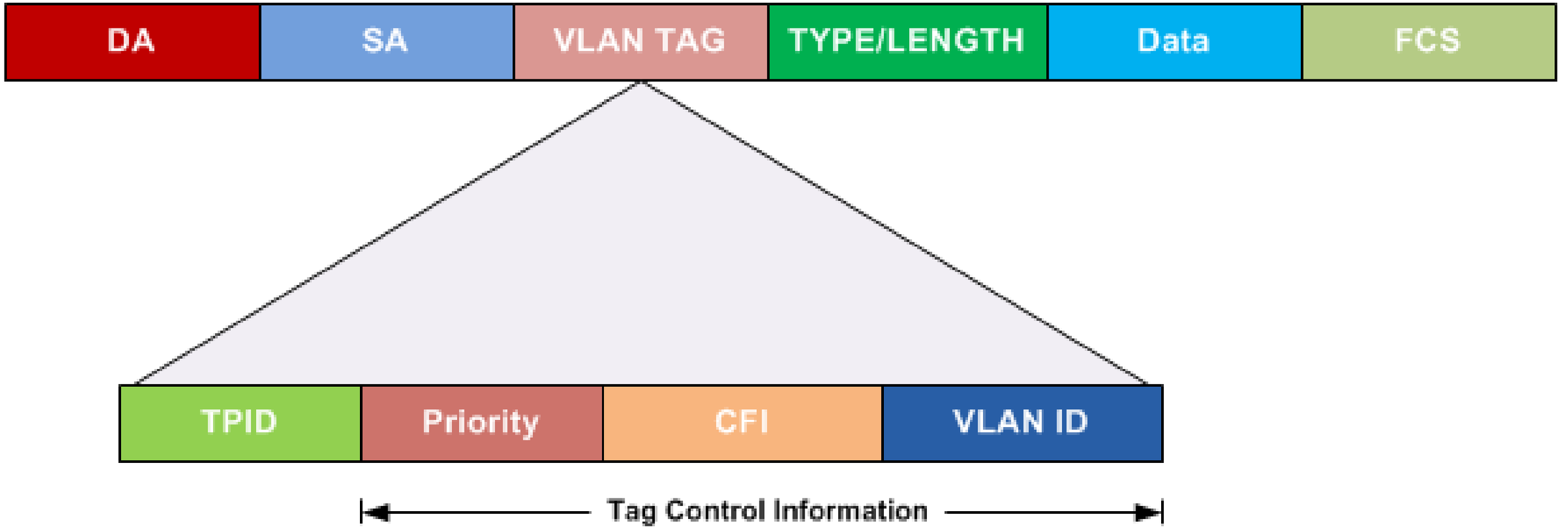
Traffic Isolation



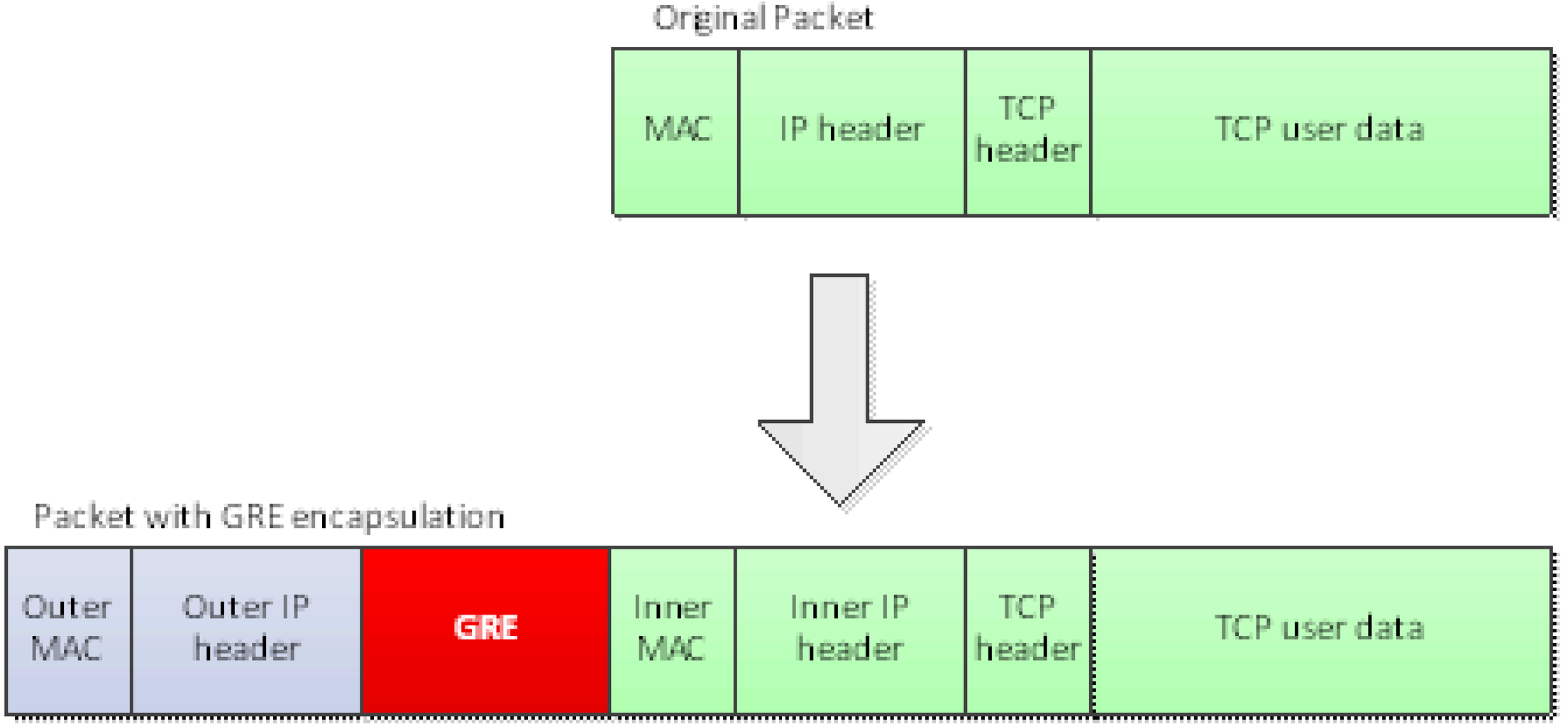
Traffic Isolation – VLAN Tagging



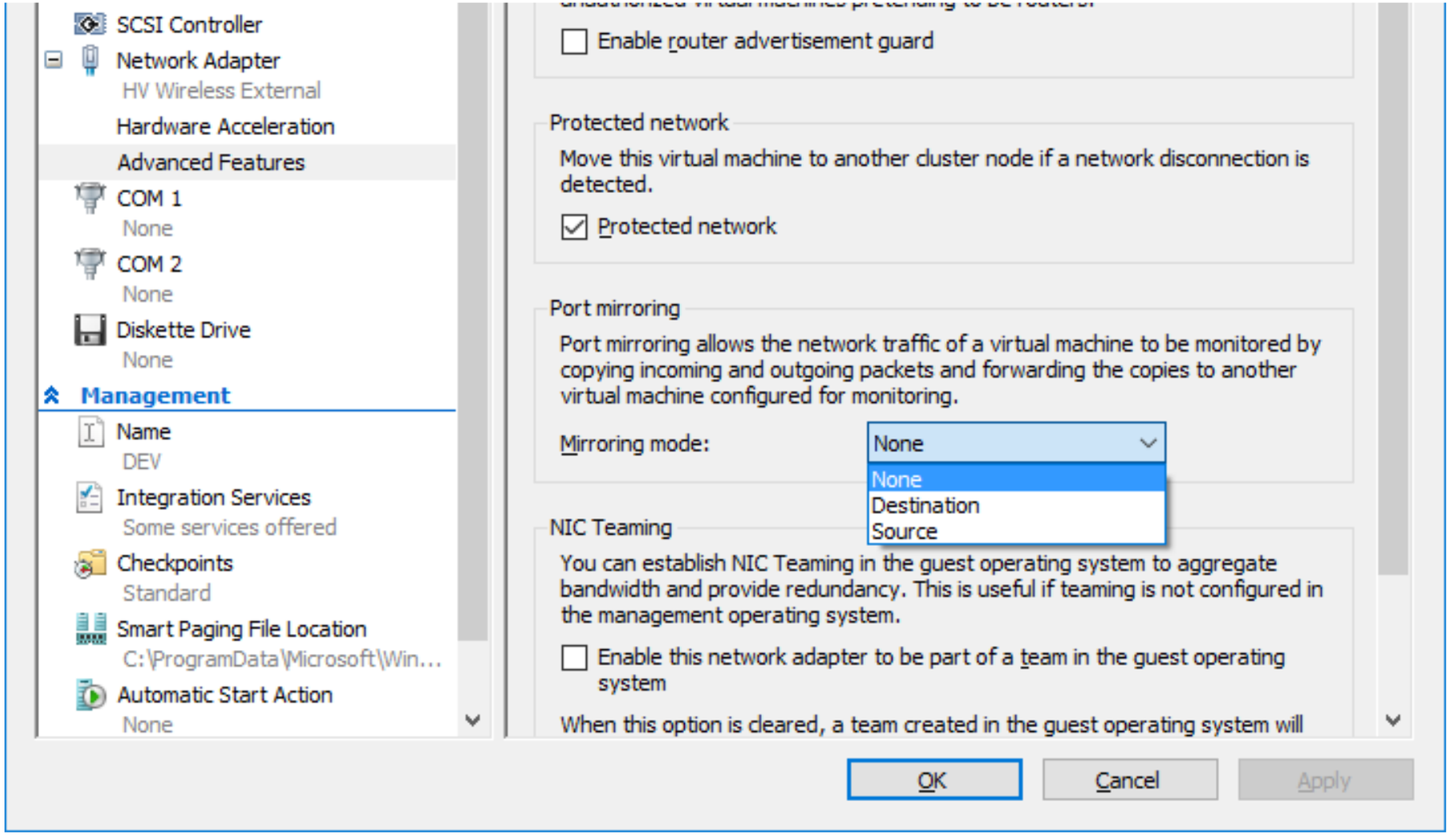
Traffic Isolation – VLAN Tagging



Traffic Isolation - NVGRE



Traffic Monitoring



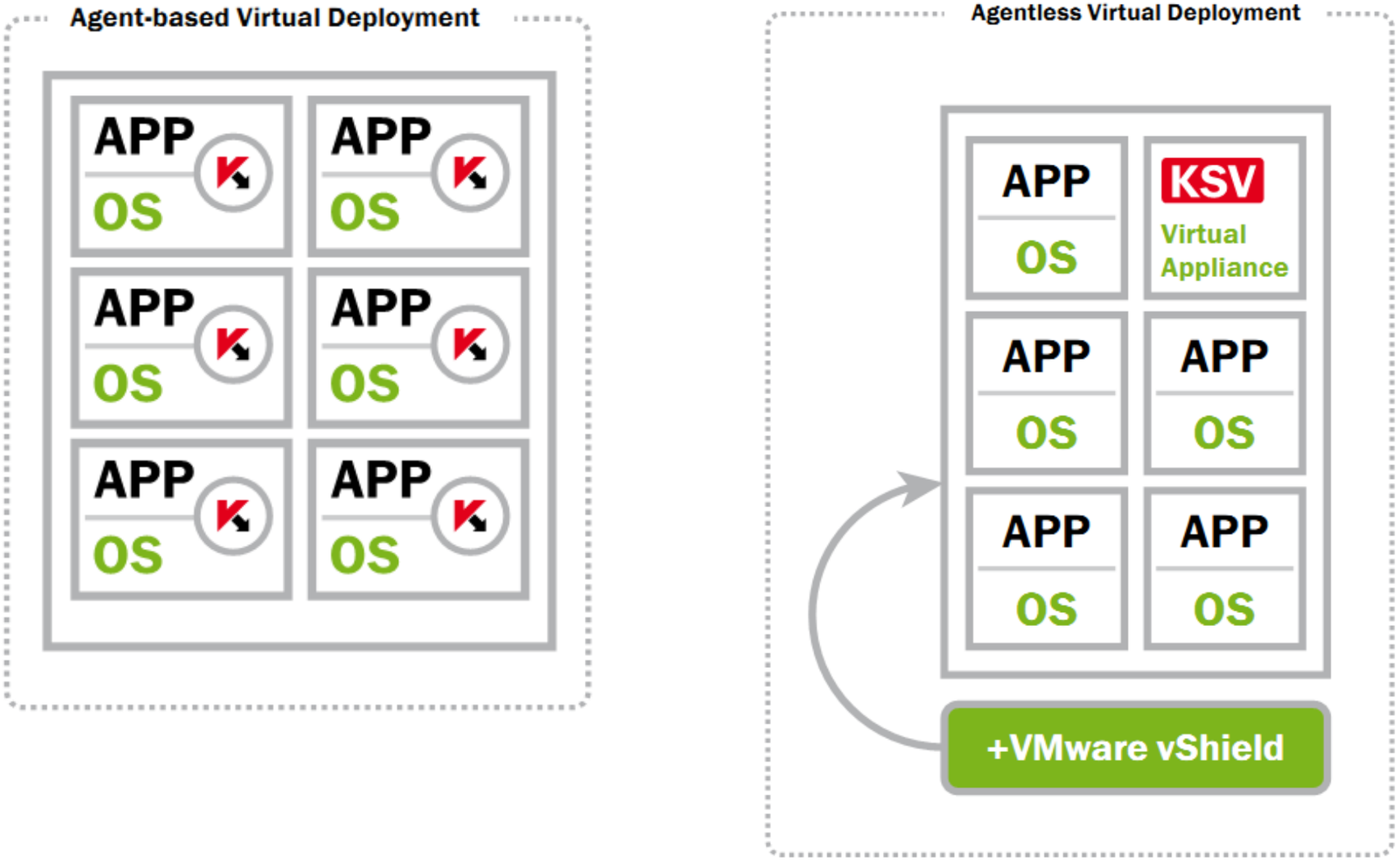
Other risks of virtualization

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

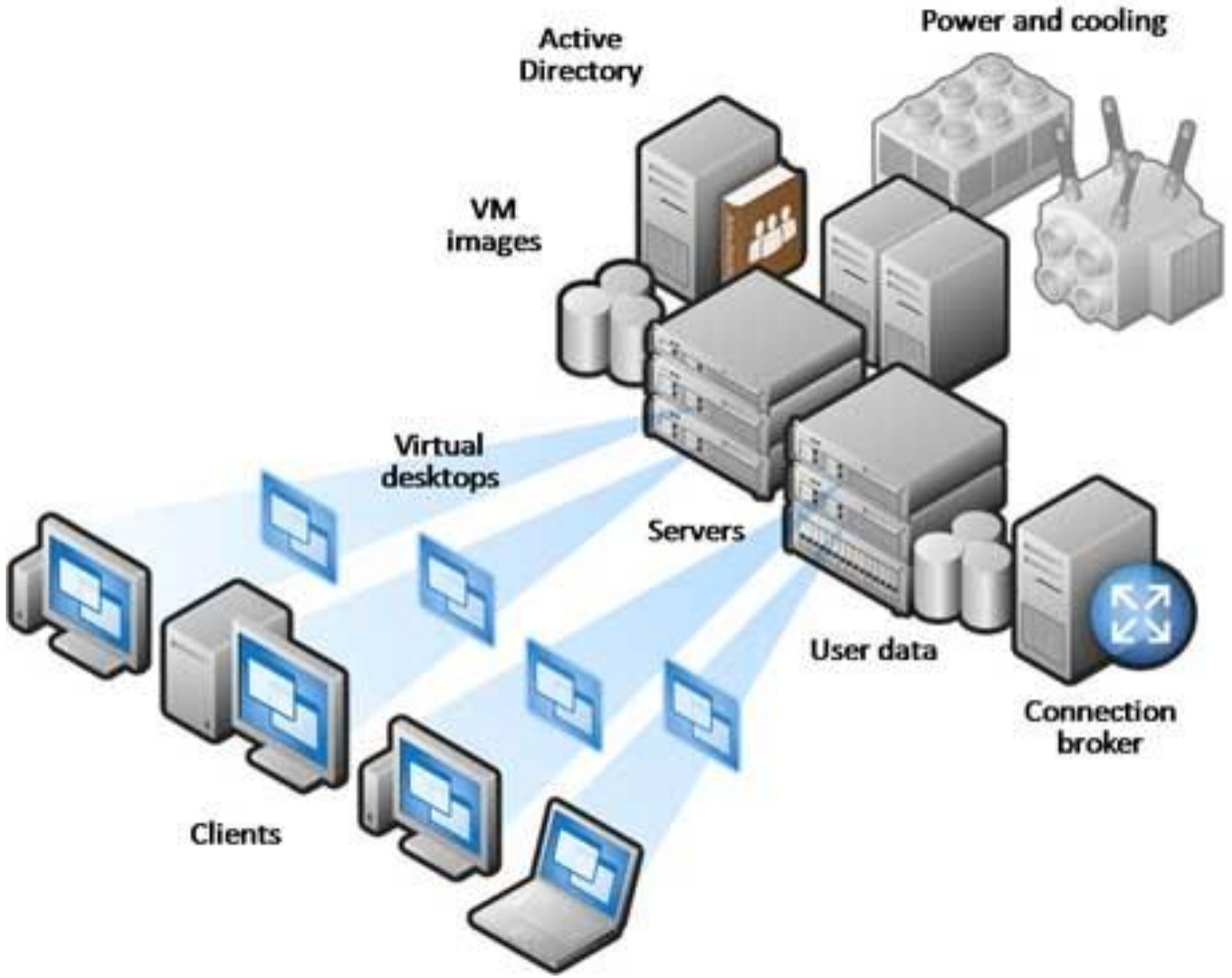
Security Solutions

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

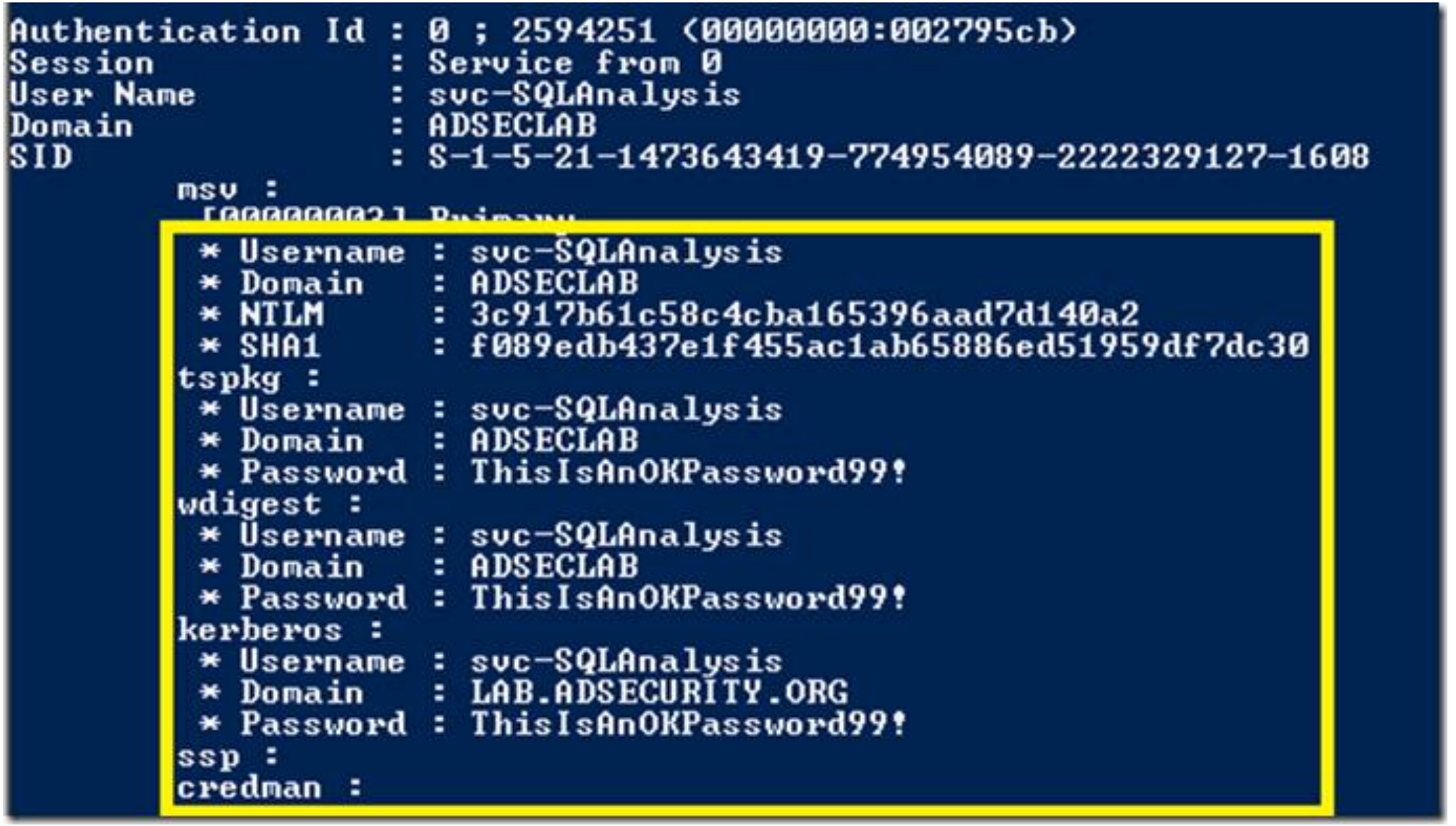
Agentless AV



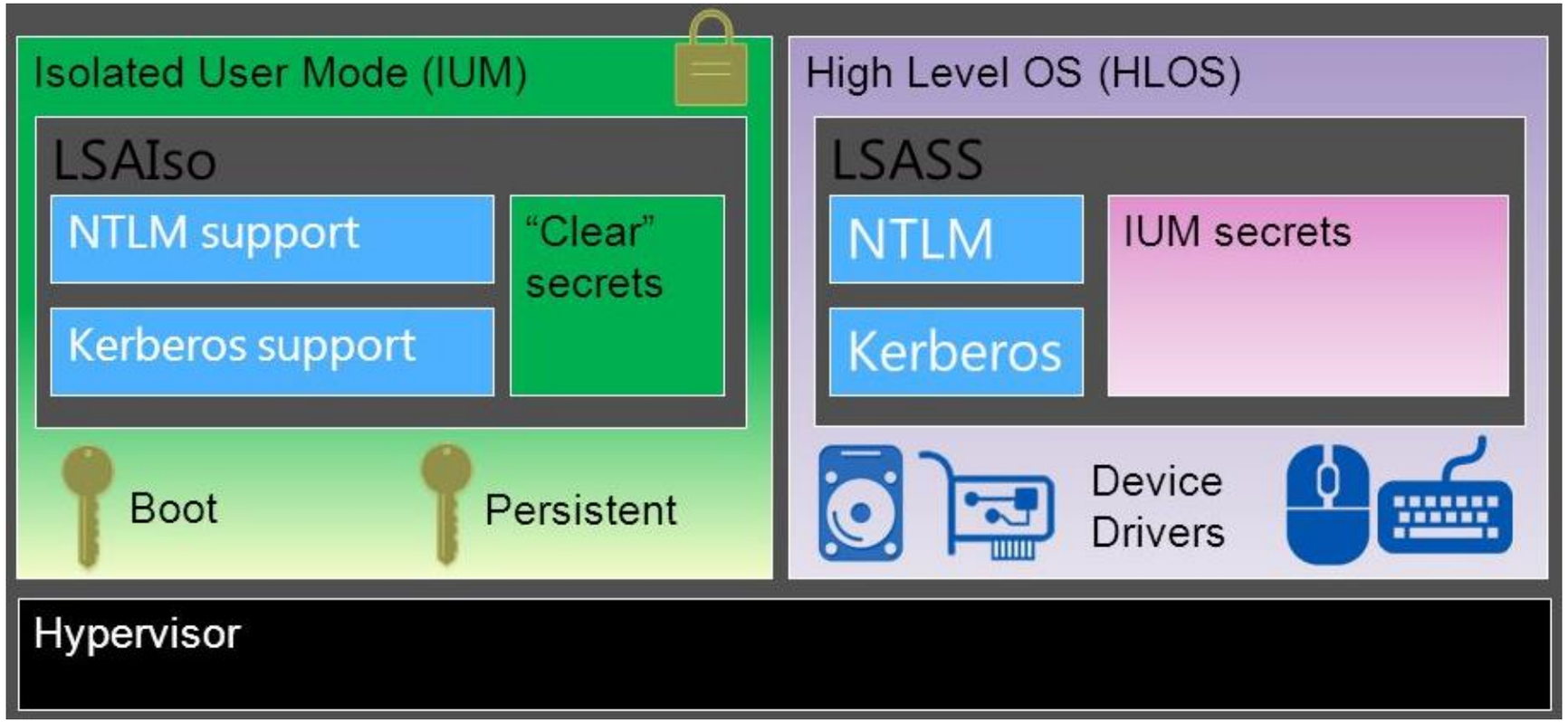
Virtual Desktop Infrastructure



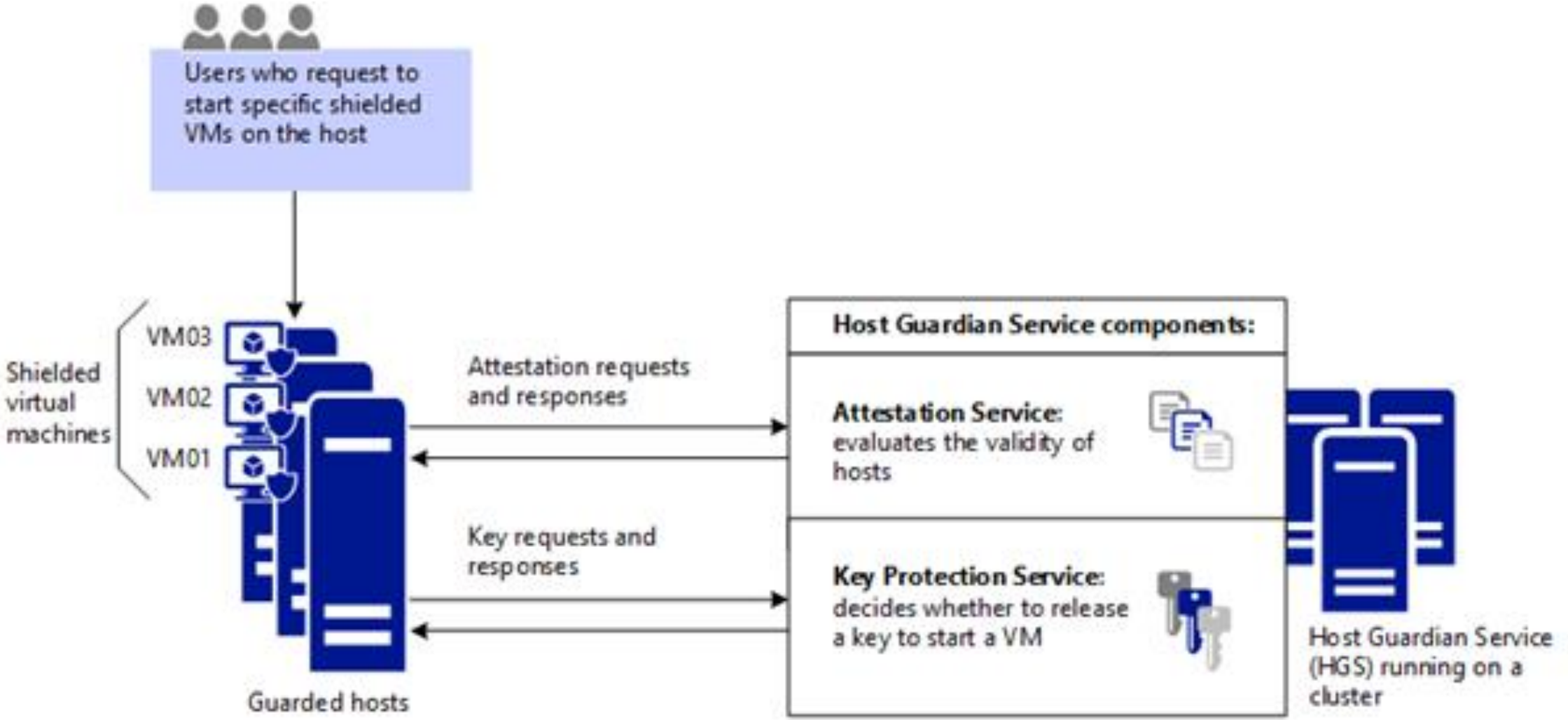
Windows 10 Virtual Secure Mode: Motivation



