Virtualization + Cloud & Security

Mgr. Michael Grafnetter

Agenda

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

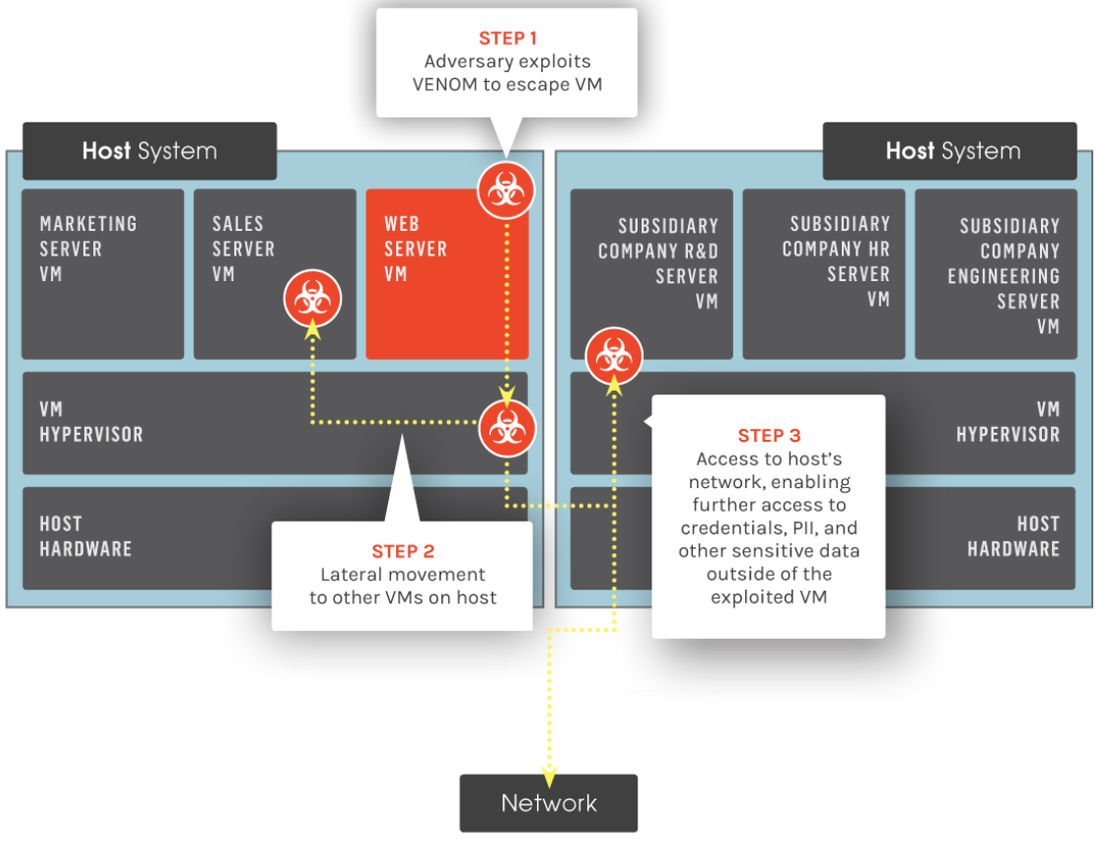
Virtualization Security Risks and Solutions

Blue Pill Attack

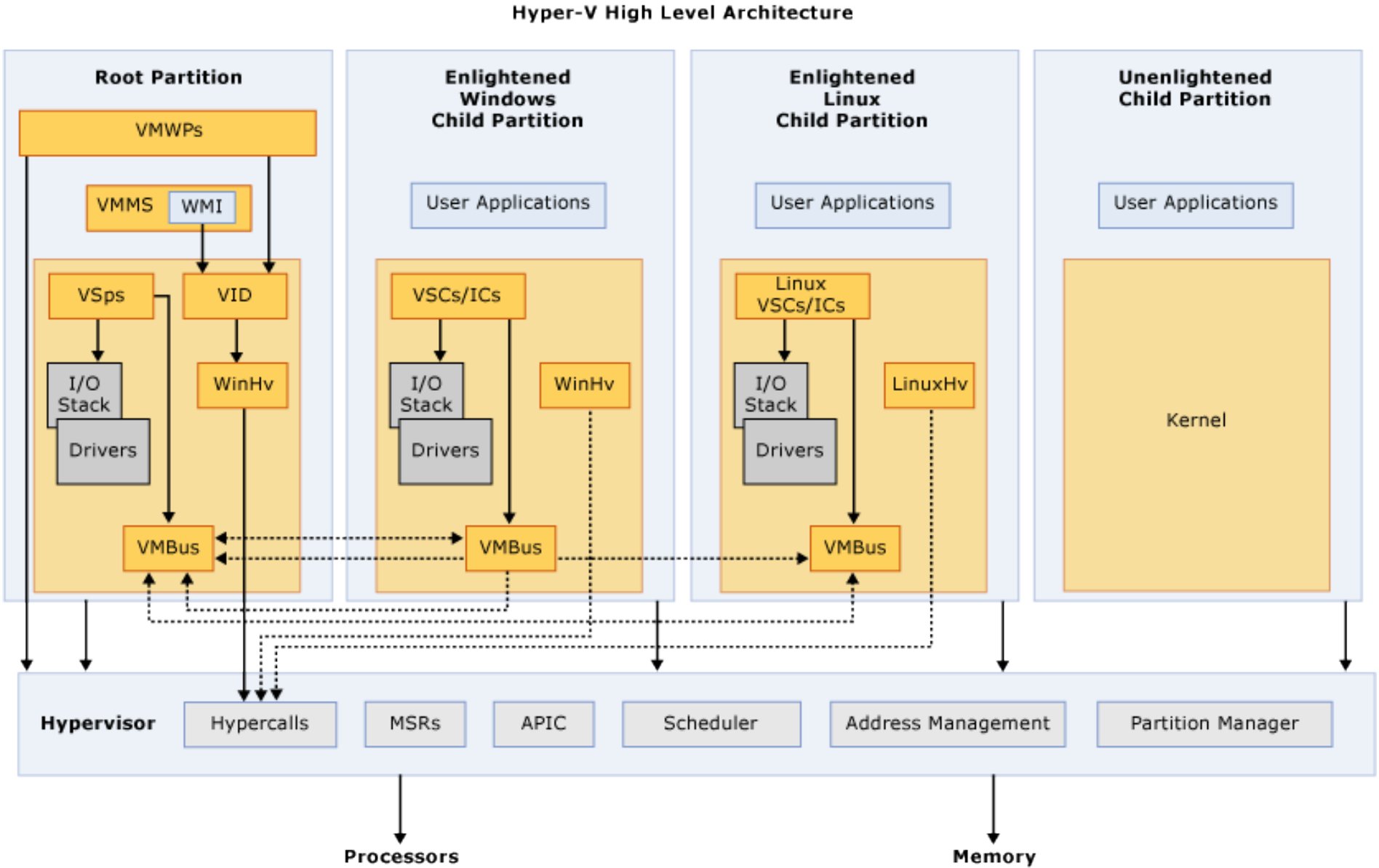
Blue Pill Attack

- 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

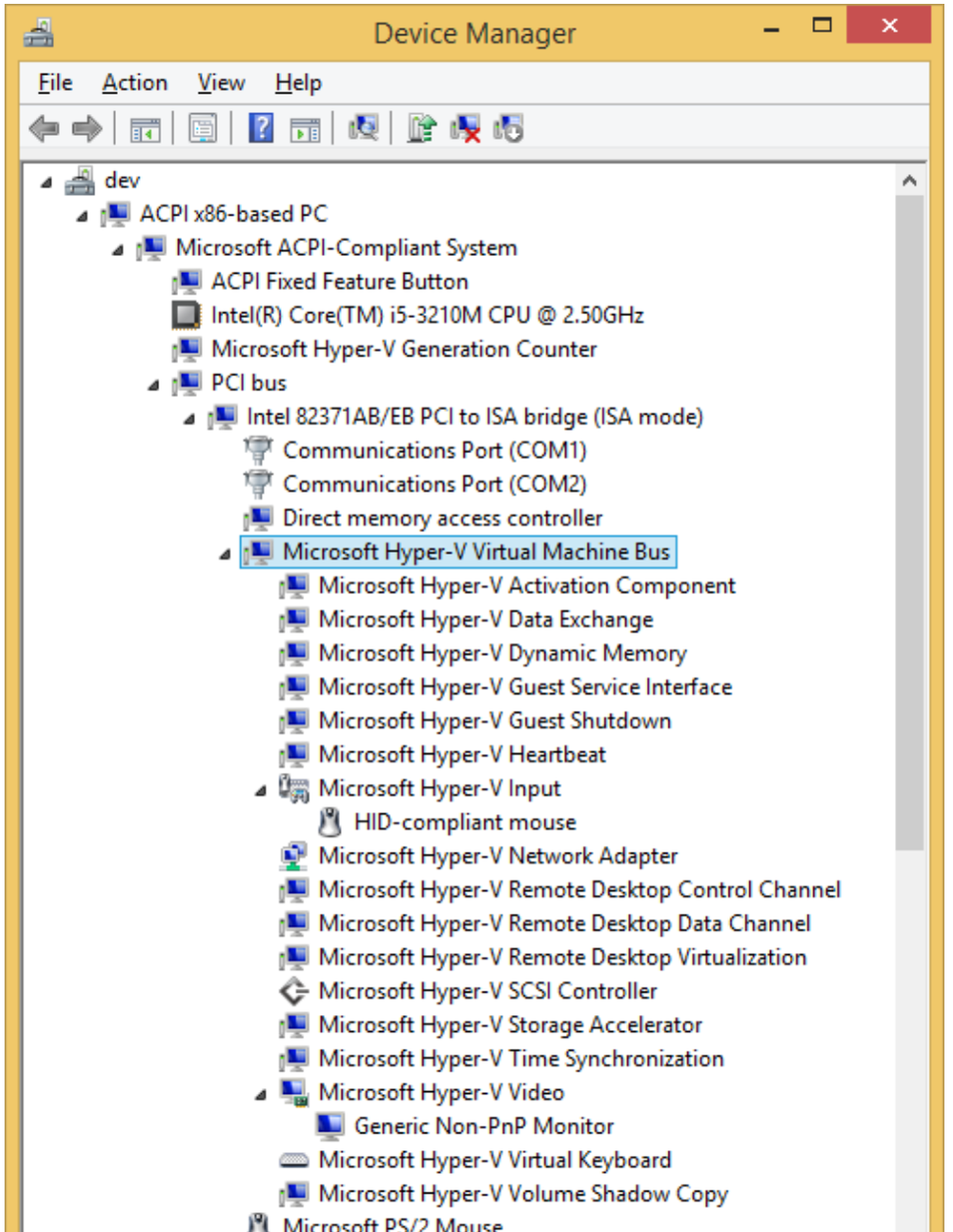
VM Escape Vulnerabilities



VM Escape Vulnerabilities



VM Escape Vulnerabilities



Known VM Escape Vulnerabilities

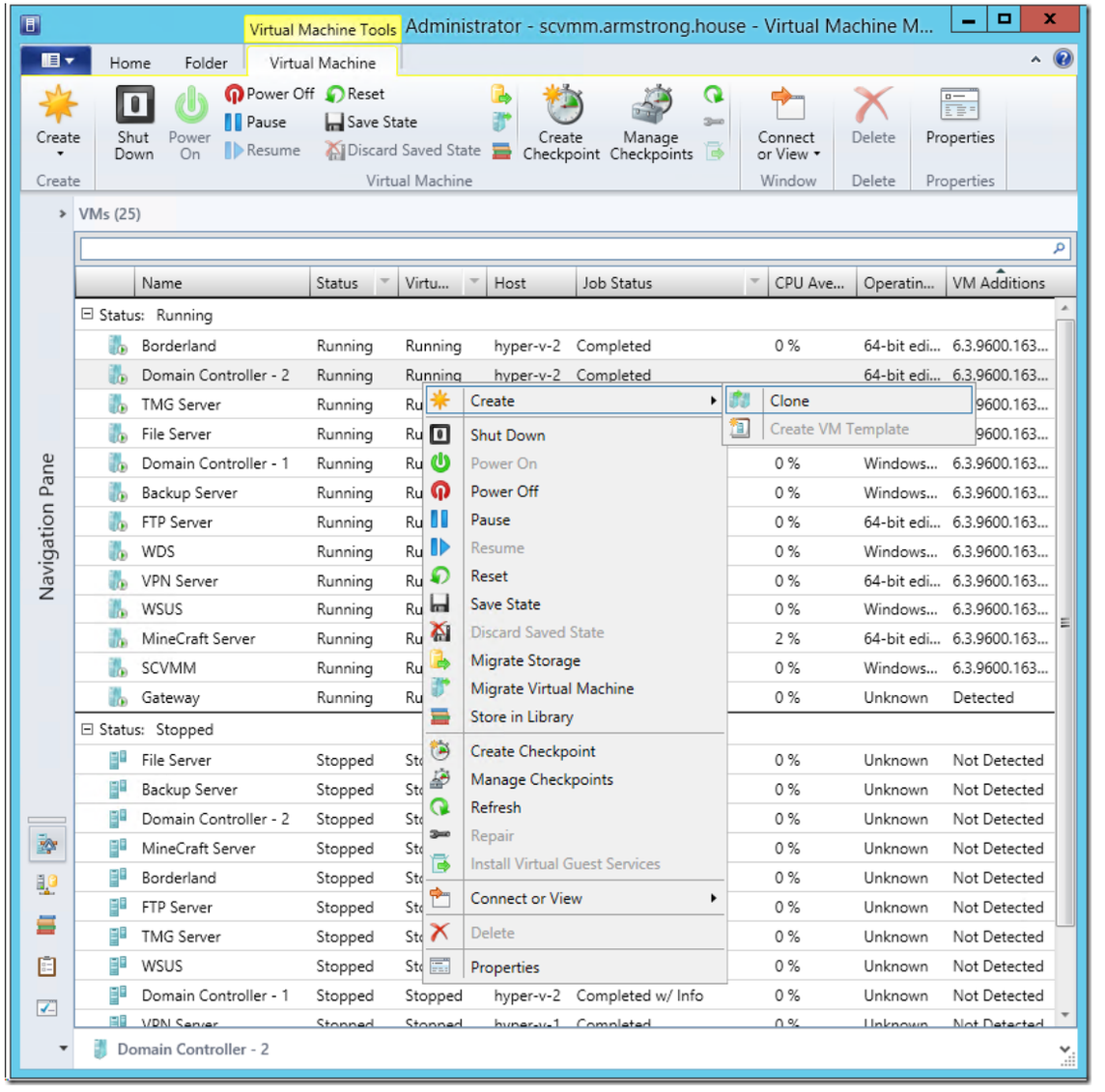
CVE-2007-1744	VMware Workstation
CVE-2008-0923	VMware Workstation
CVE-2009-1244	VMware ESXi, Workstation, Fusion
CVE-2012-0217	Xen Hypervisor
CVE-2014-0983	Oracle VirtualBox
CVE-2015-3456	QEMU
CVE-2015-7835	Xen Hypervisor
CVE-2016-6258	Xen Hypervisor
CVE-2016-7092	Xen Hypervisor
CVE-2017-0075	Microsoft Hyper-V
CVE-2017-0109	Microsoft Hyper-V
CVE-2017-4903	VMware ESXi, Workstation, Fusion
CVE-2017-4934	VMware Workstation, Fusion
CVE-2017-4936	VMware Workstation, Horizon View
CVE-2018-2698	Oracle VirtualBox

