Federated Identity in Cloud
USE CASES
Use Case Contributions

- Connect.gov – Jonathan Prisby
- Trust Elevation – Thomas (Tom) Jones
- Software Defined Perimeter (SDP) – Juanita Koilpillai
- OpenStack, Cloud Federation – Craig Lee
- Amazon Case Study – Chad Clostio
- Federated Single-sign On – Don MacLean
- Labs Collaboration – Ketan Mehta
- FIDO – Ketan Mehta
- Credentials for Citizens by Government – Cheng-Yin Lee
Use Case Contributions

- **Connect.gov** – Jonathan Prisby
- Trust Elevation – Thomas (Tom) Jones
- Software Defined Perimeter (SDP) – Juanita Koilpillai
- OpenStack, Cloud Federation – Craig Lee
- Amazon Case Study – Chad Clostio
- Federated Single-sign On – Don MacLean
- Labs Collaboration – Ketan Mehta
- FIDO – Ketan Mehta
- Credentials for Citizens by Government – Cheng-Yin Lee
Challenge

76% Network Intrusions Exploited Weak or Stolen Credentials

46% Of consumers will abandon a site rather than attempt to reset their passwords or answer security questions

25 ...is the average number of accounts a user has that require passwords

6.5 ...is the average web passwords held by a user

54% ...of users leave the site or do not return when asked to create a new password
What is Connect.Gov?

Connect.Gov is a shared service that enables agencies to provide online services to consumers using government approved commercially-issued digital credentials with greater security, privacy and efficiency.
Federated Identity for Federal Government

Authenticate User’s Identity Once – Re-use Across Government

CONNECT.GOV
CONNECT.GOV IS CURRENTLY IN ITS FIRST PHASE OF OPERATIONS

**September 2009:**
The Identity, Credential, and Access Management Subcommittee (ICAMSC) released the Trust Framework Provider Adoption Process.

**October 2011:**
OMB released a memo – Requirements for Accepting Externally Issued Identity.

**April 2011:**
The National Strategy for Trusted Identities in Cyberspace (NSTIC) was released.

**December 2011:**
The White House convened a meeting with targeted agencies who provide extensive externally-facing services to citizens.

**March 2012:**
The Federal Cloud Credential Exchange (FCCX) tiger team convened to define a common cloud-based service.

**May 2012:**
Federal IT Shared Services Strategy was released.

**December 2013:**
National Strategy for Information Sharing and Safeguarding was released.

**January 2014:**
Contracts awarded to Verizon and ID.me to provide LOA 2 and 3 credentials.

**October 2014:**
Executive Order – Improving the Security of Consumer Financial Transactions was released.

**December 2014:**
USPS Connect (SecureKey) granted FedRAMP JAB Provisional Authorization.

**August 2013:**
USPS awarded broker contracts to SecureKey.

**March 2015:**
LOA 2 and LOA 3 CSPs Go Live
Identities are verified via an online enrollment process

- FICAM certified to NIST Level of Assurance 2 & 3

Citizens can select devices and methods for multi-factor log-in

- Mobile app, QR scan, text, e-mail, tokens, interactive voice response

User combines something they know plus something they have

- Vendors can use innovative approved authentication methods
## Policy & Standards Compliance

<table>
<thead>
<tr>
<th>NSTIC</th>
<th>Adheres to the President’s National Strategy for Trusted Identities in Cyberspace</th>
</tr>
</thead>
<tbody>
<tr>
<td>HSPD-12</td>
<td>Mandates secure and reliable forms of identification and authentication</td>
</tr>
<tr>
<td>OMB M-04-04, M-07-16</td>
<td>Requires the review transactions to ensure proper levels of identity proofing and authentication</td>
</tr>
<tr>
<td>NIST SP 800-63-2</td>
<td>Provides for authentication and four levels of identity proofing</td>
</tr>
<tr>
<td>Executive Order 13681</td>
<td>Mandates ID proofing, multi factor authentication; implementation plan will direct use of government-wide shared service</td>
</tr>
</tbody>
</table>
How Do I Get Started?