Windows 10 Virtual Secure Mode



Shielded VMs



Microsoft

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

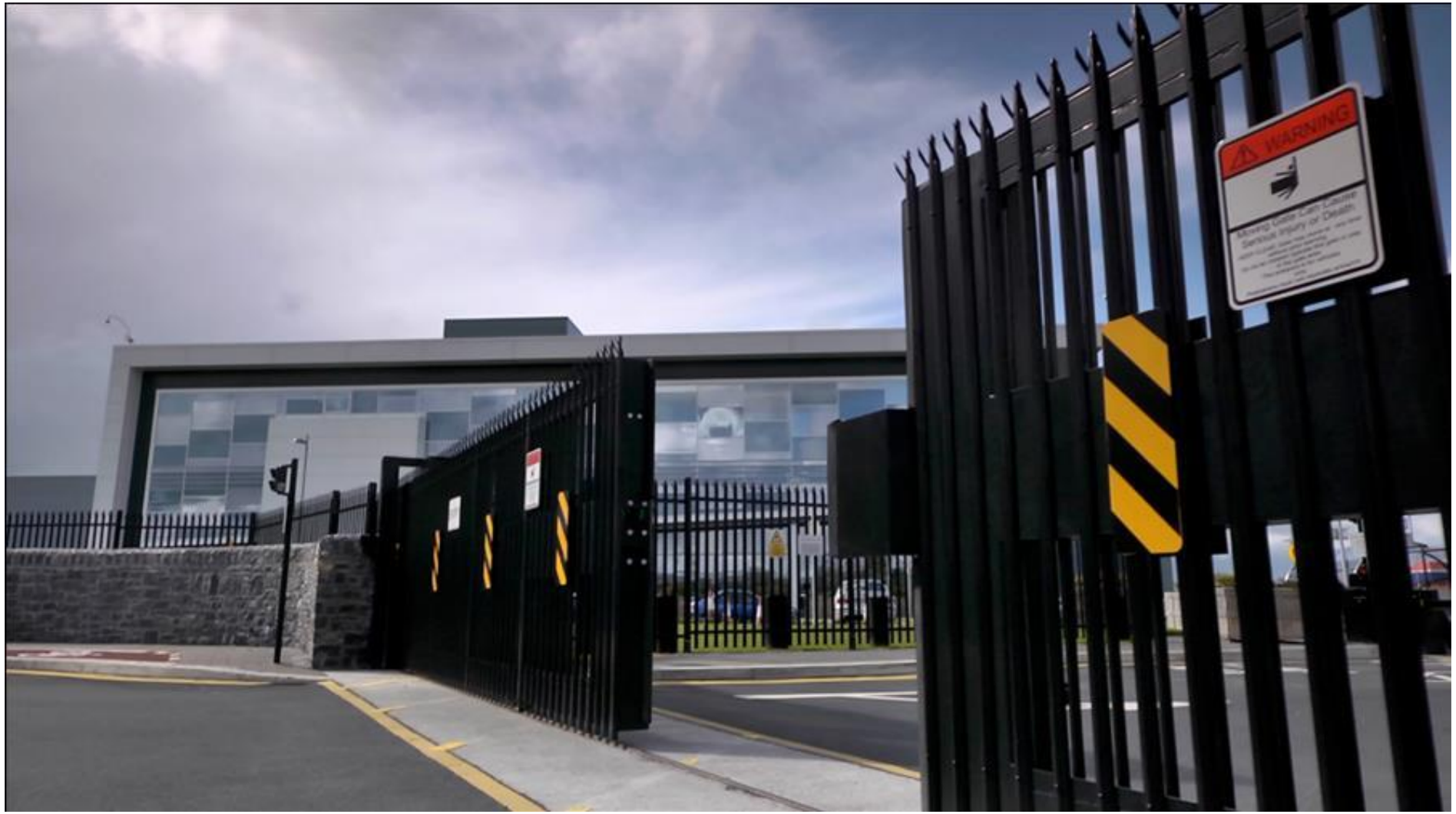
Anti-Virus/Anti-Malware
PROTECTION

Penetration **TESTING**

DDoS **DEFENSE**

Physical Security

Physical Security

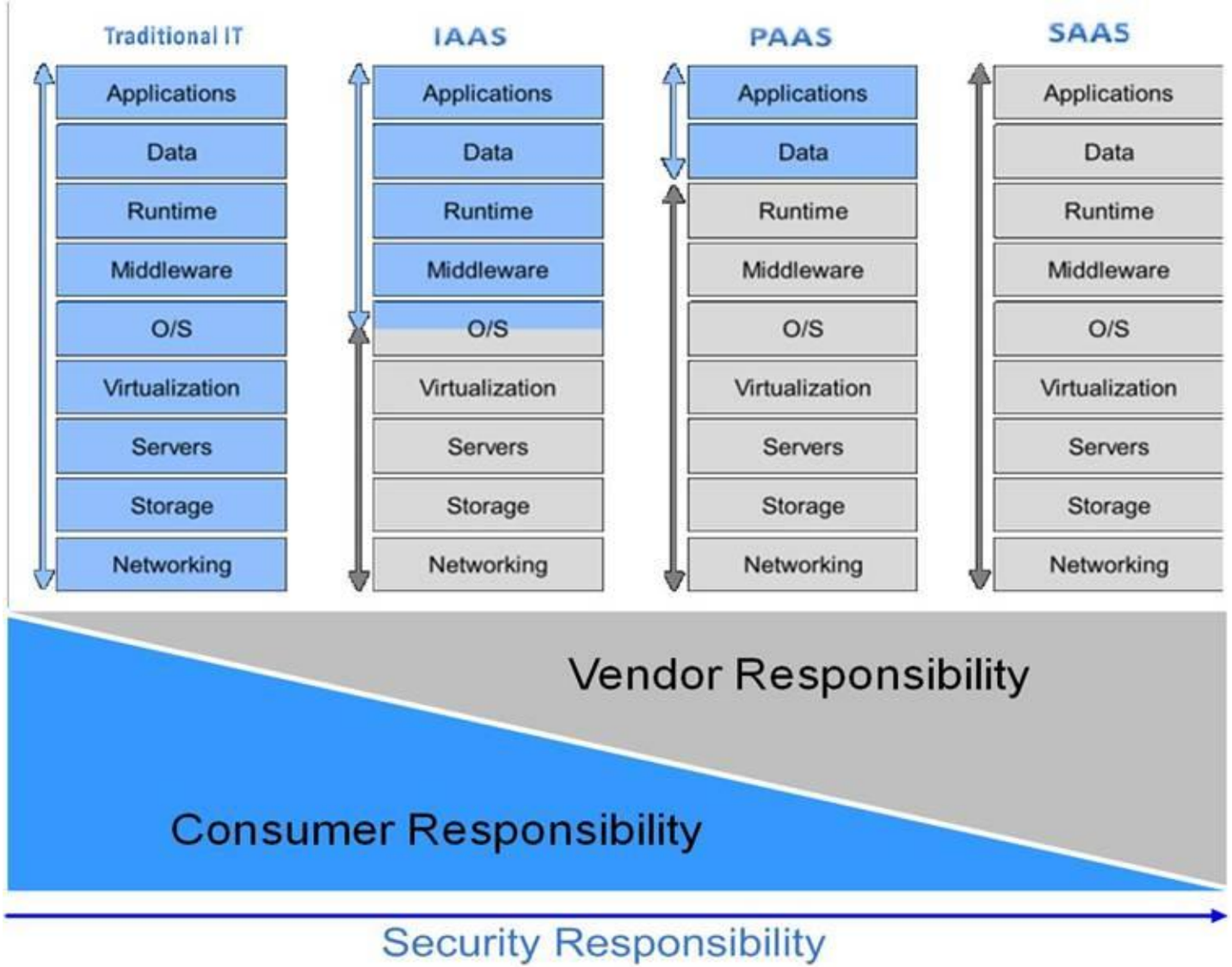


Physical Security

Physical Security

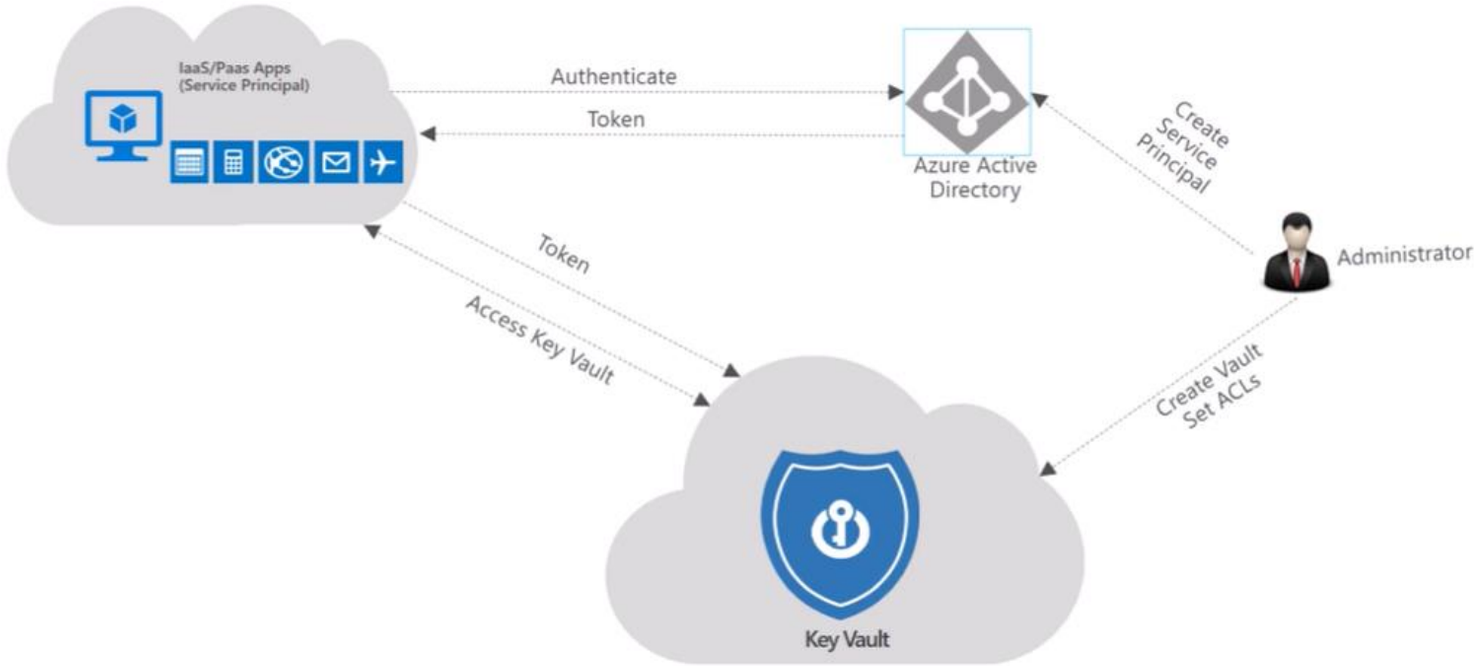
Hard Disk Crushers

Shared Responsibility

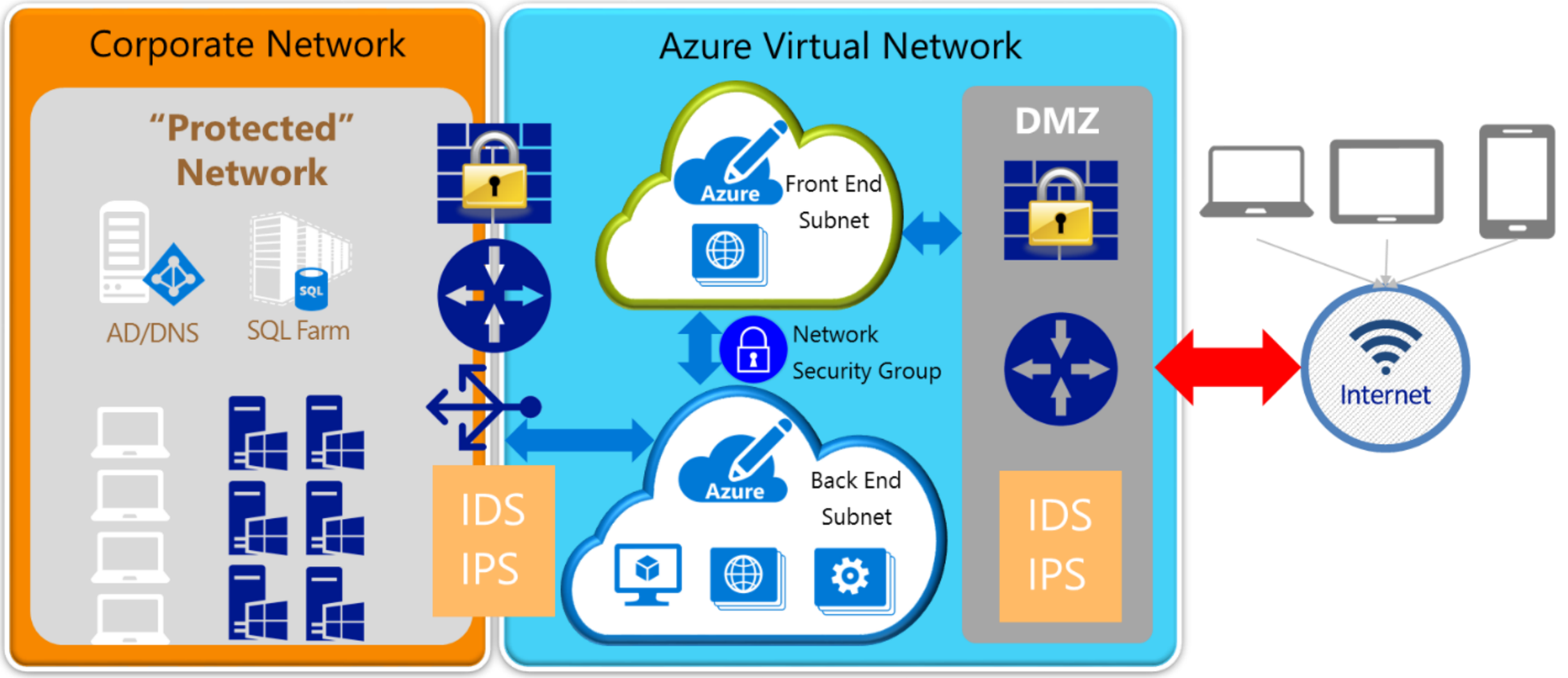


Custom Penetration Testing

Azure Key Vault



Hybrid Network Topology



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

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

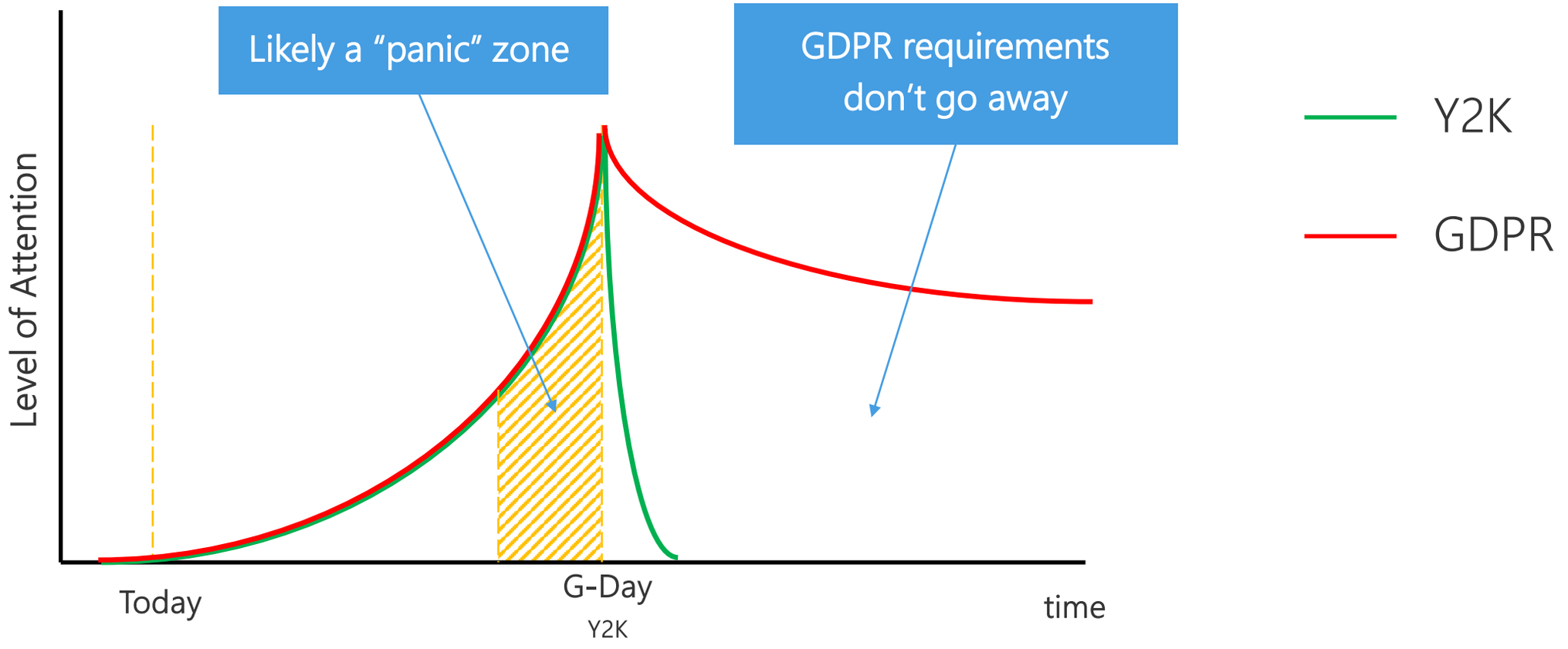
33 & 34: Notification of breaches

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

Microsoft

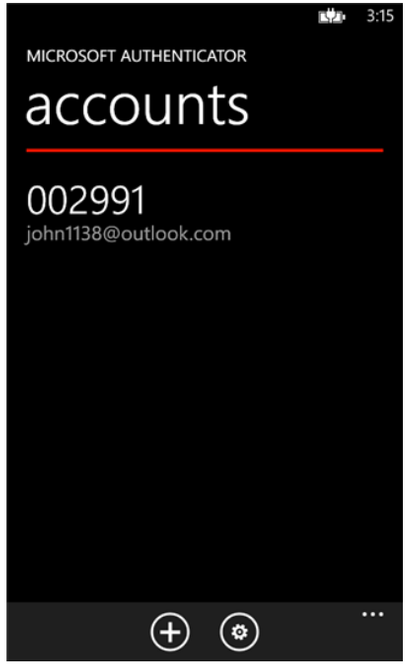