CPU Vulnerabilities

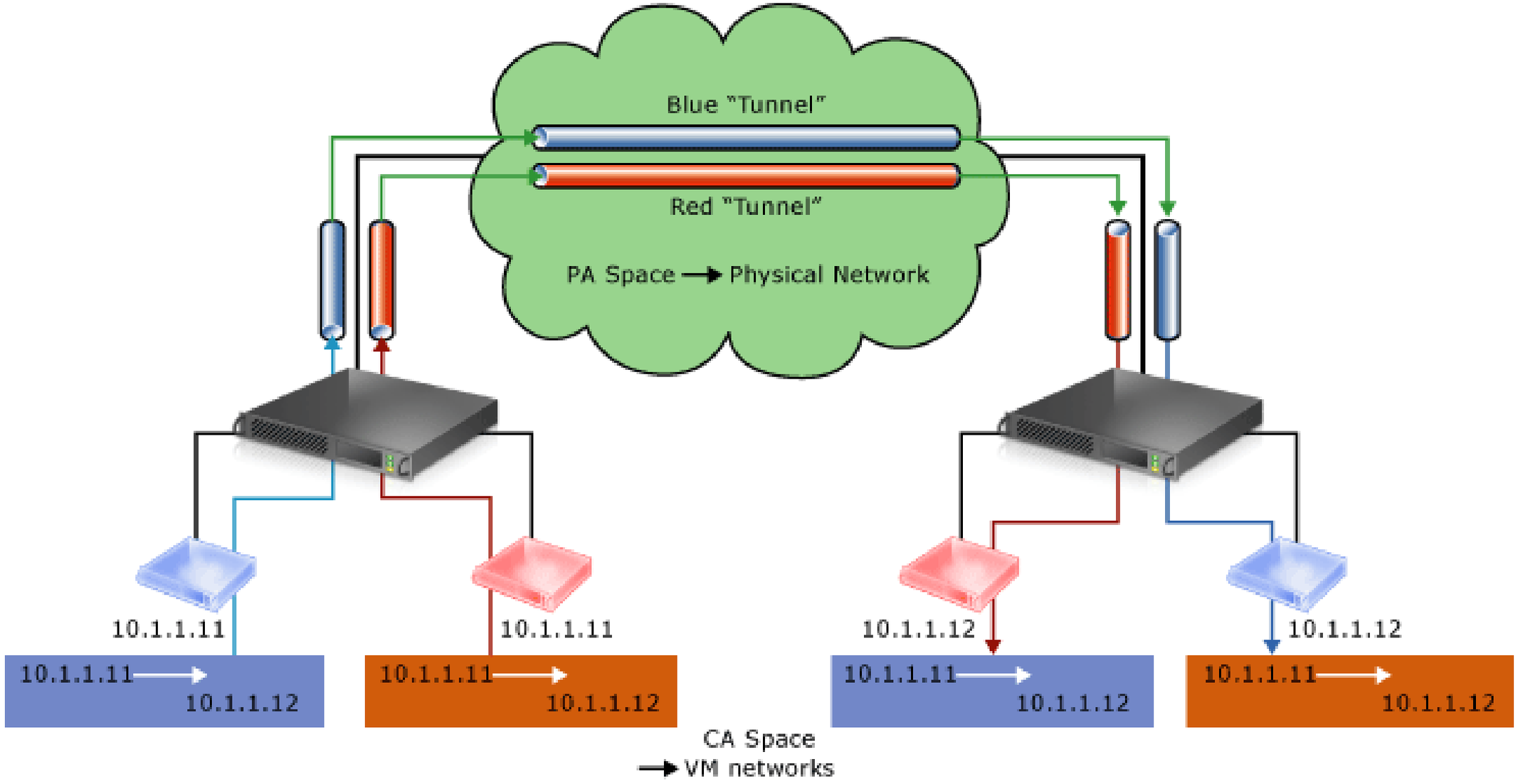
Post-Exploitation – VM Management

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

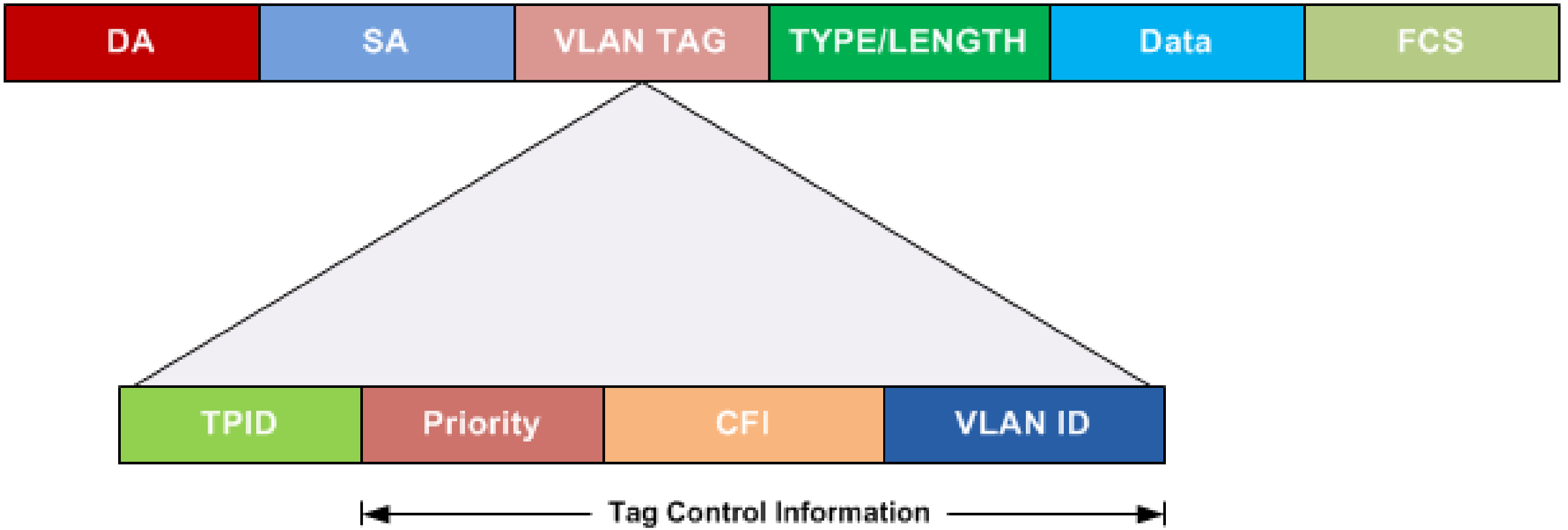
Post-Exploitation - Datacenter Management SW



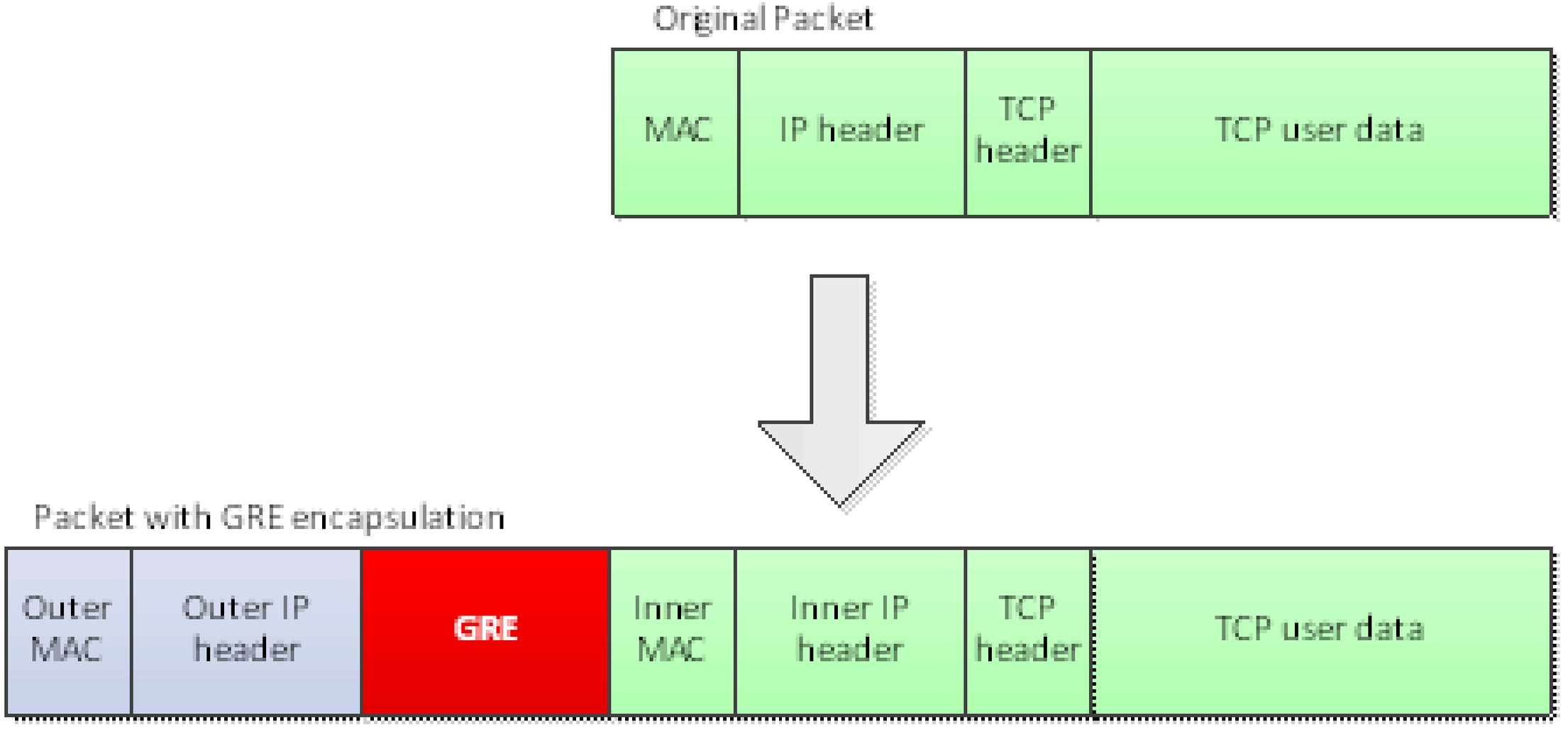
Traffic Isolation



Traffic Isolation – VLAN Tagging



Traffic Isolation - NVGRE



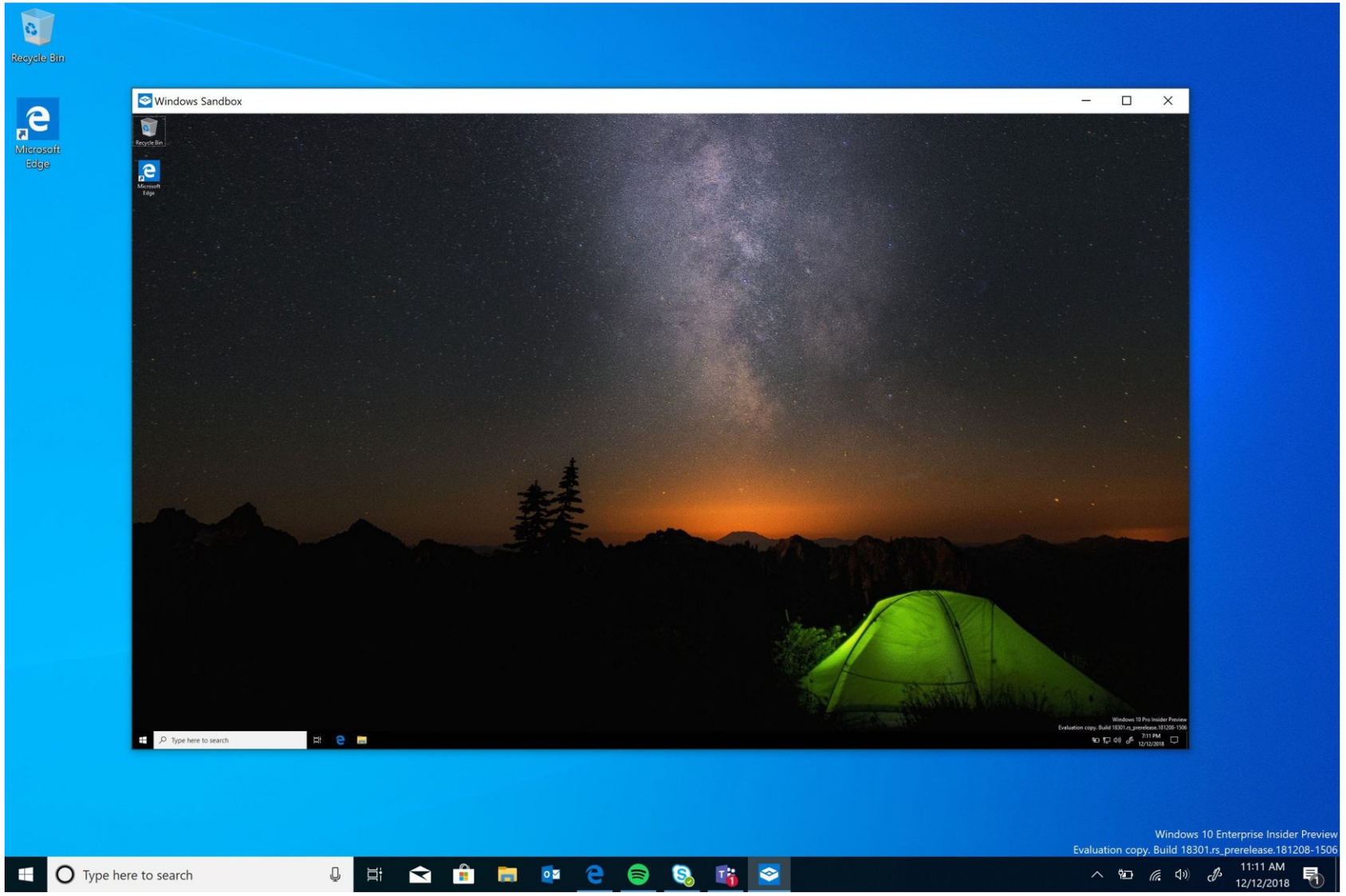
Other risks of virtualization

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

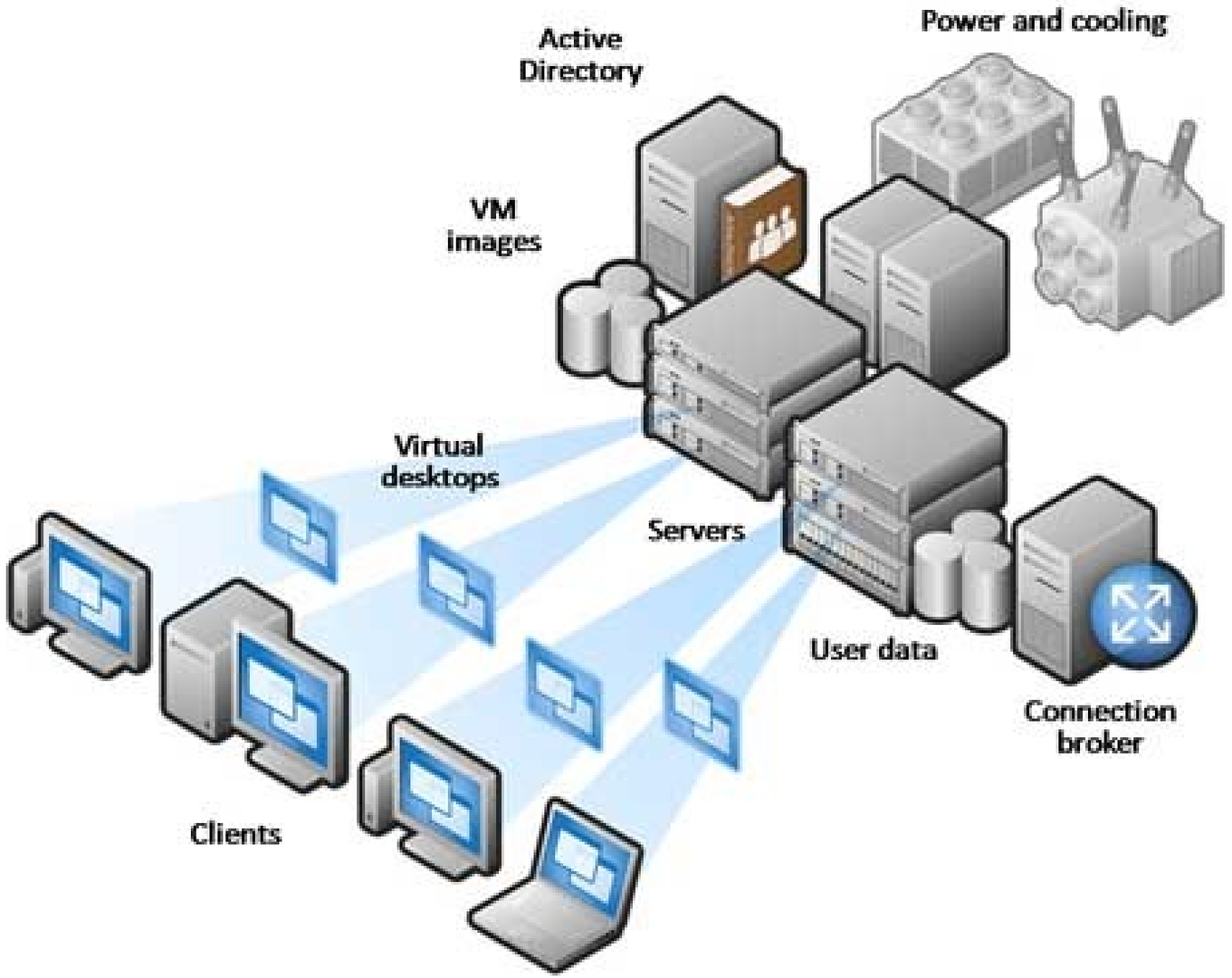
Virtualization-Based Security Solutions

- Sandboxing
- Agentless Antivirus
- Virtual Desktop Infrastructure (VDI)
- Windows 10 Credential Guard
- …

