

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



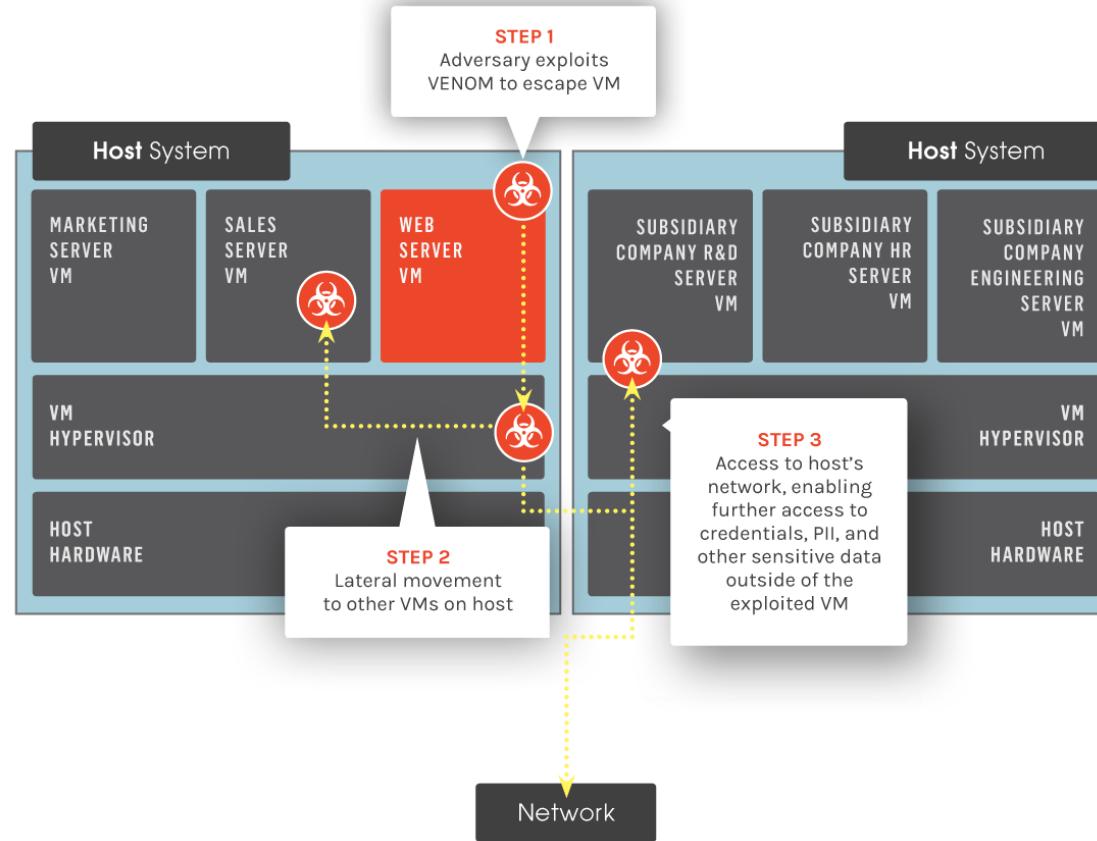
Blue Pill Attack



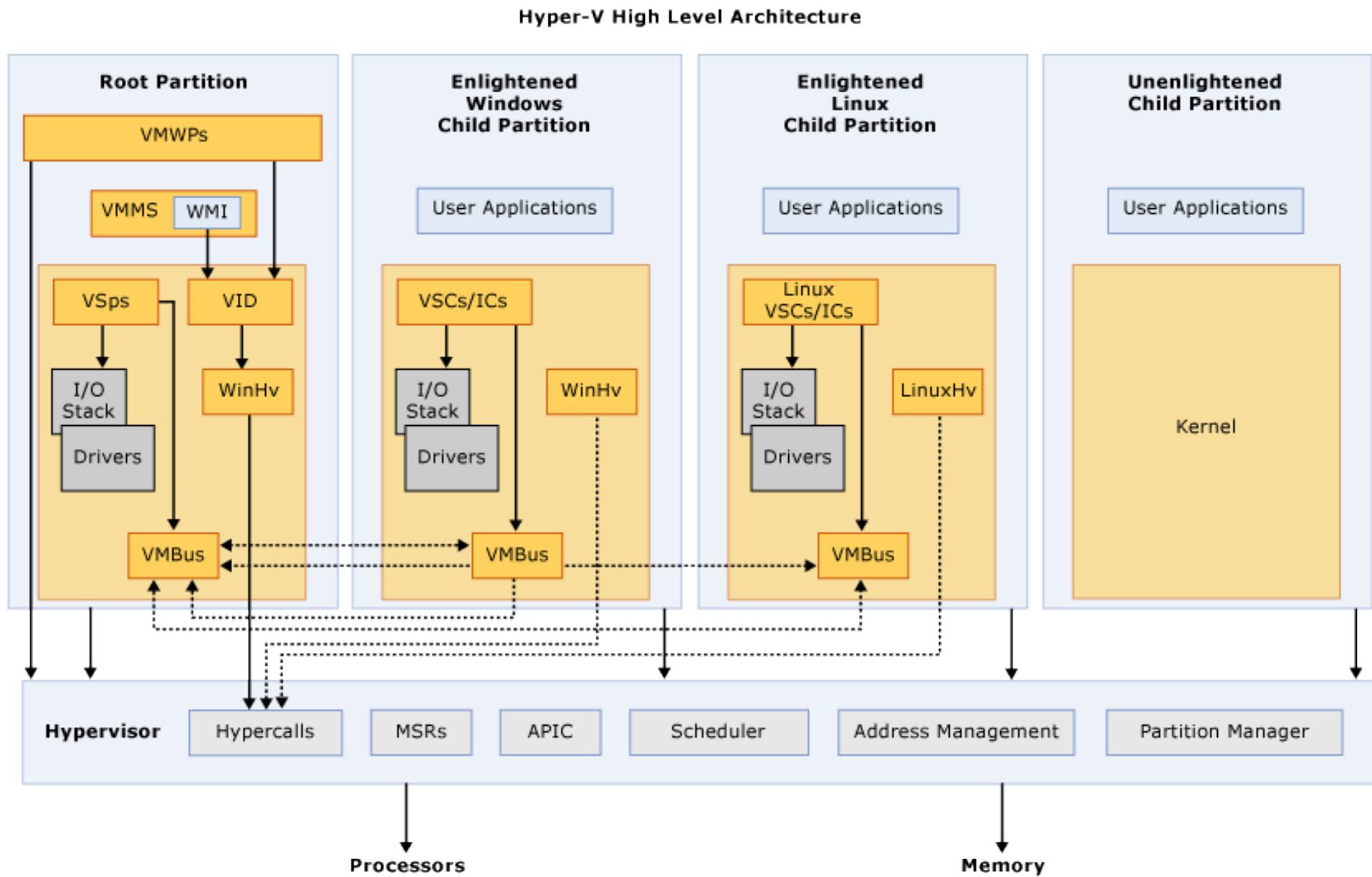
Blue Pill Attack

- 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

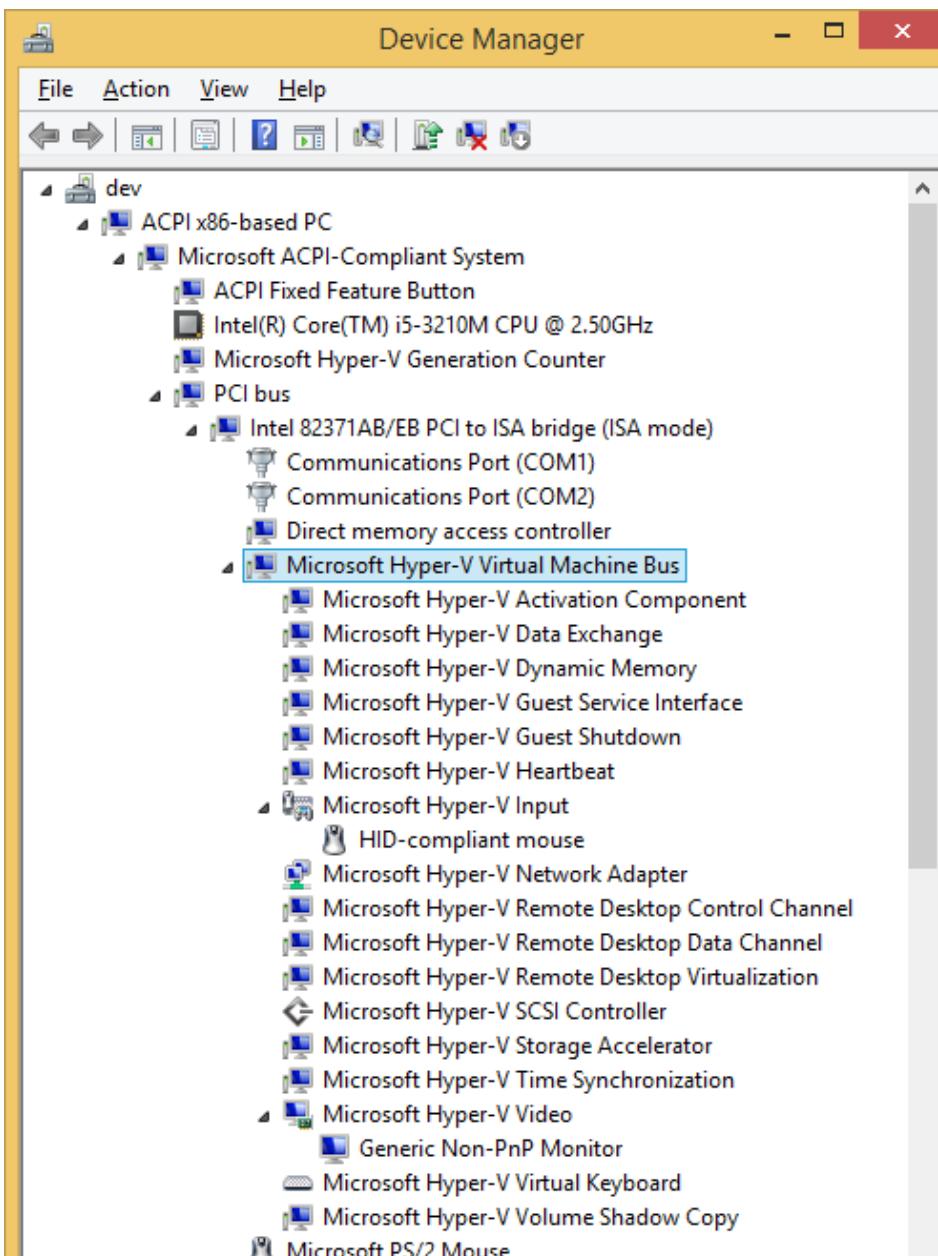
VM Escape Vulnerabilities



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

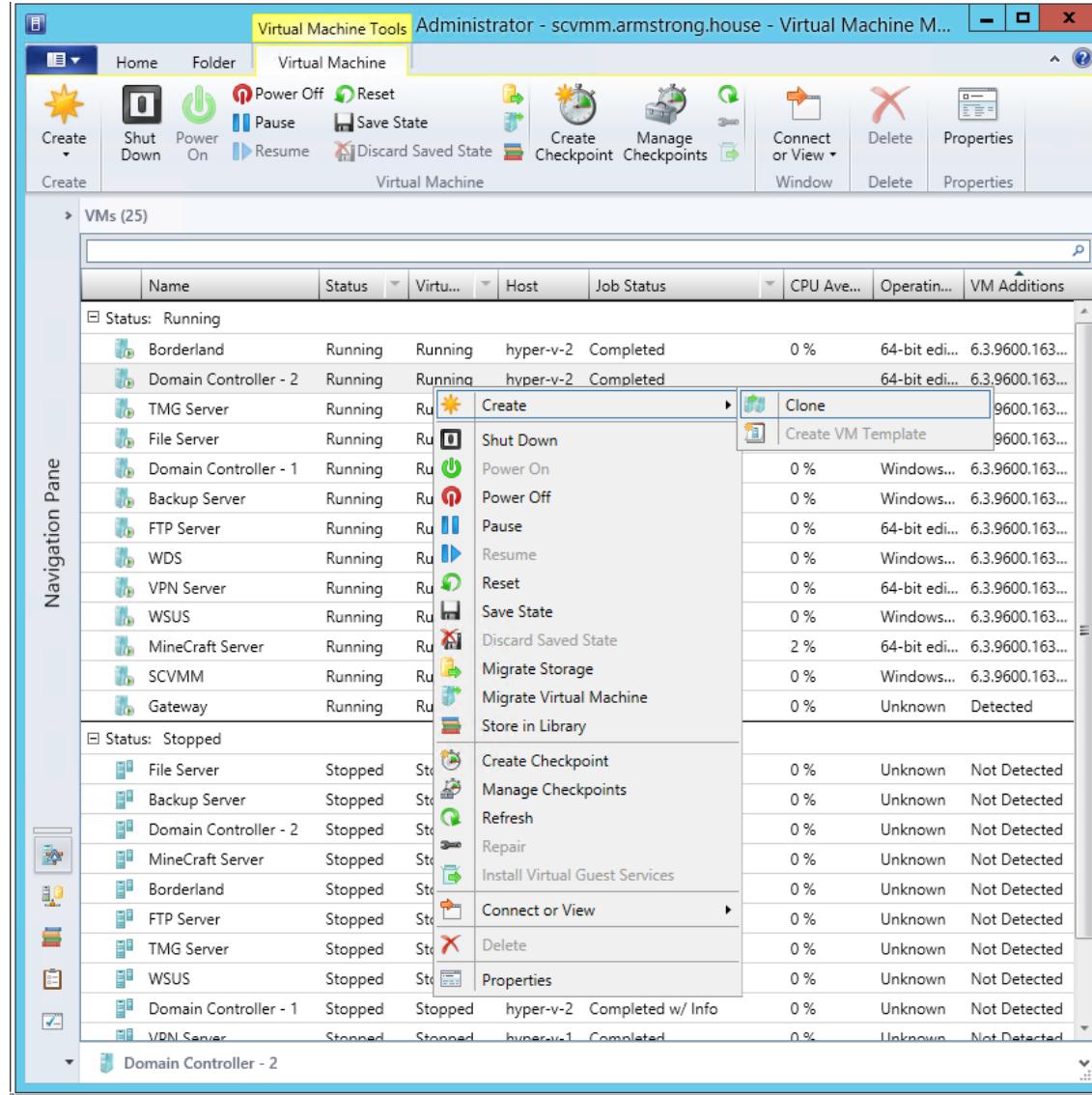
CPU Vulnerabilities



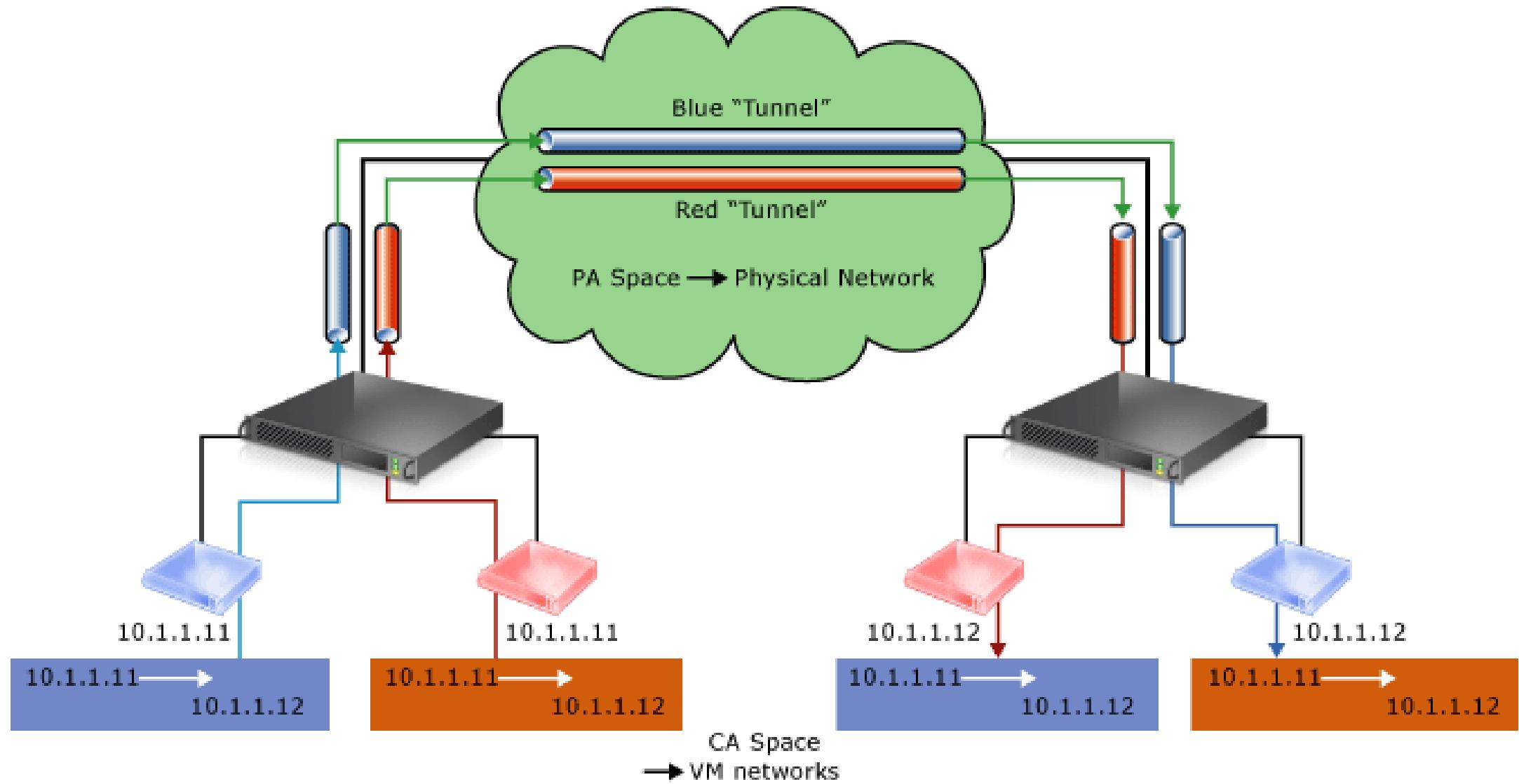
Post-Exploitation – VM Management

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

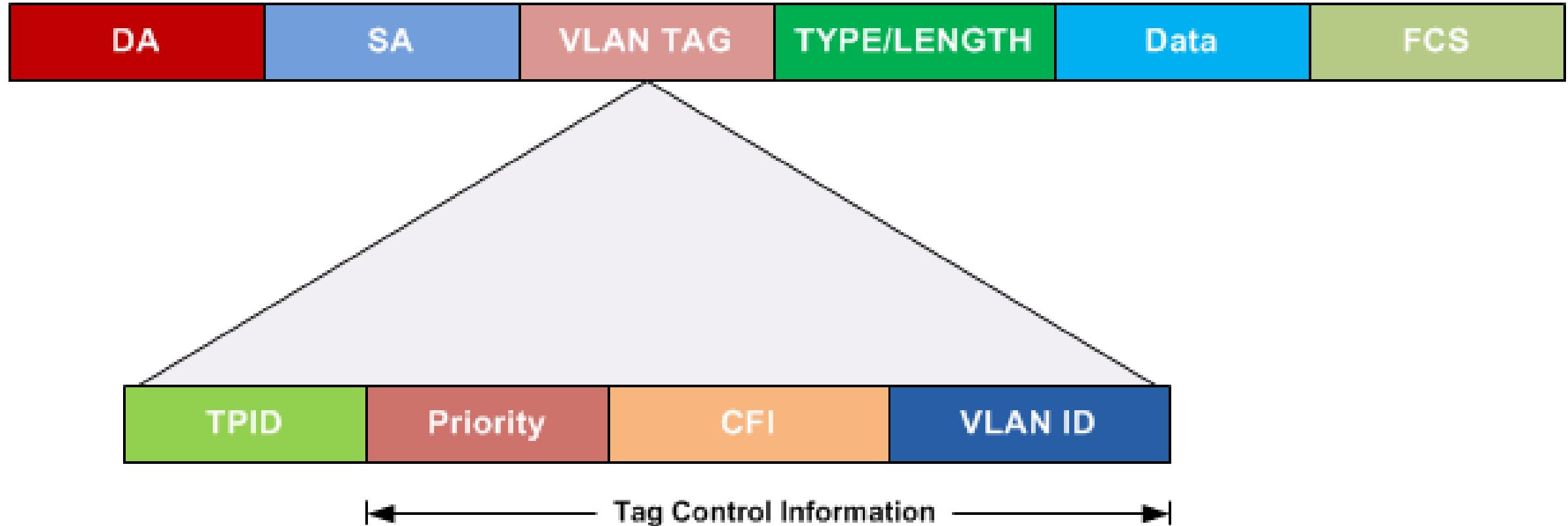
Post-Exploitation - Datacenter Management SW