Authentication in Cloud Applications

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

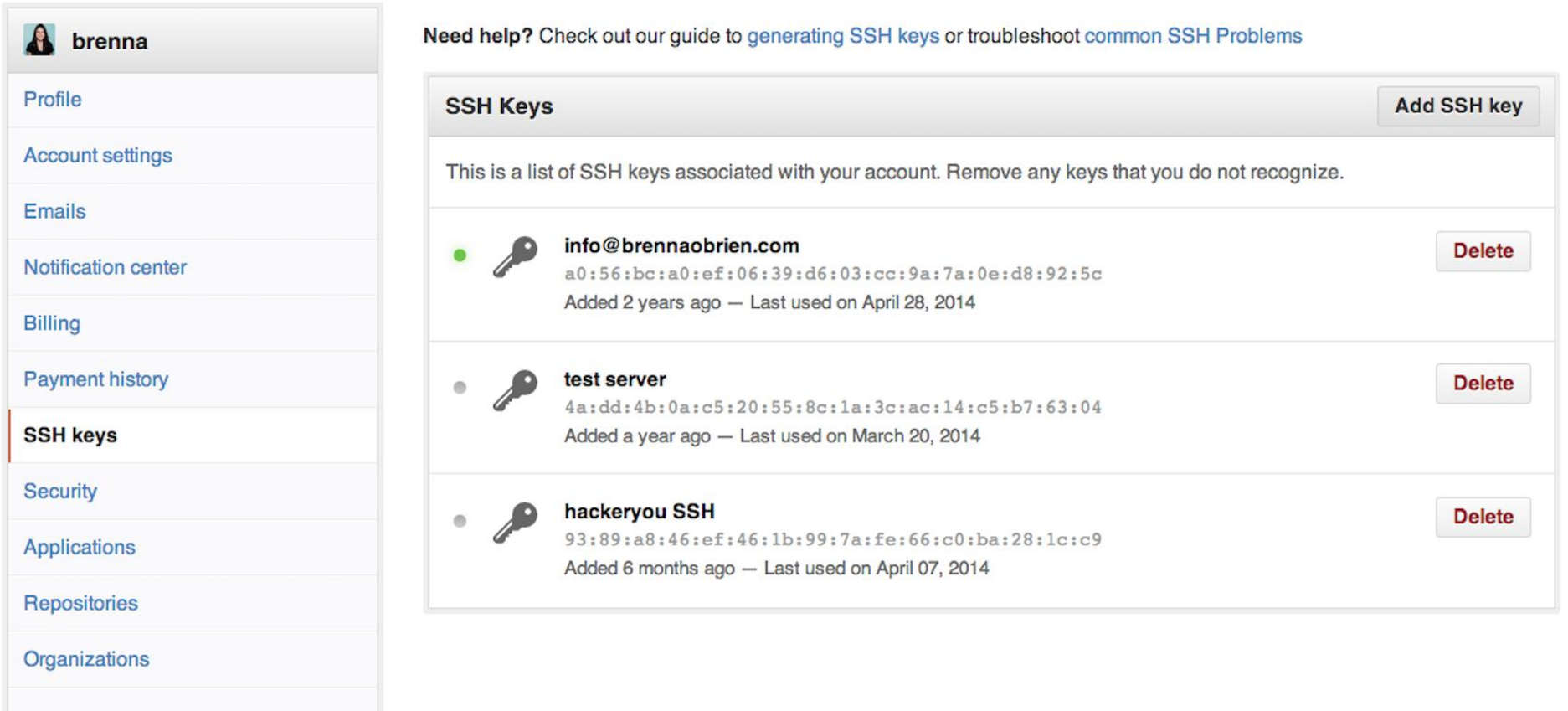
C – Counter/Clock

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



Microsoft

Claims-Based Identity

Microsoft Services

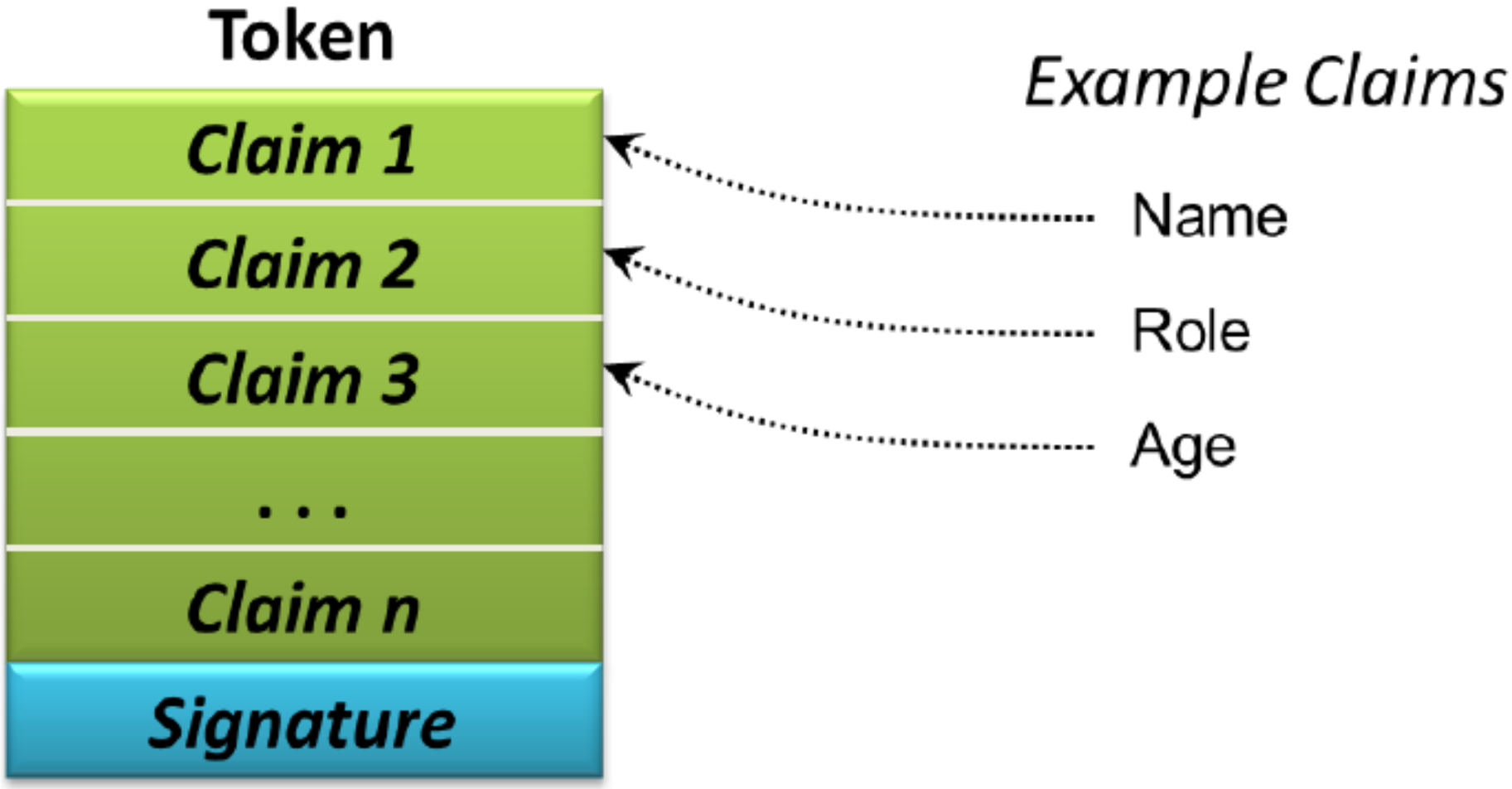
Most Common Technologies

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

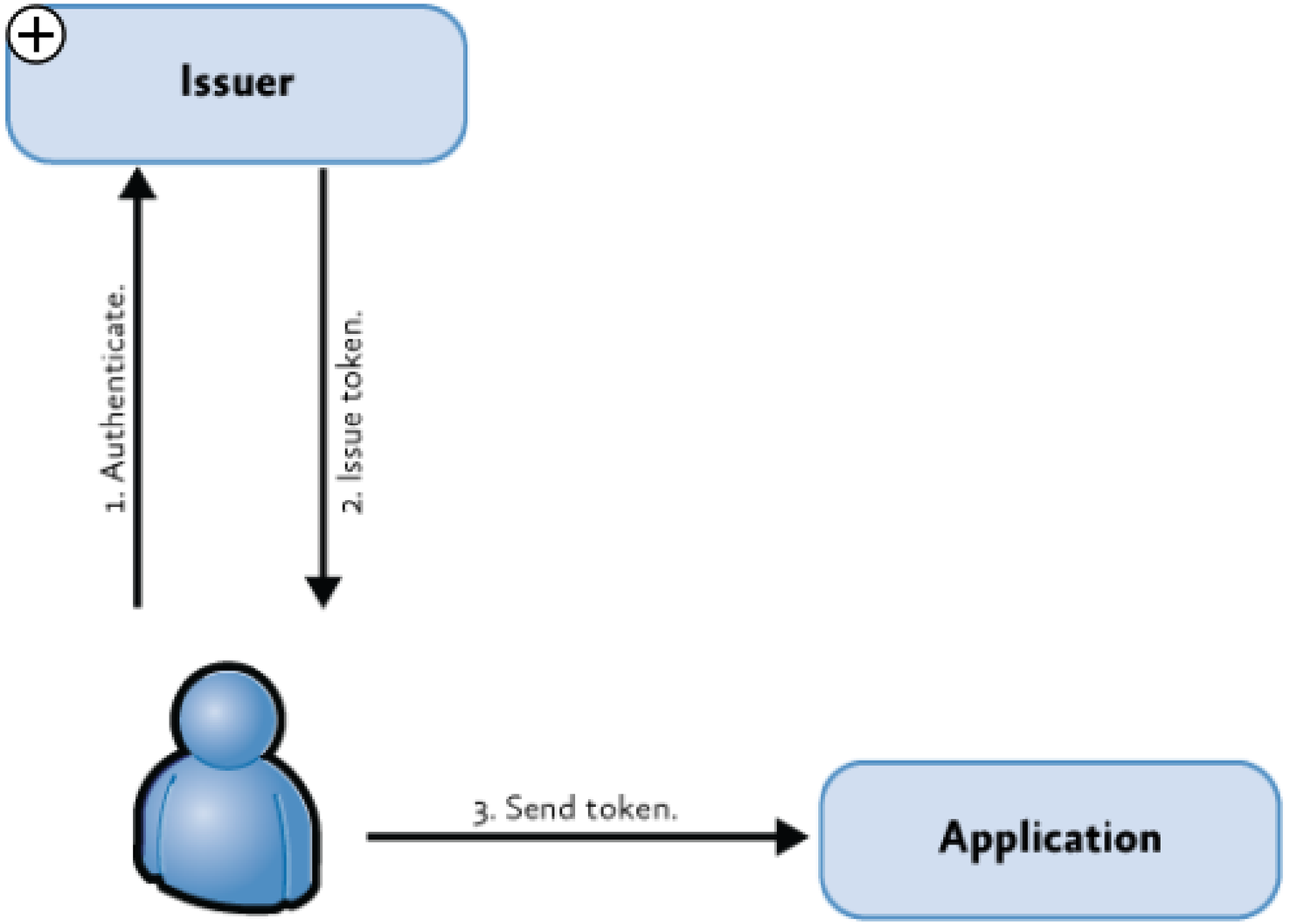
Claims-based Identity

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

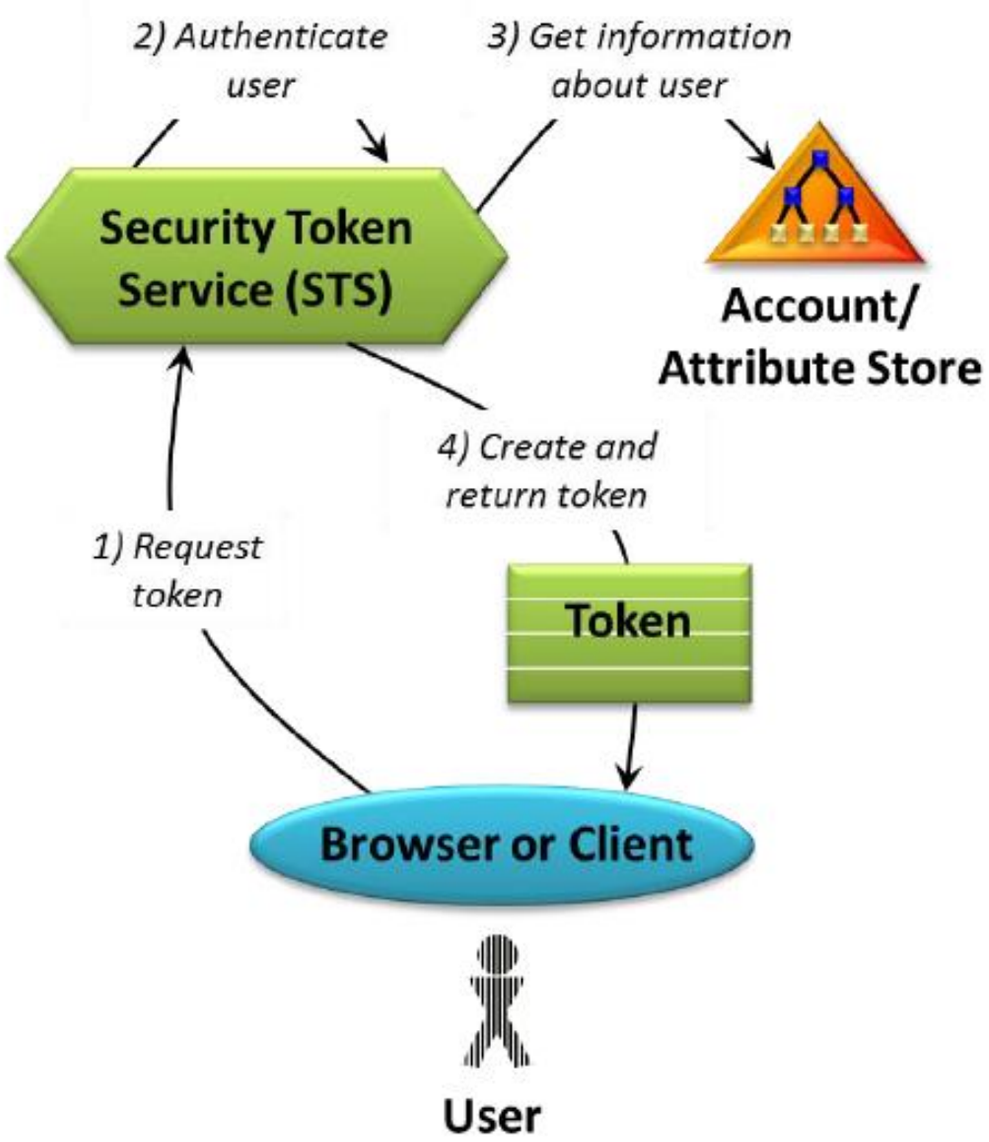
Tokens


Token
Claim 1
Claim 2
Claim 3
. . .
Claim n
Signature
Example Claims
Name
Role
Age

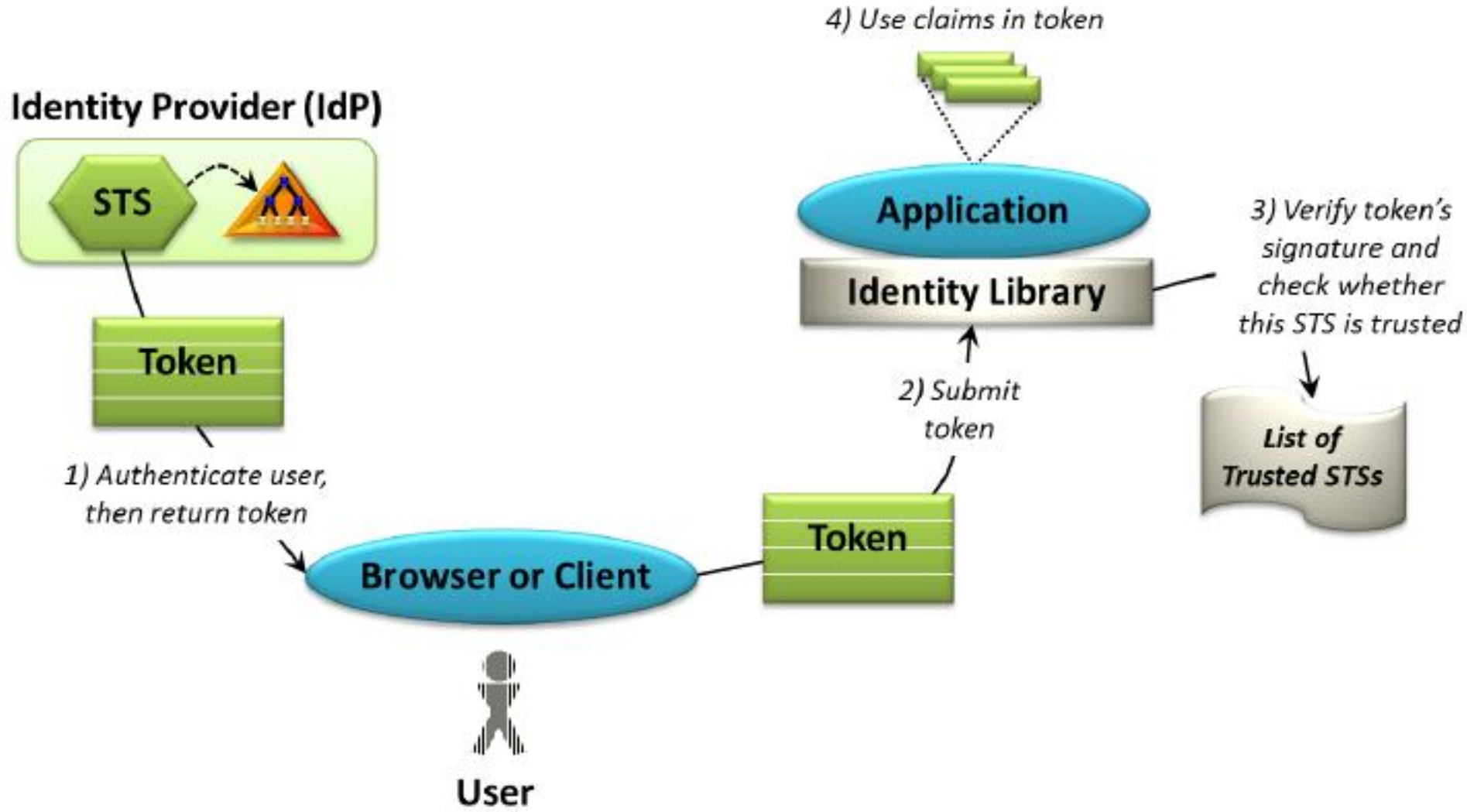
Basic Communication Pattern



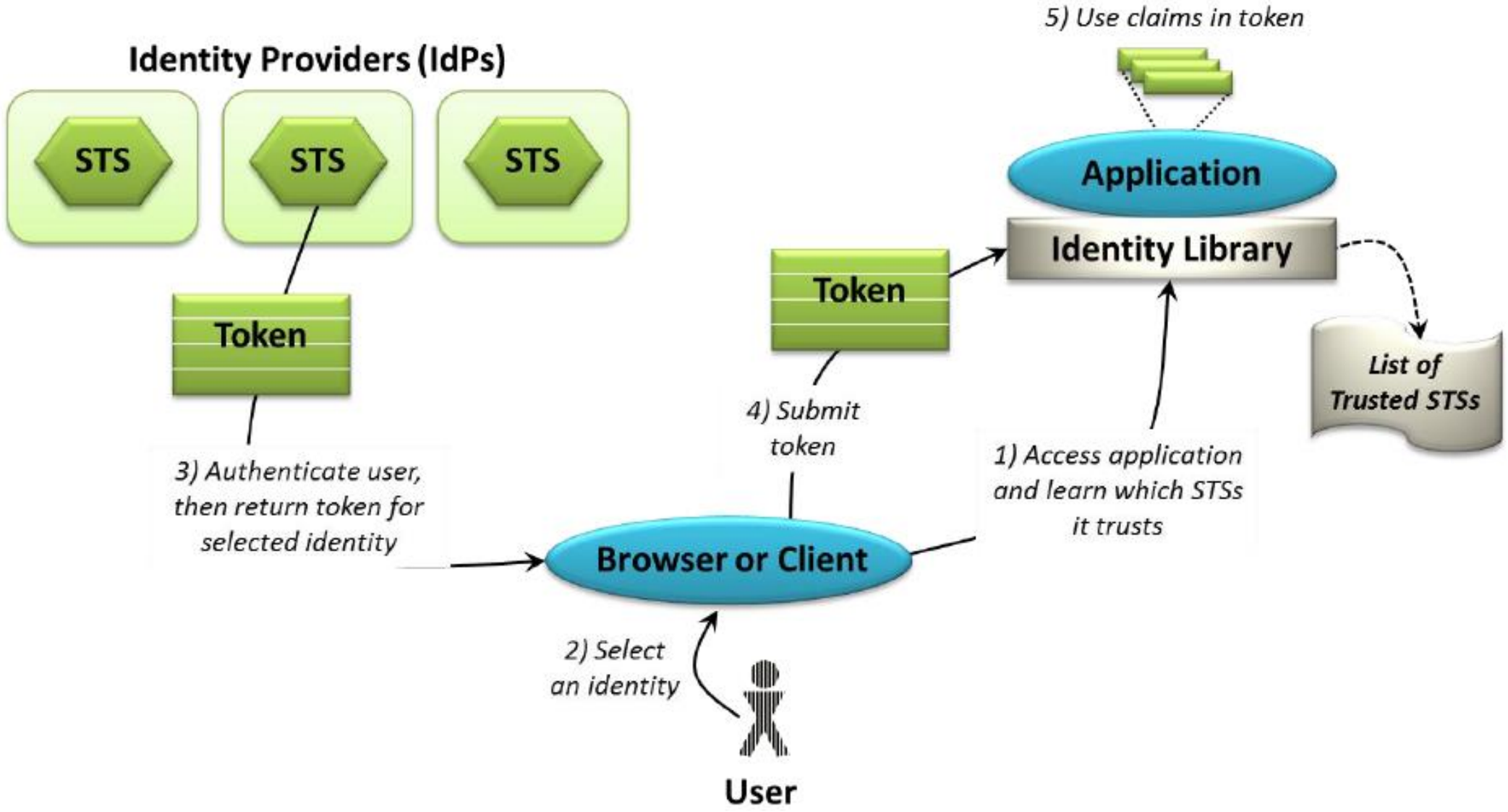
Token Issuance



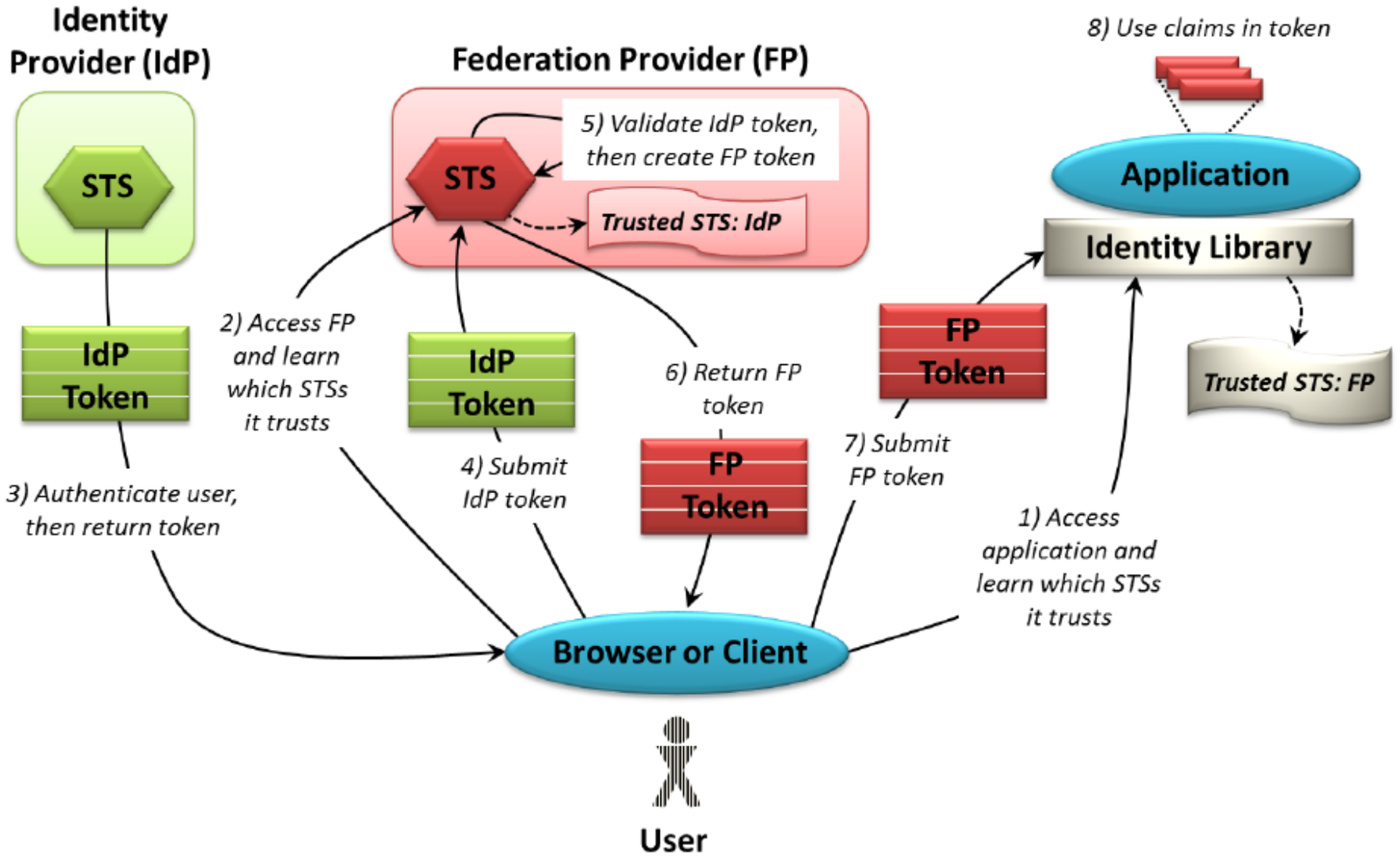
Identity Providers and Identity Libraries