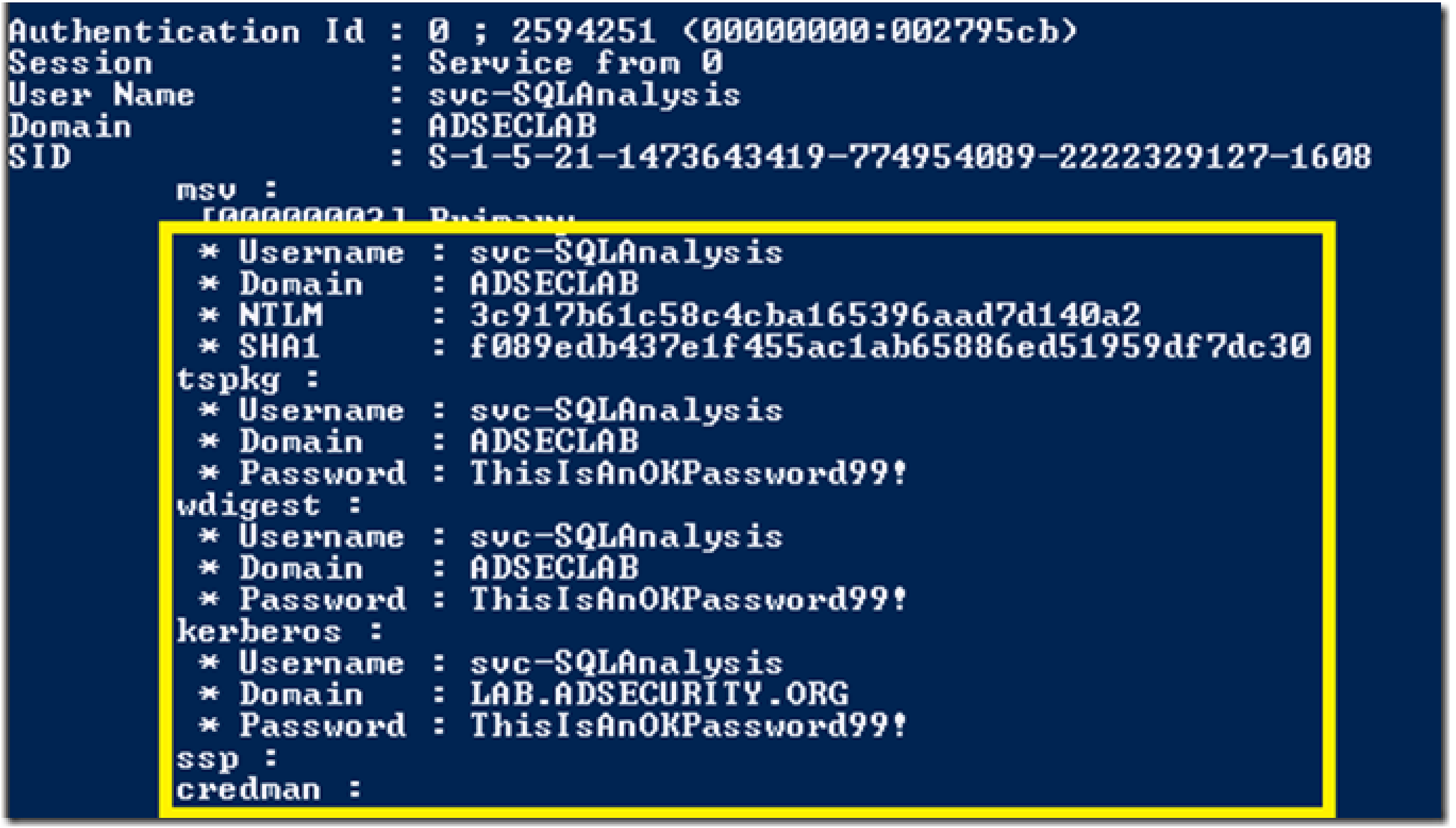
Sandboxing


Recycle Bin
Microsoft Edge
Windows Sandbox
Recycle Bin
Microsoft Edge
Type here to search
Windows 10 Pro Insider Preview
Evaluation copy. Build 18301.rs_prerelease.181208-1506
7:11 PM
12/12/2018
Type here to search
Windows 10 Enterprise Insider Preview
Evaluation copy. Build 18301.rs_prerelease.181208-1506
11:11 AM
12/12/2018

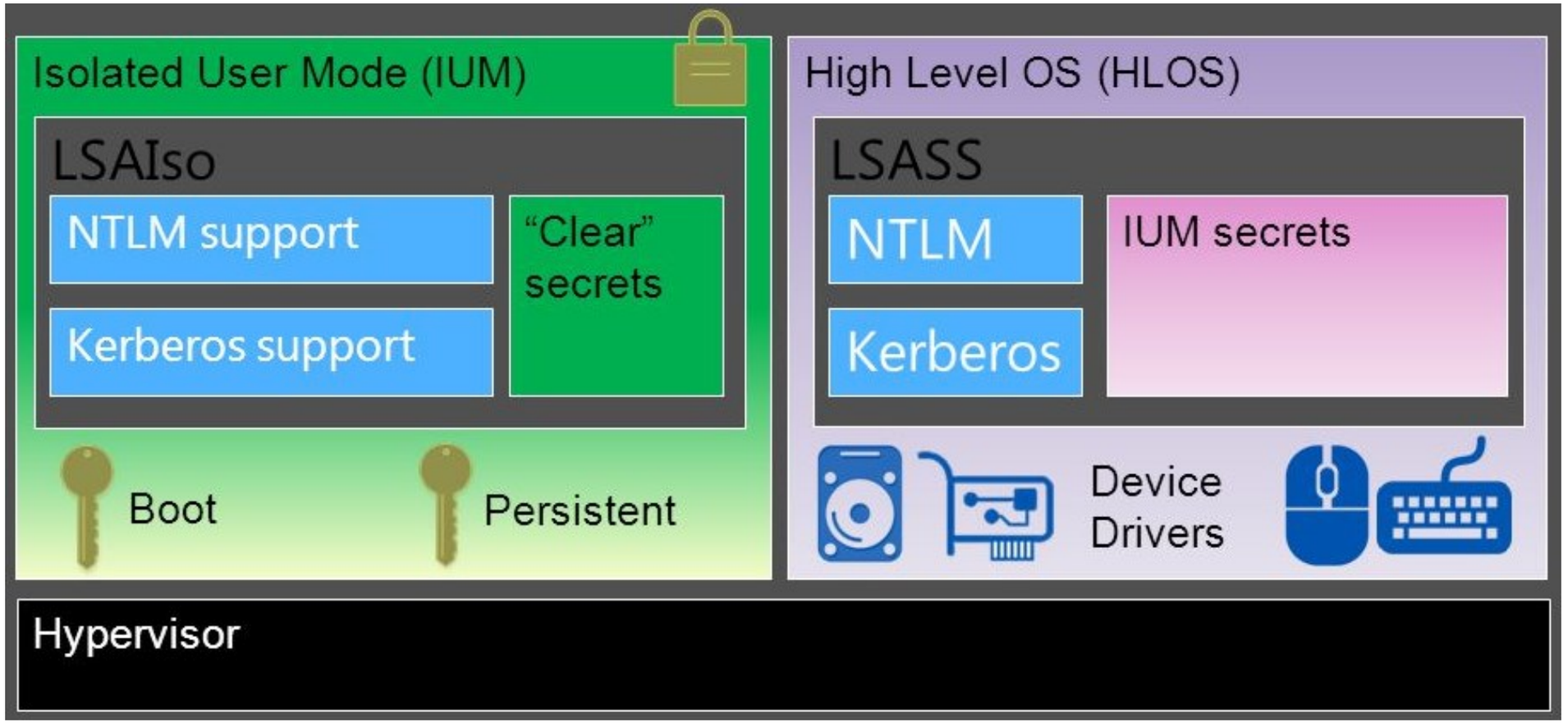
Virtual Desktop Infrastructure



Windows 10+ Virtual Secure Mode: Motivation



Windows 10+ Virtual Secure Mode



Cloud Computing Security Risks

Who has access to our data?

