State of Connecticut
Criminal Justice Information System

Connecticut Information Sharing System (CISS)
Technology Workshop 2:
CISS Security Overview

September 5th, 2012

CISS Security: Vision and Scope

Vision

The vision is to utilize Microsoft's Active Directory Federation Services 2.0 (AD FS 2.0) to implement federated security utilizing a claims-based model according to the GFIPM metadata specification, such that CISS managed users, and users managed by other agencies, can securely access CISS resources.

Scope

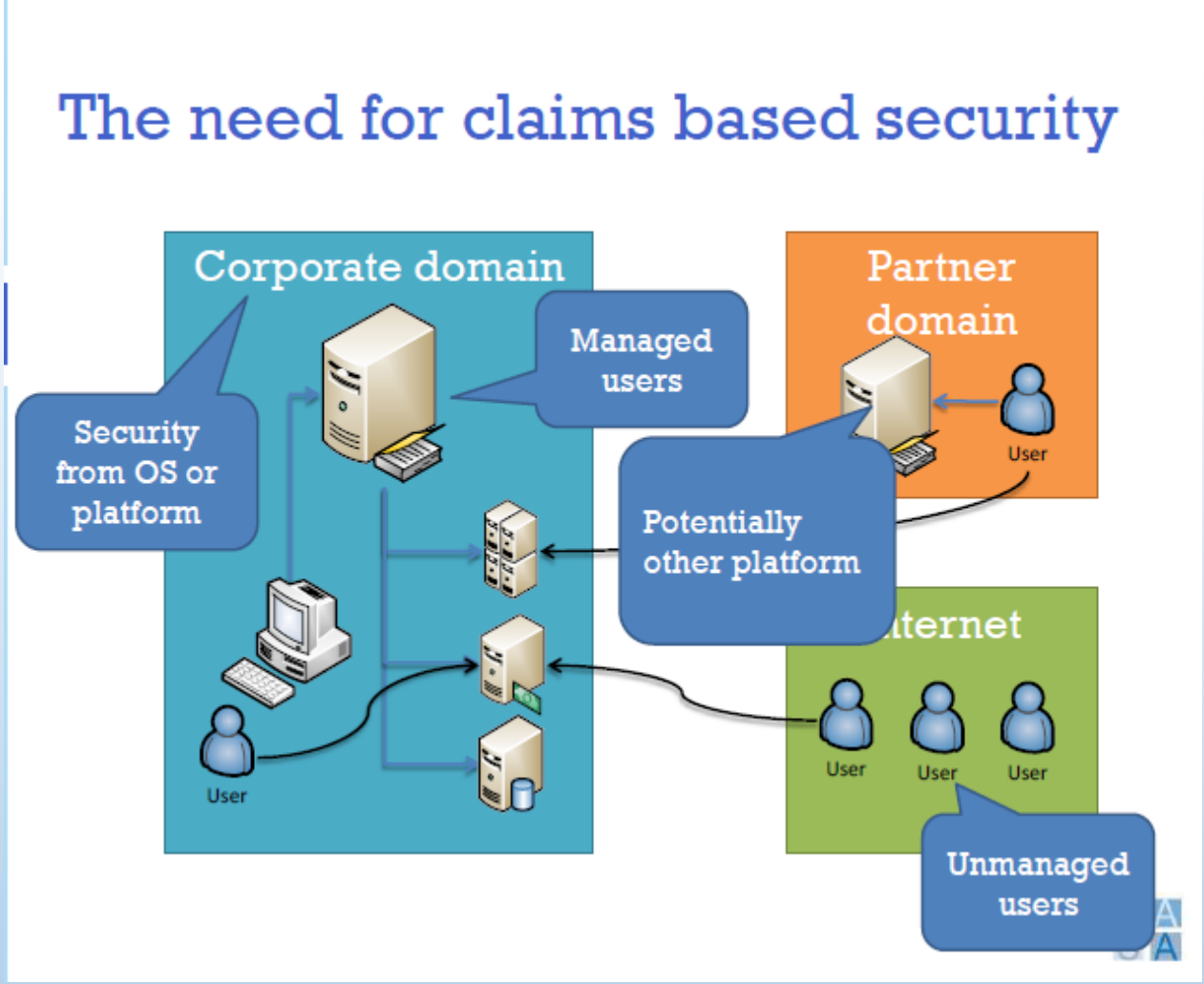
The scope of the design is to provide the required information for the implementation of a CISS Federation that consists of a CISS Identity Provider (IdP) and CISS Resources. The design allows for agencies in the State of Connecticut to provision additional Identity Providers (IdPs) in the future and as a result participate in the CISS Federation. This will enable agency-managed users to access CISS resources based on the agency's participation and inclusion in the CISS federated security model.