RP Pre-qualification & Approval
- Ensure that your agency’s infrastructure exists and is ready for integration
- Configuration Checklist
- Request and acquire certificates
- Create and agree on metadata

Technical Integration
- Determine selector mechanism
- Determine LOA
- Sign metadata, exchange certificate, exchange metadata, sign metadata, attributes specification, etc.

Operational Onboarding
- Includes process testing, operational support, and commercial launch
- Subscribes to ITIL v3 governance
## Sample Integration Timeline

<table>
<thead>
<tr>
<th>Week 1</th>
<th>Week 2</th>
<th>Week 3</th>
<th>Week 4</th>
<th>Week 5</th>
<th>Week 6</th>
<th>Week 7</th>
<th>Week 8</th>
<th>Week 9</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Initial Integration</strong></td>
<td><strong>System Integration/end to end Testing</strong></td>
<td><strong>Customer Acceptance Testing</strong></td>
<td><strong>Prepare Prod. Env.</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Certificate &amp; metadata exchange</td>
<td>• Develop test plan and cases/scripts</td>
<td>• Execute CAT</td>
<td>• Load/provide metadata</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Configuration/code updates to agency systems initial connectivity tests</td>
<td>• Execute integration testing</td>
<td>• Apply fixes to bugs/gaps identified</td>
<td>• Obtain final approval for “Go-Live”</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Test account creation and request/response validation</td>
<td>• Apply fixes to bugs/gaps identified</td>
<td>• Document results in a formal report</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Document results in a formal report</td>
<td>• Obtain sign-offs to move to CAT</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Operation On-boarding</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Held Desk Readiness</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Document Shared Secrets to contact Connect.Gov Help Desk</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Train support staff</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Execute tests to confirm call scenarios and escalation distribution list</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Final sign off and onboarding closure, verification of end-to-end connectivity between the agency &amp; Connect.Gov</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• SecureKey Change Management Process – Review and Validation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Agency Integration – CSP Display Options

Connect.Gov offers two methods of integration to allow a user to select credential of choice:

- **Imbedded Selector** – allows agencies to display the available CSPs that meet their requirements directly on the agency page (agency hosts other messaging content) (recommended option)

  CSPs are displayed based on 2 criteria supplied by the Relying Party:
  - LOA 1 – shows LOA 1 – 4 CSPs
  - LOA 2 – shows LOA 2 – 4 CSPs
  - LOA 3 – shows LOA 3 – 4 CSPs
  - LOA 4 – shows LOA 4 CSPs

- **Redirect** – allows agencies to have a link to a Connect.Gov hosted page with the CSPs shown
Connect.Gov is working with federal agencies and CSPs to determine which identity attributes they need as part of the authentication process.

<table>
<thead>
<tr>
<th>Possible Attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legal First Name, Legal Last Name, Middle Name or Initial</td>
</tr>
<tr>
<td>Current Address: (Parsed or Full)</td>
</tr>
<tr>
<td>Date of Birth: (Parsed or Full)</td>
</tr>
<tr>
<td>Social Security Number: (Parsed or Full)</td>
</tr>
<tr>
<td>Email Address</td>
</tr>
</tbody>
</table>
# Available Attributes

<table>
<thead>
<tr>
<th>Attributes Available From Commercial CSPs</th>
<th>Attributes Available from Smart Cards</th>
</tr>
</thead>
<tbody>
<tr>
<td>First Name</td>
<td>State</td>
</tr>
<tr>
<td>Last Name</td>
<td>Zip</td>
</tr>
<tr>
<td>Middle Name</td>
<td>Country</td>
</tr>
<tr>
<td>Middle Initial</td>
<td>DOB (MM/DD/YYYY)</td>
</tr>
<tr>
<td>Email</td>
<td>SSN9</td>
</tr>
<tr>
<td>Street</td>
<td>SSN4?</td>
</tr>
<tr>
<td>City</td>
<td></td>
</tr>
</tbody>
</table>
High Level Design

AGENCIES’ WEB SITES (RELYING PARTIES – RP)