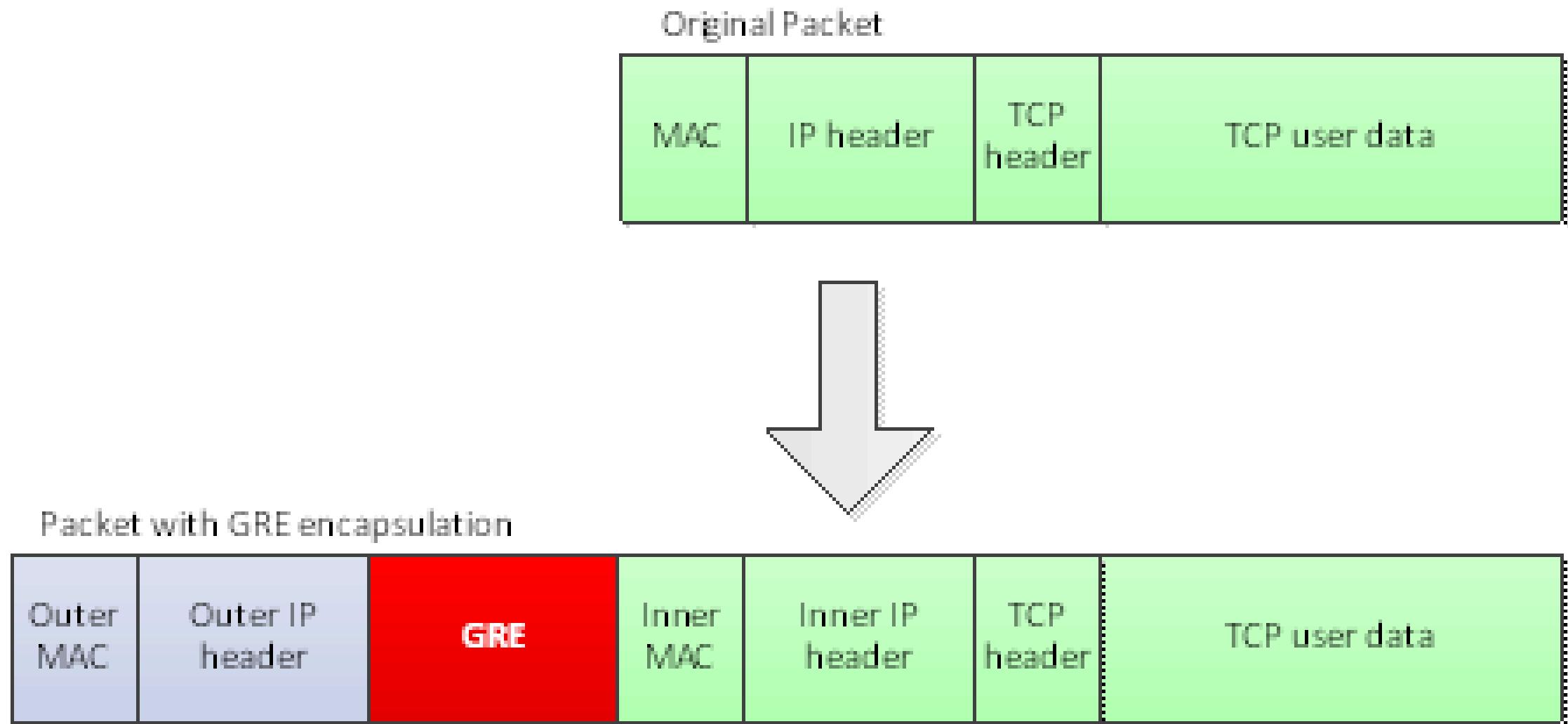
Traffic Isolation



Traffic Isolation – VLAN Tagging



Traffic Isolation - NVGRE



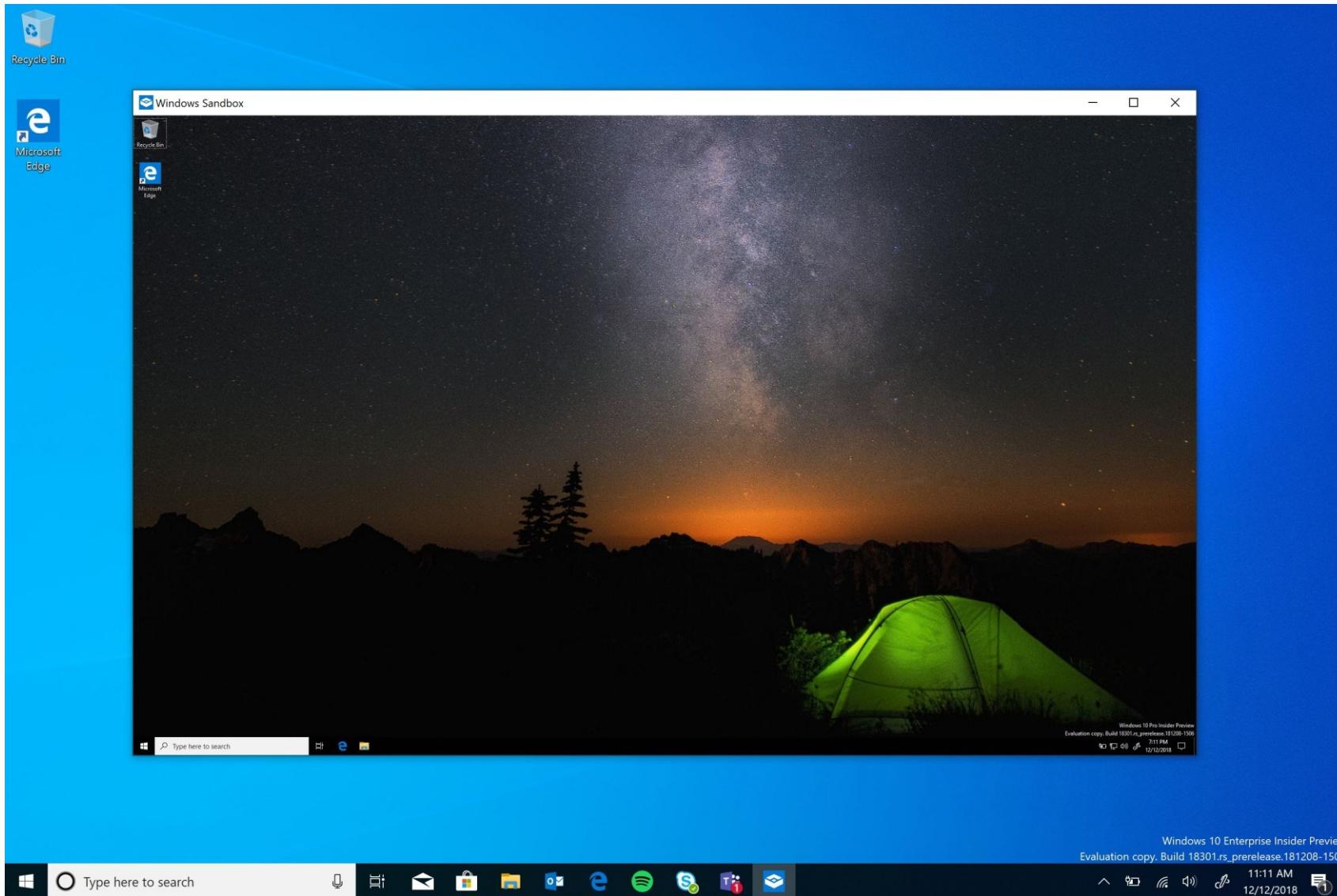
Other risks of virtualization

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

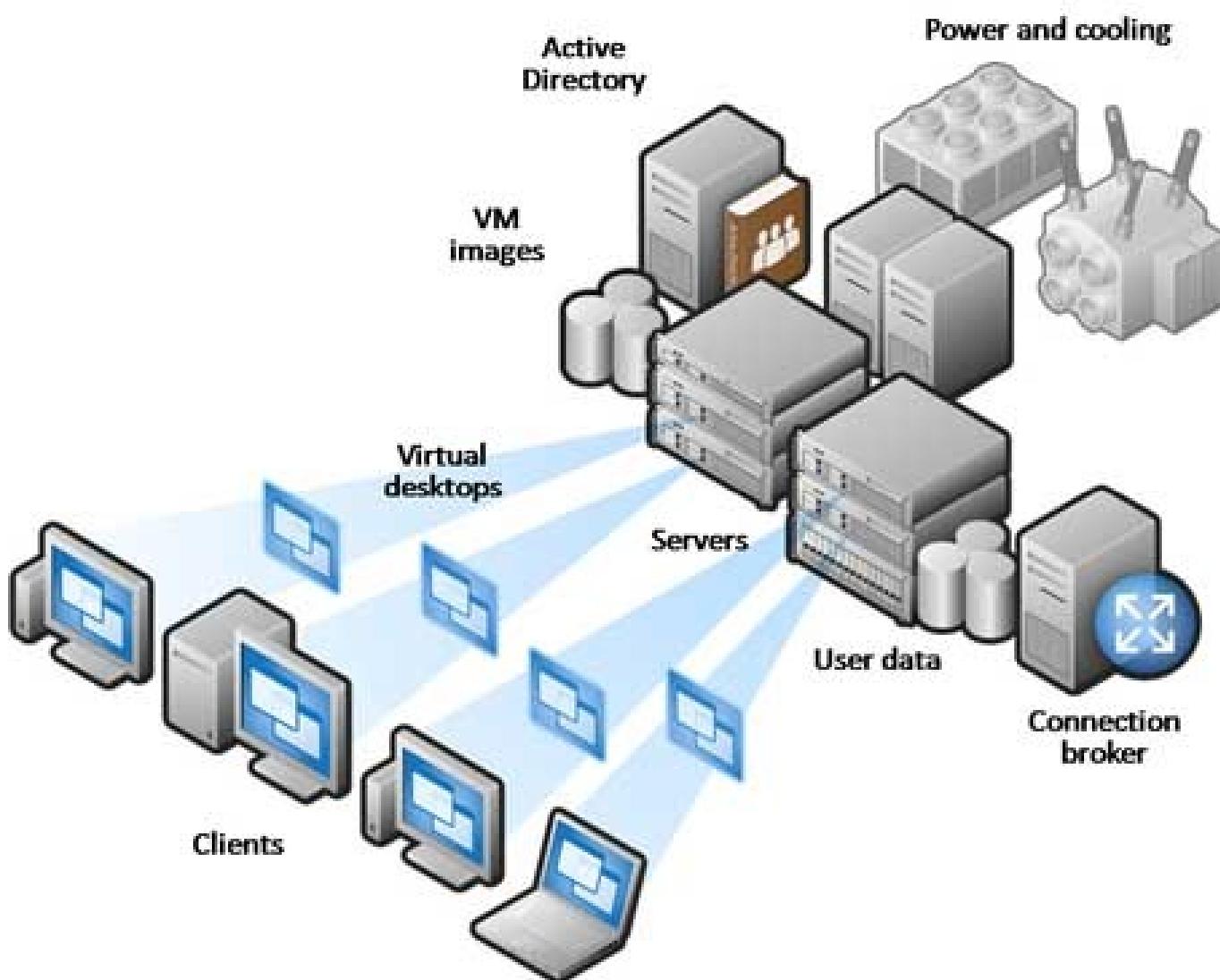
Virtualization-Based Security Solutions

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

Sandboxing



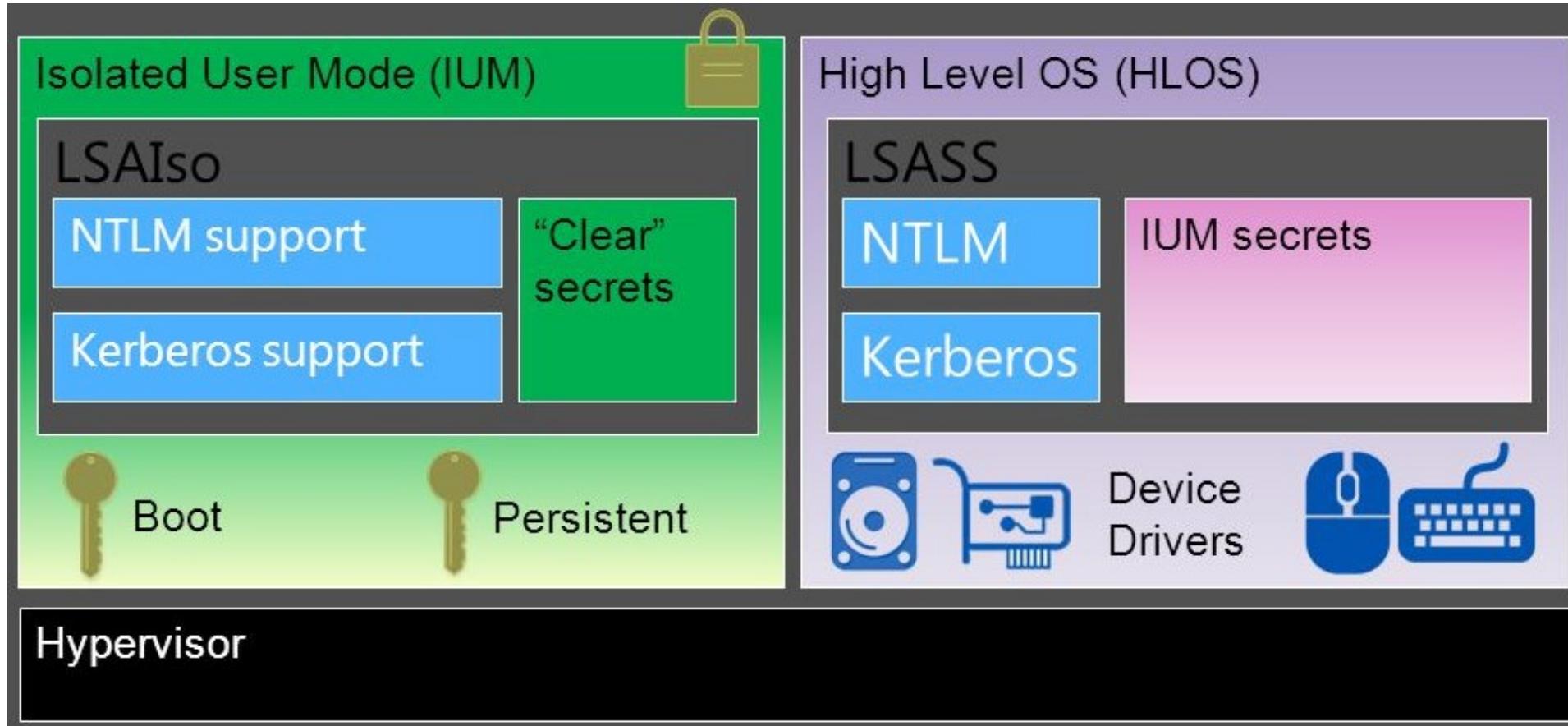
Virtual Desktop Infrastructure



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 :
    [REDACTED] Password
        * 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



Cloud Computing Security Risks



Who has access to our data?