The Connecticut Information Sharing System (CISS) requires a federated security model based on the Global Federated Identity and Privilege Management (GFIPM) specification. The CISS federated security model design provides federated access to CISS resources, and could be used by the state of Connecticut as its model for single sign-on access to systems and applications located across the organization.

Legal Regulatory Requirements Summary

1. CISS is required to conform to the applicable requirements of the Criminal Justice Information Systems (CJIS) Security Policy.
2. For partners using a local identity provider and performing local authentication, it is the responsibility of the agency to comply with the CJIS Security Policy and other CISS security requirements for advanced authentication and other aspects of CISS security (e.g. password length, expiration, etc.).
3. CISS requires a security environment that enables management of access and information delivery. The environment should follow the GFIPM standards and should logically apply access privileges for users and restrictions to data. As a result the CISS security architecture should be logically layered into two major levels:
    - Internal Security Architecture – A GFIPM-conformant security architecture that will allow systems and justice agencies' internal users to use the services and capabilities in the CISS environment.
    - External Security Architecture – A GFIPM-conformant security architecture that will ultimately allow systems and external users to use the services and capabilities in the CISS environment.

Claims-Based Security Overview



Claims-Based Security Overview

Leverage existing identities

Web identities

Corporate identities

Application identities

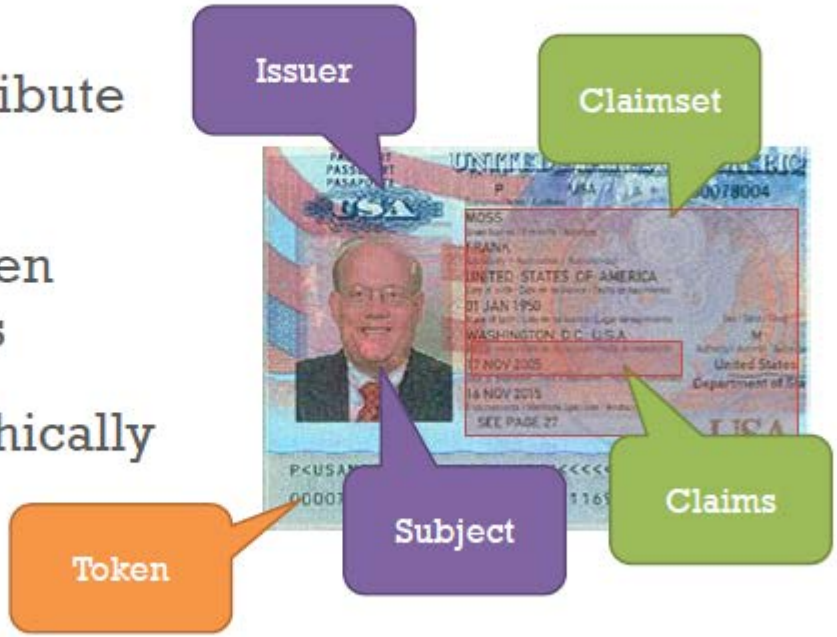
Issued identities

- Users already have identities
- Reputation of provider
- Capabilities

Claims-Based Security Overview

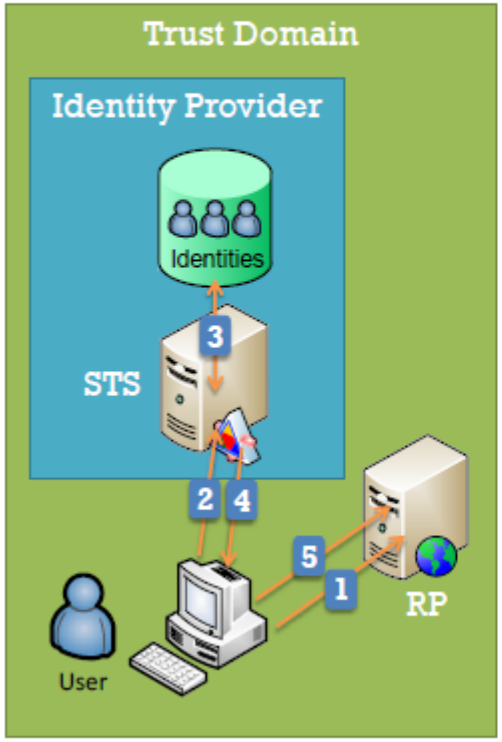
Claims, issuers, subjects and tokens

- Claim is attribute of identity
- Security token holds claims
- Cryptographically signed
  - Optionally encrypted



Claims-Based Security Overview

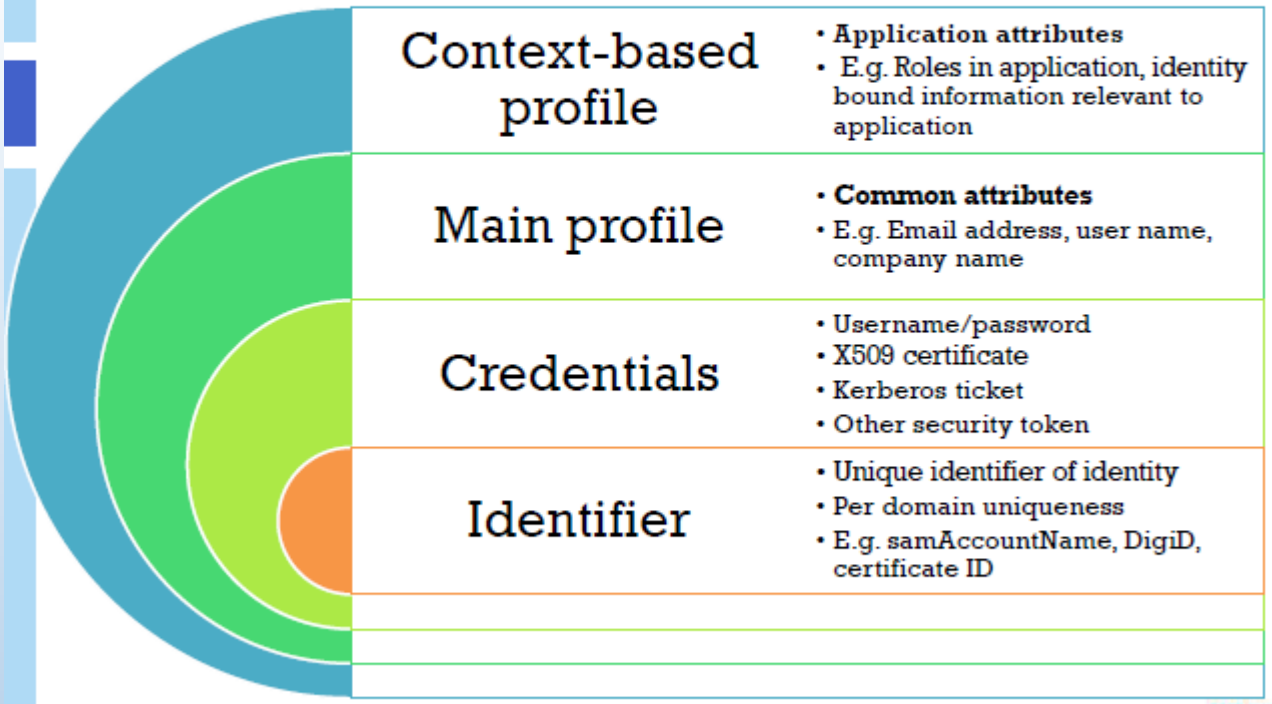
Elements of claims-based architecture



- Identity Provider
  - Identity store
  - Security Token Service
- Relying Party (RP)
  - Application using claims
- Subject
  - User
  - Entity with identity
- Security token