RP1  RP2  RP3  RPN

CREDENTIAL SERVICE PROVIDERS

CSP1  CSP2  CSP3  CSPN

Consumer Accessing Government Services

Federation Manager

Credential Broker

SAML, PKI, Open ID 2.0, OpenID Connect

HTTPS
Application

HP ECS-VPC for US Public Sector System Boundary

Key

- MBUN – Meaningless but Unique Number
- IPAI – Internal Persistent Anonymous Identifier
- rpPAI – Relying Party Persistent Anonymous Identifier
Connect.Gov Contacts

CONTACTS

Jonathan Prisby
jonathan.prisby@gsa.gov

Jane Quenk
Jane.E.Quenk@usps.gov

PMO

TECHNOLOGY MANAGEMENT
Use Case Contributions

- Connect.gov – Jonathan Prisby
- **Trust Elevation** – Thomas (Tom) Jones
- Software Defined Perimeter (SDP) – Juanita Koilpillai
- OpenStack, Cloud Federation – Craig Lee
- Amazon Case Study – Chad Clostio
- Federated Single-sign On – Don MacLean
- Labs Collaboration – Ketan Mehta
- FIDO – Ketan Mehta
- Credentials for Citizens by Government – Cheng-Yin Lee
Architectural Diagram

Identity Ecosystem Trust Framework with Trust Elevation

User device

User agent

Claims

Value Provider Attribute Verifier

User Authorization Claims validation

Agency Service Provider

Browsing 1
Public Content 2
Request for ID 3
PseudoNym Claims 4
Personalized Content 5
Request for Attributes 6
Real User ID Claims 7
High Value Services 8

Identity and Attribute Providers

Credential

Trust Elevation

User

Queries
Architectural Components

- The user at a computer display of at least 600x800
- An internet shared by all parties
- A service provider with multiple trust levels
- One or more identity or attribute providers
- A value provider to authorize user requests
- Pre-existing trust relationships among providers
Cloud Provider Relationships

- Service Level Agreements must be published
  - Different levels are required and are not codified yet
  - NIST levels are a start, but do not relate to needs
  - Cloud ID providers must create SLAs that meet needs

- Agency service provider to the end user must enable trust with Identity Providers that meet their SLA

- Value provider may be different from user agency
  - Inter-agency interchange needs a standard
Specific Examples

IRS – the user wants to get information to determine if there exists a reason to claim a deduction or ask for a refund anonymously. When the user asks for a refund they need to identify themselves and the tax year involved for lookup by the IRS.

State Benefits provider - the user explores their state web site looking for benefits that might be helpful to their case. In order to examine the results of different situations they create multiple pseudonyms to compare the different combinations of benefits that might be most beneficial to them. When they have identified a program that will provide them with value they need to identify themselves and their attributes to meet the benefits criteria. Perhaps they link to the state DMV to provide the required strong identity.
Specific Scenario

- User browses to an agency hub anonymously.
- User provides a low assurance identity to store history. Assume that the agency selected Fed Connect for this.
  - Third party ID is acquired from (e.g.) Google.
- User navigates to a URL that requires higher assurance.
  - The agency could use Fed Connect or its own list of IdP.
  - Some UX requires the user to completely re-authN.
  - The better UX will be for user context to continue.
  - The best UX will pre-populate the authN attributes.
- The user is always in complete control of data that will be sent to any IdP for authentication.
The Best UX Scenario

- The user has low assurance token
  - Acquired from a cloud IdP (e.g. Google)

- The user needs high assurance token
  - There may be multiple cloud IdP available

- The user context is maintained after elevation
  - The agency can link the low assurance token ID to the high assurance token ID (unavoidable risk)
  - Linkage between IdPs is too be avoided
  - See detailed issues below

- The data from the low assurance logon is used
  - Potentially the user identifier is provide by the IdP (foo@gmail.com)
Many IdP require user to have proprietary ID

foo@gmail.com, foo@Comcast.com, etc.