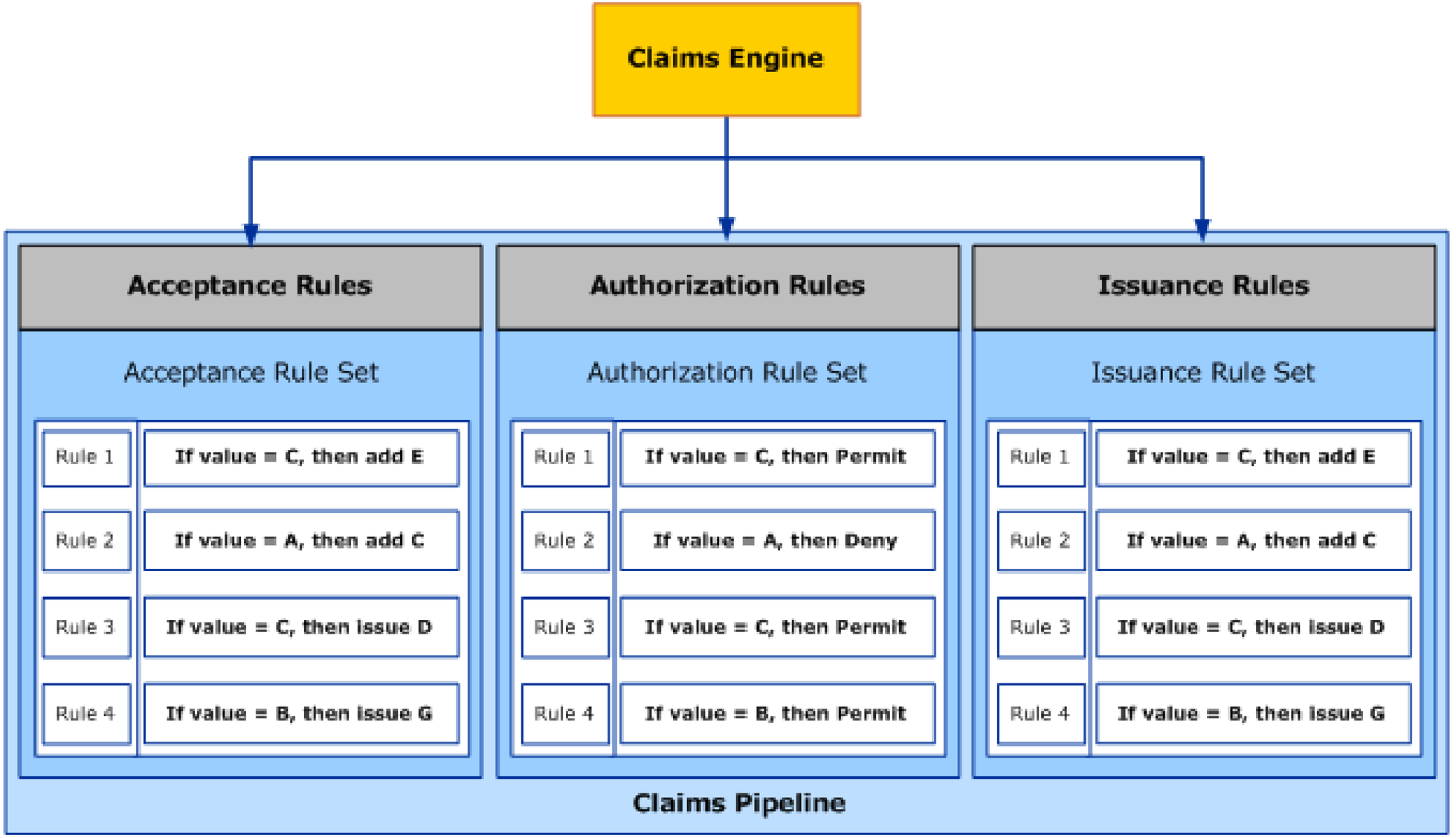
Multiple Identity Providers



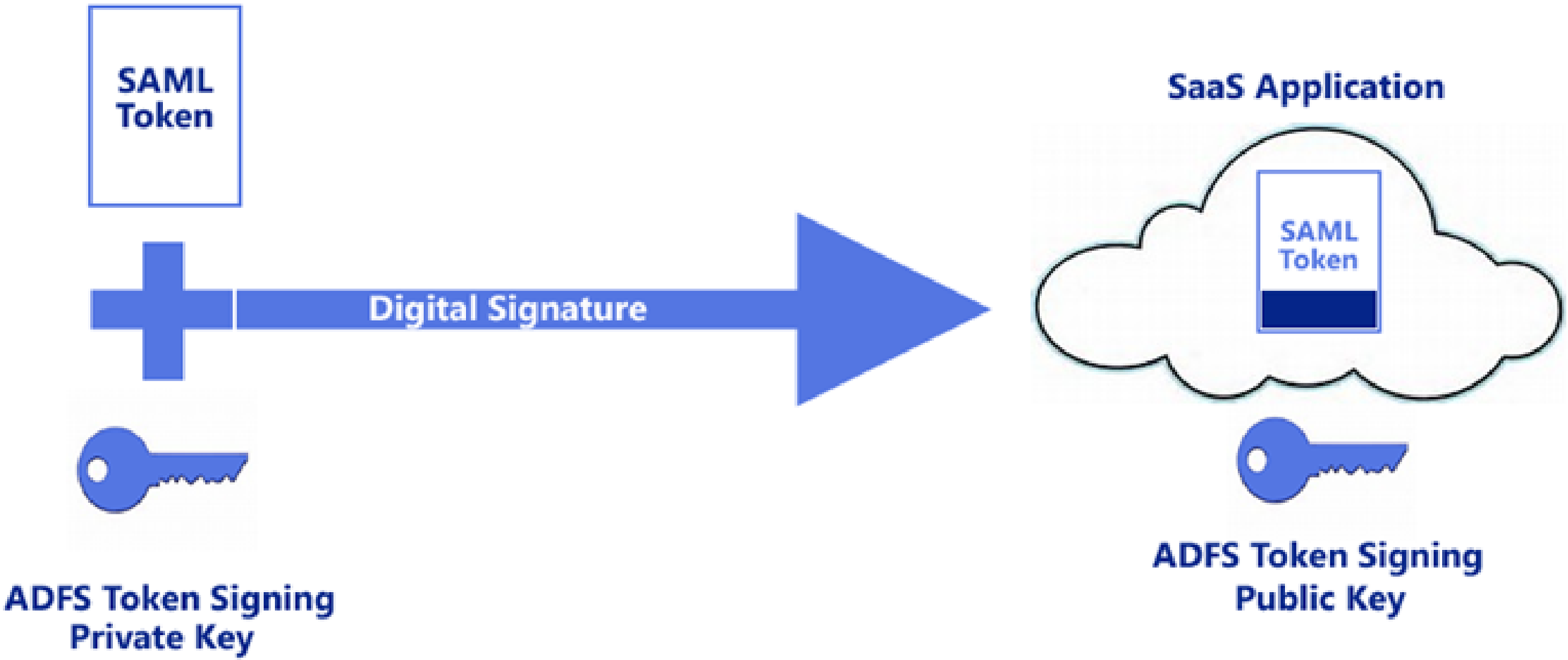
Identity Federation



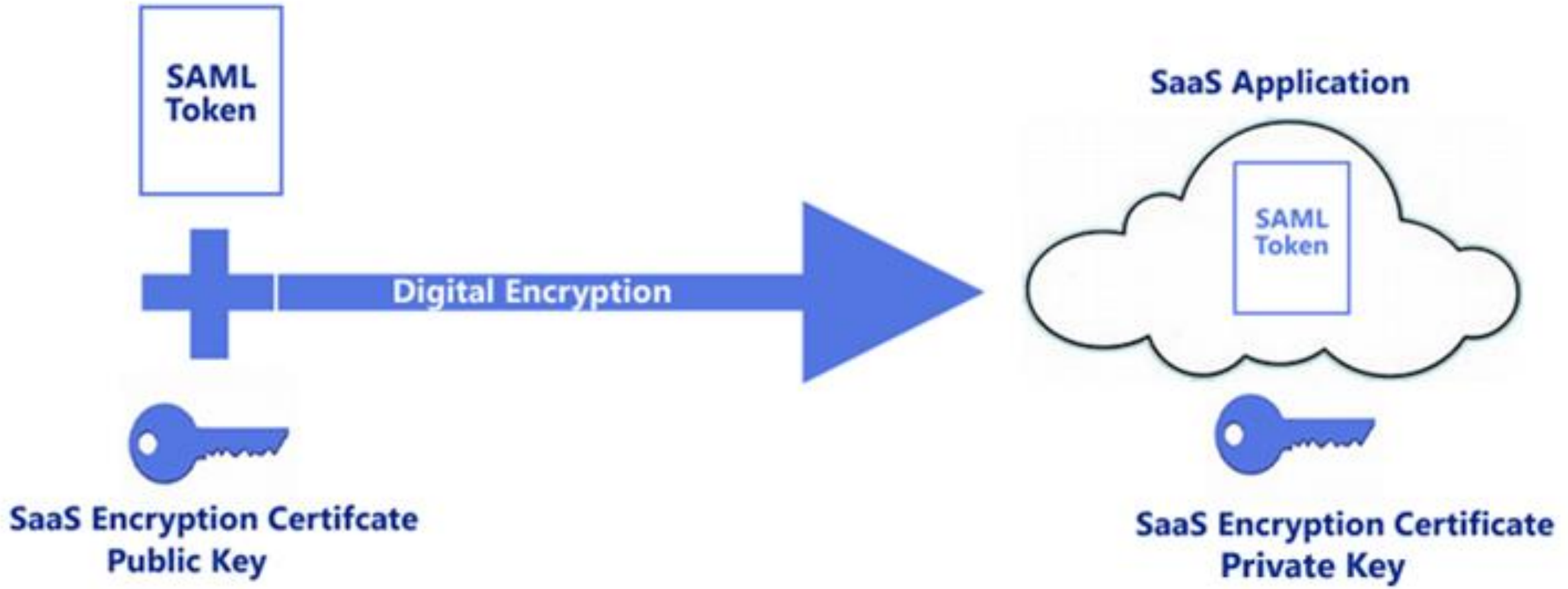
Claims Rule Engine



Token Digital Signature



Token Encryption



Shibboleth

- SAML-based federation portal
- Open Source

Demo


Base Reactions
1 Arrhenius Theory
2 Acidity and Alkalinity
Microsoft
7:30 PM

Microsoft

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.

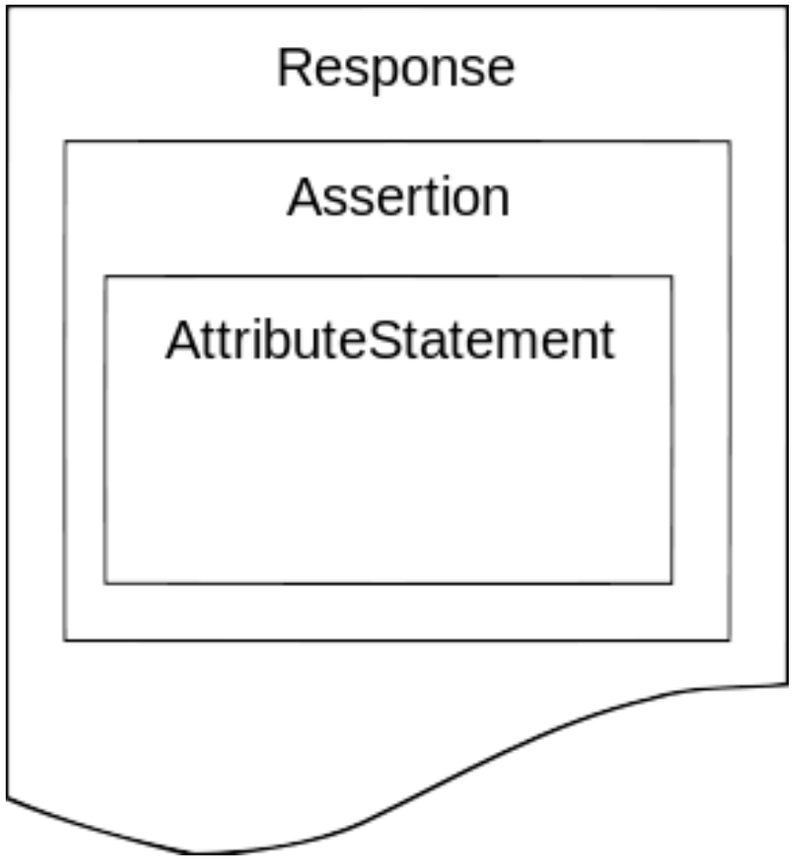
- Authentication statements
- Attribute statements
- Authorization decision statements

Demo


Base Reactions
1 Arrhenius Theory
2 Acidity and Alkalinity
Microsoft
7:30 PM

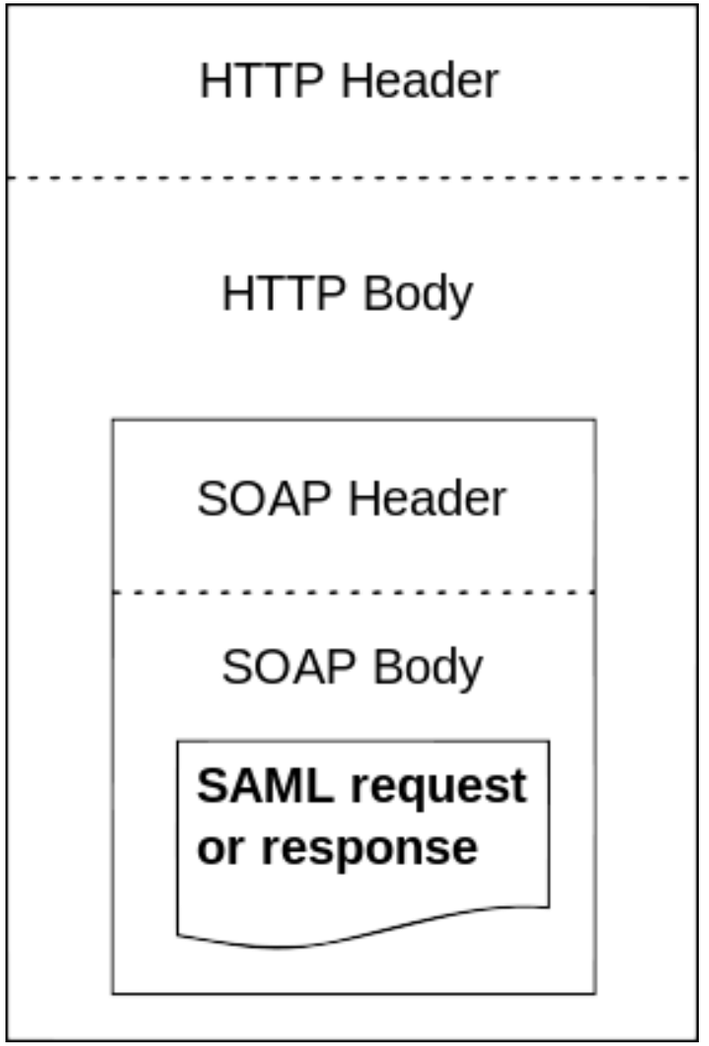
SAML Protocols

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



SAML Bindings

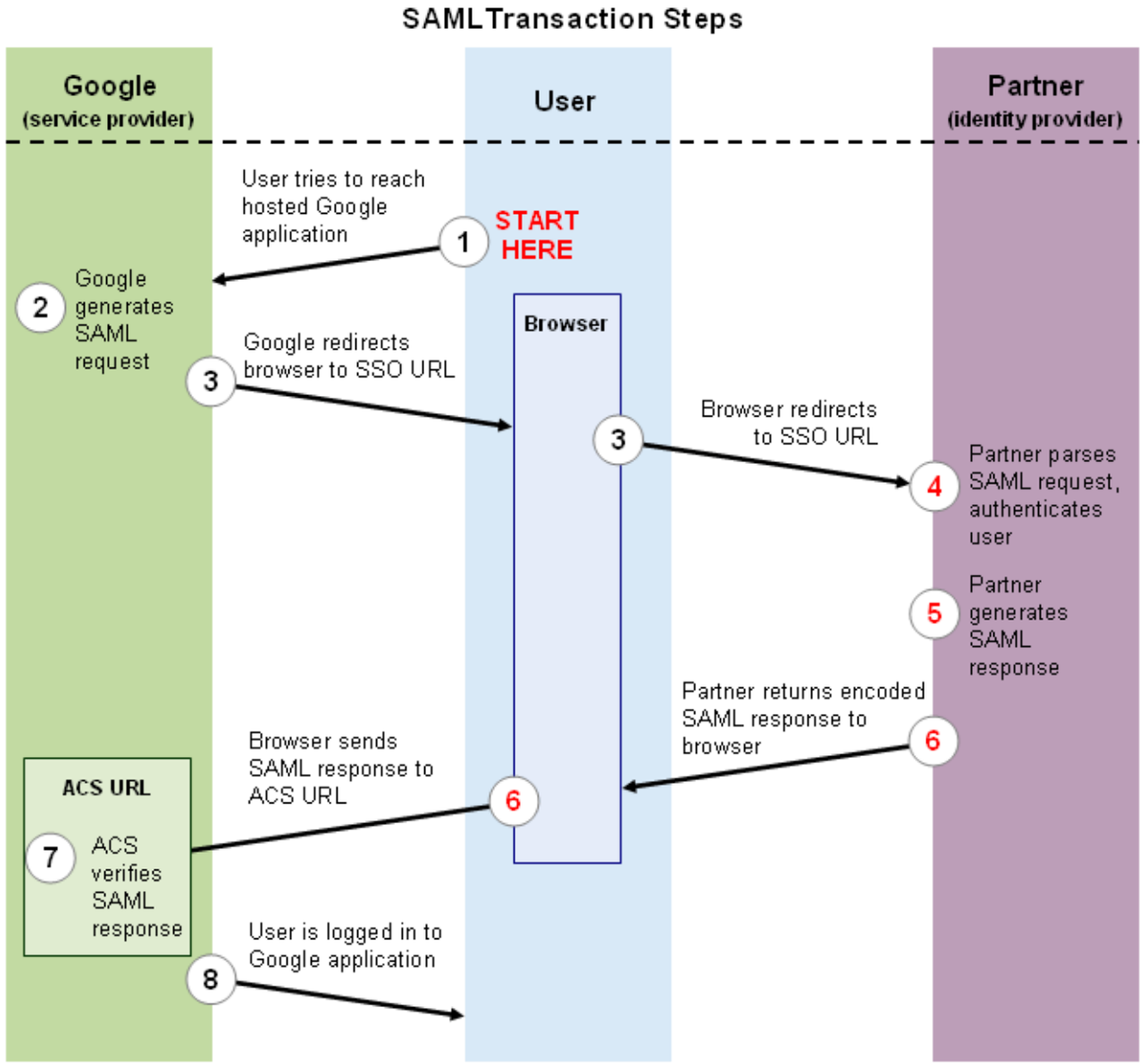
- SAML SOAP Binding
- Reverse SOAP (PAOS) Binding
- HTTP Redirect (GET) Binding
- HTTP POST Binding
- HTTP Artifact Binding
- SAML URI Binding



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:1.3.6.1.4.1.5923.1.1.1.1"
          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

https://sts.cloudready.ms/adfs/ls/?SAMLRequest=jZFRT4Mw-FIX%2FCun7KC3OjWaQ4PbgkqIkoA%2B%2BmAKdNCkt9hZ1%2F14Gmk-wfFI%2Fv%0APfc7p6cr4K3qWNq7Ru%2FFWy%2FAeZ%2Bt0sDGRYx6q5nhIIFp3gp-grmJ5erdj1A9Y%0AZ40zIVHISwGEddLotdHQt8Lmwr7LSjzudzFqnOuAYQyNLP1Kmb62gtd-HvwWc%0AD6PSKOEaH8DgE5ni7CEvkLcZokjNT9AzhIM%2FBF4fACvAyNtuYvRSRSI-iZXIN%0AwrIY0CriSxKGhNLDFeXhYjkfZAC92GpwXLsY0YCEM0JnQVQESxaEj-CyekZd9%0AP%2BxG6Irq18stIJMI2G1RZLMp%2FJOwMAYfBChZnbpko7E9a%2FcyIv9UipJ%2FF-bjC%0AZy6TZcfuB%2Bx2kxkIq6OXKmU%2B1sOpEzEiCCfTye%2FfT74A%0A&RelayState=cookie%3A29002348&SigAlg=http%3A%2F%2Fwww.w3.org%2F2000%2F09%2Fxmldsig%23rsa-sha1&Signature=M0xoWQfcN3Yp94T2HiqIdJzEkxYqGc6hhopqi8xOI%2B2BtPSLufFD-dQIF7z6Xjm6XdLq1MH9Av5xz2QWYs84ZYhIG3fHtZCjjaoI2wZqpIRszHIa%2BjtZoW20NGDe-pDsCRT0AKNkhe%2B4Yj3LshrM6EX5O3obx2Mypy8EcsoURkTF3kf1dwKqsGA3ka7ehbRmUQGJUXD0u4iF-Bog7YgkL4Q9FYMTanZeRo2X4%2FkAeNxT8ormKWJfYnAzg0F4Ku60zDd5N7jYu4XeyOsXDthEFI5H4WYu-cAprREI2hgSUI21J782kKzrsIaIIaJ5BKPIO50NPCIb5Sf6Zw4maLpZrFEfrw%3D%3

Microsoft

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

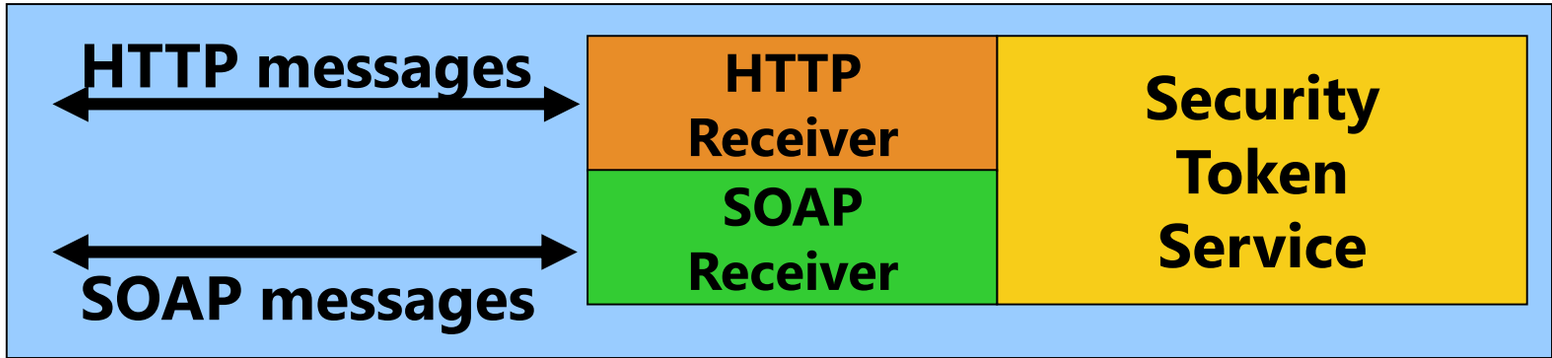
- OASIS Standard from 2007
- Deals with the issuing, validating, and renewal of security tokens
- Defines the concept of the Security Token Service
- Defines formats of messages used to request security tokens (RST) and respond to those requests (RSTR)
- Defines mechanisms for key exchange