Azure Datacenter Security

- 24 hour monitored
PHYSICAL SECURITY

- Centralized
MONITORING AND ALERTS

- Update
MANAGEMENT

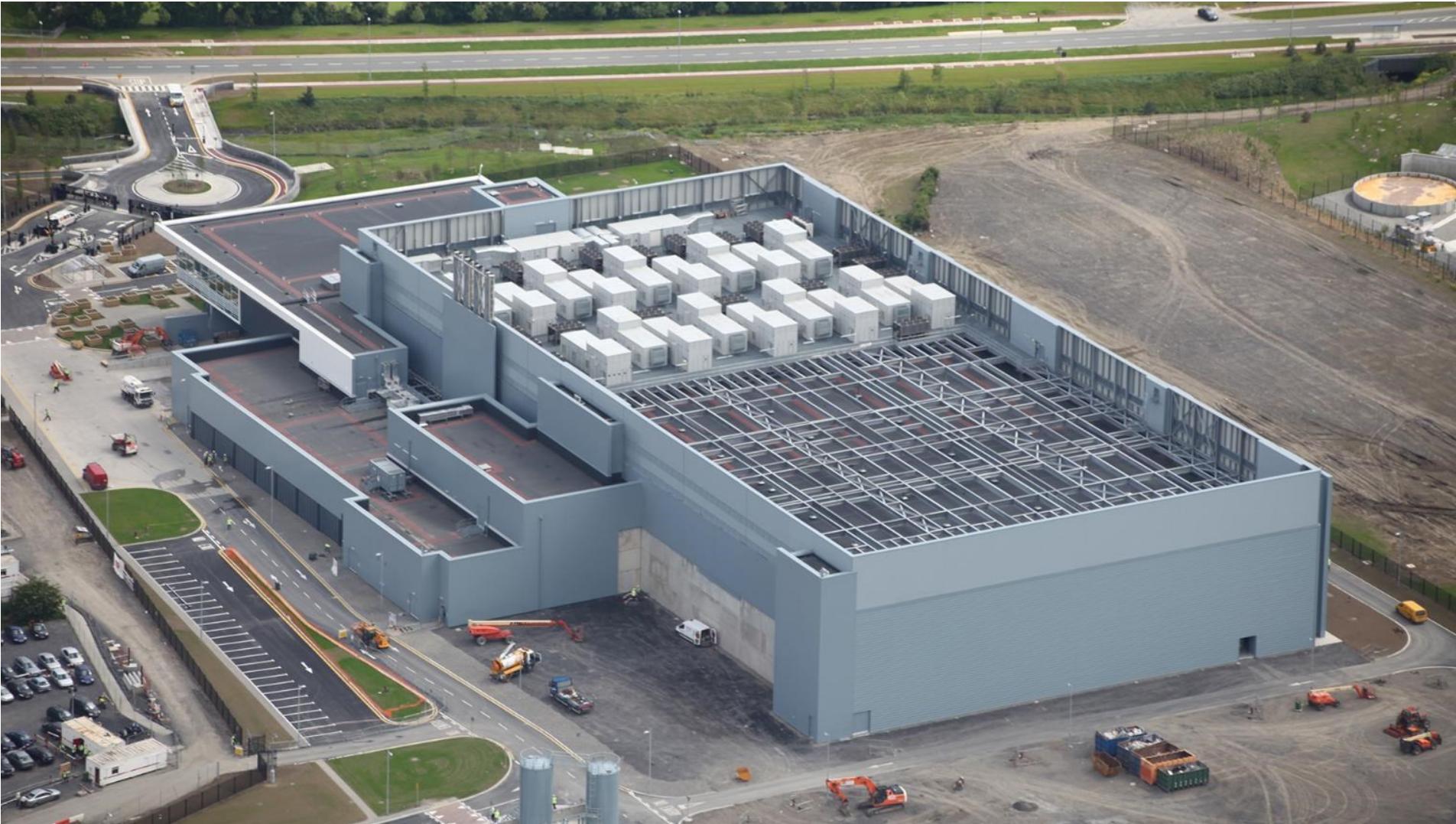


- Anti-Virus/Anti-Malware
PROTECTION

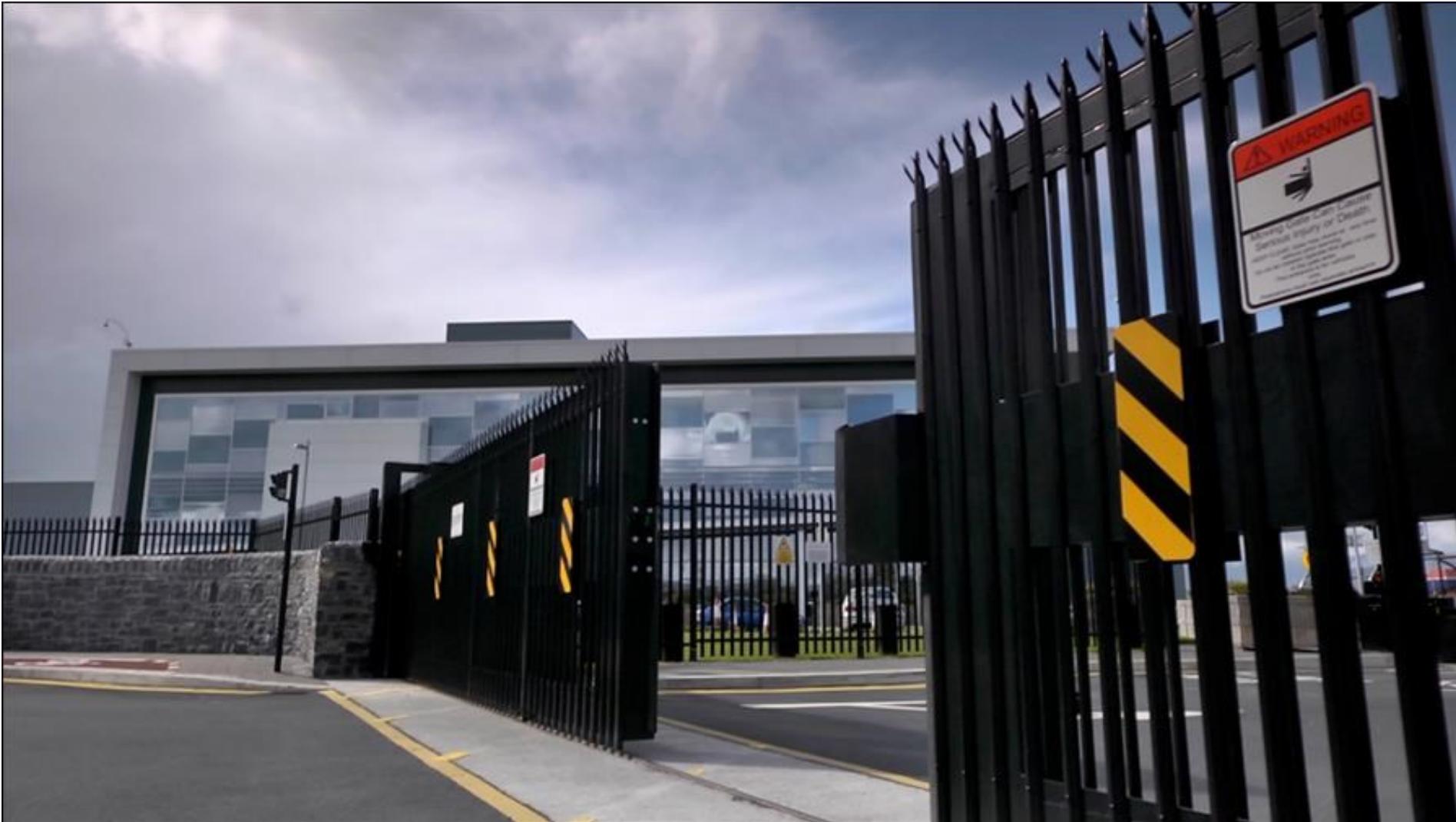
- Penetration **TESTING**

- DDoS **DEFENSE**

Physical Security



Physical Security



Physical Security



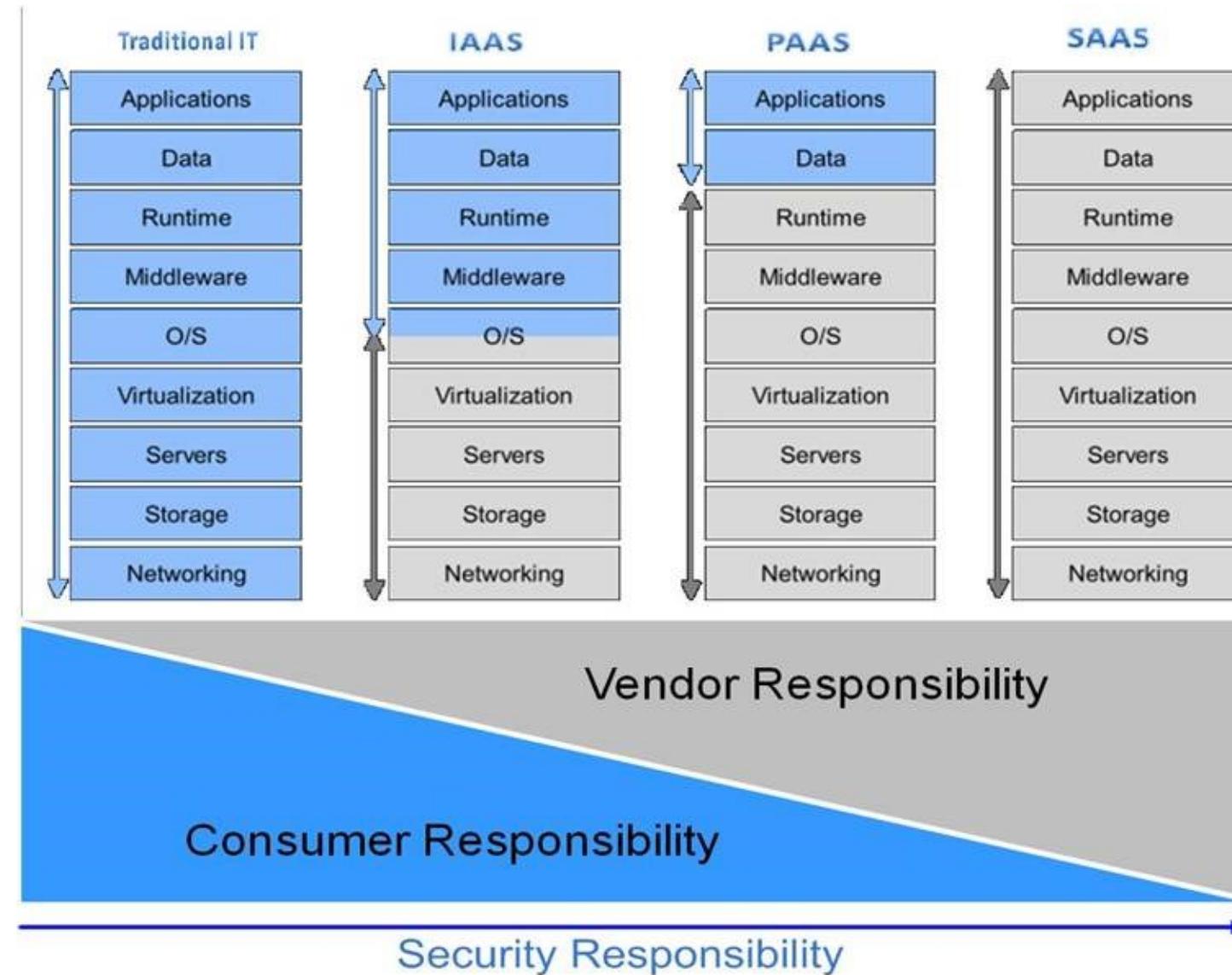
Physical Security



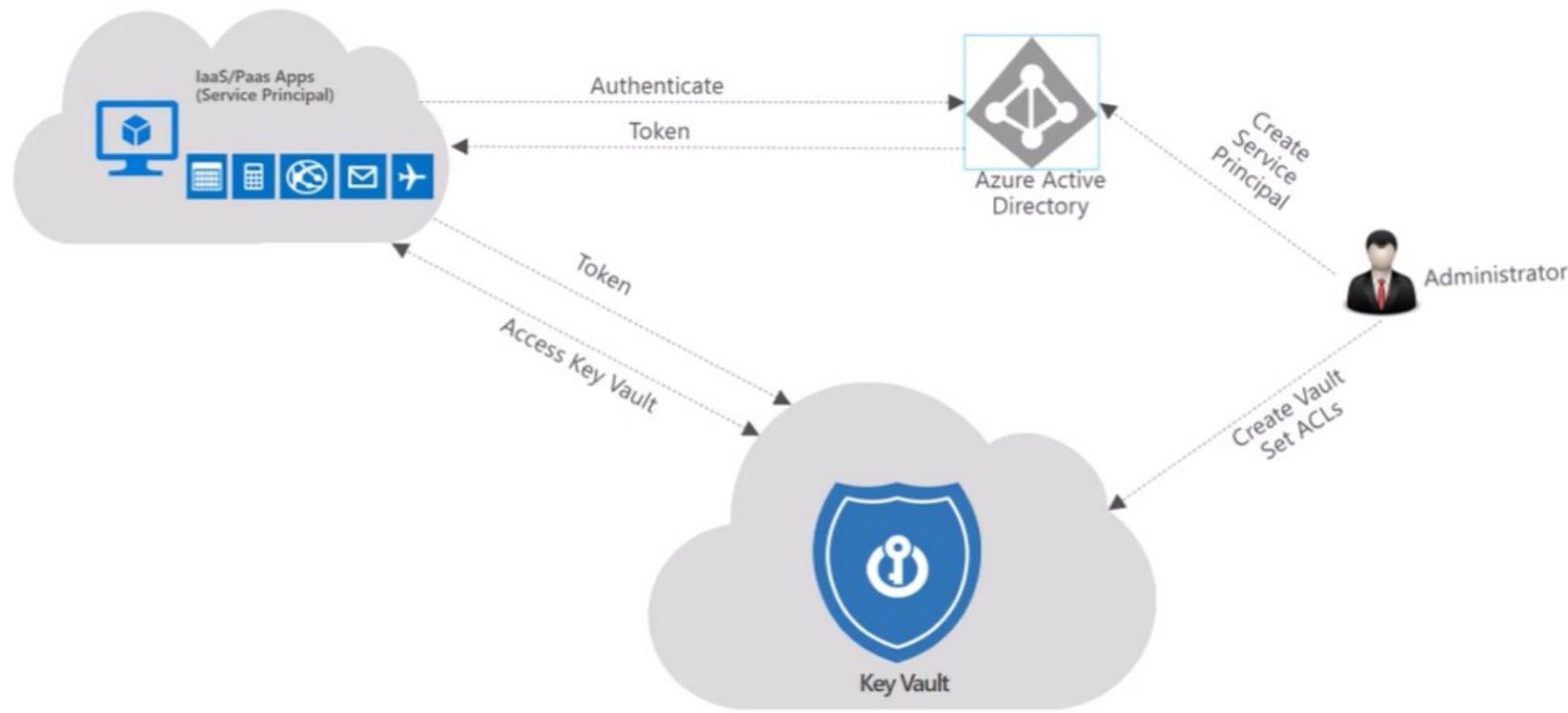
Hard Disk Crushers



Shared Responsibility (Misconfigurations)



Secrets in Source Code Repositories



Demo: Managing Secrets in CI

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

The screenshot shows a web-based dashboard titled "Cloud App Discovery". At the top, there's a navigation bar with links for "Dashboard", "Cloud App Disc.", and "Logout". Below the navigation, a header bar displays "last 30 days • business cloud apps •". A breadcrumb trail shows "dashboard > apps". On the right, there's a "sort by highest session count" dropdown. The main area features a circular donut chart labeled "categories" and 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. To the right of the chart is a 4x6 grid of application icons, each with a small label below it. The icons include Office 365 Exchange Online, Office 365 SharePoint Online, Dropbox, msdn, AddThis, New Relic, Symantec Trust Center, Orga, DigCert, Yammer, GlobalLogic, Enterprise Security Center, Sogos, bazaaronline, GitHub, Amazon Web Services (AWS), Cloudflare, Imaginatik, Salesforce, Drupa, intuit, SurveyMonkey, sf, CodePen, and others partially visible like R, G, box, n, and Q.

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

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

326	5,575,703,782	83,835	91,310,138
owned websites	owned accounts	pastes	paste accounts

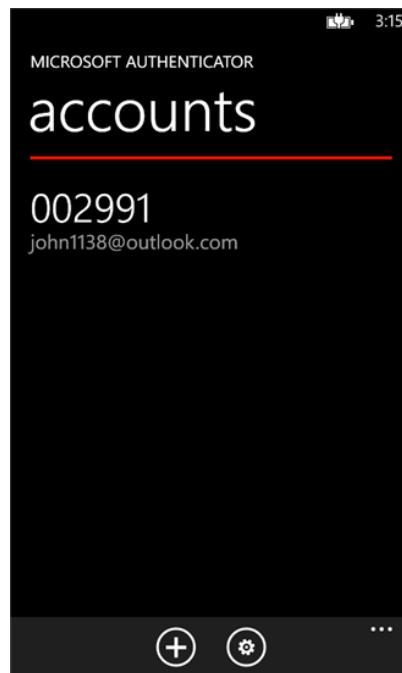
Largest breaches

	711,477,622	Onliner Spambot accounts
	593,427,119	Exploit.In accounts
	457,962,538	Anti Public Combo List accounts
	393,430,309	River City Media Spam List accounts
	359,420,698	MySpace accounts
	234,842,089	NetEase accounts
	164,611,595	LinkedIn accounts
	152,445,165	Adobe accounts
	131,577,763	Exactis accounts
	125,929,660	Apollo accounts

Recently added breaches

	9,363,740	Adapt accounts
	411,755	HTH Studios accounts
	5,788,169	Elasticsearch Instance of Sales Leads on AWS accounts
	1,957,600	KnownCircle accounts
	24,990	Rbx.Rocks accounts
	14,609	Società Italiana degli Autori ed Editori accounts
	858	WPSandbox accounts
	22,477	JoomlArt accounts
	326,714	Mac Forums accounts
	846,742	Baby Names accounts

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

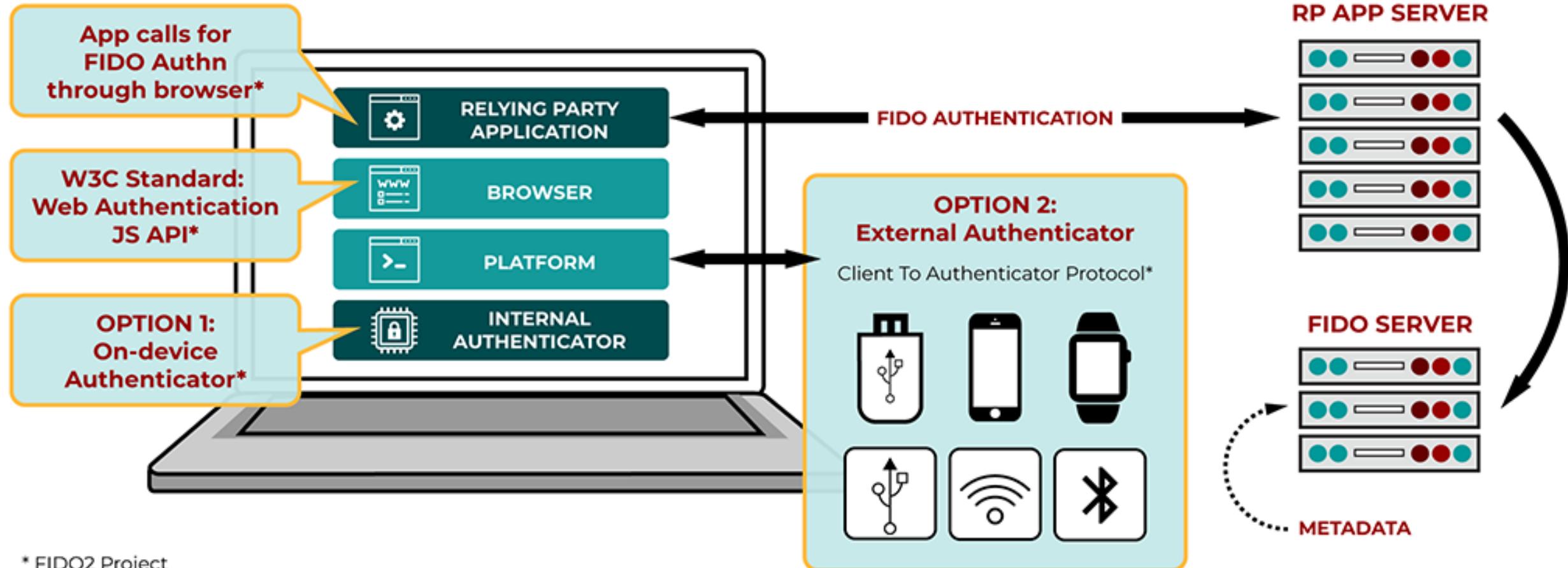
$HMAC(K, C) :=$
 $\text{SHA1}(K \oplus 0x5C5C... \parallel \text{SHA1}(K \oplus 0x3636... \parallel C))$