Agency may use proprietary ID for user

This approach is becoming common in industry

But that is a problem if user changes IdP

It is also a problem if the user has multiple levels

Assurance Level one Token may not have the same user ID as Assurance Level two Token

This is not an issue if the same IdP can provide both tokens

NIST standardization would really help for linkage issues

Link to the IDESG use case

Cloud Specific Threats

- Agency to Fed Connect or to any IdP
  - Data leakage - send no user private data
  - User spoofing - specifically user token reuse
  - Data tampering – specifically man-in-the-middle attack
  - Agency spoofing – attacker can harvest user creds

- Multiple IdPs for one user (elevation or migration)
  - Data leakage – IdP can harvest user data

This section needs input from security experts
Use Case Contributions

- Connect.gov – Jonathan Prisby
- Trust Elevation – Thomas (Tom) Jones
- **Software Defined Perimeter (SDP)** – Juanita Koilpillai
- OpenStack, Cloud Federation – Craig Lee
- Amazon Case Study – Chad Clostio
- Federated Single-sign On – Don MacLean
- Labs Collaboration – Ketan Mehta
- FIDO – Ketan Mehta
- Credentials for Citizens by Government – Cheng-Yin Lee
Use Case – Software Defined Perimeter

Secure Architecture (SDP) that addresses security at all network layers

Integrates user authentication to always allow ONLY good traffic into the perimeter
Use Case Workflow Eg. – Usage/Access

3. When users wish to access a protected site they would click on the SDP client on their device.

4. Info in the unique SPA packet must match id of user. This is the key that opens the gateway to the client (ie. port on firewall).

5. If the device and user identity are valid the users will be granted access. (IP address can be verified to match the stored location for dedicated clients).

Works in cloud (IaaS, PaaS, SaaS) or on premise
Any client, fat, thin, mobile or IoT
Client Experience – On-boarding Process

- Client needs a CERT or a token in addition to user name and password
- Client registers their devices
Use Case Workflow Eg. – Onboarding/Issuance

1. All Internet facing servers of US government sites are hidden by SDP gateway. (ie. default drop all packets)

2. Internet users who desire access to a protected site would be on-boarded with a unique ID (eg. client CERT, encryption keys, etc.)
Website in the Cloud

Linux Server (CentOS)

- SDP Gateway
- SDP Monitor
- Apache (GUI)

iptables (DROP ALL)

Database

Events

Events
Nmap port scan

Nmap scan report for x.x.x.x
Host is up (0.033s latency).
All 65535 scanned ports on x.x.x.x are filtered
Try to Reach Website

HTTPS Request (want to connect to GUI)

iptables (DROP ALL)

Linux Server (CentOS)

- SDP Gateway
- SDP Monitor
- Apache (GUI)

Database

Events
Website Unreachable

This webpage is not available

ERR_CONNECTION_REFUSED

Reload

Details
Website Unreachable

- iptables has no rule to allow access to this machine

- Listing rules in fwnopd iptables chains...

Chain FWKNOP_INPUT (1 references)
num target prot opt source destination

Linux Server (CentOS)

- SDP Gateway
- SDP Monitor
- Apache (GUI)

Events

STOP

HTTPS Request (want to connect to GUI)
SPA – The Magic Word

Single Packet Authorization (SPA)
- UDP
- Encrypted
- Cryptographically Signed

Listing rules in fwknopd iptables chains...

Chain FWKNOP_INPUT (1 references)
num target prot opt source destination

Linux Server (CentOS)
- SDP Gateway
- SDP Monitor
- Apache (GUI)

SPA Packet

Events

Database
Gateway Answers the Door...

SDP Gateway adds a rule to iptables to allow only that machine and only on the desired port.

Listing rules in fwknopd iptables chains...

Chain FWKNOP_INPUT (1 references)
num target prot opt source destination tcp dpt:443 /*_exp_1446756830*/
1  ACCEPT tcp  --  X.X.X.X  0.0.0.0/0
NOTE: The server does not send any response to the requestor.

Listing rules in fwknopd iptables chains...

Chain FWKNOP_INPUT (1 references)
num target prot opt source destination
tcp dpt:443 /*_exp_1446756830*/
Attempt to Reach Website Again

Listing rules in fwknopd iptables chains...