Demo


Base Reactions
1 Arrhenius Theory
2 Acidity and Alkalinity
Microsoft
7:30 PM

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

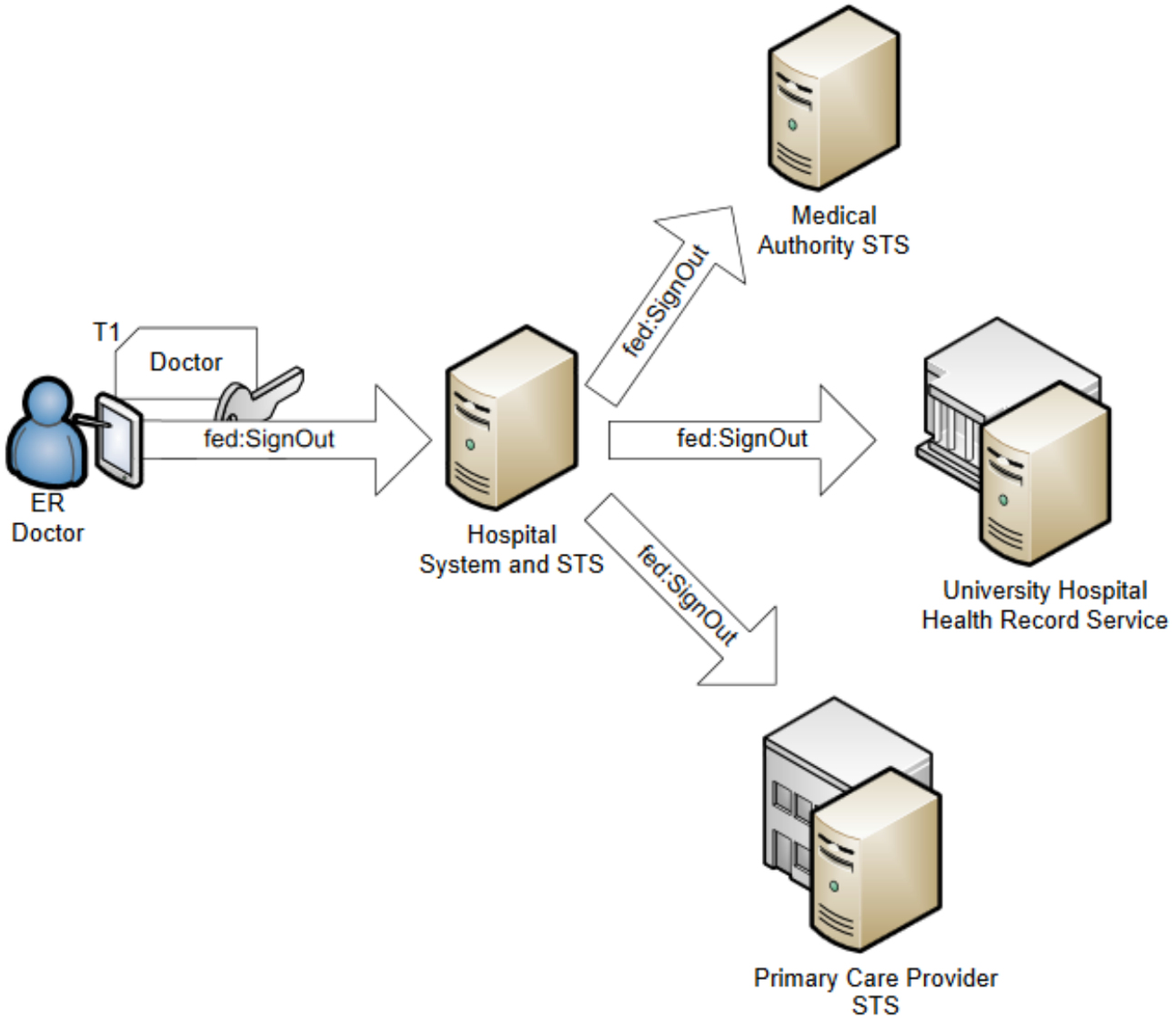
#	Result	Protocol	Host
1	302	HTTPS	claimsweb.cloudready.ms
2	200	HTTPS	sts.cloudready.ms
3	302	HTTPS	sts.cloudready.ms
5	200	HTTPS	corp.sts.microsoft.com
6	200	HTTPS	sts.cloudready.ms
7	200	HTTPS	claimsweb.cloudready.ms

Federated SSO: Claims

WELCOME CLAIMSWEB!

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

Single SignOut



FederationMetadata

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

Demo


Base Reactions
1 Arrhenius Theory
2 Acidity and Alkalinity
Microsoft
7:30 PM

Microsoft

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

Microsoft

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

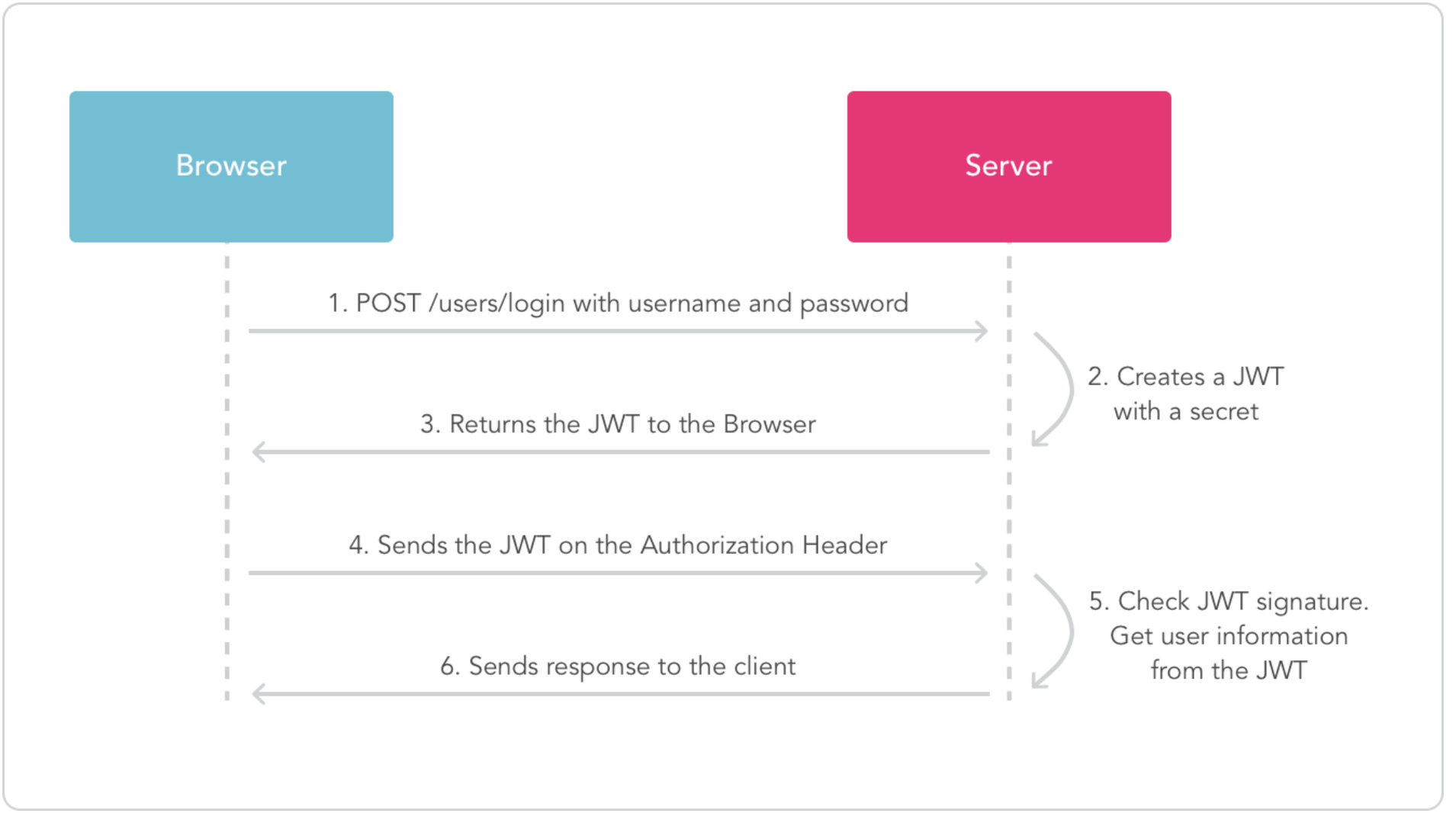
Header: { typ: 'JWT', alg: 'HS256' }
Payload/Claims:
{
    user: john,
    admin: true,
    exp: 8.10.2016, 15:27
}
Signature