$HOTP(K, C) :=$
 $\text{Truncate}(HMAC(K,C)) \And 0x7FFFFFFF$

K – Secret Key

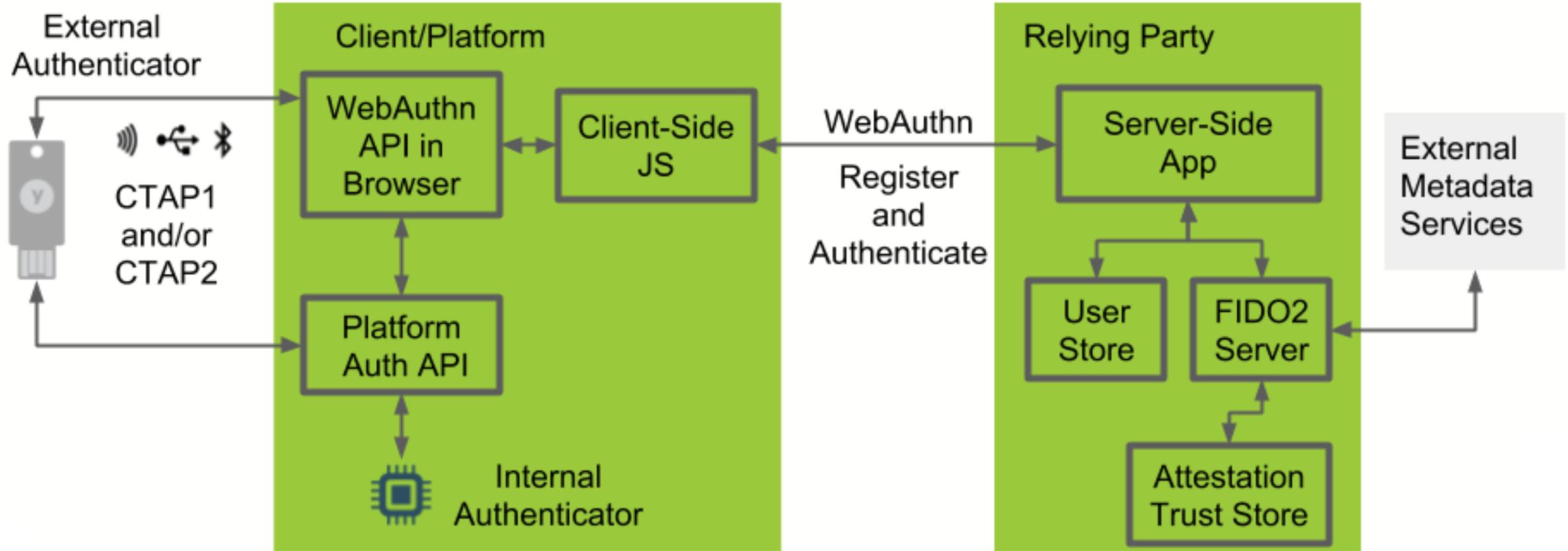
C – Counter/Clock

Passkeys / FIDO2 / W3C Web Authentication



* FIDO2 Project

FIDO Protocols



Demo: Passkeys



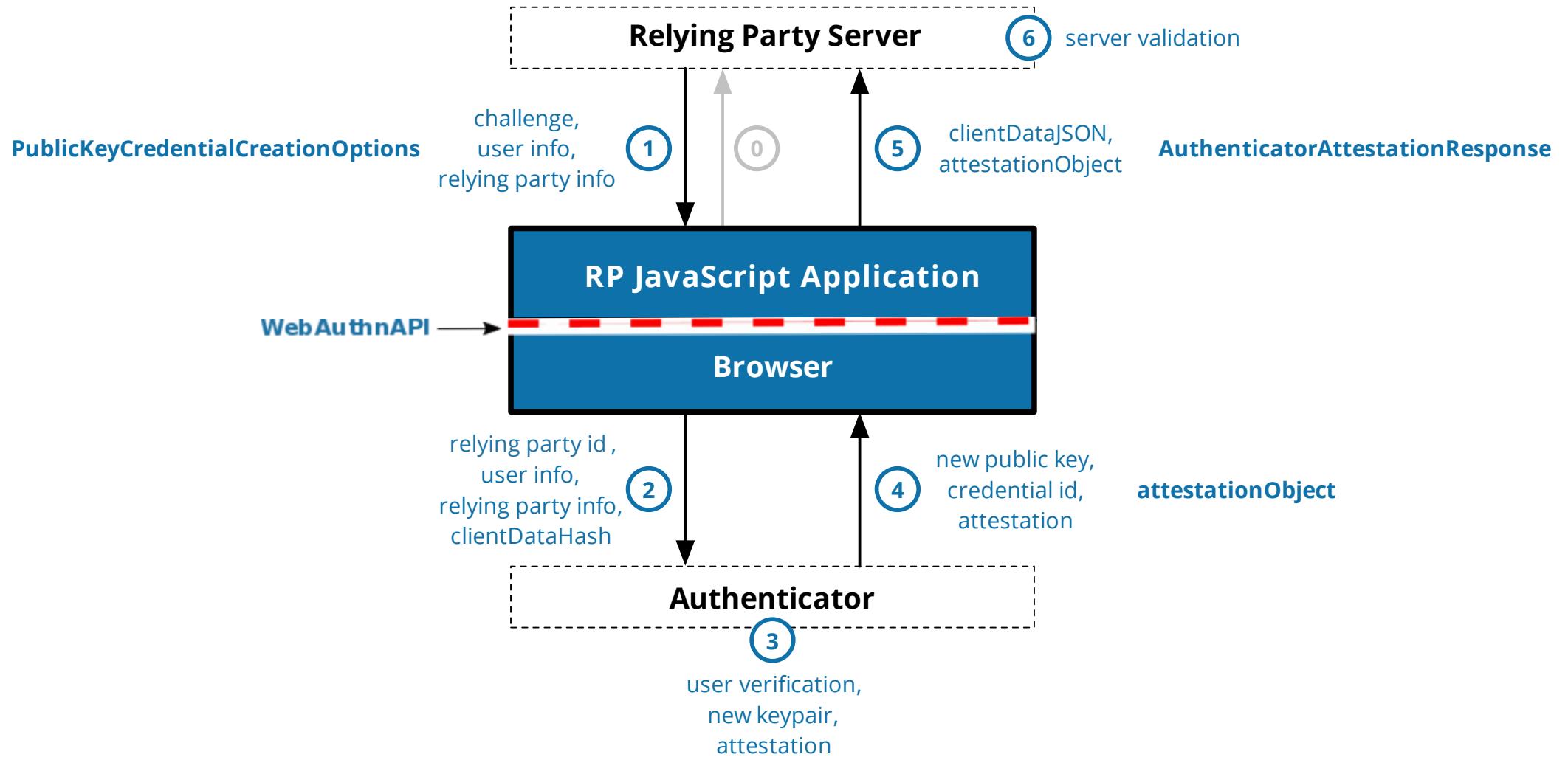
WebAuthn API

```
// 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
});
```