Chain FWKNOP_INPUT (1 references)

<table>
<thead>
<tr>
<th>num</th>
<th>target</th>
<th>prot</th>
<th>opt</th>
<th>source</th>
<th>destination</th>
<th>tcp dpt:443 /* _exp_1446756830 */</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ACCEPT</td>
<td>tcp</td>
<td>--</td>
<td>X.X.X.X</td>
<td>0.0.0.0/0</td>
<td>tcp dpt:443 /* _exp_1446756830 */</td>
</tr>
</tbody>
</table>

SDP Gateway
SDP Monitor
Apache (GUI)

SDP Gateway
SDP Monitor
Database
Mutual TLS Session Established

Apache is now reachable, BUT...
Apache requires a client certificate, making this a Mutual TLS (MTLS) session

Listing rules in fwknopd iptables chains...

Chain FWKNOP_INPUT (1 references)
num target prot opt source destination
tcp dpt:443 /*_exp_1446756830*/
Multifactor Authentication – client certificate (something I have) combined with username and password (something I know)
Gateway Removes Expired Firewall Rule

- The firewall rule is removed seconds after it was created
- The MTLS session persists while the firewall is dark once again

Listing rules in fwknopd iptables chains...

Chain FWKNOP_INPUT (1 references)
num target prot opt source destination

Linux Server (CentOS)

SDP Gateway

SDP Monitor

Apache (GUI)

Database
Use Case Contributions

- Connect.gov – Jonathan Prisby
- Trust Elevation – Thomas (Tom) Jones
- Software Defined Perimeter (SDP) – Juanita Koilpillai
- **OpenStack, Cloud Federation** – Craig Lee
- Amazon Case Study – Chad Clostio
- Federated Single-sign On – Don MacLean
- Labs Collaboration – Ketan Mehta
- FIDO – Ketan Mehta
- Credentials for Citizens by Government – Cheng-Yin Lee
OpenStack and Virtual Organizations as Use Cases for Federated Identity Management in the Cloud

Dr. Craig A. Lee
Senior Scientist, Computers & Software Division
The Aerospace Corporation

NIST Federated Identity Management PWG, March 23, 2016

Related Presentations at:
Ground System Architectures Workshop, Los Angeles, March 2, 2016
Federations Are Collaborative Environments

Collaborative environments must enable a user from one site to access resources at another site. This is enabled by Federated Identity Management (FIM). The remote site must "know" how to validate the user's credentials issued by a remote IdP and make the right authn/authz decisions.

What does FIM mean/entail in federated environments, and specifically in federated cloud environments?

What use cases are possible?
- OpenStack
- Virtual Organizations

How do we understand the fundamental requirements that these use cases are telling us?
- Fundamental properties affecting FIM: access, organization, and scale
- What are the fundamental federation deployment models?

Specifically what does FIM mean in a complex, federated cloud?
Use Case: OpenStack Keystone Federation Support

OpenStack is a widely supported, open source cloud project
Keystone is the security service for all other OpenStack services

Extending the Keystone API to support simple, manual federation management using two fundamental concepts:
- **Federate In:** Explicitly specify which external IdPs are trusted
- **Federate Out:** Explicitly specify which external SPs are trusted

Can be configured to use SAML or OpenID Connect

Enables a key business model: *Hybrid Clouds*
Use Case: Virtual Organizations as the Management Abstraction for Collaborative Environments

A VO is a security and collaboration context not exclusively associated with any one physical organization or site

- Participants agree upon VO structure, rules and processes
- A VO participant can be a single person, a group or an entire organization

A VO has members that are assigned roles and/or attributes

- Membership roles or attributes grant specific capabilities within a given VO as determined by each resource/service provider

VO participants contribute resources, i.e., data and services

- They retain complete control over their own resources!
- Access by VO members can be modified or revoked at any time by both the VO administrator and the resource administrator

A VO Management System (VOMS):

- Maintains member identity attributes and authorization attributes
- Enables resource (service) discovery
- Enables validation of VO member authz credentials on service invocation
How can separate organizations share data and services?