=> BASE64

Encoded and Signed Token

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.
eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4
gRG9lIiwiaXNTb2NpYWwiOnRydWV9.
4pcPyMD09olPSyXnrXCjTwXyr4BsezdI1AVTmud2fU4
```

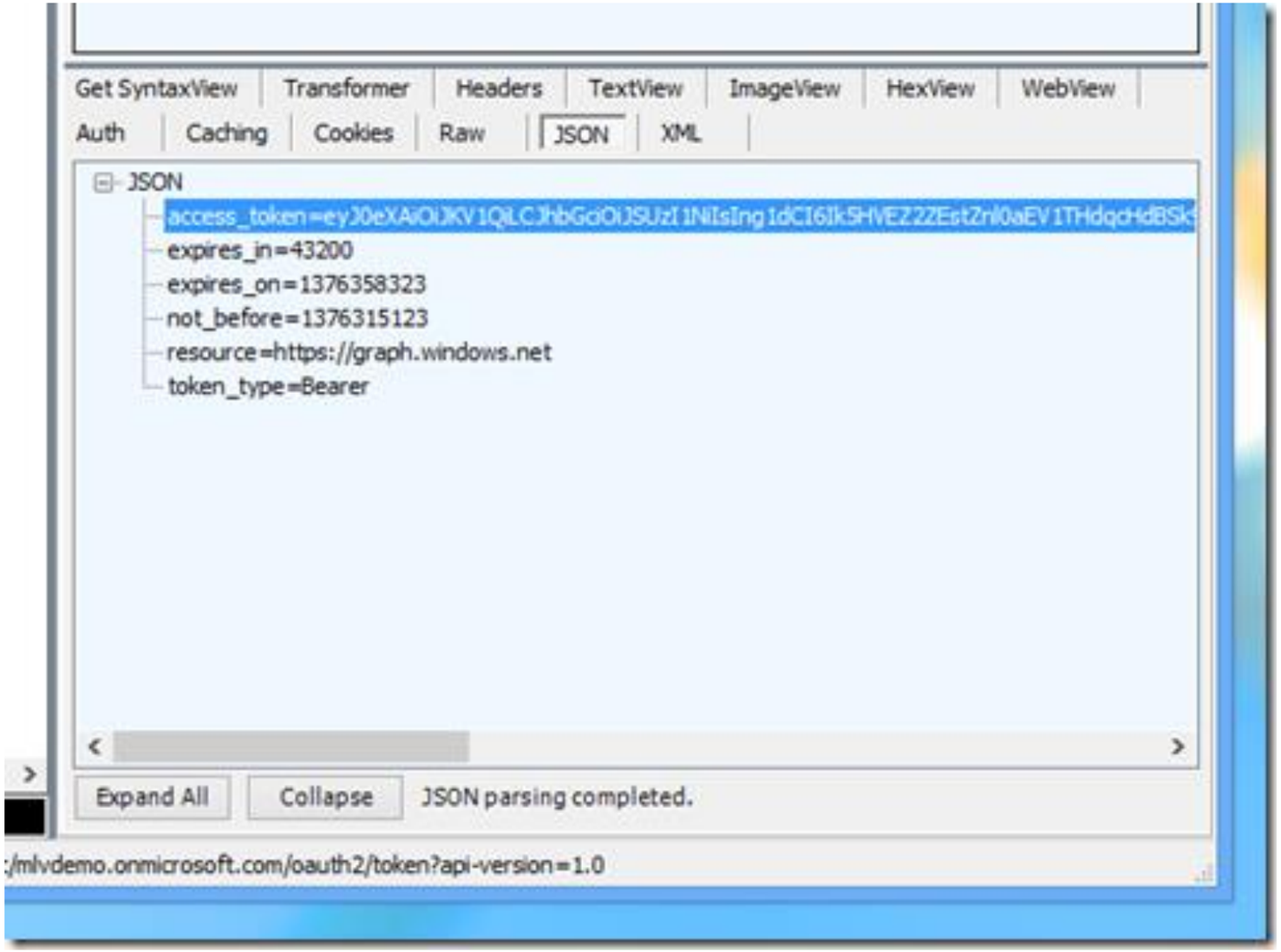
Communication



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



Demo


Base Reactions
1 Arrhenius Theory
2 Acidity and Alkalinity
Microsoft
7:30 PM

Microsoft

OAuth

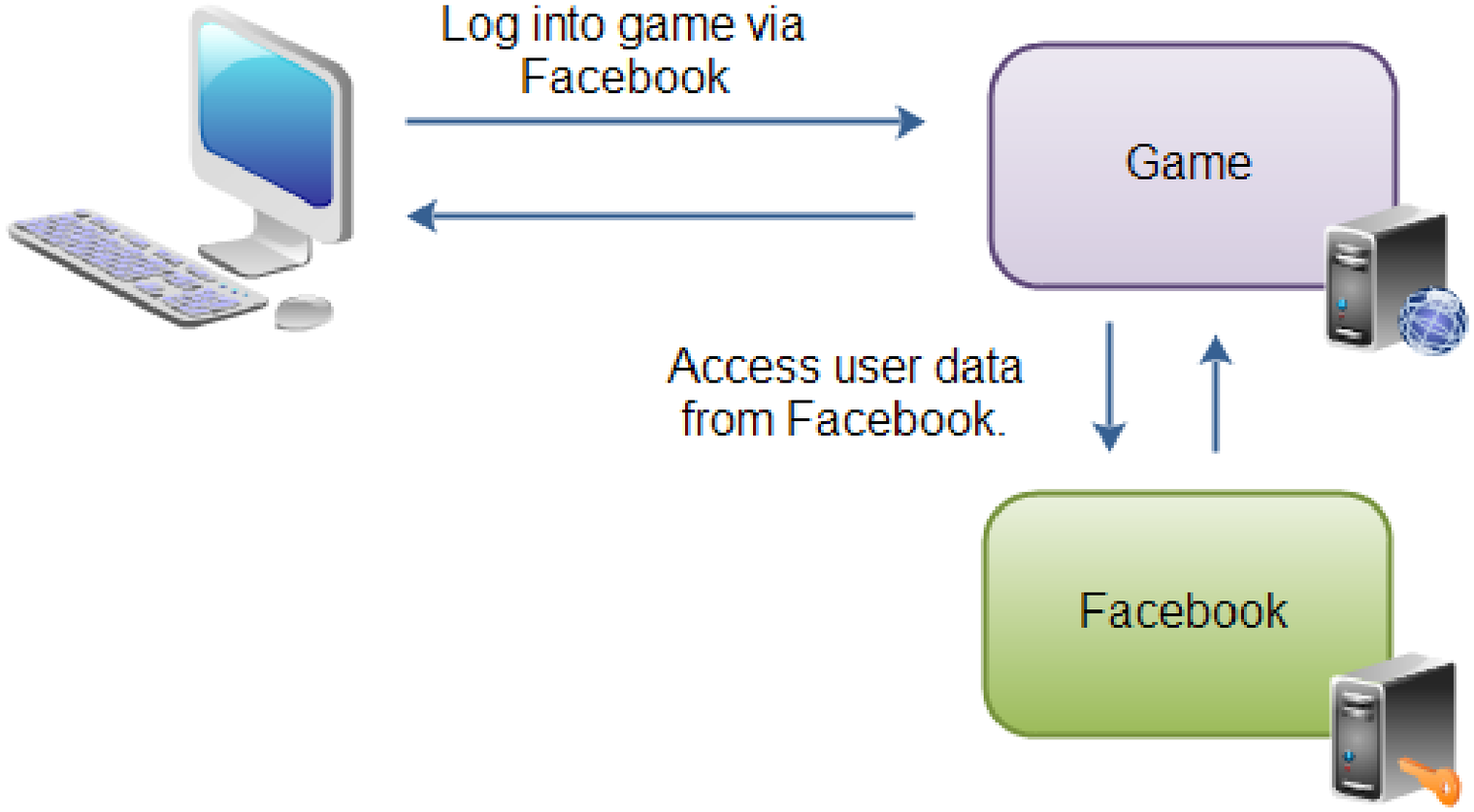
Microsoft Services

OAuth


Sign in with Facebook
Sign in with Twitter
Sign in with Google
Sign in with LinkedIn
Sign in with Yahoo
Sign in with Windows

OAuth

Used to delegate user authorization to a 3rd-party service provider



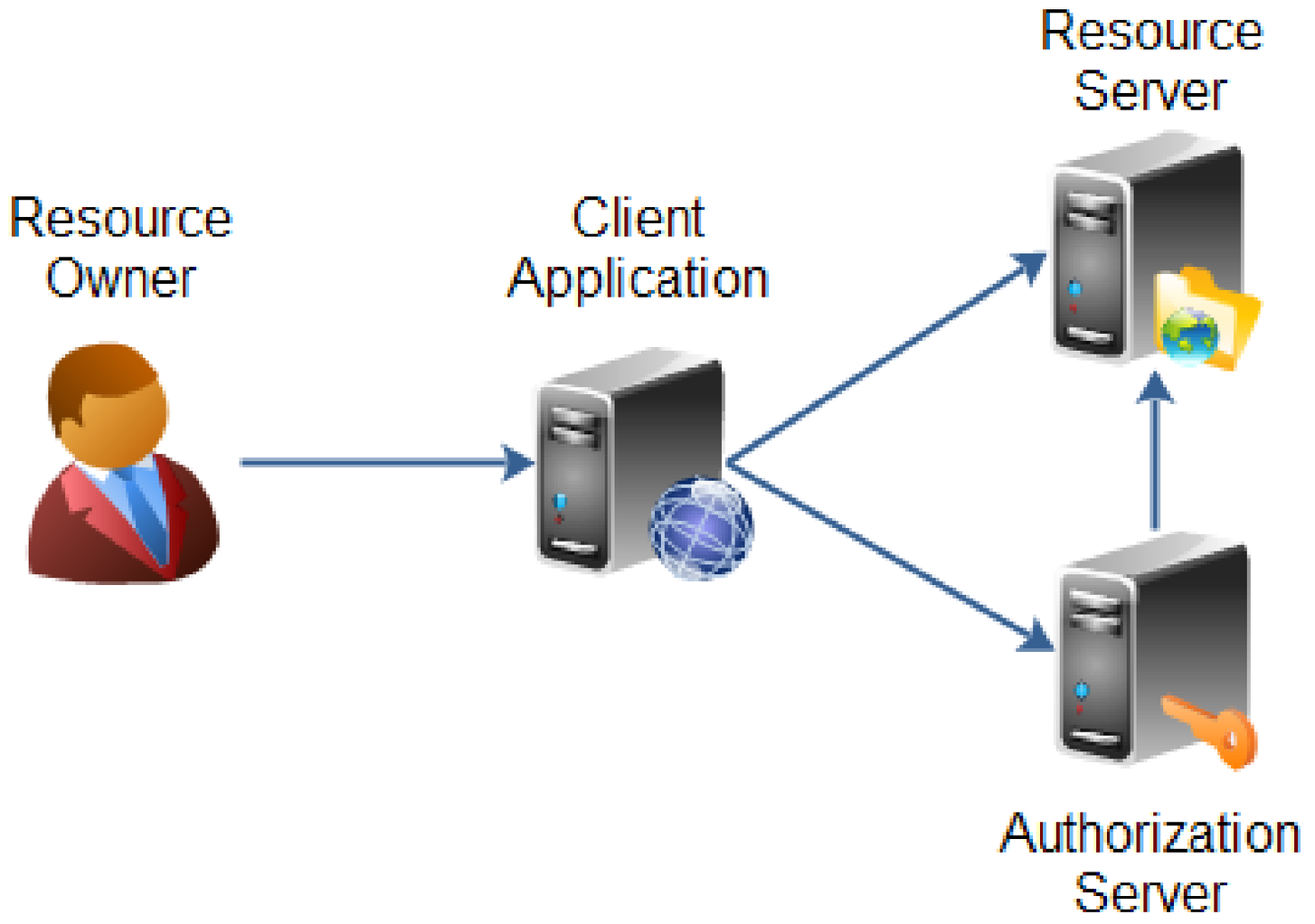
History

- 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
  - …

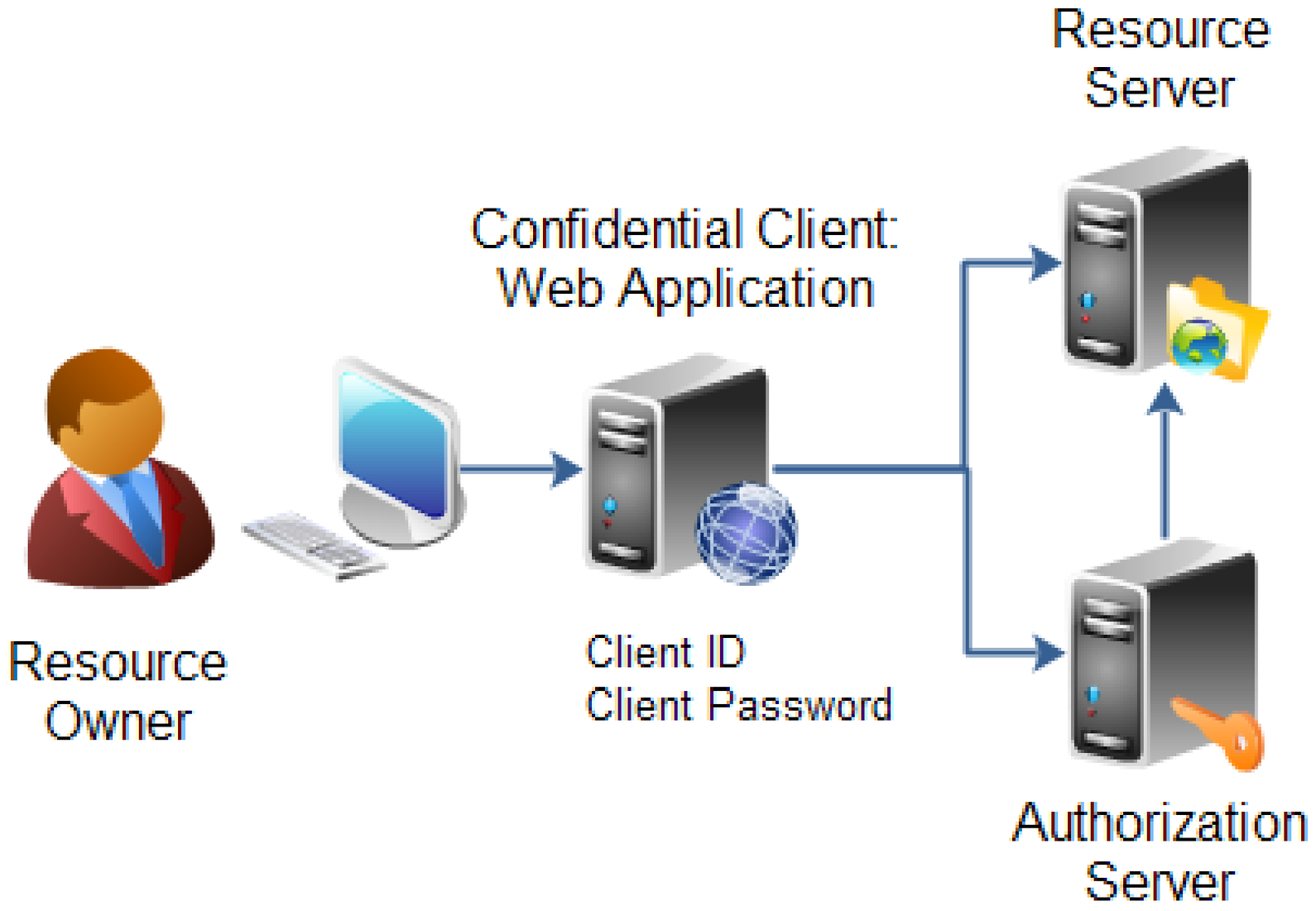
OAuth 2.0

- 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

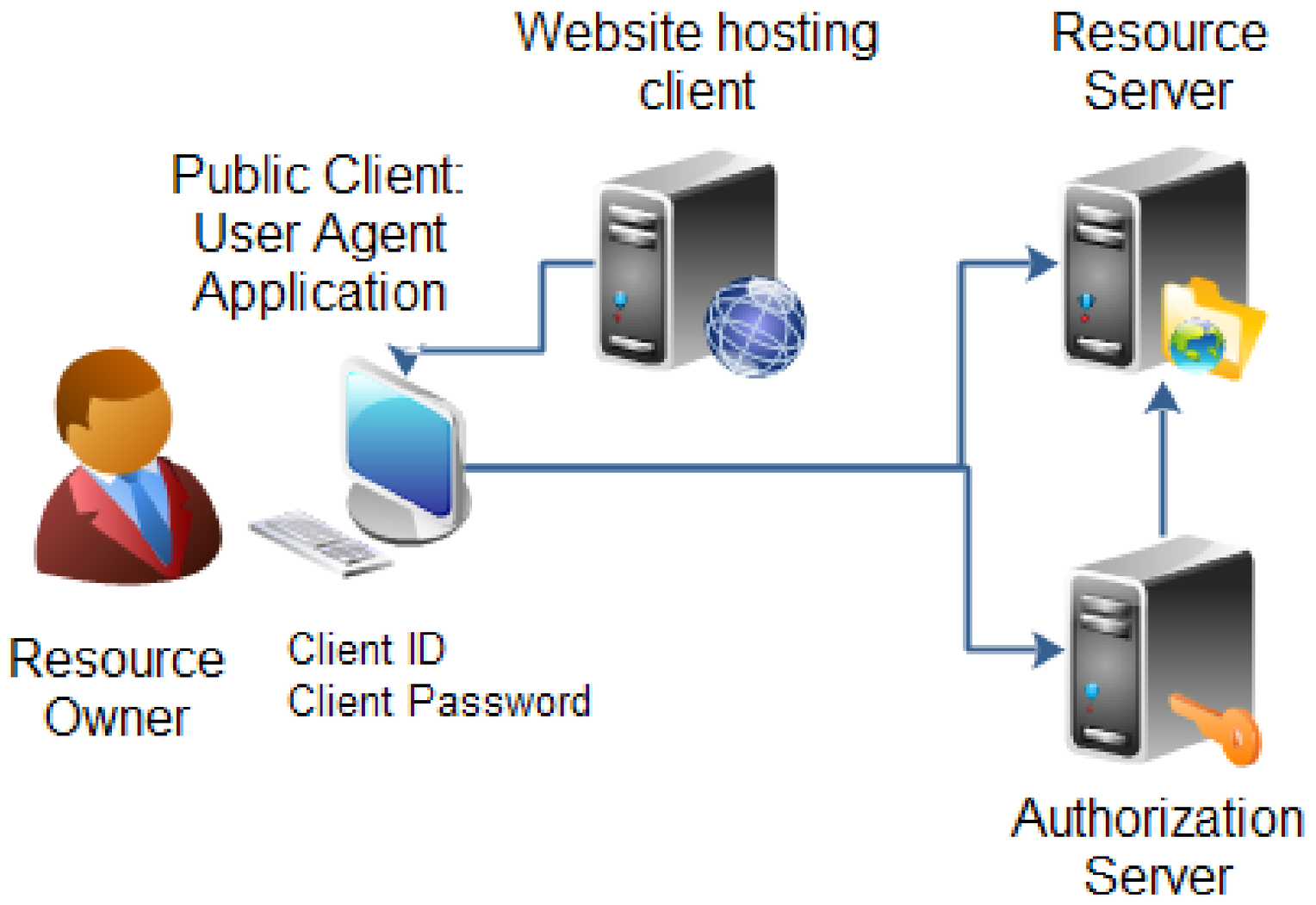
User and application roles



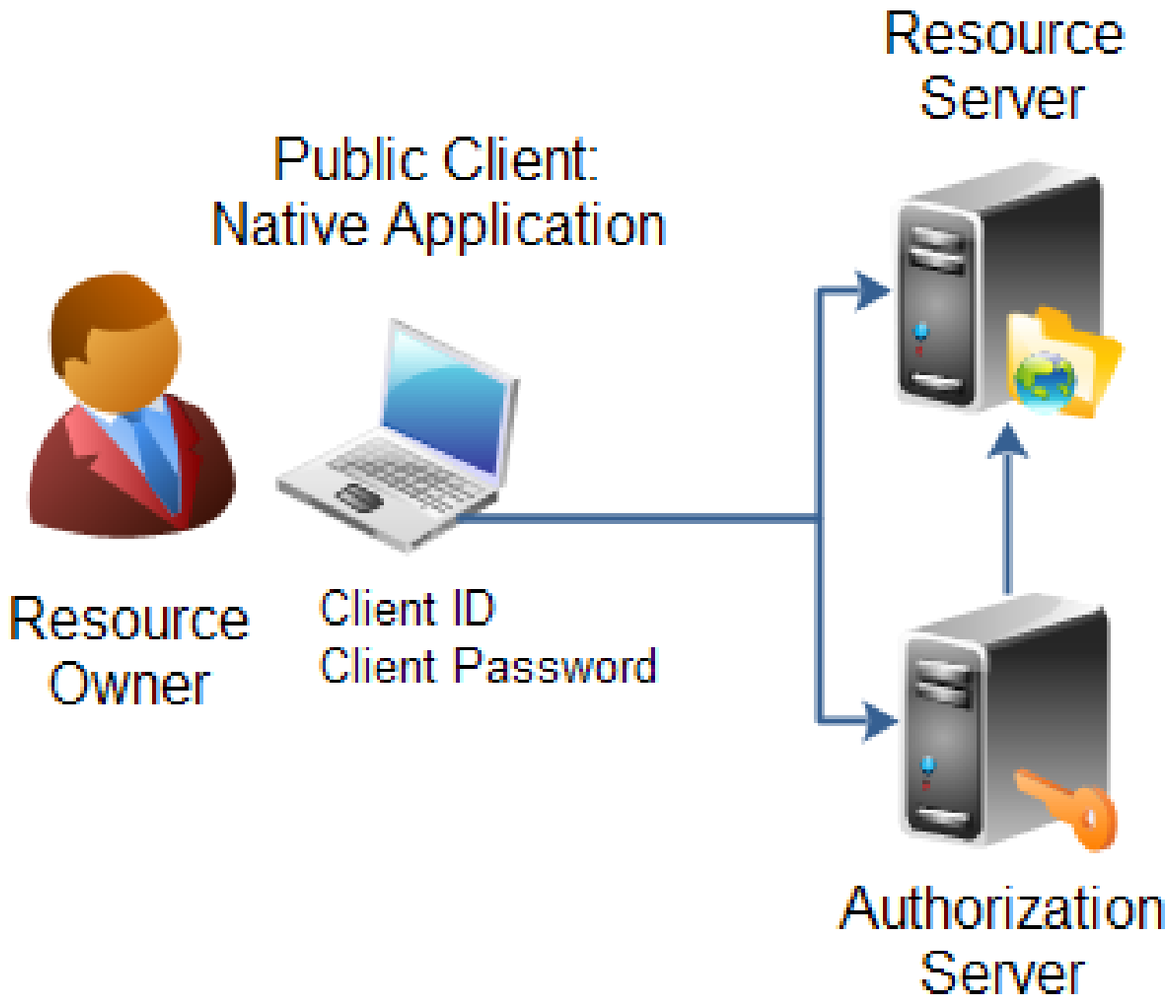
Confidential client web application



Client user agent application

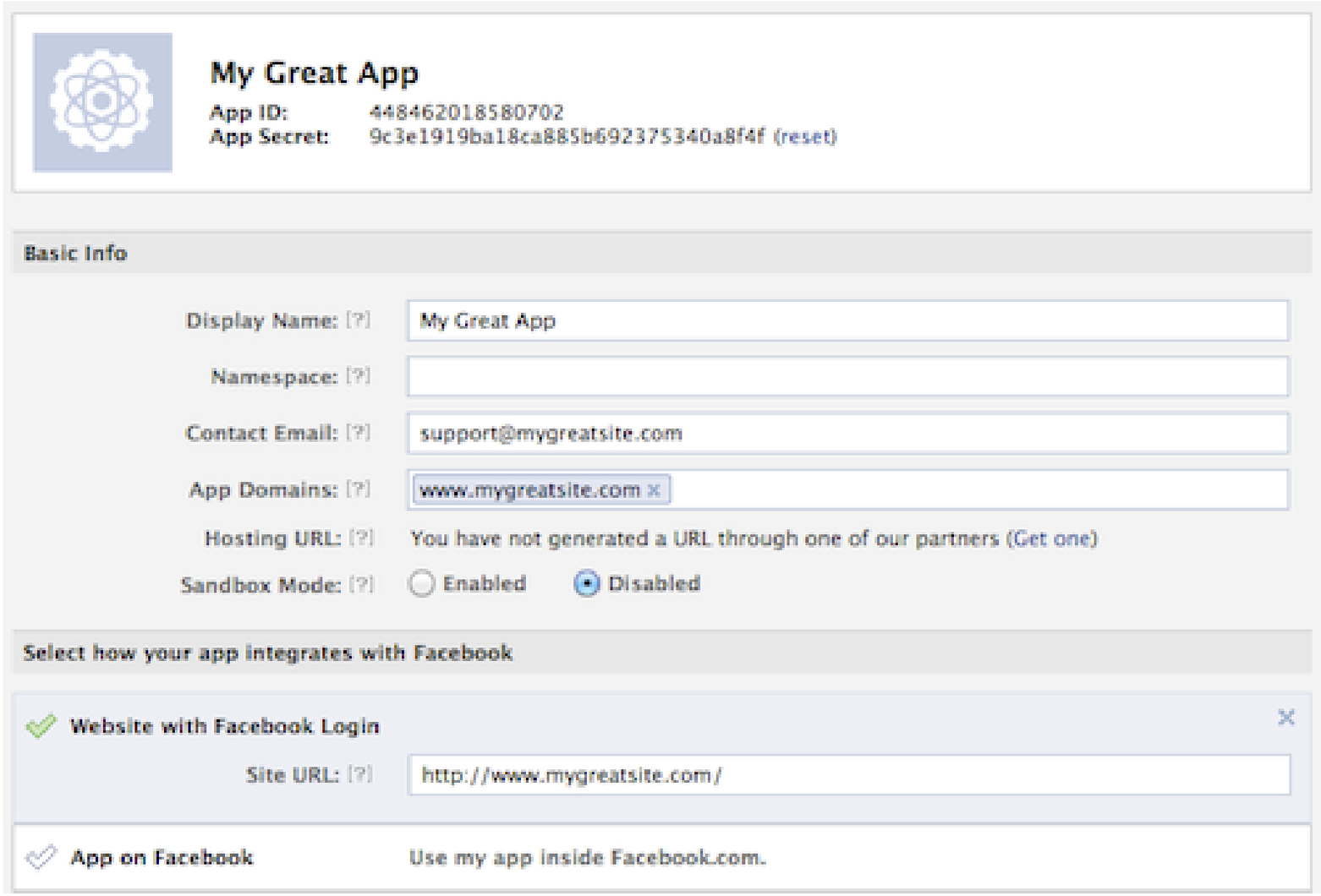


Client native application

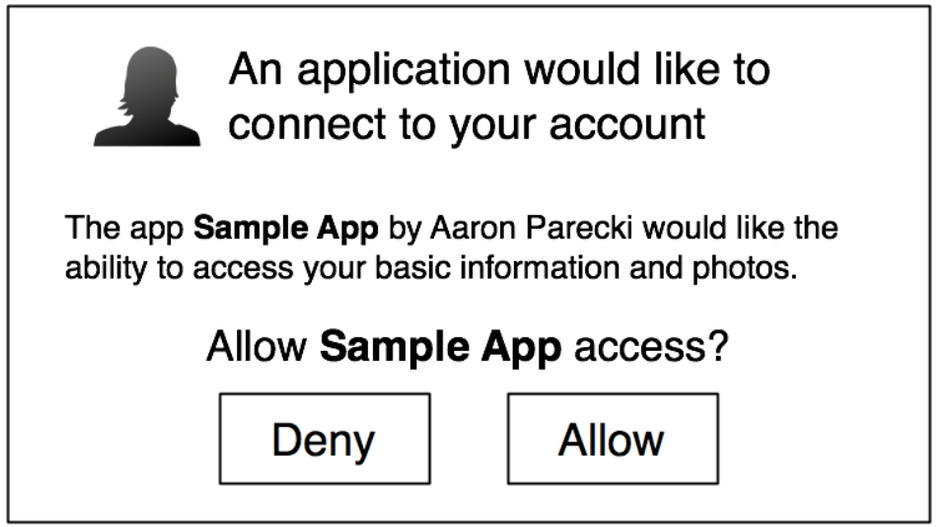


Application registration

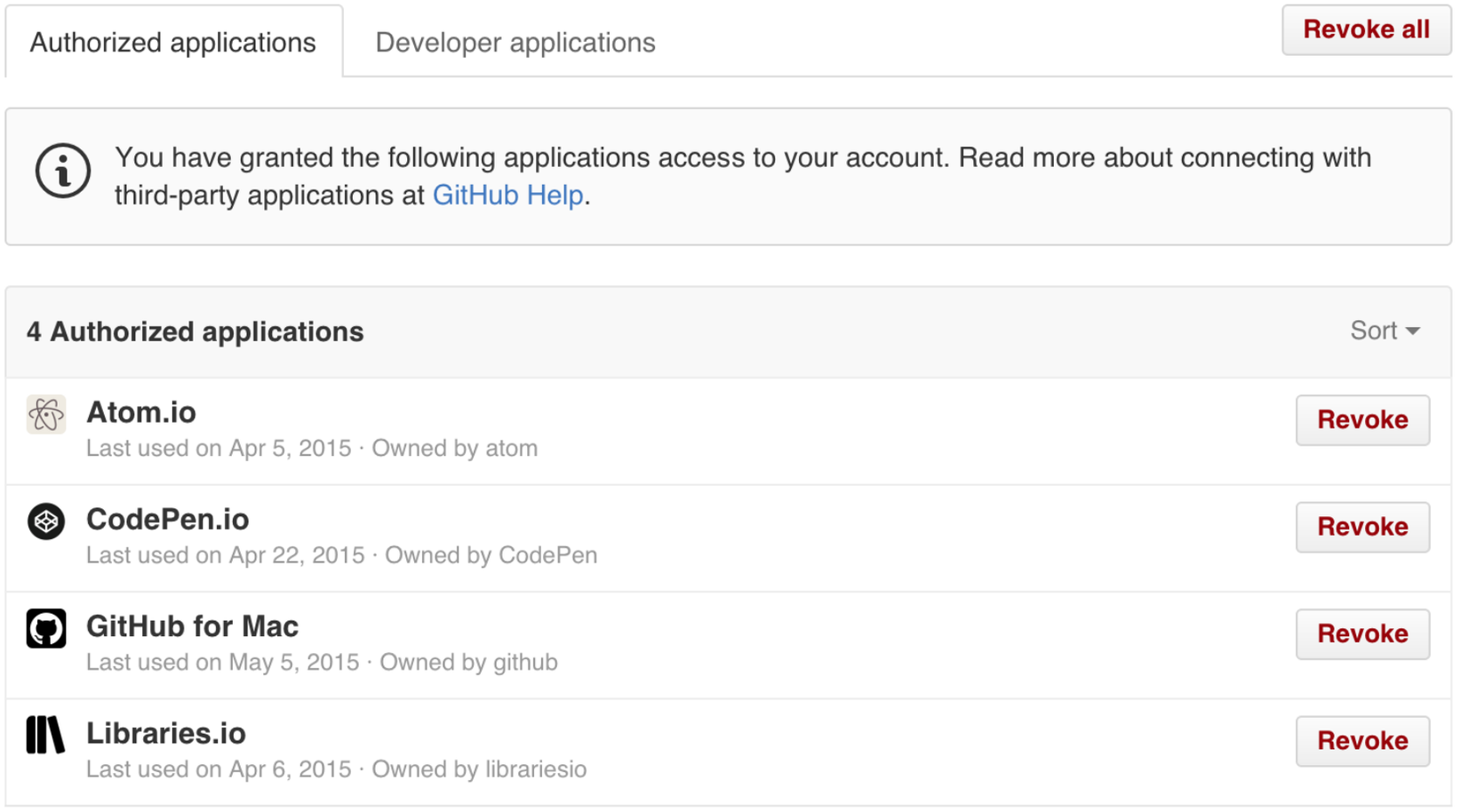