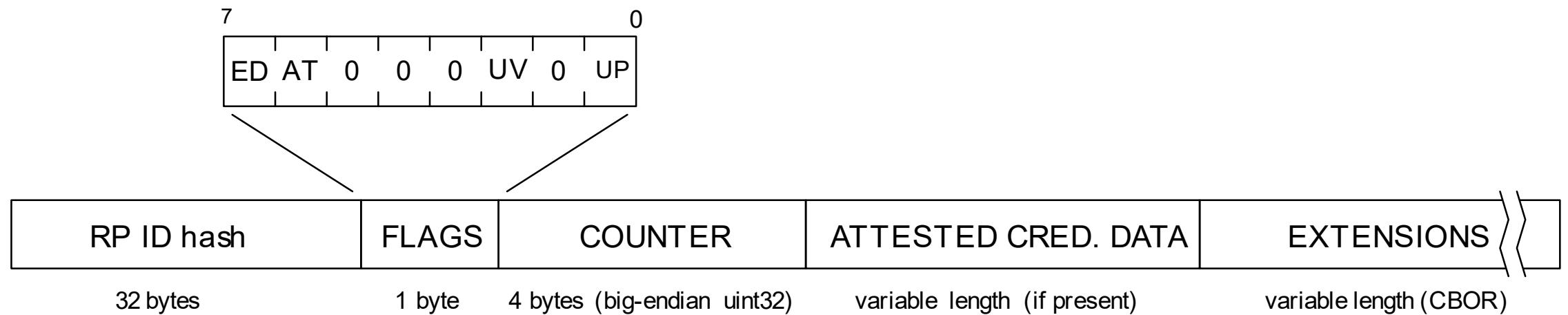
Registration Flow



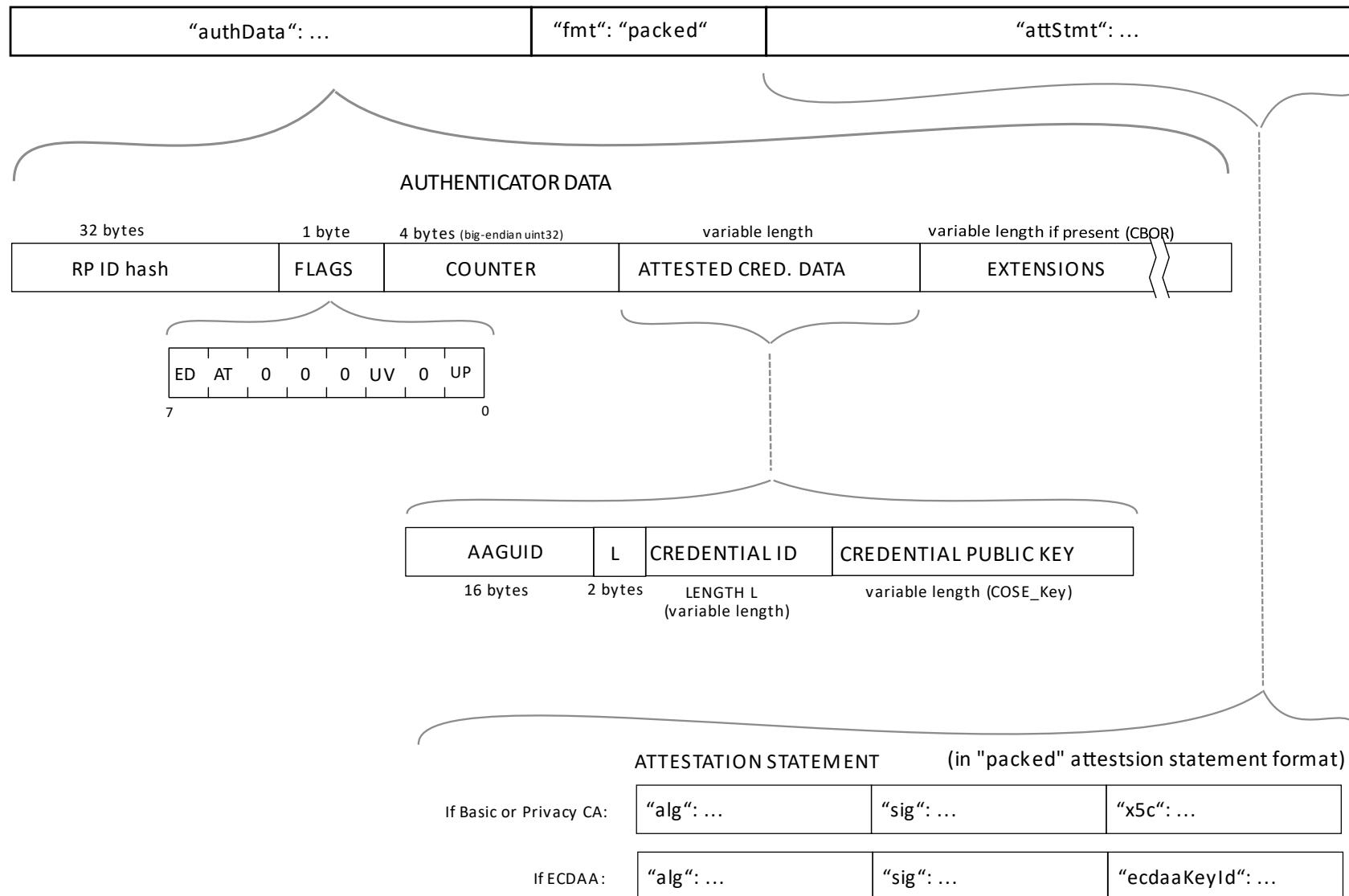
Public Key Credential Creation Options

```
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

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



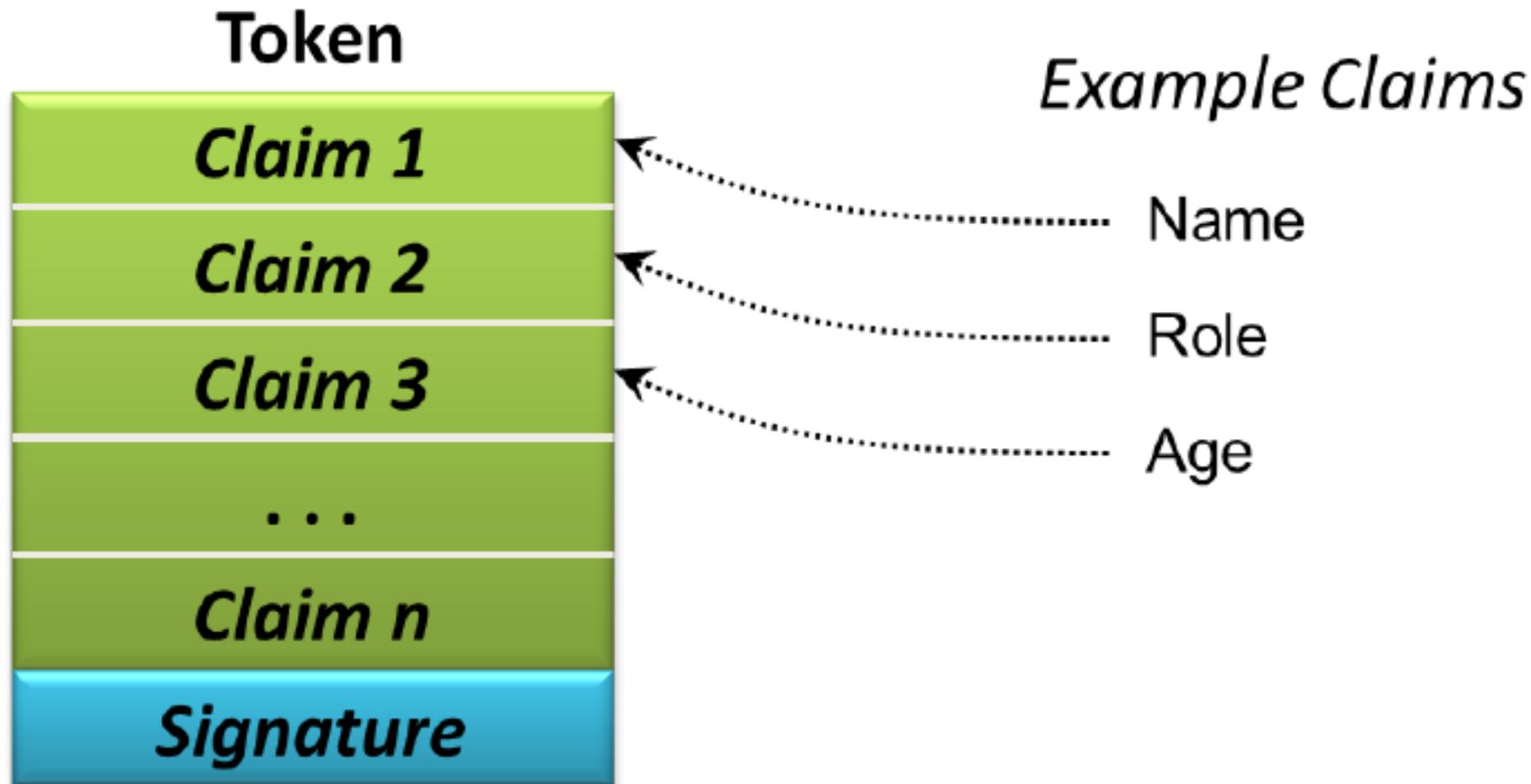
Most Common Technologies

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

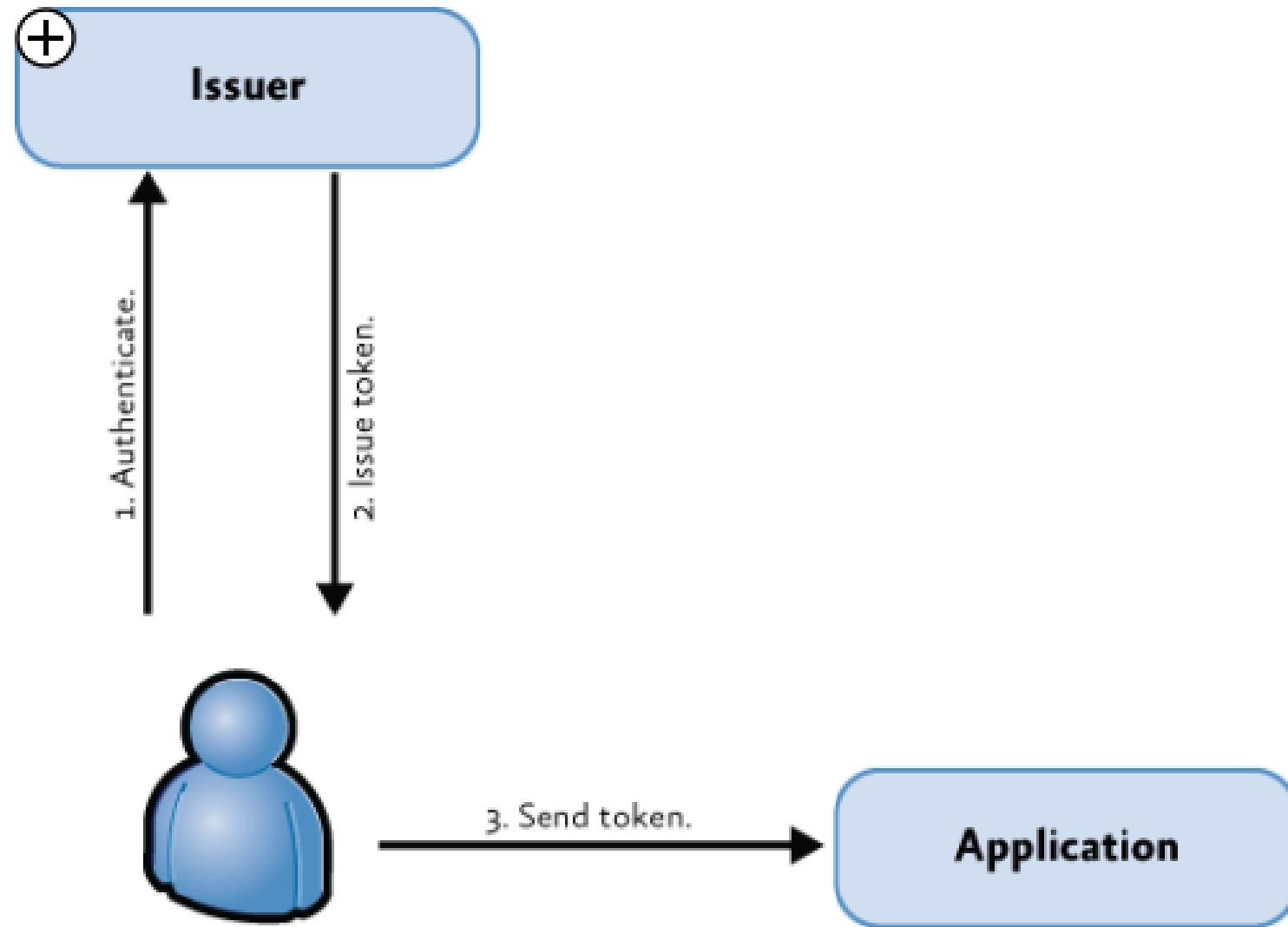
Claims-based Identity

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

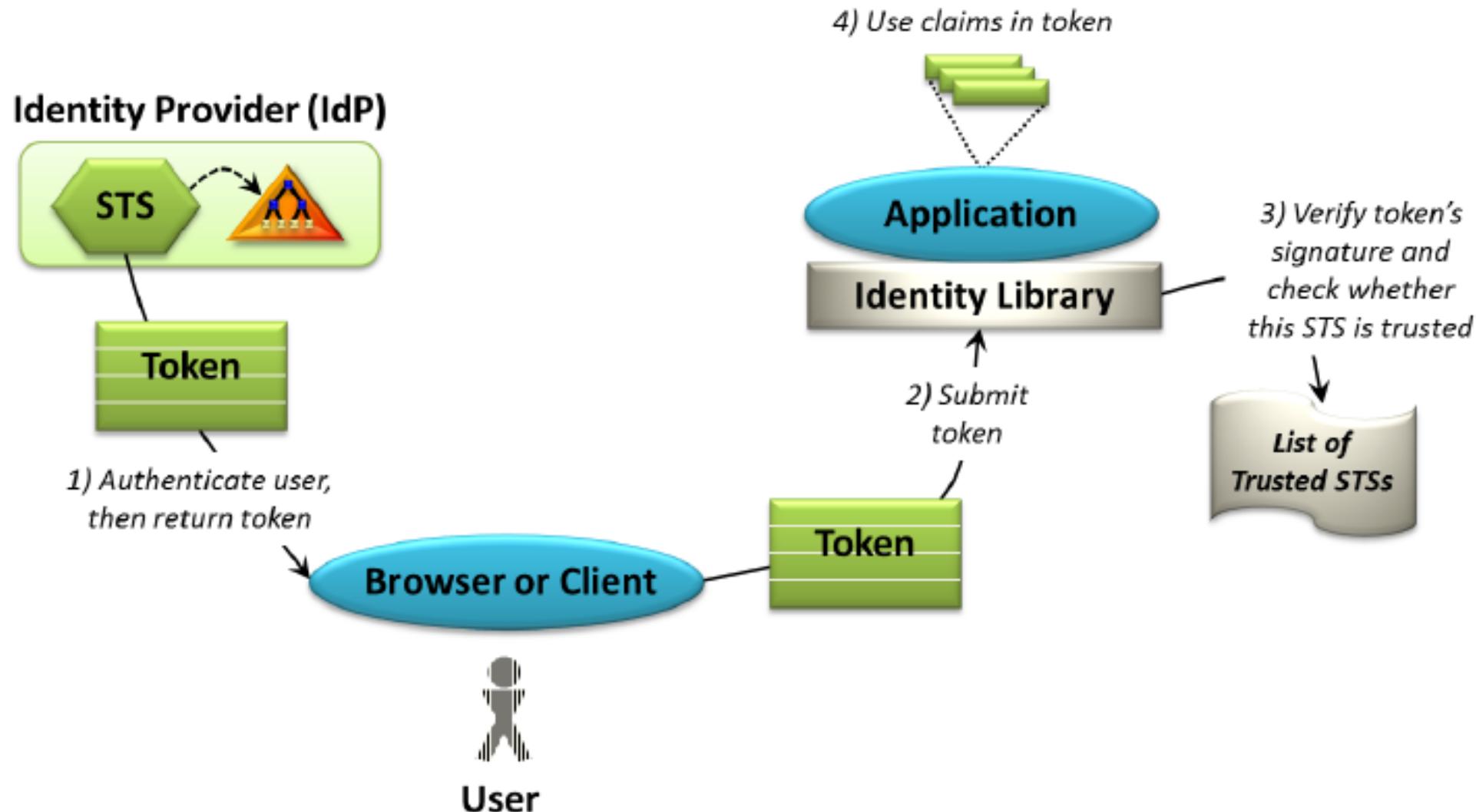
Tokens



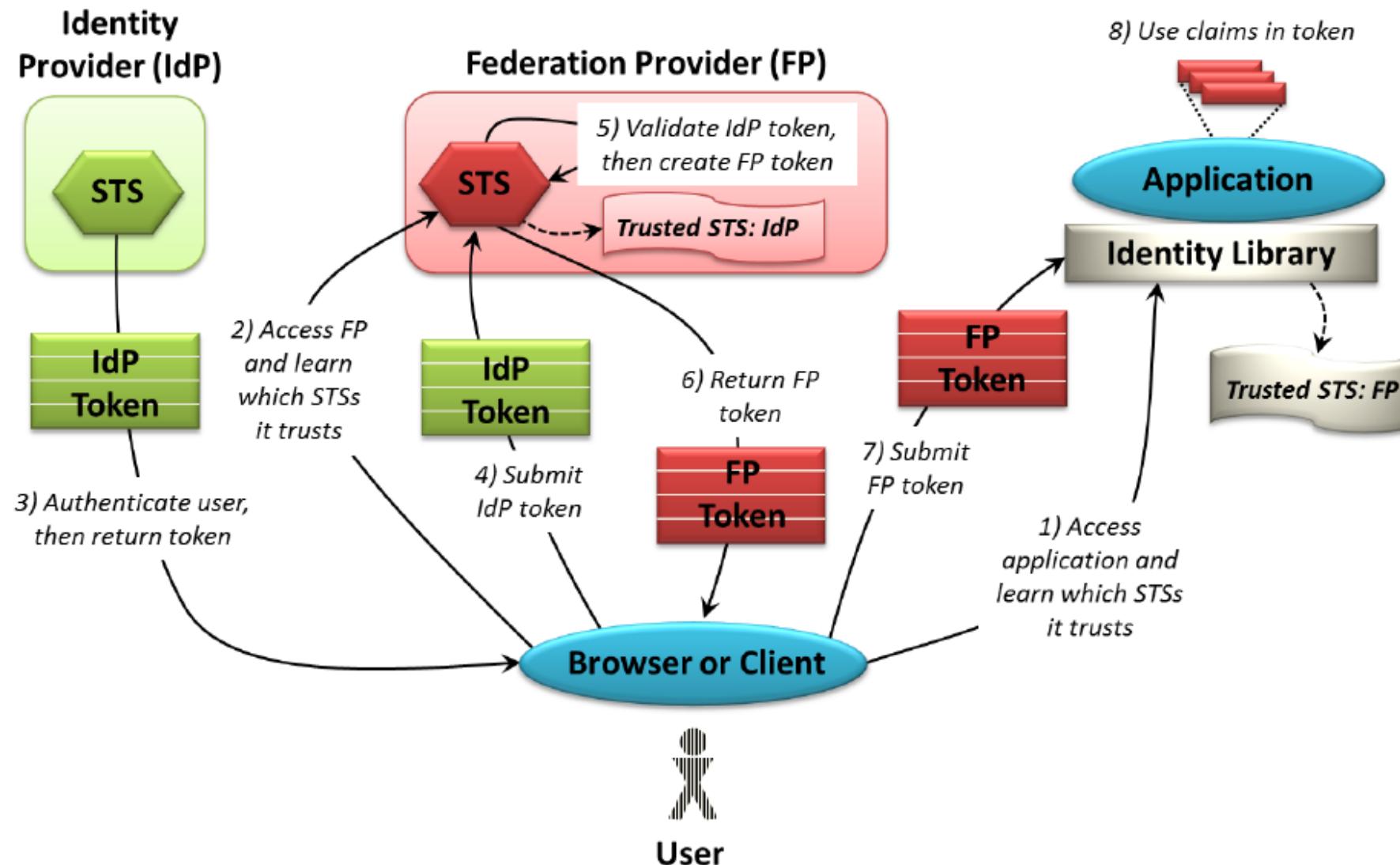
Basic Communication Pattern



Identity Providers and Identity Libraries



Identity Federation



Shibboleth

The screenshot shows the login interface for the Central Authentication Service (CAS) at the University of Prague (UK). At the top, there is a logo of the University of Prague and the text "CAS - Centrální autentizační služba UK". Below this, a large orange banner displays the message "Stránka vyžaduje přihlášení pomocí Centrální autentizační služby UK!". The main form area has a light orange background. It contains fields for "Přihlašovací jméno:" and "Heslo:", both with placeholder text. There is also a checkbox labeled "Upozornit před přihlášením k jiné aplikaci." At the bottom right of