claims-based Security Overview

Design of a claims model



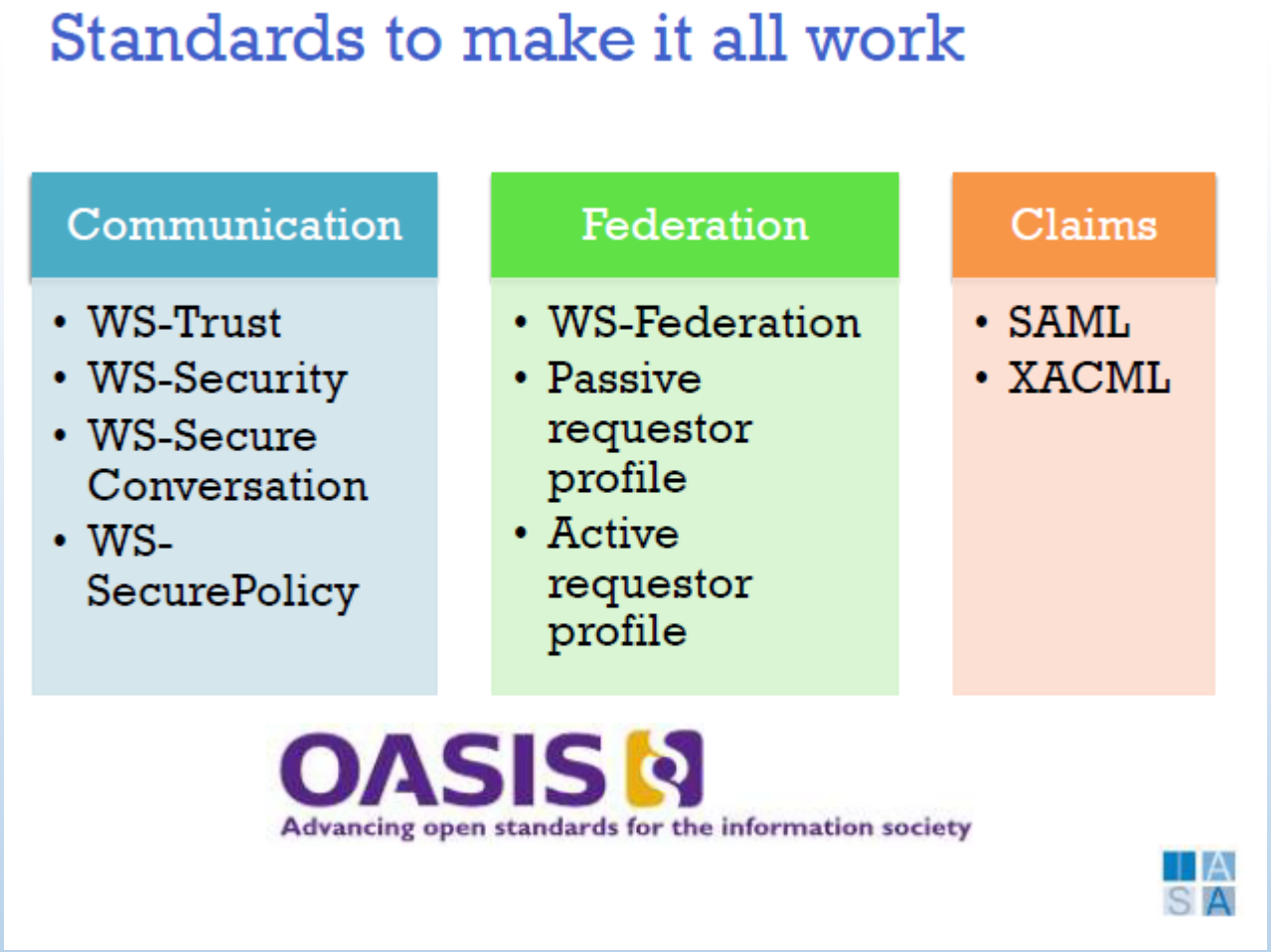
Source: Microsoft Architecture Journal #16