Azure Datacenter Security

24 hour monitored
PHYSICAL SECURITY

Centralized
MONITORING AND ALERTS

Update
MANAGEMENT

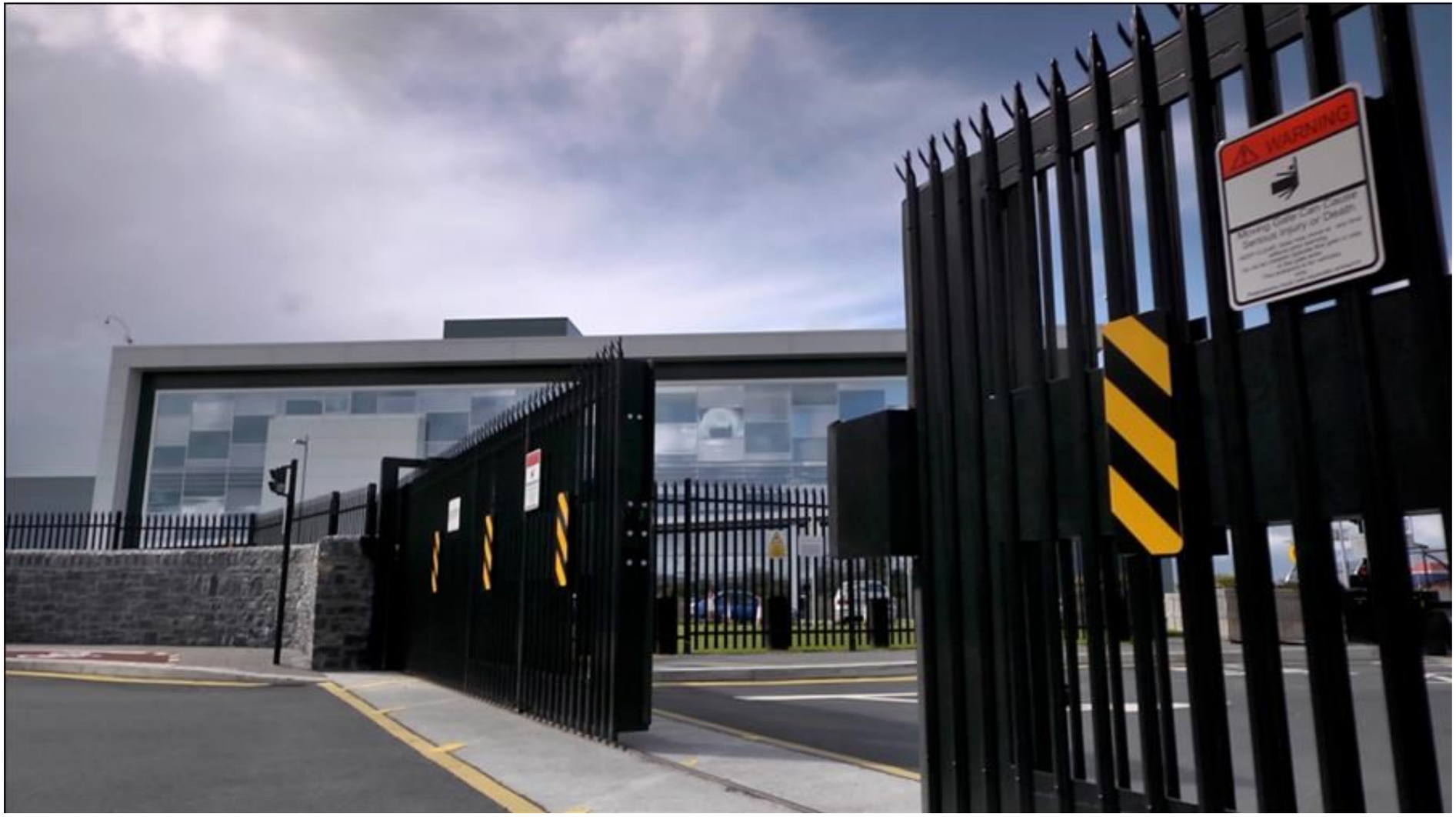
Anti-Virus/Anti-Malware
PROTECTION

Penetration **TESTING**

DDoS **DEFENSE**

Physical Security

Physical Security

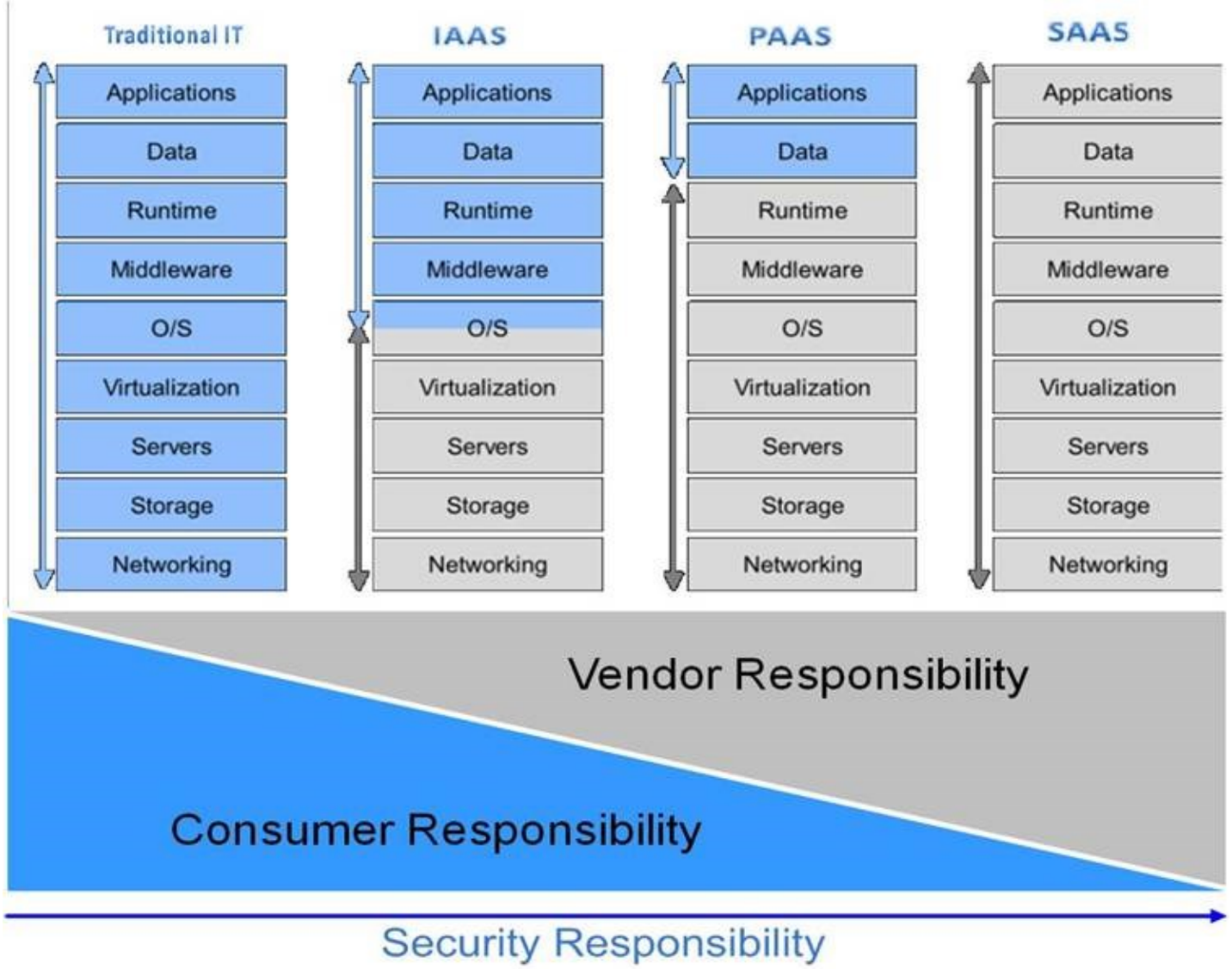


Physical Security

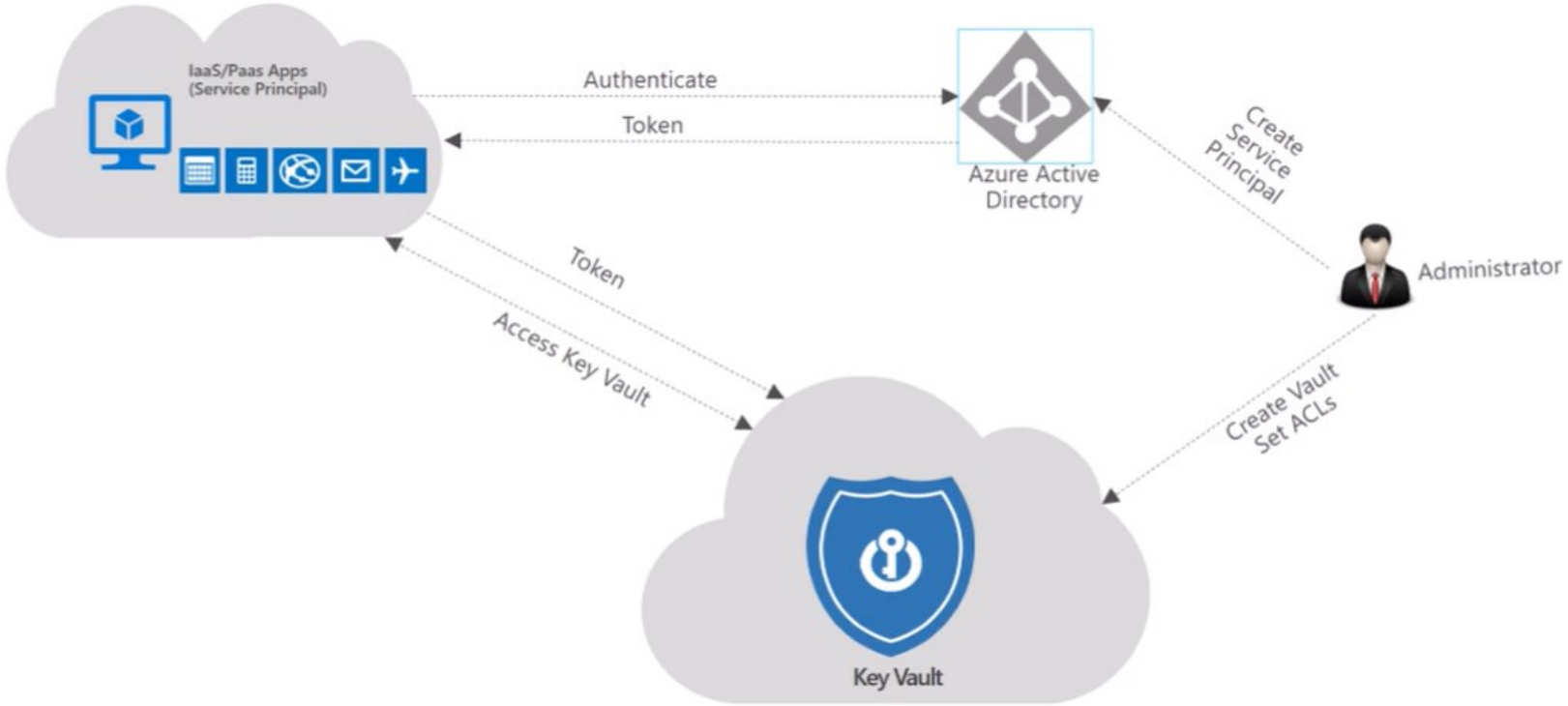
Physical Security

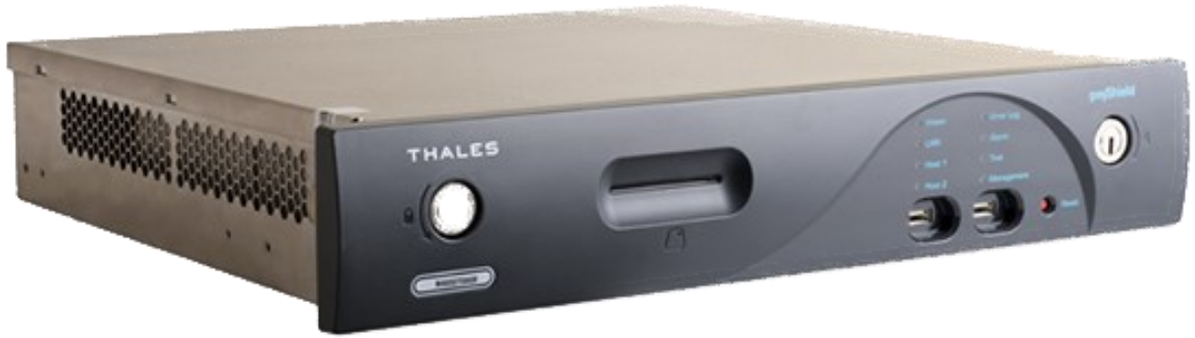
Hard Disk Crushers

Shared Responsibility (Misconfigurations)



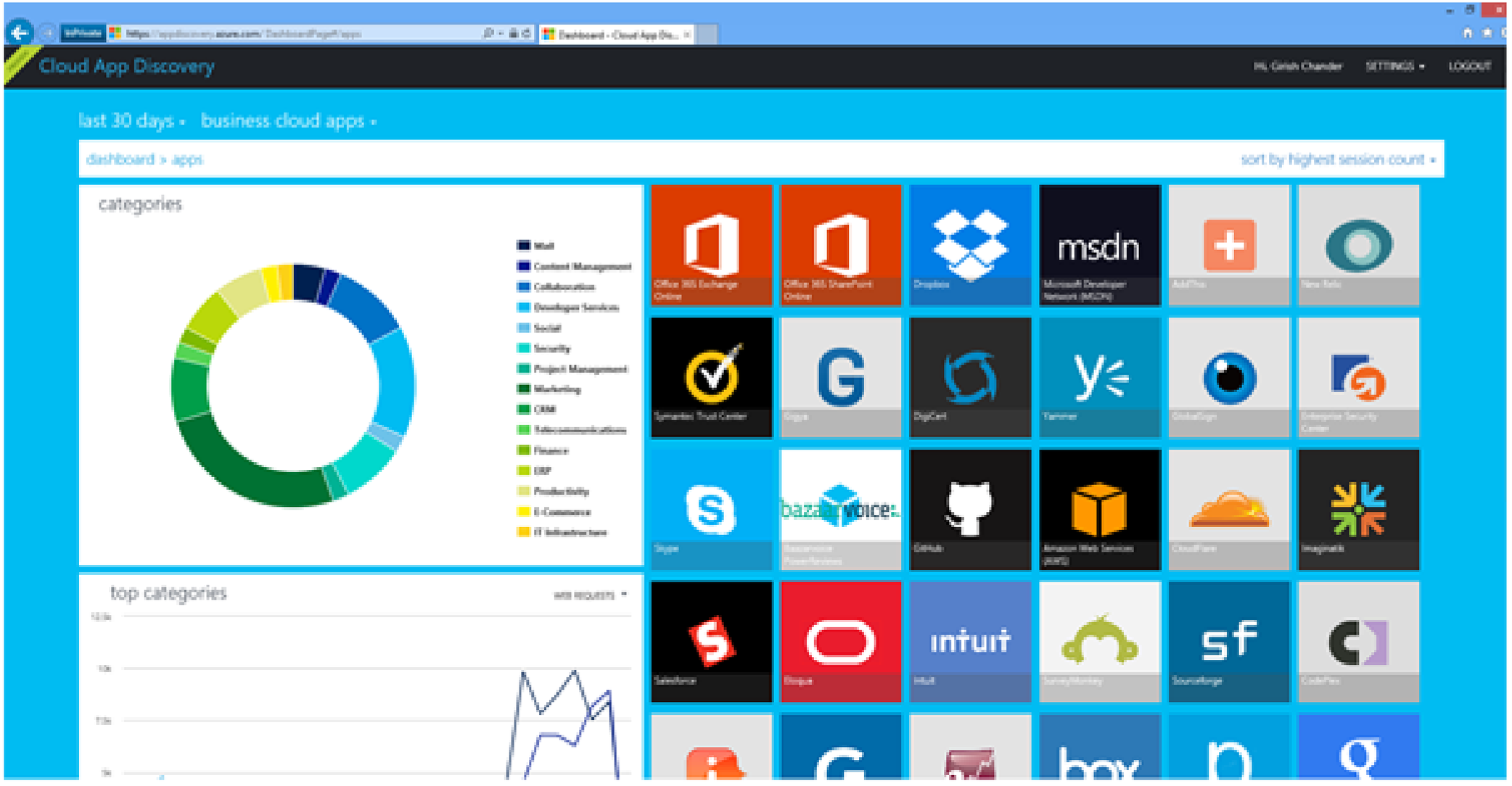
Secrets in Source Code Repositories





Demo: Managing Secrets in CI

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



Regulatory Compliance – Czech Republic

- Zákon č. 101/2000 Sb., o ochraně osobních údajů
- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti
- Zákon č. 365/2000 Sb., o informačních systémech veřejné správy
- General Data Protection Regulation (GDPR)

Other Cloud Risks

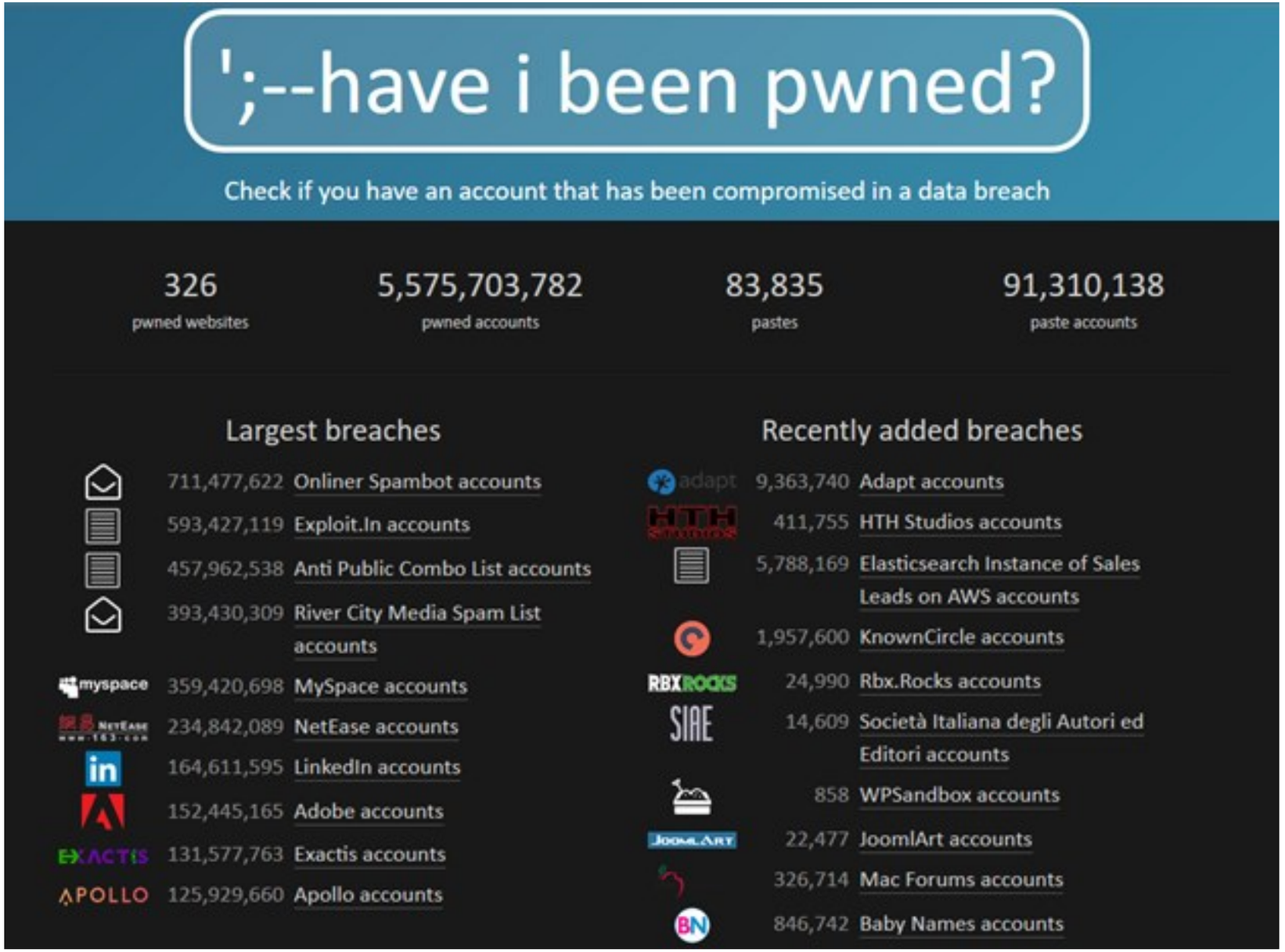
- Unclear data location
- Lack of investigative support
- Disaster recovery
- Long-term viability, vendor lock-in

Authentication in Cloud Applications

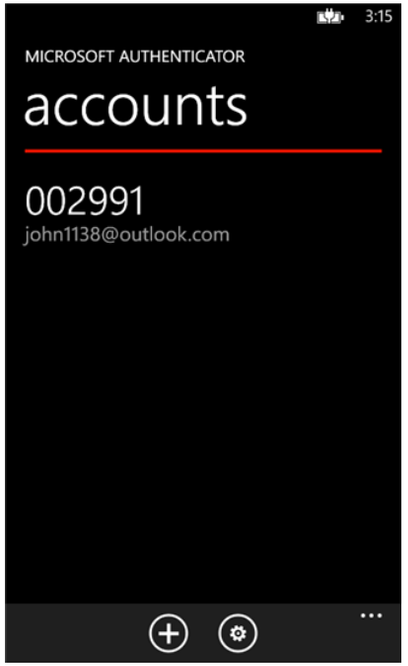
Authentication

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

Passwords Are Dead



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

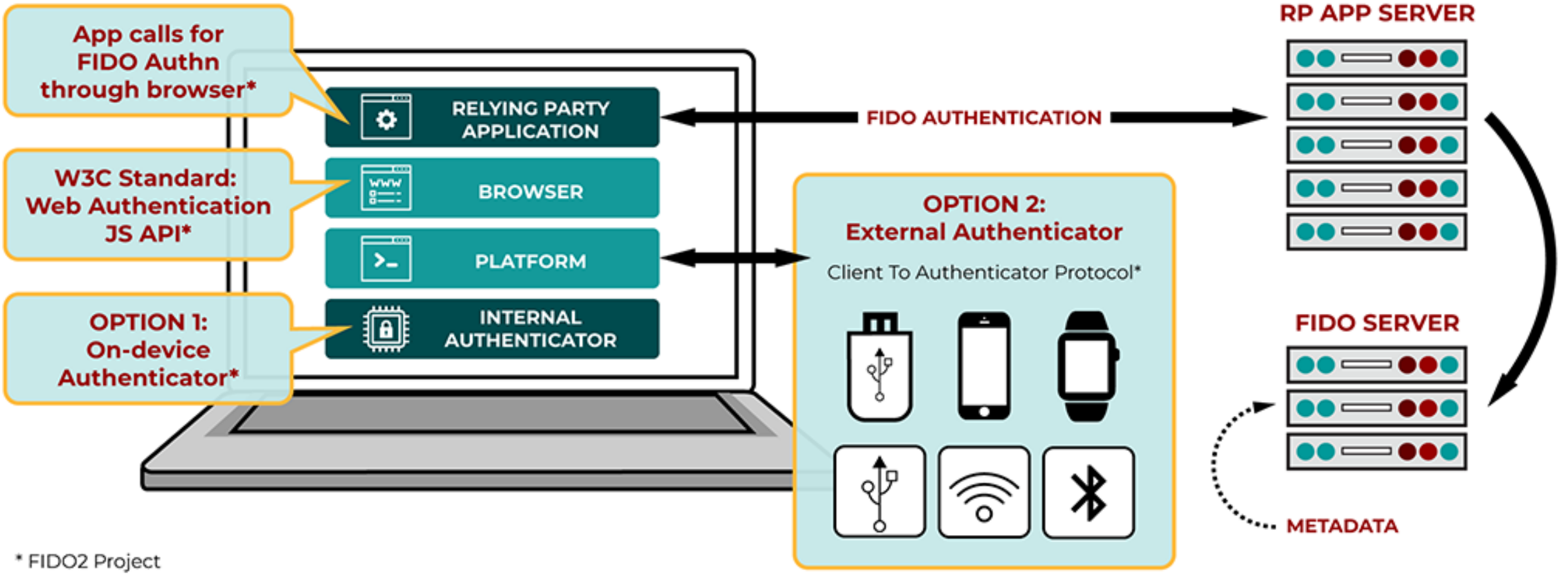
$$HMAC(K, C) := SHA1(K \oplus 0x5C5C... \| SHA1(K \oplus 0x3636... \| C))$$