the form is a red "Přihlásit" button. To the right of the form, there is explanatory text about login methods and a warning about security. At the very bottom, there are language selection 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: 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.

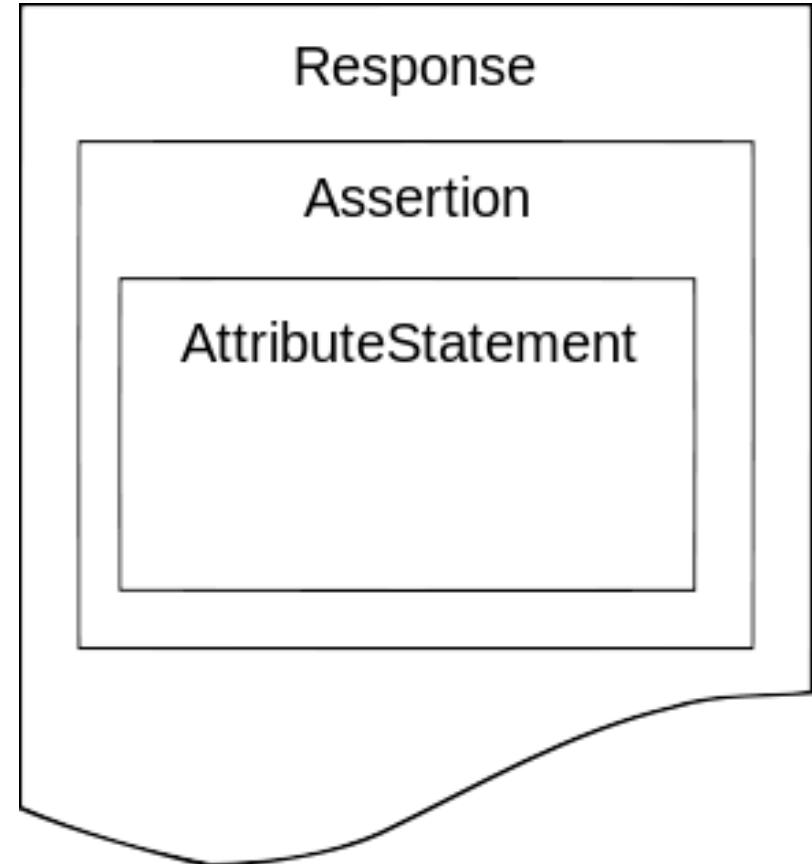
- Authentication statements
- Attribute statements
- Authorization decision statements

Demo: SAML Tokens



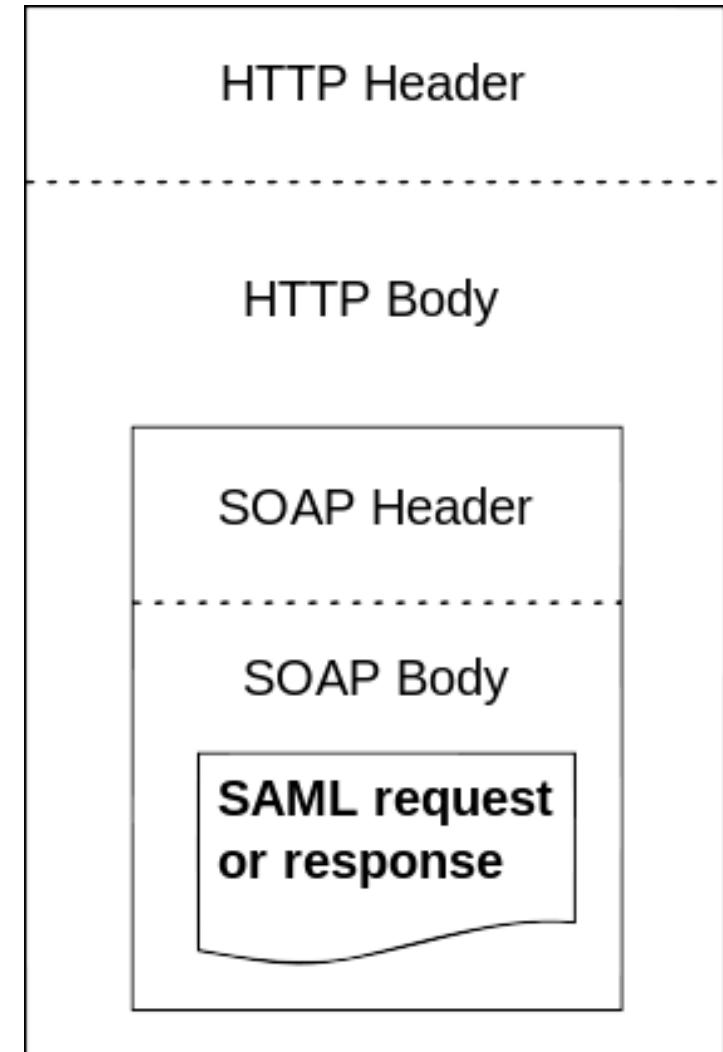
SAML Protocols

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



SAML Bindings

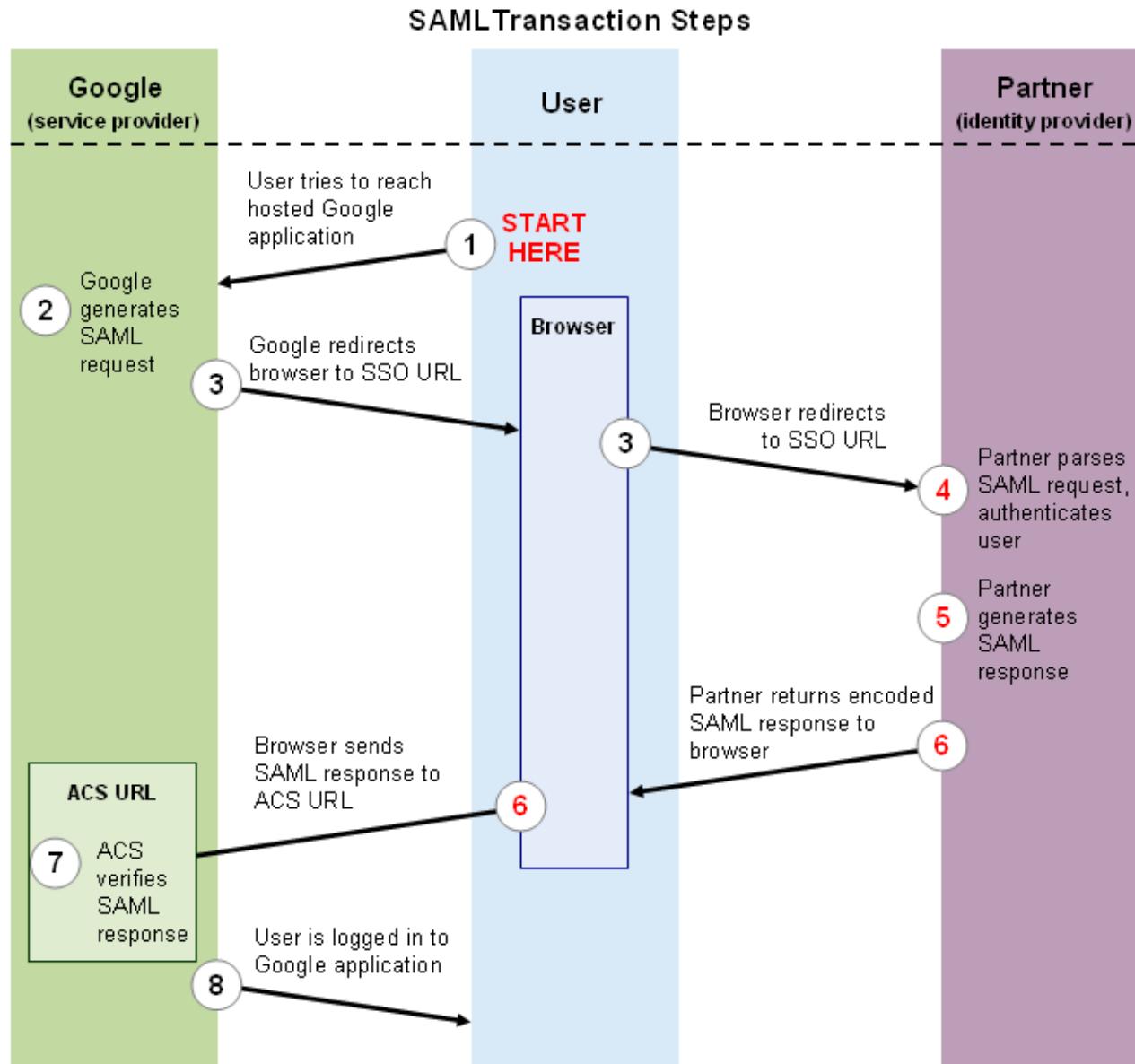
- SAML SOAP Binding
- Reverse SOAP (PAOS) Binding
- HTTP Redirect (GET) Binding
- HTTP POST Binding
- HTTP Artifact Binding
- SAML URI Binding



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

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

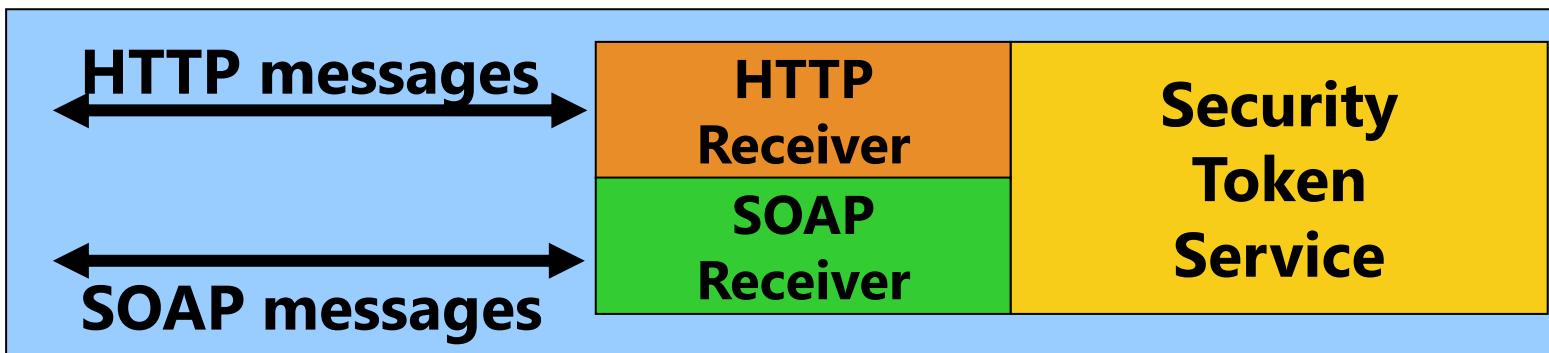
- OASIS Standard from 2007
- Deals with the issuing, validating, and renewal of security tokens
- Defines the concept of the Security Token Service
- Defines formats of messages used to request security tokens (RST) and respond to those requests (RSTR)
- Defines mechanisms for key exchange

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.

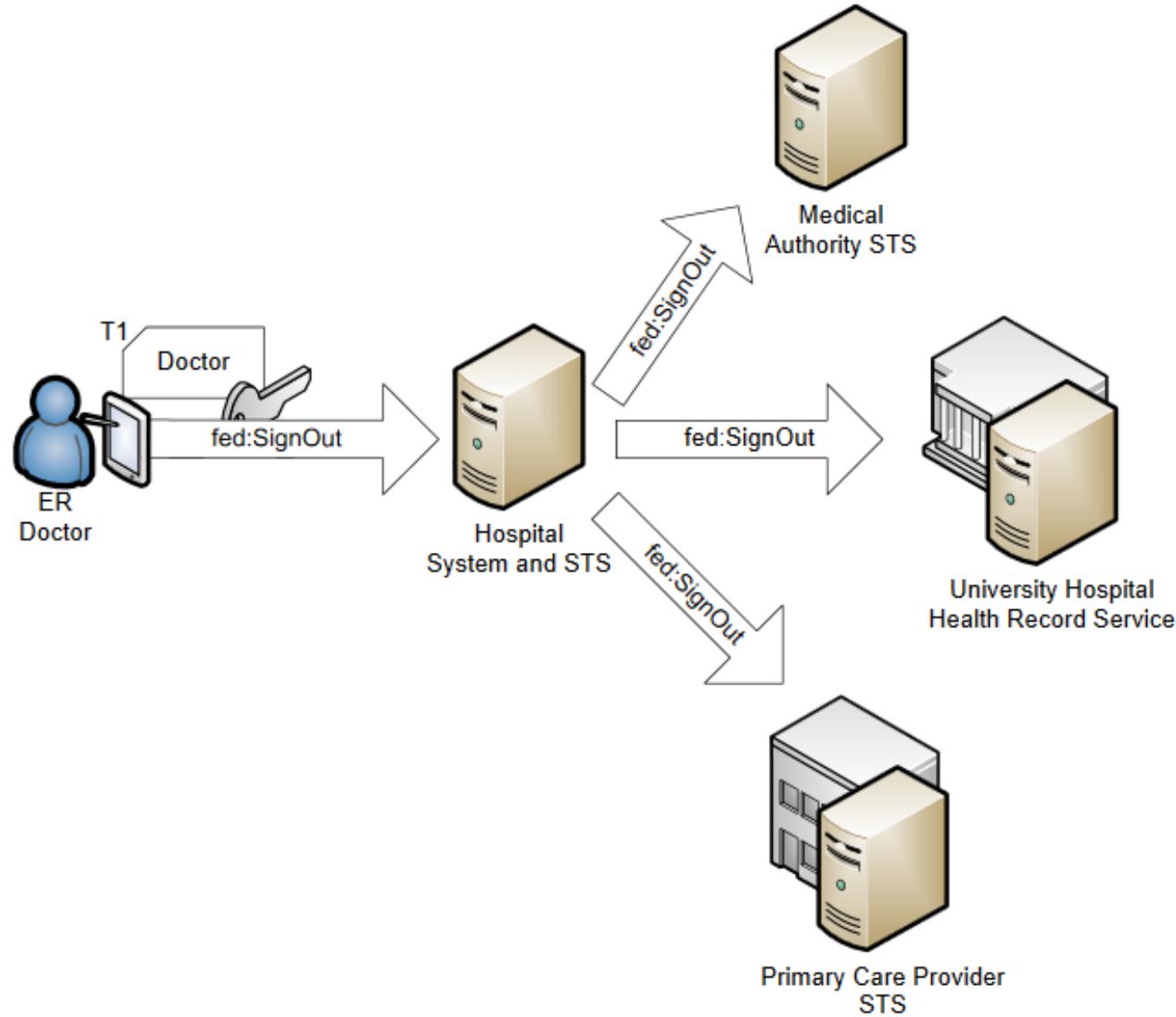