Based on their VO authorizations, members can access different services.

Participating sites register their services they wish to make available to this VO.
A VO Management System: KeyVOMS
A Centralized, Third-Party VOMS for Secure Discovery and Access across Sites

• OpenStack Keystone v3 re-purposed as a stand-alone, VO Management Service: KeyVOMS
  – Domain used as a VO
  – Service Catalog used for app-level services
  – Endpoint Filtering used
  – Inherits support for FIM, PKI, certificate caching, revocation lists, etc.

• New rule set enforces three pre-defined roles:
  – voms_admin
  – vo_admin
  – vo_site_admin

• Modular VO Policy Enforcement Point built
  – Based on WSGI

Strong Similarities with Software-Defined Perimeters

SDP Controller is very similar to Centralized, Third-Party VO Management System, e.g., KeyVOMS

VO Policy Enforcement Points constitute a software-defined perimeter

Used by permission, Juanita Koilpillai, Software-Defined Perimeter WG, Cloud Security Alliance
Next Step: A Keystone-based, General Federation Agent

- A Centralized, Third-Party VOMS was an easy "target of opportunity"
- Re-purposing a Keystone v3 enabled concepts to be demonstrated
- A centralized approach is inherently not scalable
- How can we build a distributed, general federation agent?
- Keystone has been under continuous development with important mods

Booting and Growing a VO
- Sites with Membership Granting Authority can vary from 1 to N in a federation
- Service Discovery
  - Initial replication, exhaustive query, limited query, search engines, ...
- Credential Validation
  - Local account, guest/role account, credential exchange, user mapping, ...
- A User Interface: OpenStack Horizon
  - Drop-down menu for projects which may have “VO/Domain” attribute
  - Simple approaches are being initially taken
A General Implementation Concept: *Federation Agents*

A Federation Agent is the thing that is capable of managing a local user's interactions with a federation:

- Federated Identity Management & Authentication
- Resource Discovery
- Federated Credential Validation
- Authorization

A Federation Agent (FA) can be either:

- Internal to the User's administrative domain, or
- External to the User's administrative domain

*What Federation Deployment Models are Possible?*

Federation Deployment Models
Based on the Notion of a Federation Agent

Simple, Pair-wise Federation
- Keystone
- FA
- Keystone

Hierarchical Federation
(Not pictured)

P2P Federation
- Keystone
- FA
- Keystone
- FA
- Keystone
- FA
- Keystone

Centralized, Third-Party Federations

Gateway Federation
- Keystone
- FA
- Keystone
- FA
- Keystone
- FA
- Keystone
- FA
- Keystone
- FA
- Keystone
- FA
- Keystone
- FA
- Keystone
- FA
- Keystone
Federation Deployment Models
Interclouds – The Internet of Things

Skitter data depicting internet connectivity. CAIDA.org, used by permission.
Final Observations: What Does this Mean for Federated Identity Management in the Cloud?

- What aspects of cloud computing force FIM-specific issues?
  - On-Demand Virtual Resources
    - "I got this virtual machine/container/network. Who's actually providing it, and do they know who I really am?"
  - Virtualized Administrative Domains
    - "My organization is collaborating with lots of other organizations in a virtualized administrative domain with lots of users coming from different home organizations. How does it authenticate me?"
  - Trust Topology
    - "In this virtualized administrative domain, what kind of trust relationships exist? How are those relationships used to authenticate me?"
Thank you

All trademarks, service marks, and trade names are the property of their respective owners.
Use Case Contributions

- Connect.gov – Jonathan Prisby
- Trust Elevation – Thomas (Tom) Jones
- Software Defined Perimeter (SDP) – Juanita Koilpillai
- OpenStack, Cloud Federation – Craig Lee
- Amazon Case Study – Chad Clostio
- Federated Single-sign On – Don MacLean
- Labs Collaboration – Ketan Mehta
- FIDO – Ketan Mehta
- Credentials for Citizens by Government – Cheng-Yin Lee
Cloud Architecture

Torrent Technologies provides a fully cloud based solution in the Amazon AWS cloud