Claims-Based Security Overview

Federation and trust

Federation as an alternative when identity centralization is not an option

Claims-Based Security Overview



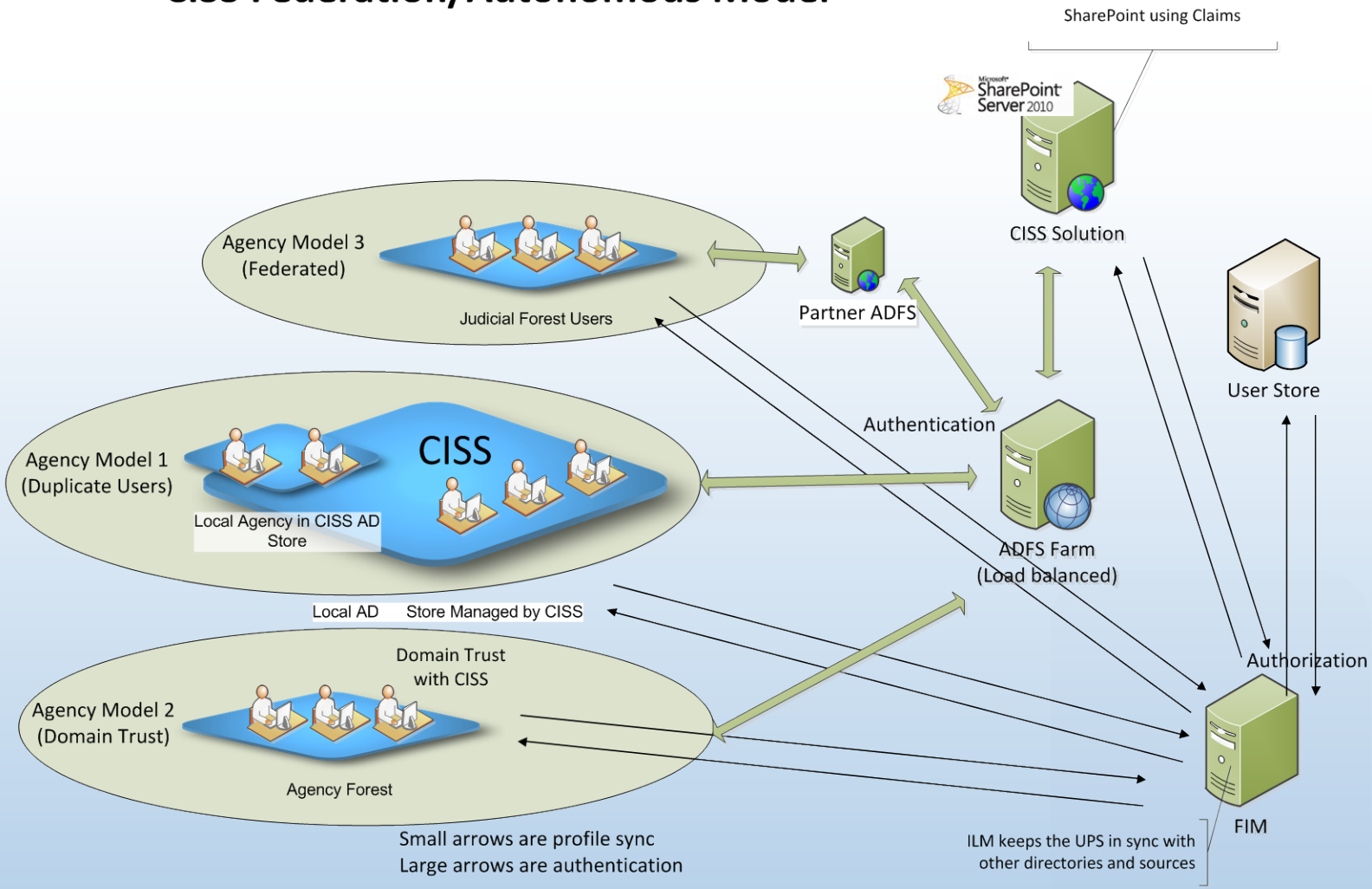
Claims-Based Security Overview

Separation of concerns

- Provisioning of identities and claims issuance by authoritative source
- Different issuers
  - Main profile: IP-STS
  - Context based profile: Resource-STS

CISS Security Architecture

CISS Federation/Autonomous Model



User Requirements Summary

There are three different sets of users which require access to the CISS application:

- Internal Users (Agency Model 1)
  - CISS managed users, maintained within the CISS user store
- External Users
  - (Agency Model 2) CJIS (domain) managed users, maintained within the CJIS user store
  - (Agency Model 3) Other Jurisdiction (OJ) participants within the State of Connecticut.