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

K – Secret Key

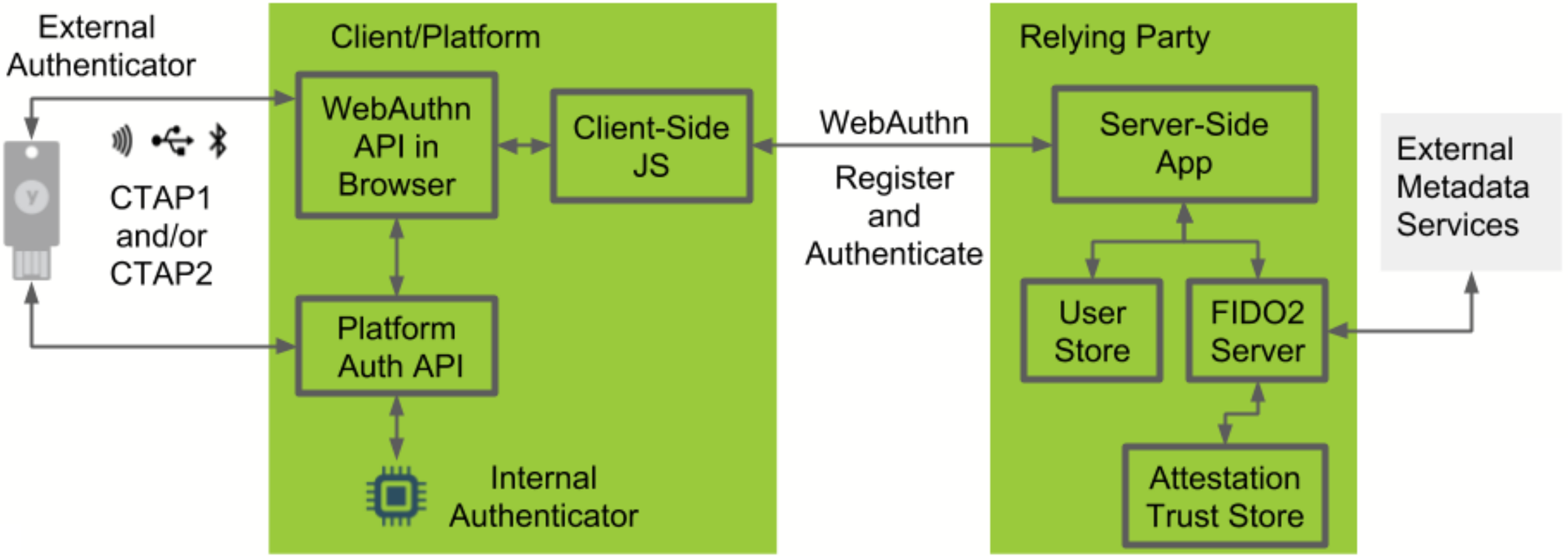
C – Counter/Clock

Passkeys / FIDO2 / W3C Web Authentication



* FIDO2 Project

FIDO Protocols



Demo: Passkeys

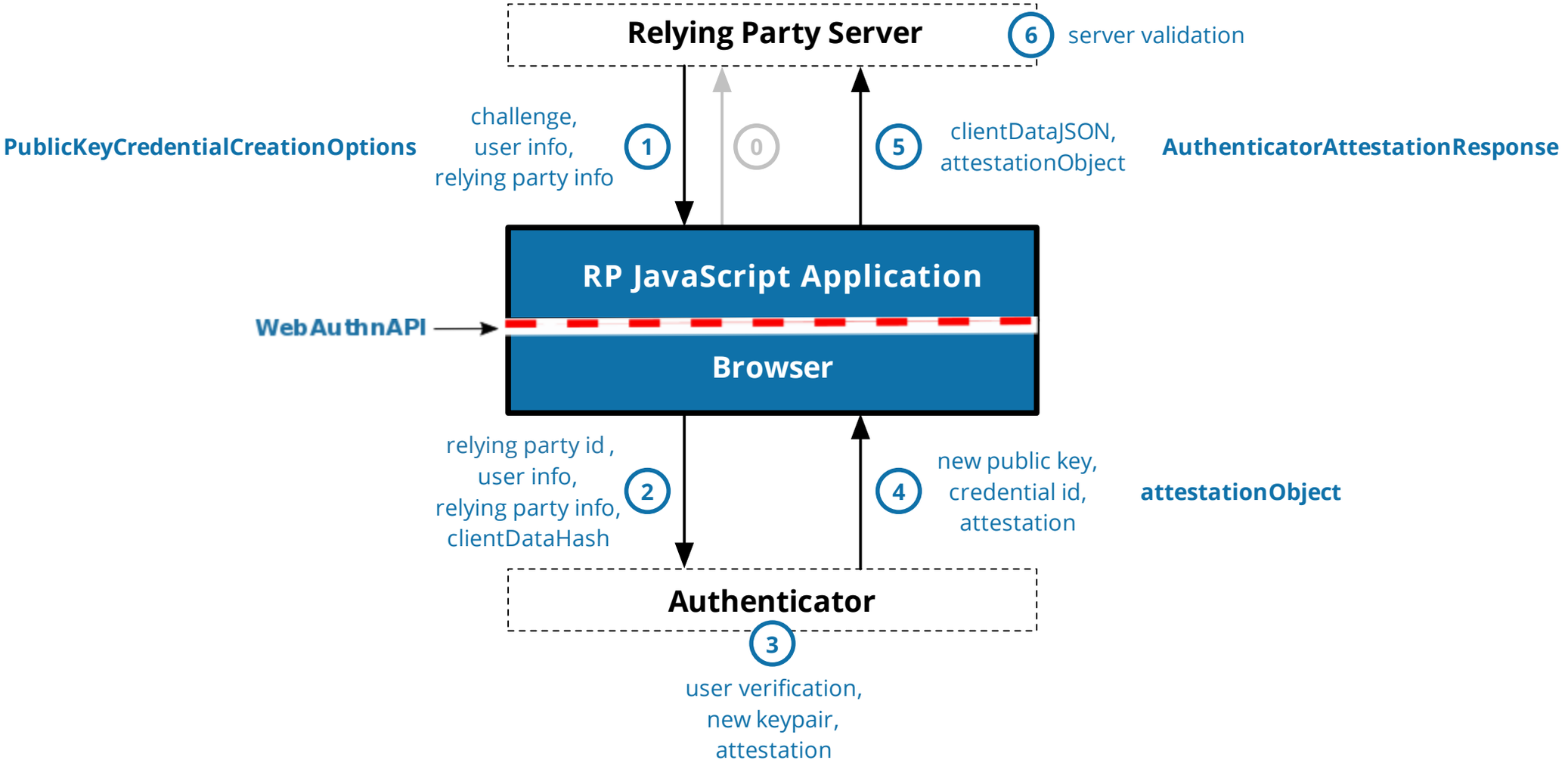
WebAuthn API

```
// Detection of WebAuthn support
if (!window.PublicKeyCredential) { /* Client not capable. Handle error. */ }

// Registration
const credential = await navigator.credentials.create({
    publicKey: publicKeyCredentialCreationOptions
});

// Assertion (Logon)
const credential = await navigator.credentials.get({
    publicKey: publicKeyCredentialRequestOptions
});
```

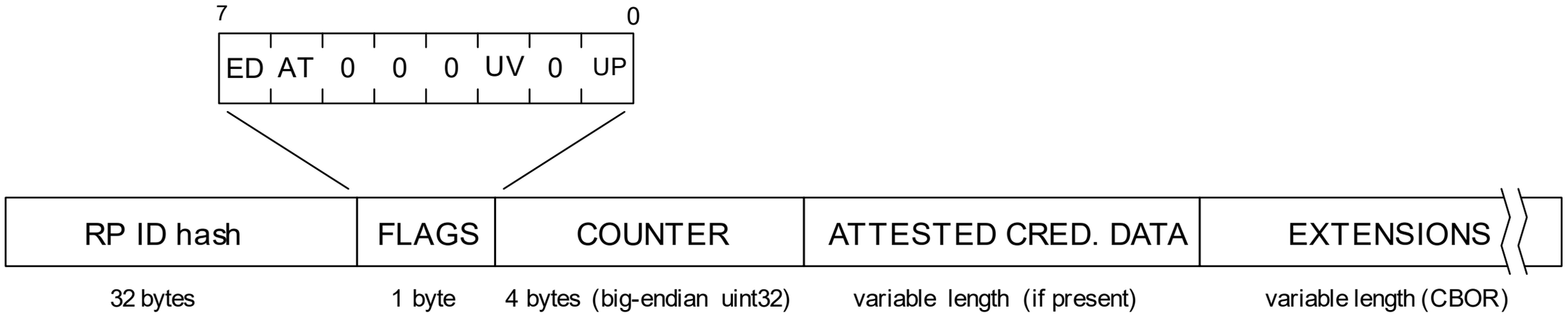
Registration Flow



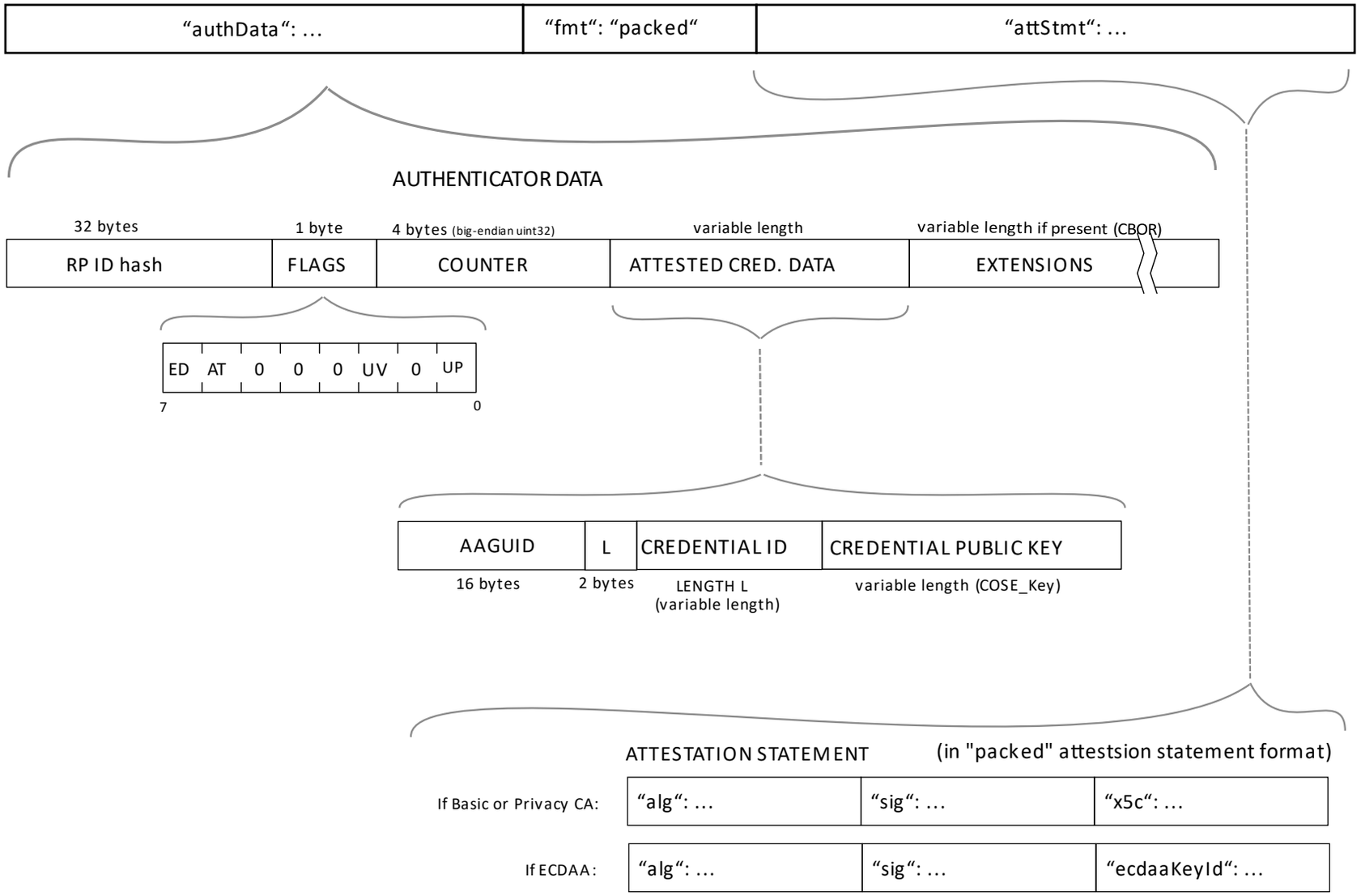
Public Key Credential Creation Options

```
const publicKeyCredentialCreationOptions = {
    challenge: Uint8Array.from(randomStringFromServer, c => c.charCodeAt(0)),
    rp: {
        name: "Microsoft",
        id: "login.microsoft.com",
    },
    user: {
        id: Uint8Array.from(window.atob("MIIBkzCCATigAwIBAjCCAZMwggE4oAMCAQIwggGTMII="), c=>c.charCodeAt(0)),
        name: "michael@dsinternals.com",
        displayName: "Michael Grafnetter",
    },
    pubKeyCredParams: [{alg: -7, type: "public-key"}],
    authenticatorSelection: {
        authenticatorAttachment: "cross-platform",
        requireResidentKey: true,
        userVerification: "required"
    },
    timeout: 60000,
    attestation: "direct"
};
```