- Client ID
- Client secret
- Redirect URI



Confirmation



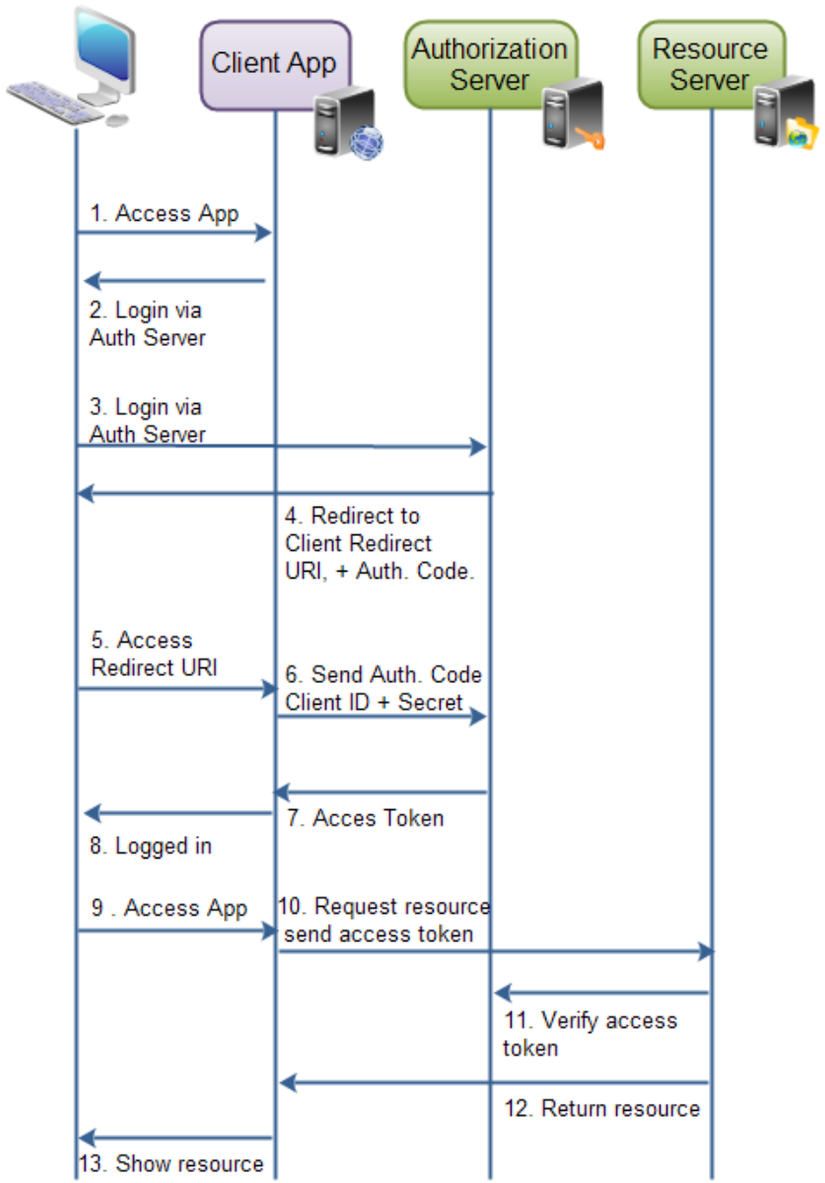
Authorization Management



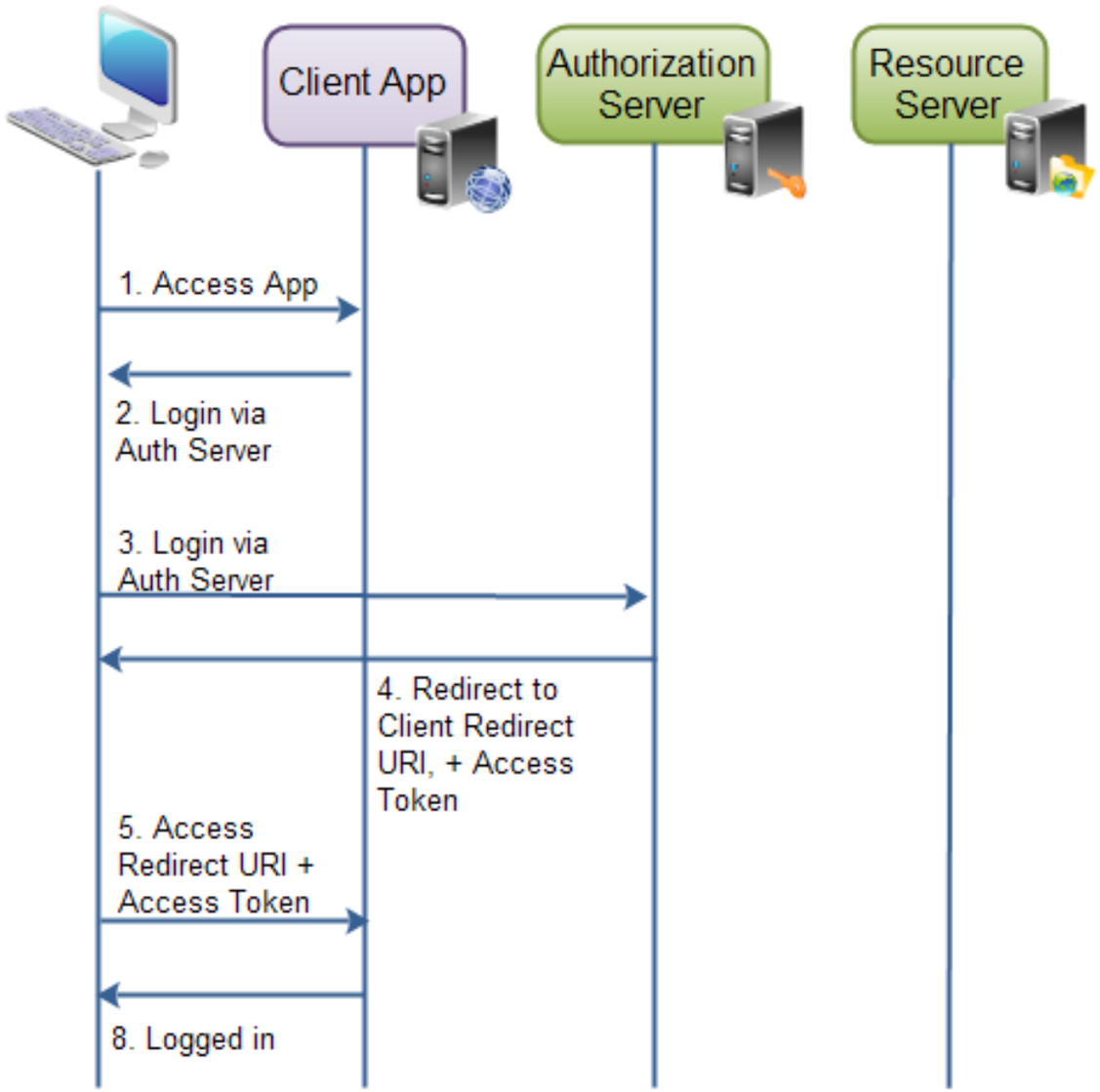
Authorization Grant Methods

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

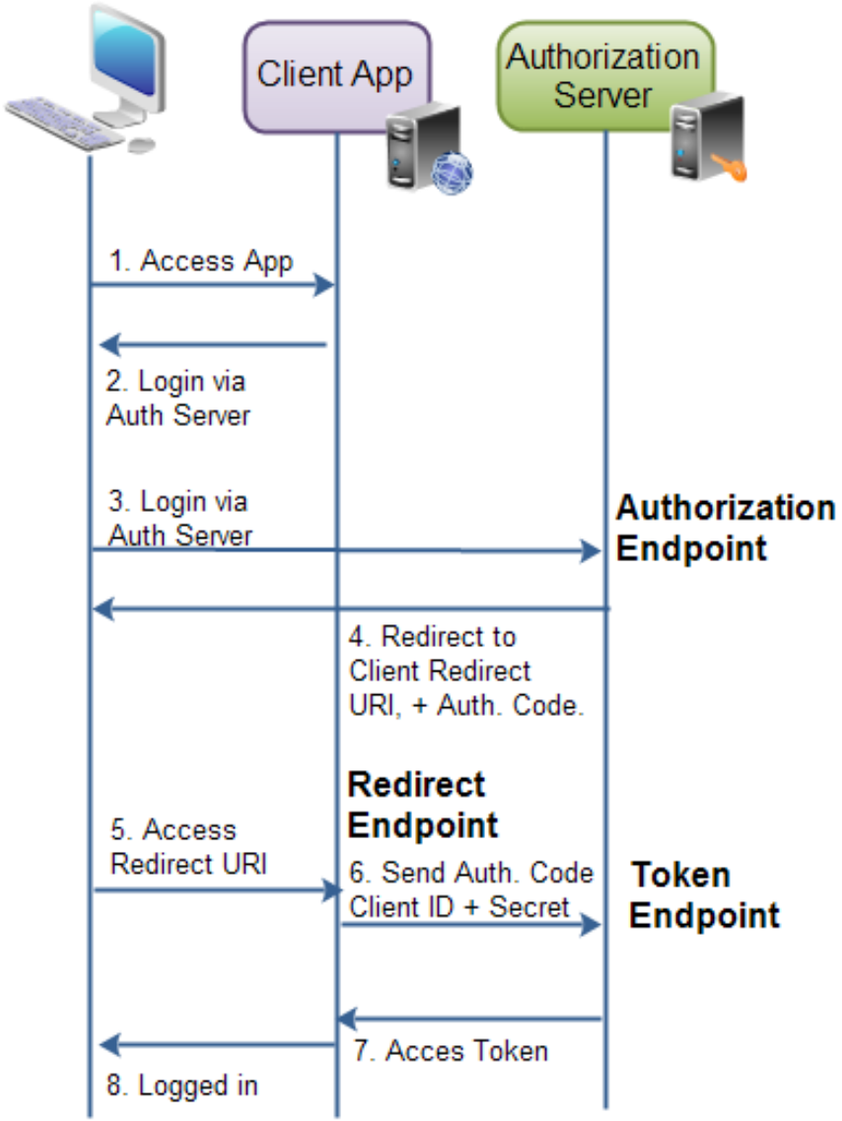
Authorization Code



Implicit Authorization Grant



Endpoints


Client App
Authorization Server
1. Access App
2. Login via Auth Server
3. Login via Auth Server
Authorization Endpoint
4. Redirect to Client Redirect URI, + Auth. Code.
Redirect Endpoint
5. Access Redirect URI
6. Send Auth. Code Client ID + Secret
Token Endpoint
7. Acces Token
8. Logged in

Authorization Request

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

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=AAAAAAAAAAAAAAAAAAAAAAAAA.lxt7fs590QgJAJqMtW9C8KN6tLE.SzhnV- R4lbKXj46nwIbFUm6SLnyryJNE72eg3797LwkSfFQsSNpr7E9sUlCYBH52xvLZDAbwwu7qXCMlqCuVciQ0j3P3-l3ep_lOSJOD3LnwDnXb3MPM1UUNcGLxxVeJmeYhEr15BasdkWqGzTYrCJKf4jbdVT0qb4HKEhpD2aQCDwqjeFF8mNwfne_KL1Ve6ZTNwBWS41SauUnbCTM9qzx-MCDWKEPrLmRR14hCxIsaWfrHmiEYbfl4JXyGcJvhUyffcL-UVwJsQSBjHGlbQXlwrb-ejvvZ6me3YC8CLoS2pvXAMzbppBfg8YAJbGzBPNplbkjM10A7OKifLT4yqQ

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-dddd776f4dfd"

Token Response