We provide a service for Insurance companies to purchase and manage Flood Insurance with the NFIP

Users of our system include insurance agents and insurance company personnel

The following are the high level components of our system:

- Thin client access from users (browser and mobile)
- F5 Load balancing
- Microsoft based web farm using a extension of the Microsoft authentication provider
- SQL server always-on technology for fully redundant and auto failover databases storing user credentials
- SAOP web services for authentication handshake
- SAML based authentication
Trust Relationship

- Security Standards
  - SOC 1/SSAE 16/ISAE 3402
  - SOC 2
  - SOC 3
  - FISMA, DIACAP, FedRAMP
  - DoD CSM Levels 1-5
  - PCI DSS Level 1
  - ISO 27001
  - ITAR
  - FIPS 140-MTCS Level 3

- Manages Cloud Security
- Certificates
- User privileges

- Enters into Contract to receive services with SLA’s
Cloud Authentication

Torrent Federated Identity Management

- User logs in from an external site or system
- Custom double handshake, initiated from secure SOAP request
  - Requires a system level account that defines the access control
  - Token based - generated and returned – encoding the credentials
  - Calling system redirects to endpoint URL with the token
- SAML 2.0 (Certificate based, public/private key)
  - Users authenticated on external system
  - SAML request authenticates calling system by certificate
  - If system is authenticated and user exists, token generated and redirected
  - Flexible for other authentication platforms/providers
Authentication

External System sends entity-level credentials to Torrent Authentication Service, which receives a token. User authenticates with the External System and receives a token. Trust relationship is established with the Entity. User has custom roles/permissions with the Torrent System.
Identity Issuance Process

Ultimately users of the Torrent system must be stored in the Torrent SQL user database

Users are provisioned
  - By Active Directory hooks for company level users
  - In mass by importing a set of users into the Torrent database
  - Manually provisioned by Agency service personnel via web interface
  - By automated XML based synchronization process between Torrent and calling systems utilizing federated authentication
Identity Usage Process

- Users within the Torrent System have custom roles and permissions

- Features of the site are based on the roles and permissions of the authenticated user and company context

- Users authenticated via Federated Identity Management must be synchronized between the calling system and Torrent to maintain the user roles, permissions, and access
User Experience

The user starts in an external company-specific web site.

The user authenticates within the external site – which initiates the FIM authentication with Torrent.

Upon success the user is redirected to the Torrent site with their roles and permission set.

User session is opened up and maintained for the life of the user interaction.
Use Case Contributions

- Connect.gov – Jonathan Prisby
- Trust Elevation – Thomas (Tom) Jones
- Software Defined Perimeter (SDP) – Juanita Koilpillai
- OpenStack, Cloud Federation – Craig Lee
- Amazon Case Study – Chad Clostio
- Federated Single-sign On – Don MacLean
- Labs Collaboration – Ketan Mehta
- FIDO – Ketan Mehta
- Credentials for Citizens by Government – Cheng-Yin Lee
Federated Single Sign-On to Applications On a Public Cloud

Cloud Architecture

- Public Cloud
- Hosts SaaS applications
- STS
- Trusts Customer IdP
Federated Single Sign-On to Applications On a Public Cloud

Customer Architecture
- On-prem IdP trusted by SaaS Provider
- Endpoints (Browser or App)
  - Laptops/Desktops
  - Tablets
  - Phone
User browses to customer portal and selects desired application.

Portal verifies the user's (local) identity.

Portal generates SAML authentication response
- Assertions identify user
- Assertions include user attributes

Portal sends SAML response to the client browser.