Authenticator Data



Attestation Object

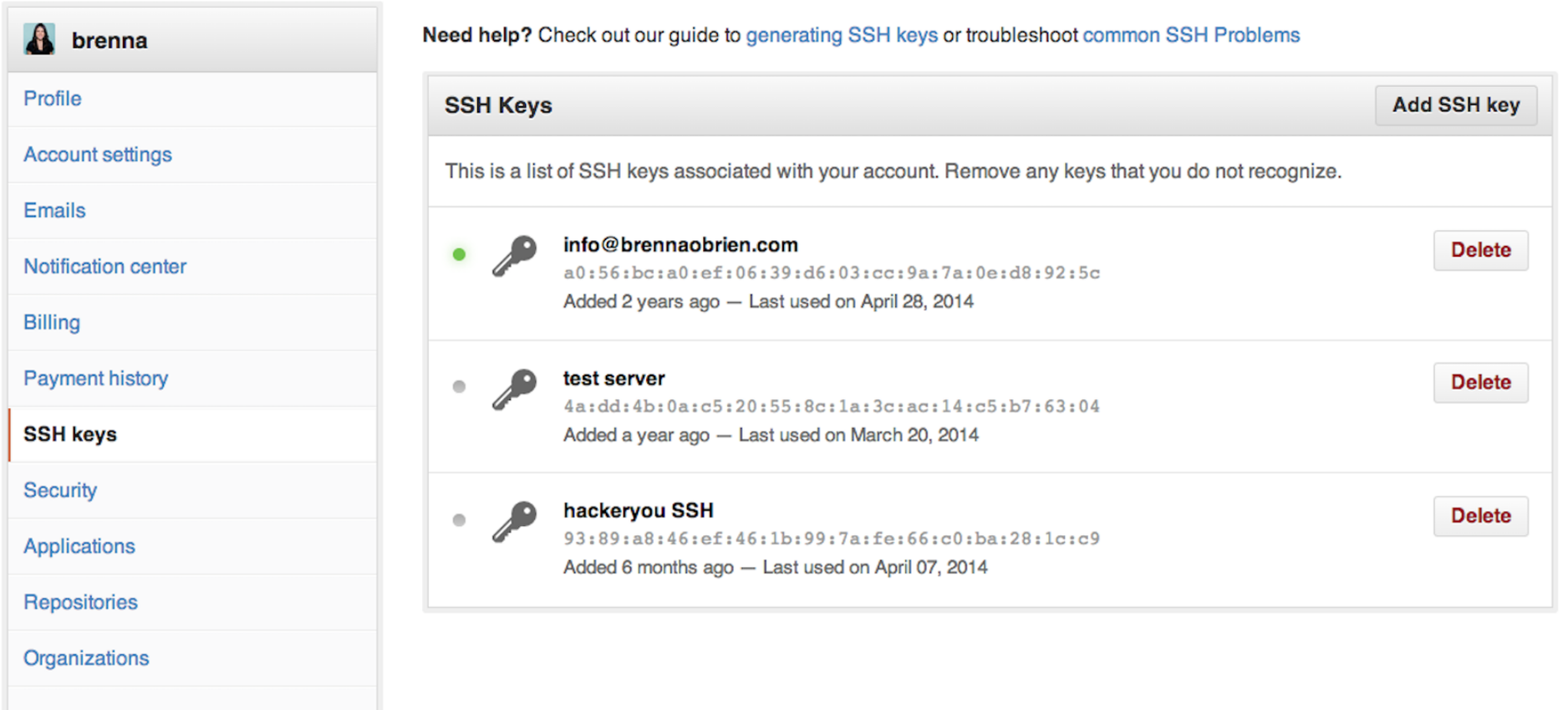


Problem: Lost Device

- Multiple Devices
- 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



Claims-Based Identity

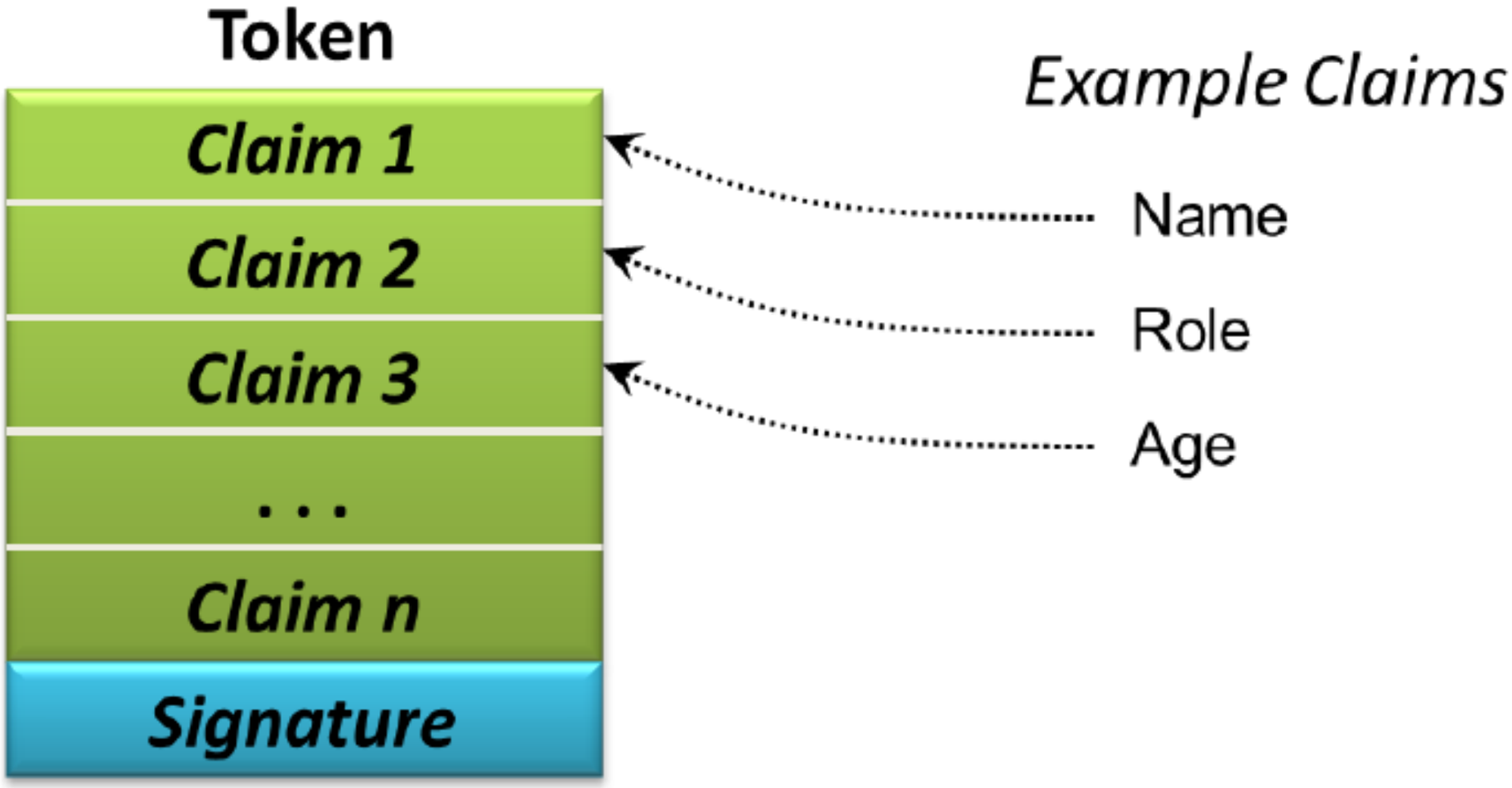
Most Common Technologies

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

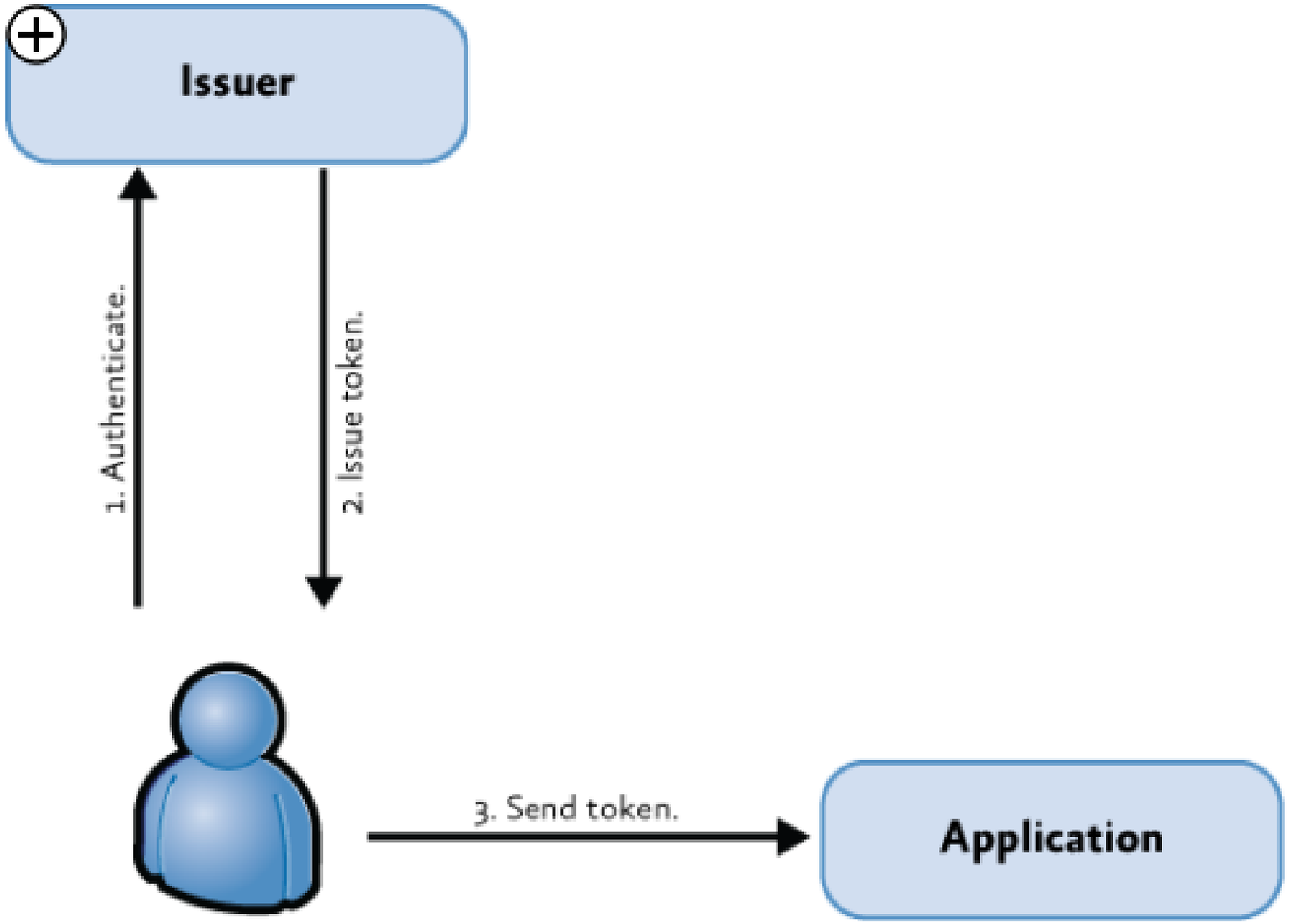
Claims-based Identity

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

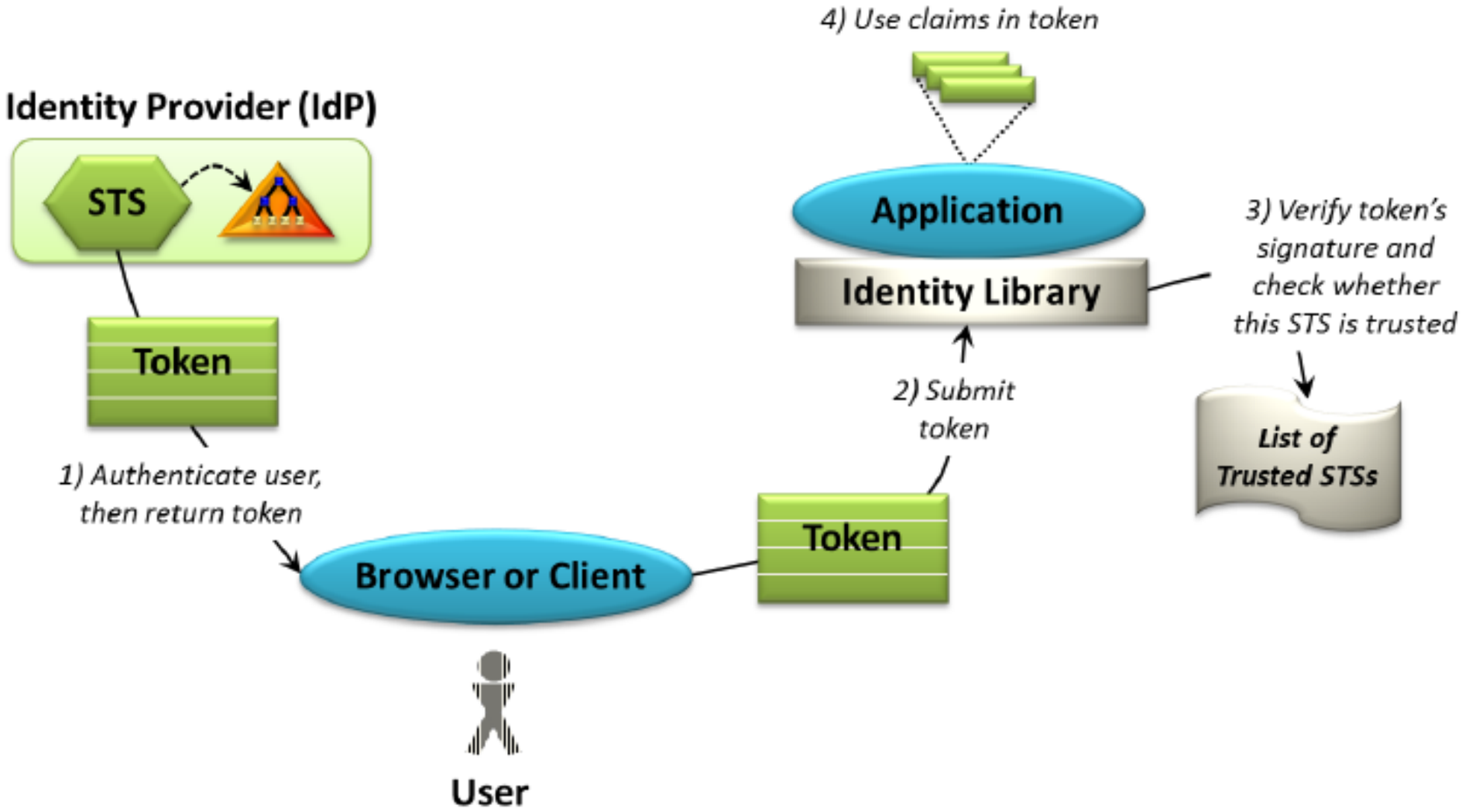
Tokens


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

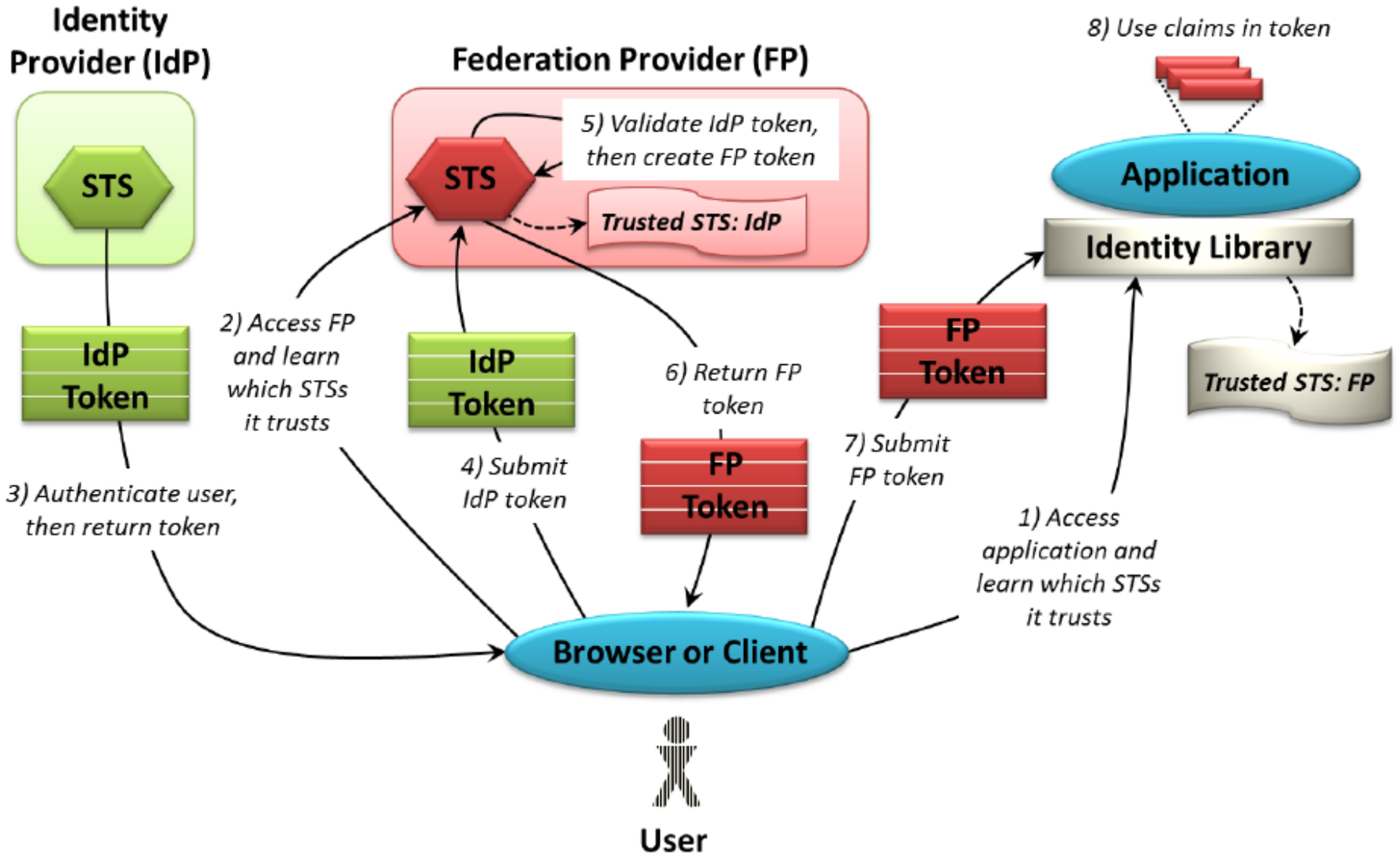
Basic Communication Pattern



Identity Providers and Identity Libraries



Identity Federation



Shibboleth

- SAML-based federation portal
- Open Source

Demo: CAS Logon to O365

SAML

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>
```

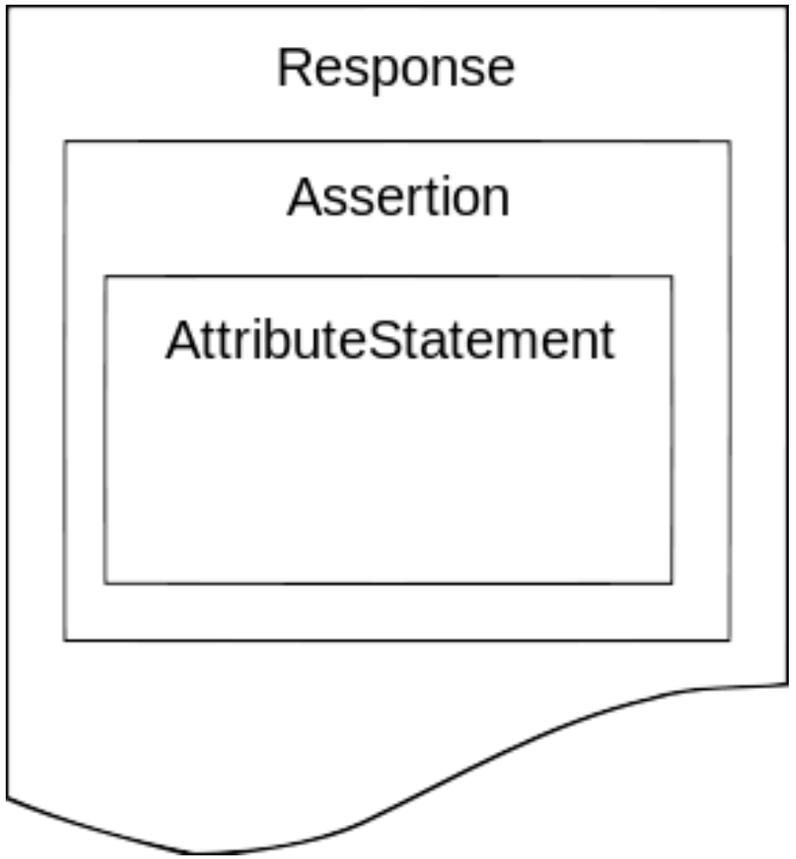
Assertion A was issued at time t by issuer R regarding subject S provided conditions C are valid.

- Authentication statements
- Attribute statements
- Authorization decision statements

Demo: SAML Tokens

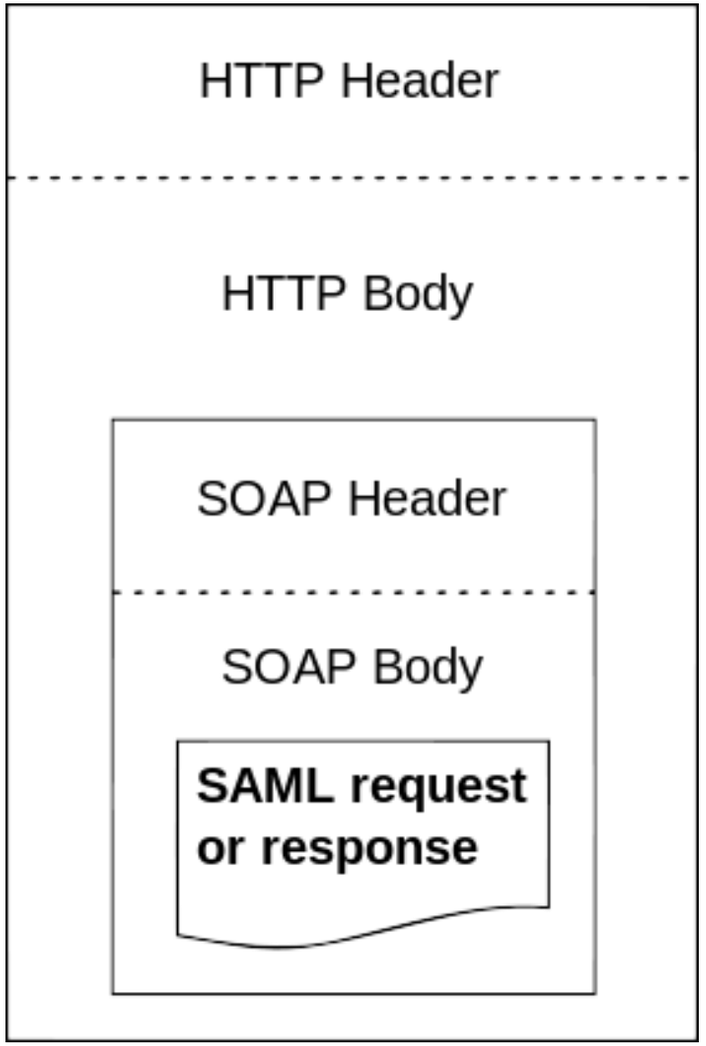
SAML Protocols

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



SAML Bindings

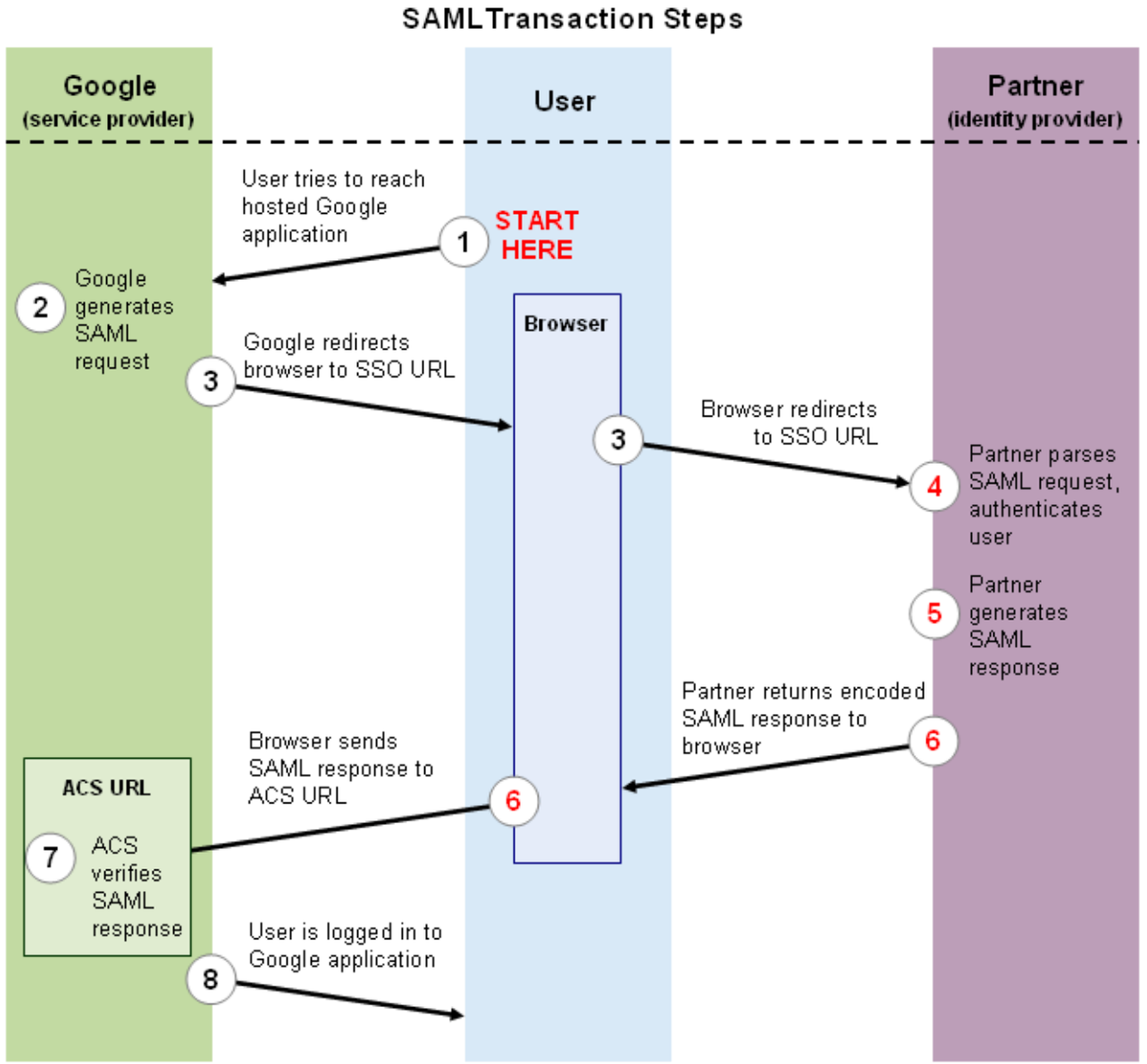
- SAML SOAP Binding
- Reverse SOAP (PAOS) Binding
- HTTP Redirect (GET) Binding
- HTTP POST Binding