Federated SSO: Claims

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/service/s/trust	http://corp.sts.microsoft.com
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn	dgreg@microsoft.com	http://sts.cloudready.ms/adfs/service/s/trust	http://corp.sts.microsoft.com
http://schemas.xmlsoap.org/claims/Group	Redmond\Corp Users	http://sts.cloudready.ms/adfs/service/s/trust	http://corp.sts.microsoft.com
http://schemas.xmlsoap.org/claims/Group	NORTHAMERICA\CloudReadyUsers	http://sts.cloudready.ms/adfs/service/s/trust	http://corp.sts.microsoft.com
http://schemas.microsoft.com/ws/2008/06/identity/claims/authenticationmethod/password	http://schemas.microsoft.com/ws/2008/06/identity/authenticationmethod/password	http://sts.cloudready.ms/adfs/service/s/trust	http://sts.cloudready.ms/adfs/service/s/trust
http://schemas.microsoft.com/ws/2008/06/identity/claims/authenticationinstant	2014-08-25T03:06:51.345Z	http://sts.cloudready.ms/adfs/service/s/trust	http://sts.cloudready.ms/adfs/service/s/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 .
4pcPyMD09o1PSyXnrXCjTwXyr4BsezdI1AVTmud2fU4

OAuth

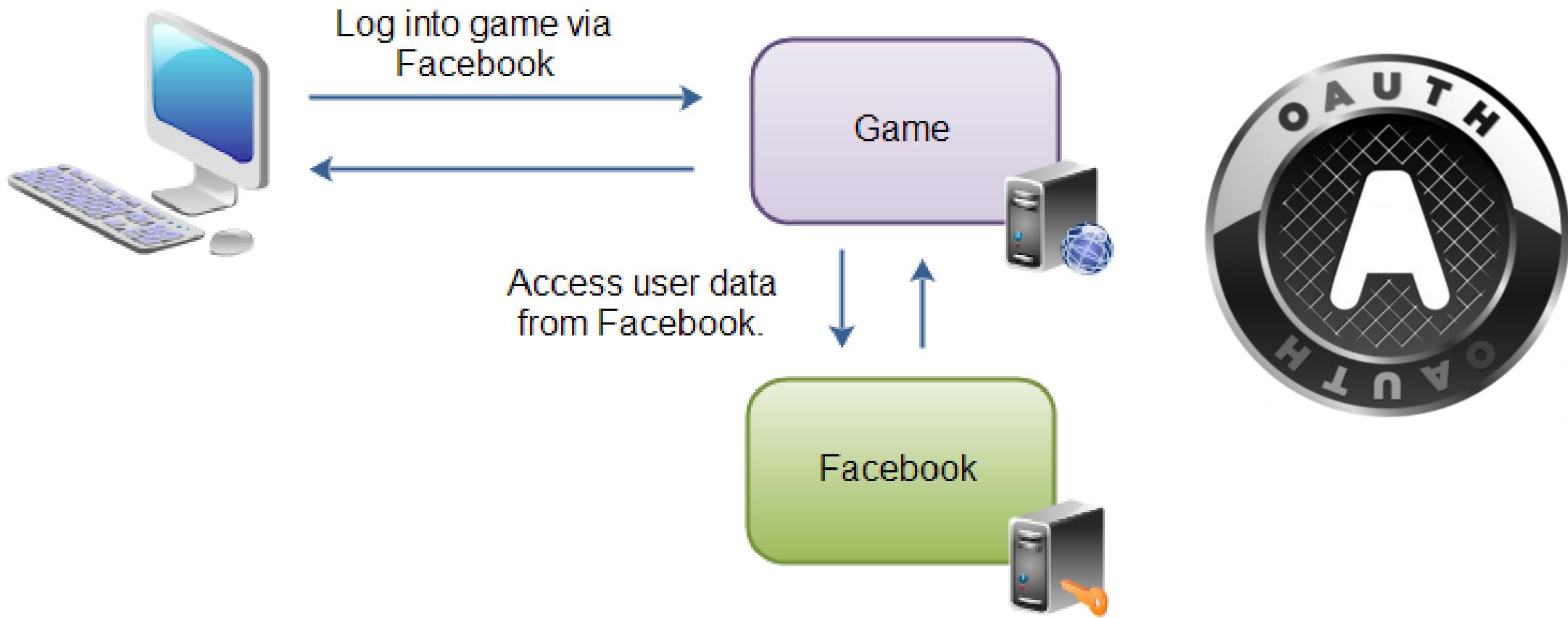


OAuth



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