{"access_token":"eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6ImpIUVEzOS1fVGRuSzRqTIJvbn-JZYTF2a0pIWSJ9.eyJhdWQiOiJodHRwczovL3d3dy5kYXZIdGVzdGFwcC5jb20iLCJpc3MiOi-JodHRwOi8vc3RzLmNsb3Vkcm

VhZHkubXMvYWRmcy9zZXJ2aWNIcy90cnVzdCIsImlhdCI6MTQwNzE3MjQ4OSwiZXhwI-joxNDA3MTc2MDg5LCJIbWFpbCI6ImRncmVnQG1pY3Jvc29mdC5jb20iLCJ1cG4iOiJkZ3JIZ0BjbG91ZHJ-IYWR5LmIudGVybmFsIiwiYXV0a

F90aW1IIjoiMjAxNC0wOC0wNFQxNzoxNDo0OC44NTZaIiwiYXV0aG1IdGhvZCI6InVybjpvYXN-pczpuYW1Iczp0YzpTQU1MOjIuMDphYzpjbGFzc2VzOlBhc3N3b3JkUHJvdGVjdGVkVHJhbnNwb3J0Iiwid-mVyIjoiMS4wIiwiYXBwaWQ

iOiIzZmIyYTM3Zi00Y2VkLTQwOWMtOTM3Yy1kZGRkNzc2ZjRkZmQifQ.bkMvnIJaB6DRdyCiTLsxsTPtvqGyd-cAmsXQjEumMjH4IN75jx2uCCLg44PU-aXSHZ6R-dOth1iqD-Lf-xy4SKw0O0Z5_oQhPn-3-H0DII3SxtDuR5vr-BObKVc-DT8HGxEPQqPPB5EyF_H21fJ_cqjz-dNyVXK_WoTbM1gQf44Lz5250NjFKjIA1M4sG8bjh-mjo-HZMhR3SwtixCNmQKqYai_8S5KZz1Srg1oIGprwRDbT-NVdzh7Qv0vg1RgaejF3i1J-kWmf2Zx_PVQfITAfzu01BUvAiQCOK7-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

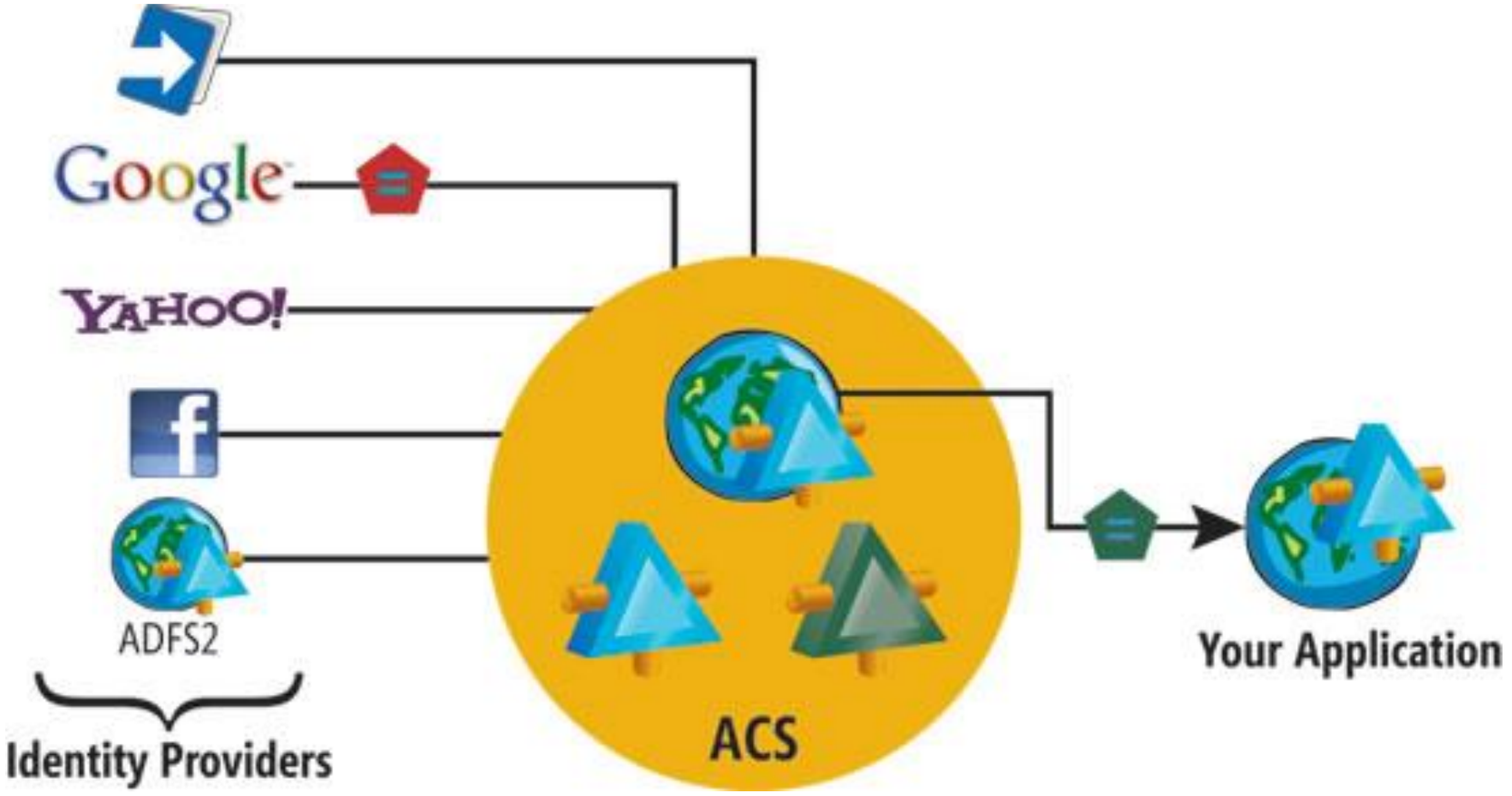
DoS Risk


facebook
Sorry, something went wrong.
We're working on it and we'll get it fixed as soon as we can.
Go Back
Facebook © 2015 · Help Center

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



Microsoft

Virtualization + Cloud & Security

Mgr. Michael Grafnetter

Microsoft Services