- HTTP Artifact Binding
- SAML URI Binding



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 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

WS-*

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**

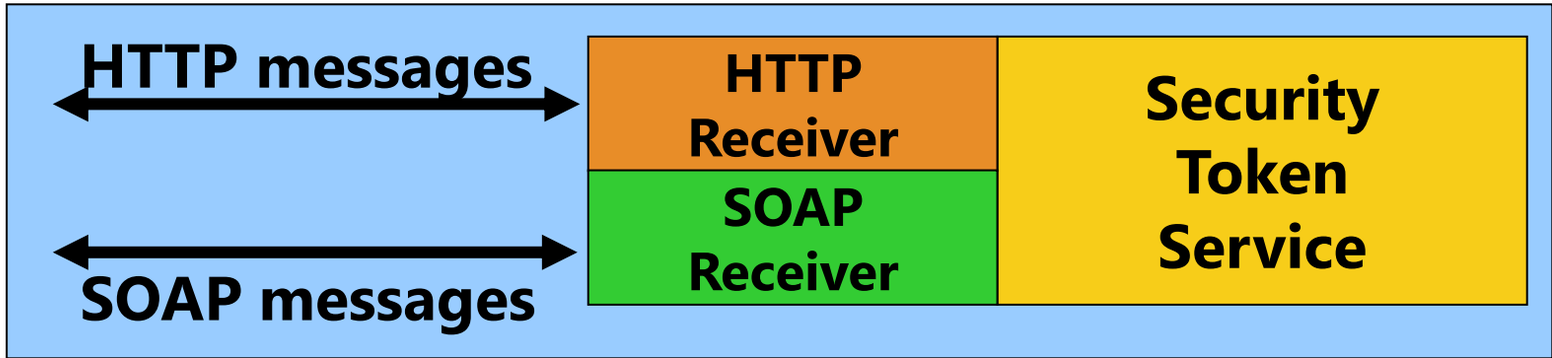
WS-Trust

- 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-Trust

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:

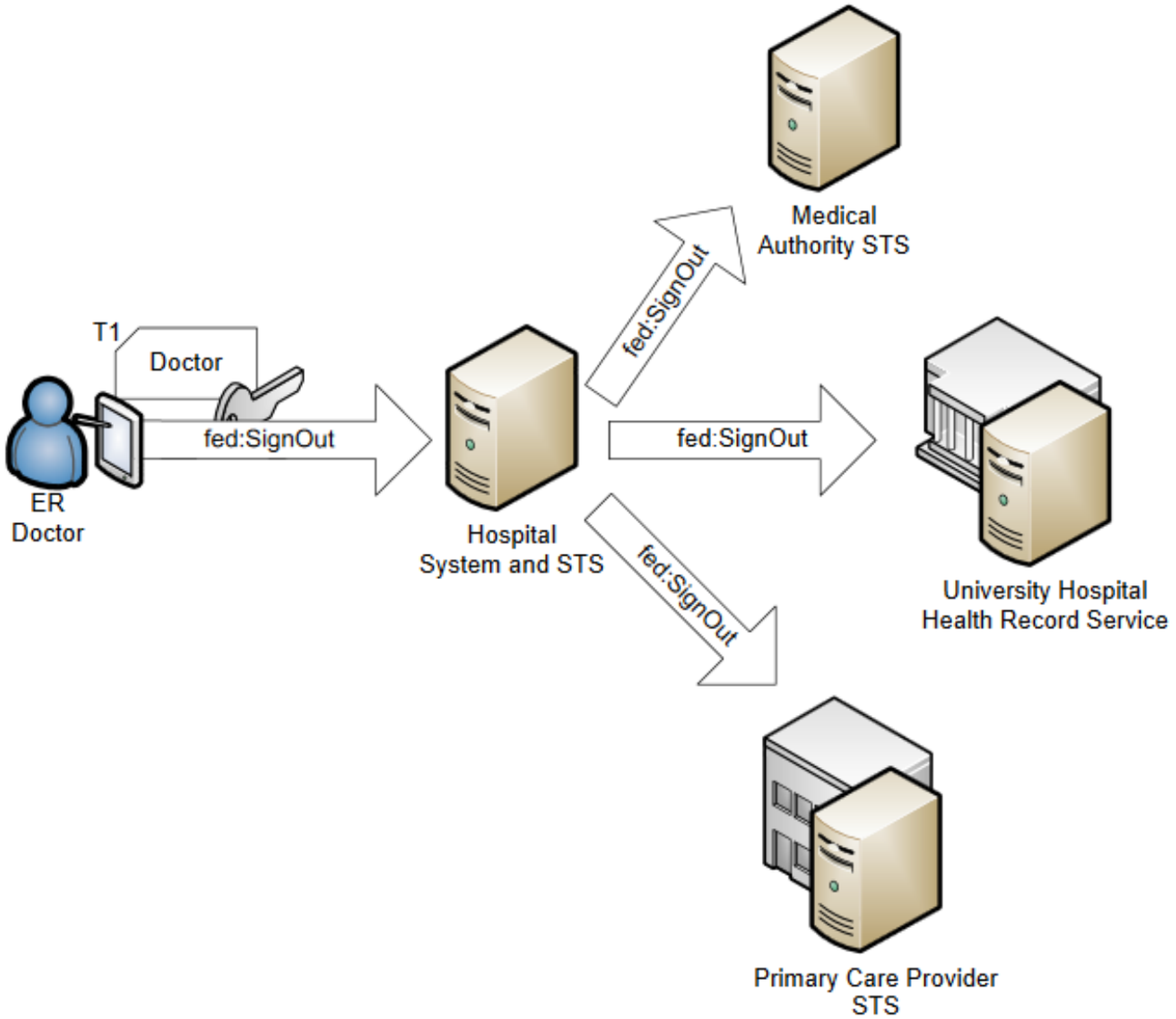
- **Wa=signin1.0:** This tells the ADFS server to invoke a login for the user.
- **Wtrealm:** This tells ADFS what application I was trying to get to. This has to match the identifier of one of the relying party trusts listed in ADFS.
- **Wctx:** This is some session data that the application wants sent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

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: Federation Metadata

JSON Web Token

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
```

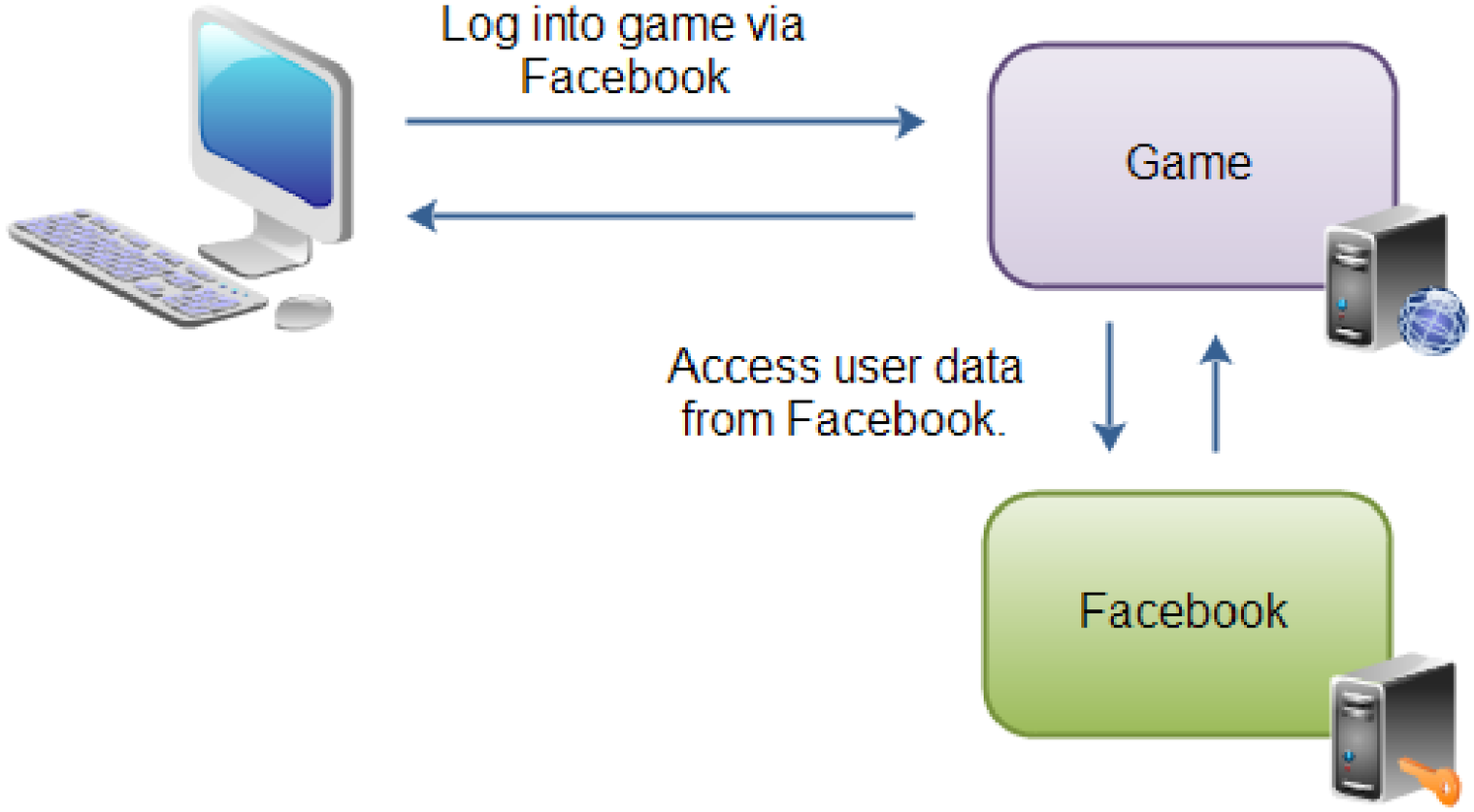
OAuth

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

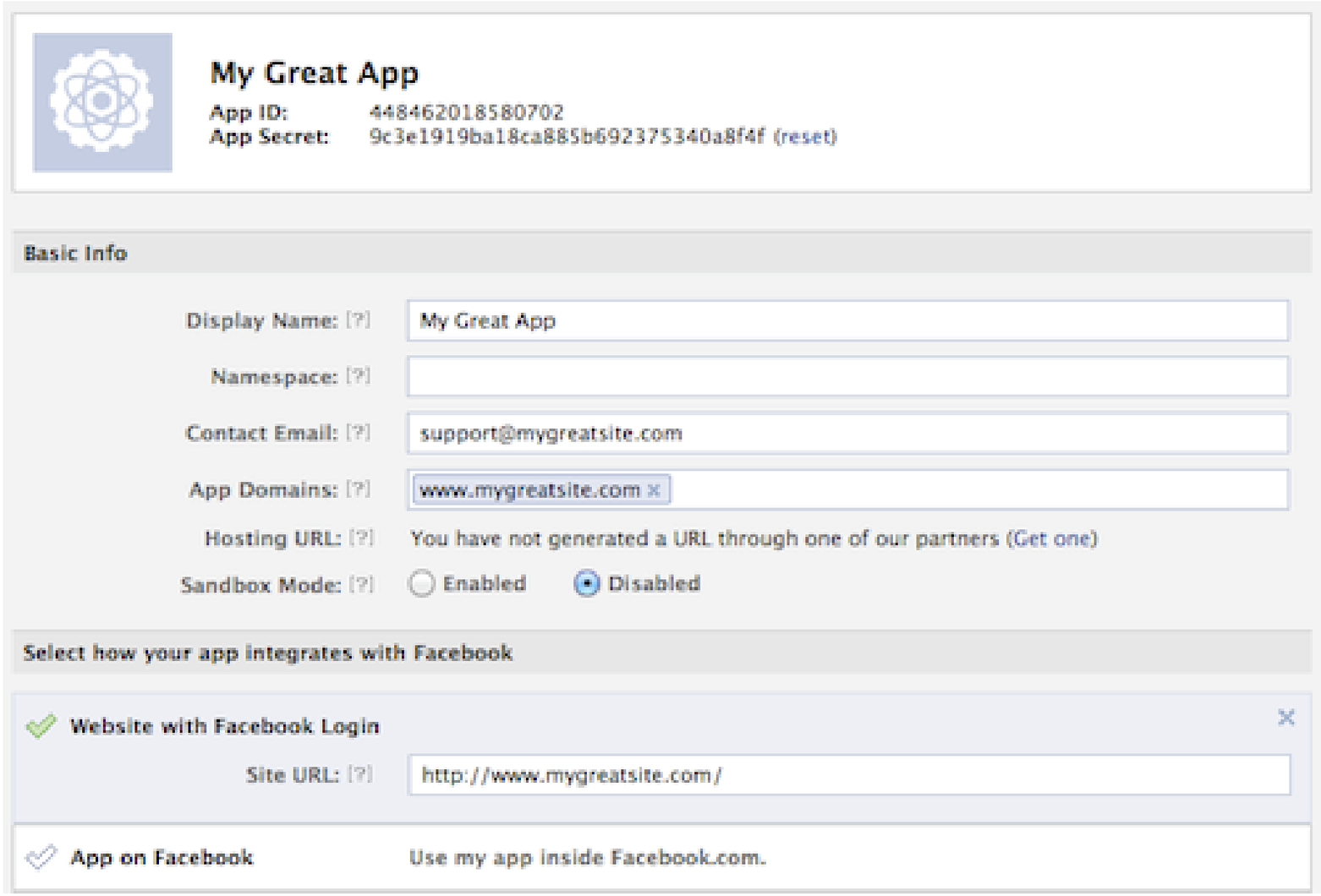
- 2006 – Twitter missing delegation in OpenID
- 2007 – OAuth Core 1.0 (Twitter, Google,…)
- 2010 – OAuth 1.0 (IETF RFC 5849)
- 2012 – OAuth 2.0
  - Framework - RFC 6749
  - Bearer Token Usage - RFC 6750
  - Threat Model and Security Considerations - RFC 6819
  - …