The screenshot shows the Facebook App Dashboard for an application named "My Great App". The dashboard is divided into sections: "Basic Info", "Select how your app integrates with Facebook", and "Advanced Settings".

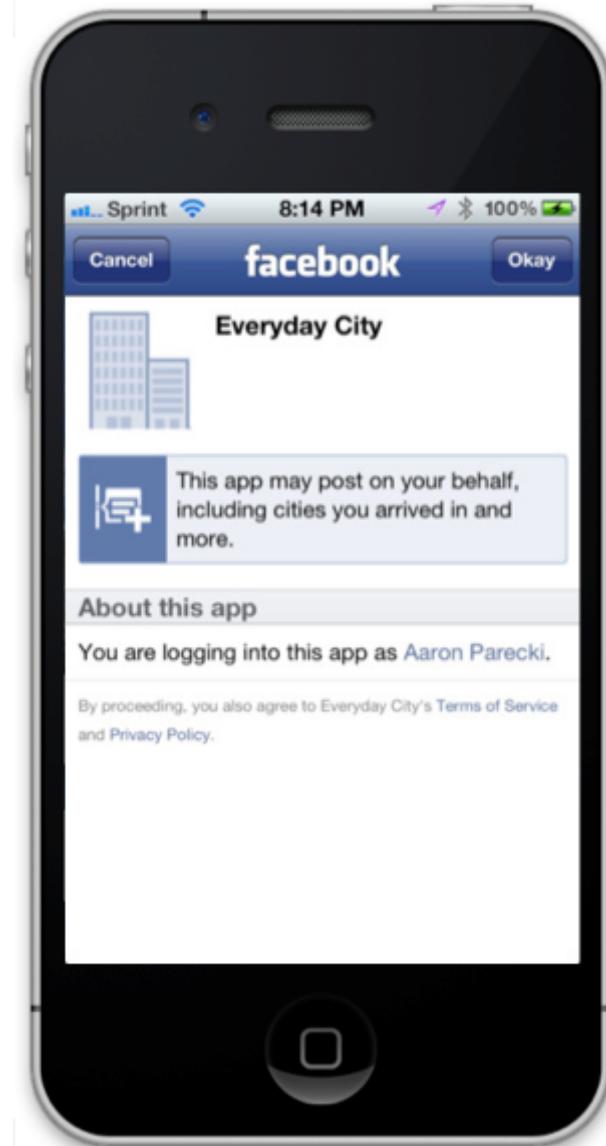
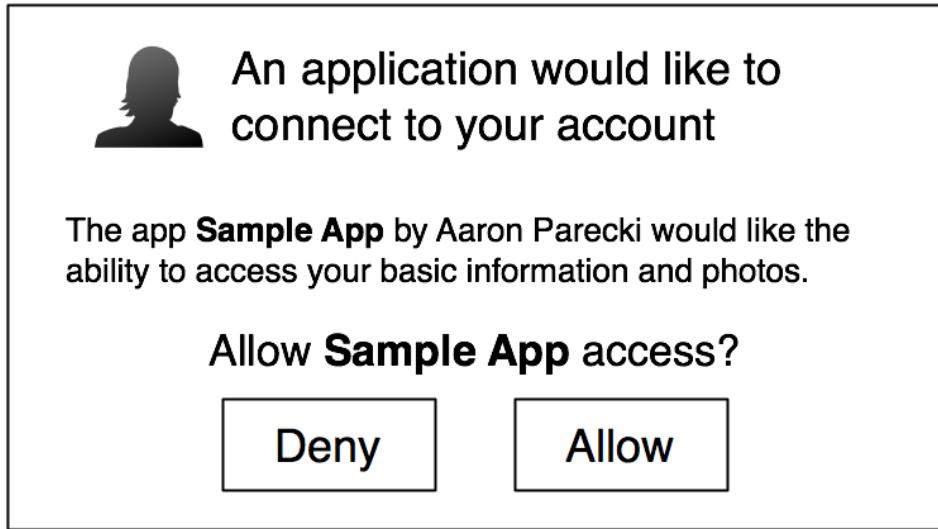
Basic Info

Display Name:	My Great App
Namespace:	
Contact Email:	support@mygreatsite.com
App Domains:	www.mygreatsite.com
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

<input checked="" type="checkbox"/> Website with Facebook Login	X
Site URL:	http://www.mygreatsite.com/
<input checked="" type="checkbox"/> App on Facebook	Use my app inside Facebook.com.

Confirmation



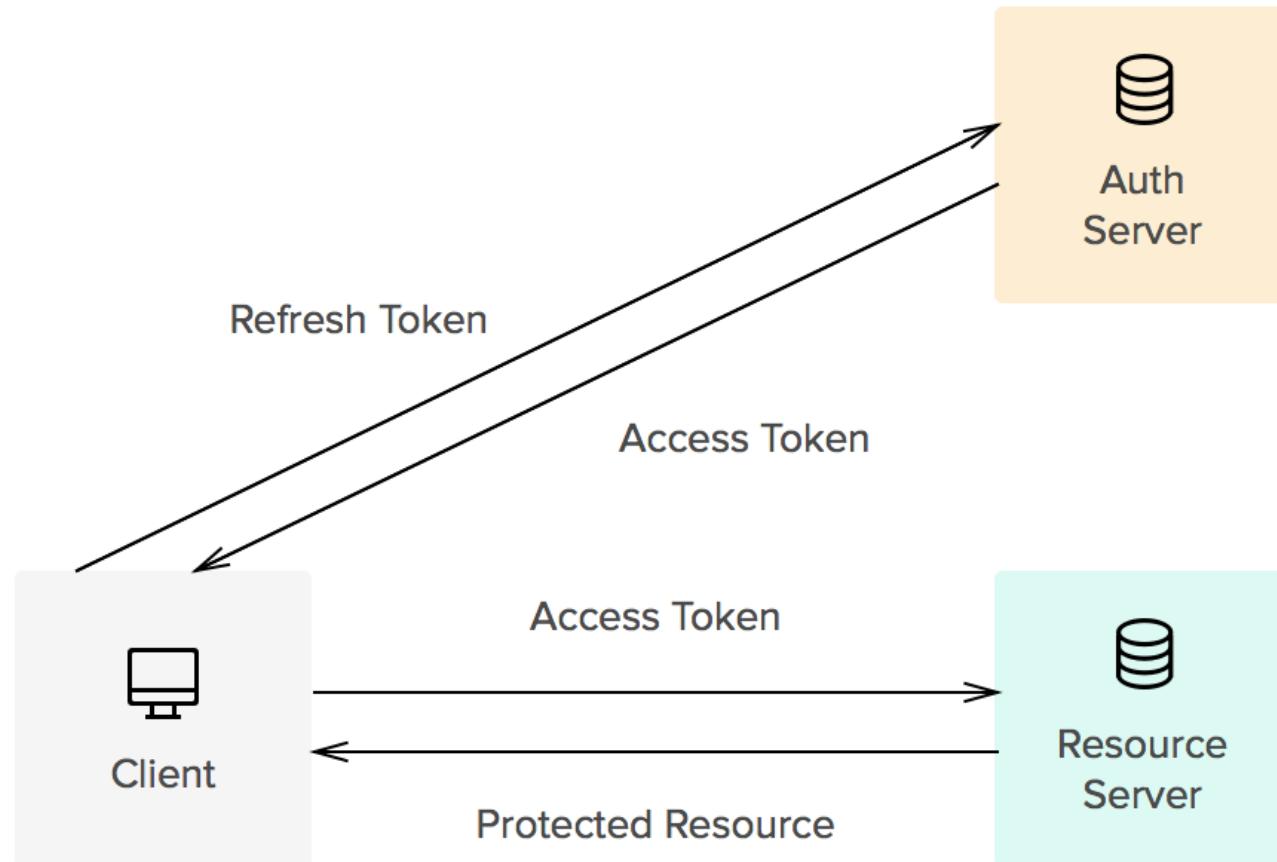
Authorization Management

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 ▾
	Atom.io Last used on Apr 5, 2015 · Owned by atom	Revoke
	CodePen.io Last used on Apr 22, 2015 · Owned by CodePen	Revoke
	GitHub for Mac Last used on May 5, 2015 · Owned by github	Revoke
	Libraries.io Last used on Apr 6, 2015 · Owned by librariesio	Revoke

Token Types

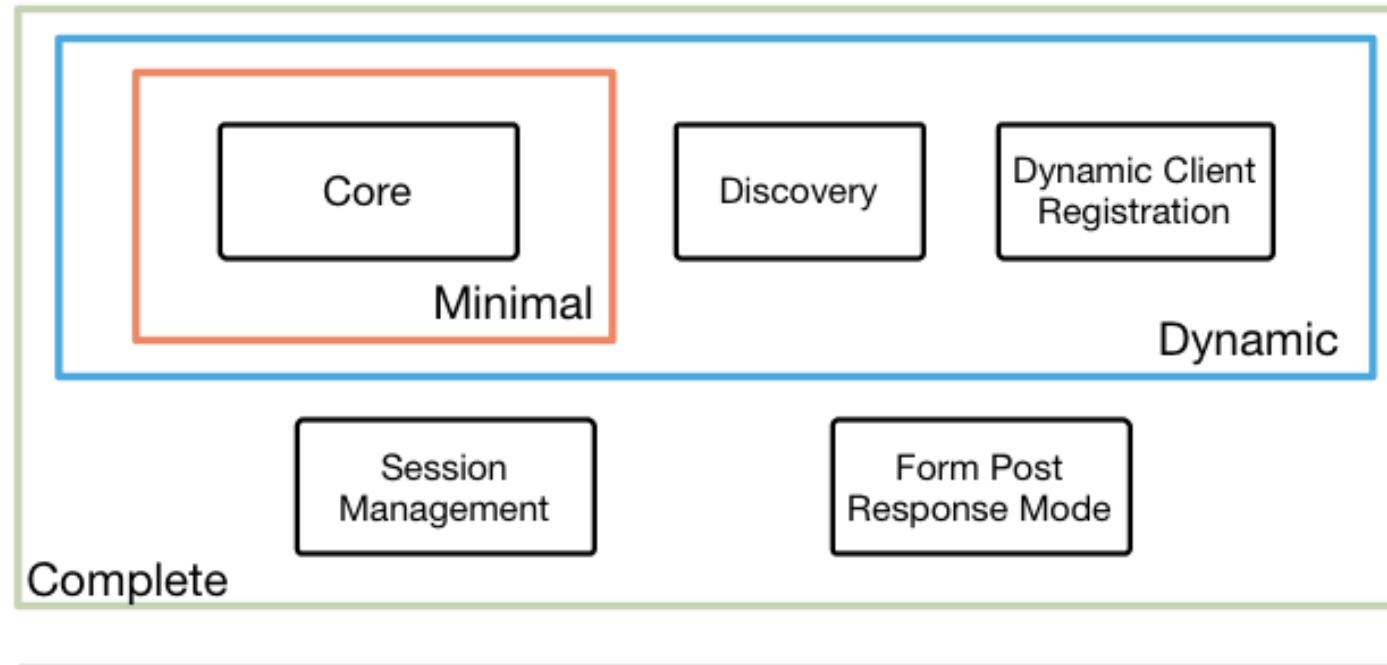


OpenID Connect

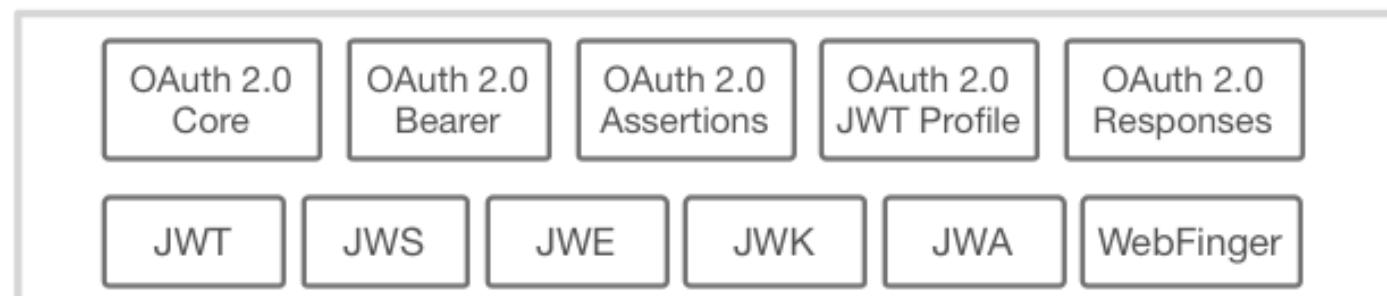
4 Feb 2014

OpenID Connect Protocol Suite

<http://openid.net/connect>



Underpinnings



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

Virtualization + Cloud & Security

Mgr. Michael Grafnetter