Client browser is redirected to the SSO endpoint

(cont.)
Federated Single Sign-On to Applications On a Public Cloud

- Browser posts the SAML assertion.
- SSO endpoint requests temporary security credentials
- SSO endpoint creates sign-in URL that uses those credentials.
- SSO endpoint sends sign-in URL back to the client as a redirect.
- Client browser is redirected to the application
- Client can optionally choose roles if multiple roles were included in SAML assertion
Federated SSO

(1) SSO EP Trusts IDP/STS

(2) Authentication and Token Request

(3) STS grants token

(4) Token Presented to SSO EP

(5) Access Granted per Business Logic

User

On-prem IdP Identity Store

Provider - SSO EP - STS
Federated Single Sign-On to Applications On a Public Cloud

- Identity is issued and managed at customer site
- User signs in once, and chooses application from customer portal
- Access to resources centrally managed on-prem
Use Case Contributions

- Connect.gov – Jonathan Prisby
- Trust Elevation – Thomas (Tom) Jones
- Software Defined Perimeter (SDP) – Juanita Koilpillai
- OpenStack, Cloud Federation – Craig Lee
- Amazon Case Study – Chad Clostio
- Federated Single-sign On – Don MacLean
- Labs Collaboration – Ketan Mehta
- FIDO – Ketan Mehta
- Credentials for Citizens by Government – Cheng-Yin Lee
Two Labs currently maintain their own websites that includes data such as:
- Product Certification Submissions and Status Updates
- Product Design & Other Proprietary Information
- Vendor’s Information
- Laboratory Information

Each Lab issues credentials to their employees / vendors / laboratory personnel to allow access to view and act on the data.

Some data is duplicated while some data is unique to the agency.

Both Labs are planning to migrate to Cloud to share data as well as to outsource web site management to a cloud service.
Current Architecture

Each Party Manages Their Own System

Lab 1 User
Lab 1 IDP
Lab 1 Data Server
Lab 2 User
Lab 2 IDP
Lab 2 Data Server

Issue LOA 3 Credential
Trust Relationship
Authenticate to Server
Get Access to Resources

Issue LOA 1 Credential
Trust Relationship
Authenticate to Server
Get Access to Resources

Labs Collaboration
Labs Collaboration

Data Share in Cloud

Lab 1 User
- Issue LOA 3 Credential
- Signed Token - LOA 3
- User ID & Password - LOA 1
- Issue LOA 1 Credential
- Trust Relationship

Lab 1 IDP
- Trust Relationship

Lab 1 DATA

Lab 1 Data Server

Lab 2 User

Lab 2 IDP

Lab 2 DATA

Shared Data

Lab 2 Data Server
Use Case Contributions

- Connect.gov – Jonathan Prisby
- Trust Elevation – Thomas (Tom) Jones
- Software Defined Perimeter (SDP) – Juanita Koilpillai
- OpenStack, Cloud Federation – Craig Lee
- Amazon Case Study – Chad Clostio
- Federated Single-sign On – Don MacLean
- Labs Collaboration – Ketan Mehta
- FIDO – Ketan Mehta
- Credentials for Citizens by Government – Cheng-Yin Lee
Fast Identities Online

Use Case

This is a special case that we should consider including in our analysis and recommendation.

The concept is very simple. There are two functions: Make Credential and Get Assertion. Relying Parties use Make Credential to create credentials on the device and use Get Assertion to subsequently authenticate the device.

The Make Credential requires trusted device which is proven by device attestations.

Get Assertion requires user authentication (PIN / Biometrics) before the device can generate signature.

Both Labs are planning to migrate to Cloud to share data as well as to outsource web site management to a cloud service.
FIDO Use Case

User Authentication

Device Authentication

Client App / Browser

TLS Authenticated session to Server / Get Access to Resources

Relying Party Services

Device-based authenticators

Device Authentication
FIDO Use Case

Client

Client App / Browser

Cloud Service Provider

Device-based authenticators

User Authentication

Device Authentication

Relying Party 1

Relying Party 2

Relying Party 3

Relying Party 4
Security Considerations

- Phishing attack
- Man-in-the-middle attack
- Replay attack
- Counterfeit
- Denial of Service attack
- User Privacy – “big brother watching”
- Data Exposure
Next Steps

- One more use case left.

- Come up with Generic Use Cases that encapsulates all the concepts we have discussed so far.

- Create a spreadsheet template to start doing use case analysis.

- Start populating the template for each use case.

- Volunteers for:
  - Develop spreadsheet template
  - Use Cases Summary