OAuth 2.0

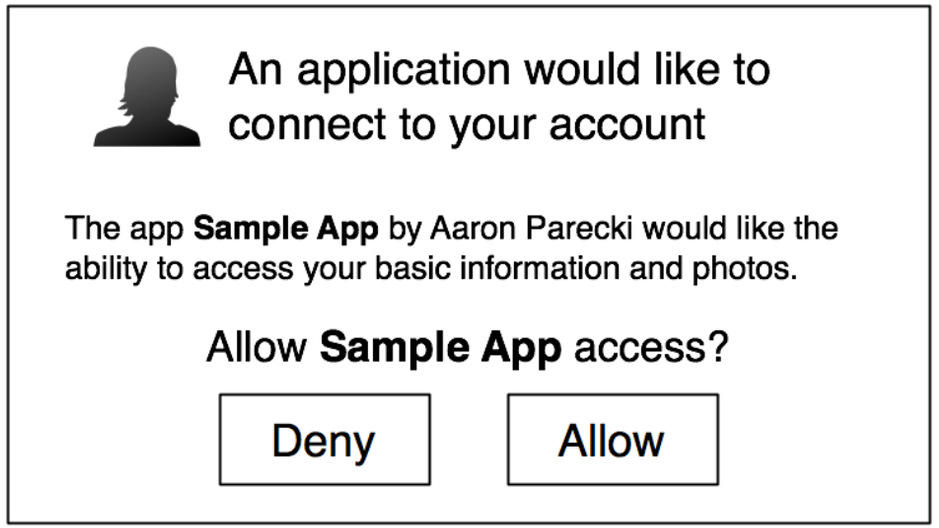
- Not backwards compatible with OAuth 1.0
- Framework -> Non-interoperability
- Authorization flows for web, desktop, mobile and TV applications
- Client types
  - Public
  - Confidential
- Client Profiles
  - Web Application
  - User Agent
  - Native

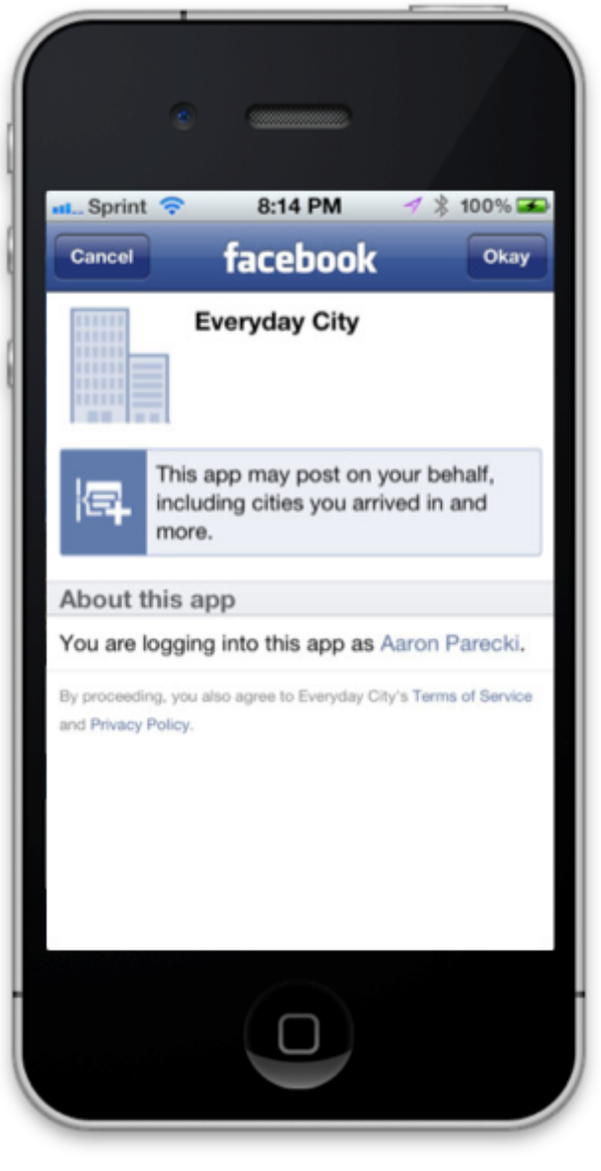
Application registration

- Client ID
- Client secret
- Redirect URI

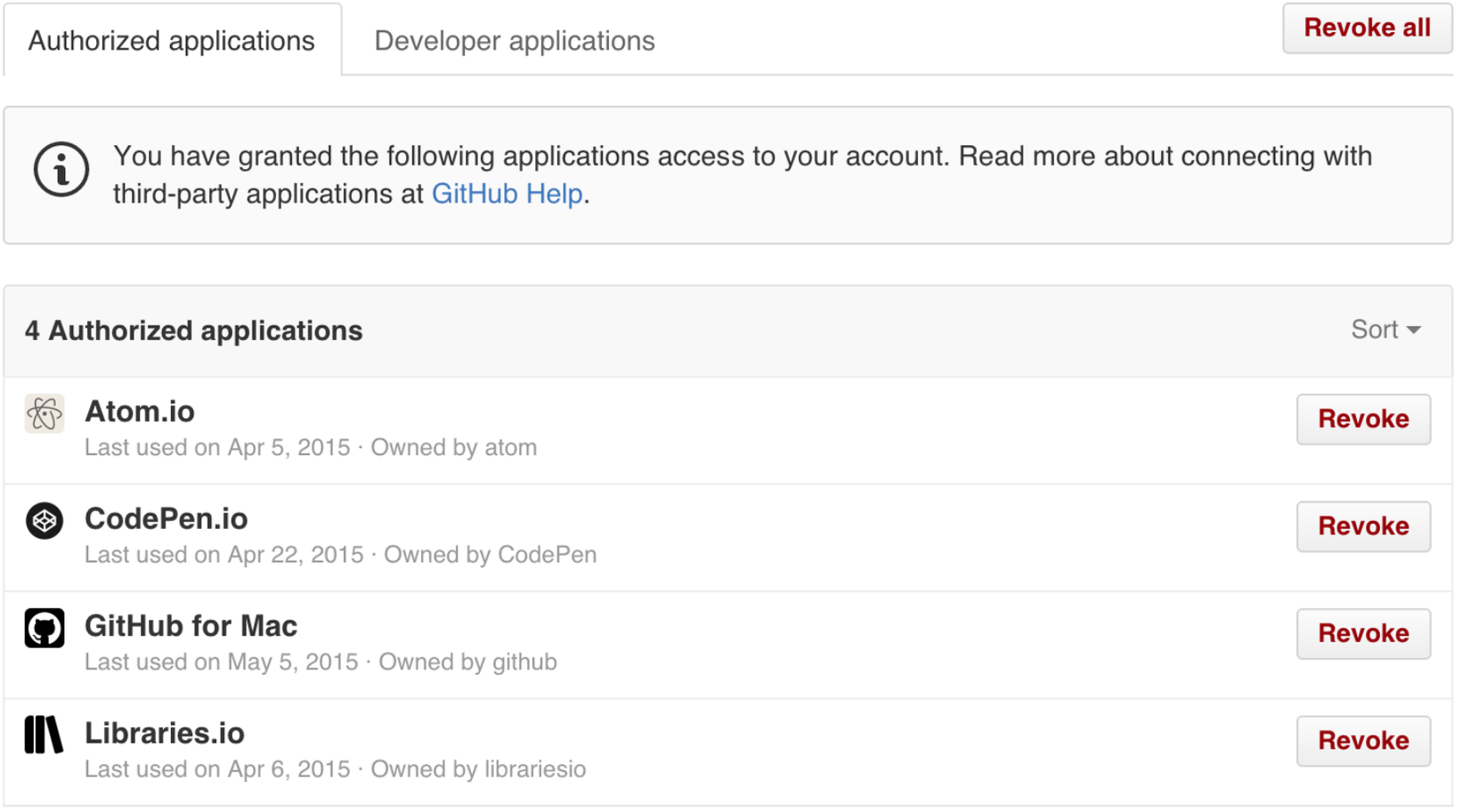


Confirmation

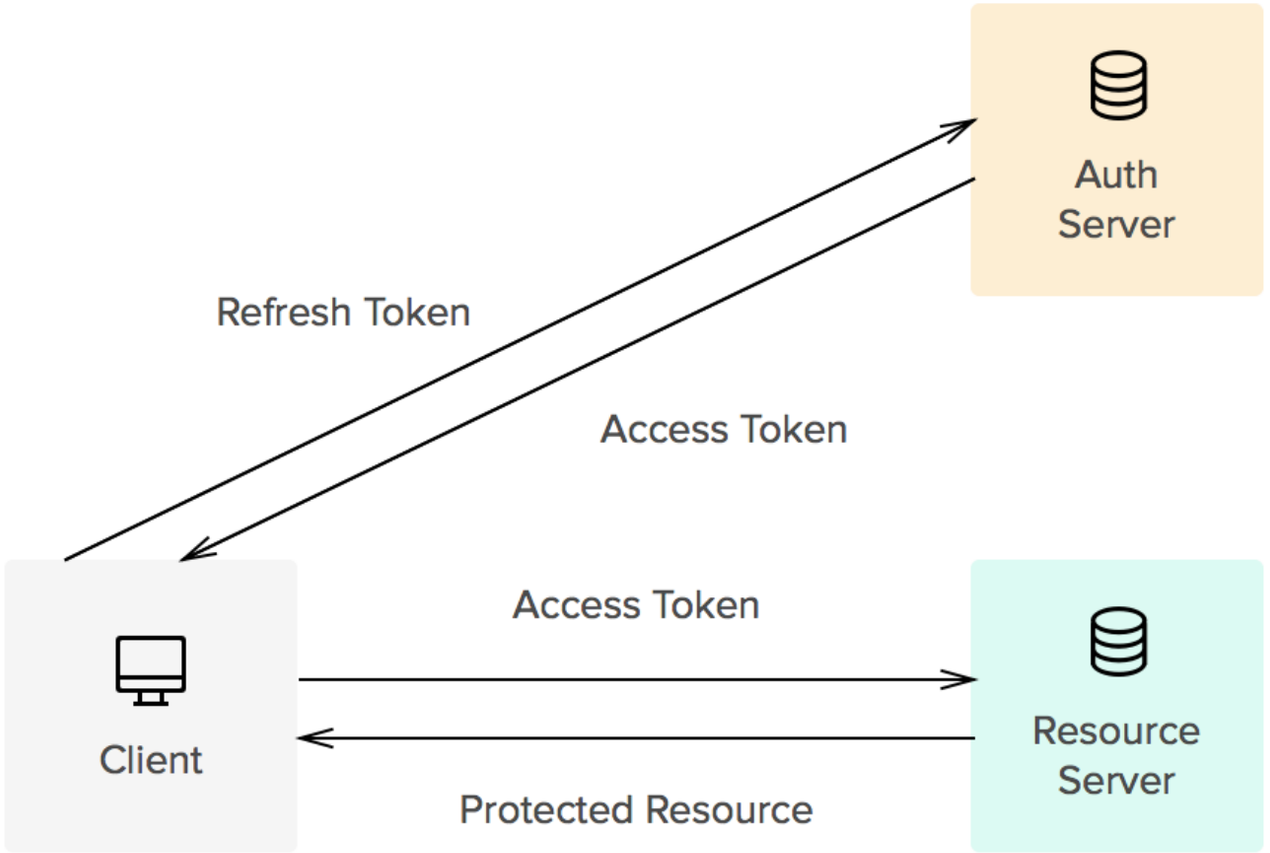




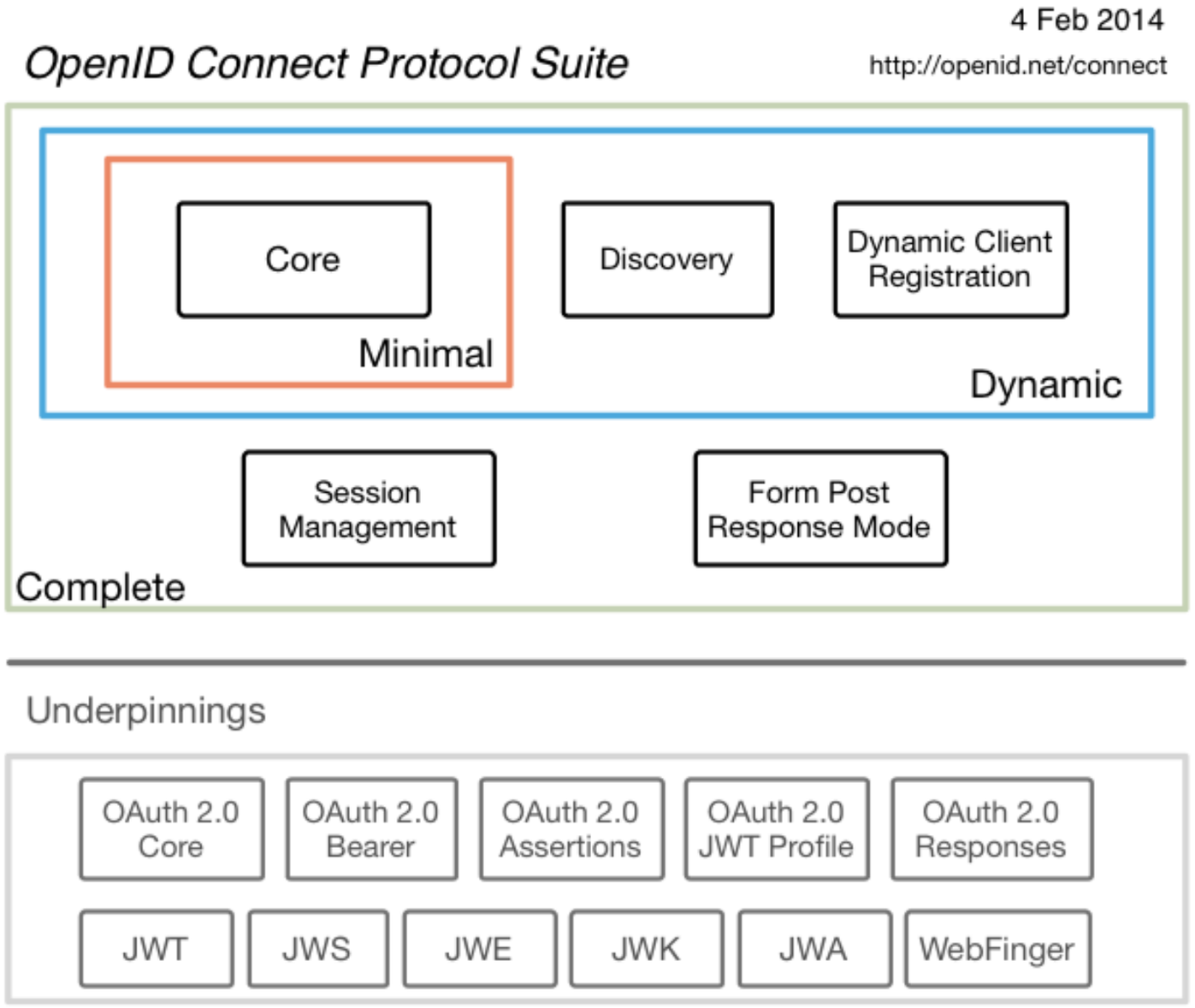
Authorization Management



Token Types


Auth
Server
Refresh Token
Access Token
Access Token
Client
Resource
Server
Protected Resource

OpenID Connect



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

Virtualization + Cloud & Security

Mgr. Michael Grafnetter