To meet these requirements, access to CISS resources will be controlled based on user-claims. The Microsoft SharePoint (SPS) claim token service will allow access to SharePoint and as a result security will be handled via claims and SharePoint Groups with Custom Permission sets within the SharePoint environment. Synchronization will be achieved leveraging Microsoft Forefront Identity Manager (FIM).

Agency Model 1 – CISS Managed Users

- A CISS-managed user is using a web browser to access the SharePoint application.
- The user is redirected to the CISS Identity Provider (IdP) (ADFS in the above diagram) if no token is found in their browser cache (no active session).
- The CISS user selects the CISS IdP to be authenticated against.
- The CISS-managed user is prompted to provide their user certificate as one of the two authentication factors for this model.
- The CISS IdP authenticates the user against AD and determines if the user is valid. If the user provides the wrong credentials, a message will appear that the username or password is incorrect.
- If the password has been forgotten or lost, the user has the choice to retrieve the password or reset the password and then try to login again. AD policies conformant with the CJIS security policy apply for requirements like password length and complexity.
- The CISS IdP builds the Token (based on the endpoint requirements) and redirects the browser to the SharePoint application with the Token (all claims included as retrieved from the SQL User Store).
- The SharePoint application determines the authorization rights of the user based on the SharePoint Group the user belongs to. If the user doesn't have access rights to SharePoint, an Access Denied message will appear.
- A cookie is then set in the CISS user's browser.
- The CISS user is able to browse the SharePoint site and use the functionality they have rights to access.

Agency Model 2 – Domain Trusts

- A user whose account is managed by the CISS domain is using a browser to access the CISS Portal SharePoint application.
- The user is redirected to the CISS Identity Provider (IdP) if no token is available in the browser cache (no active session).
- The user selects the CISS IdP to be authenticated against.
- The user provides their user certificate and the IdP authenticates the user against AD and determines if the user is valid. If the user provides the wrong credentials, a message will appear that the username or password is incorrect.
- The IdP builds the Token (based on endpoint requirements) and redirects the browser to the SharePoint application with the Token (all claims included are retrieved from the SQL User Store).
- The SharePoint application determines the authorization rights of the user based on the SharePoint Group the user belongs to. If the user doesn't have access rights to SharePoint, an Access Denied message will appear.
- A cookie is then set in the user's browser.
- The user is able to browse the SharePoint site and use the functionality they have rights to access.

Agency Model 3 – Federated

- An Other Jurisdiction (OJ) user is using a browser to access the SharePoint application assuming the OJ Identity Provider has established federated trust with the CISS IdP.
- The user is redirected to the CISS Identity Provider (IdP) if no token is available. The user then gets redirected to the OJ IdP provider via the CISS IdP provider.
- The OJ user selects its own OJ IdP to be authenticated against.
- The OJ user is redirected to the selected IdP. Agencies participating in this use case are required to provide their own Identity Provider which builds security tokens with the claims that are required by the CISS Federation. This is not the token that goes back to SharePoint, it is only used as proof that they been authenticated so that a new token can be created.
- The OJ IdP authenticates the user against its own AD and determines if the user is valid. If the user provides the wrong credentials, a message will appear that the username or password is incorrect.
- The OJ IdP builds the Claim Token and redirects back to the CISS IdP (AD FS) to have the token augmented with the attributes retrieved from the central SQL User Store, then redirect the browser to the SharePoint application with the Token. The only task the OJ IdP does is to authenticate the user and pass the user back to the CISS IdP.

Agency Model 3 – Federated, cont'd

- The SharePoint application determines the authorization rights of the OJ user based on the SharePoint Group the user belongs to. If the OJ user doesn't have access rights to SharePoint, an Access Denied message will appear.
- A cookie is then set in the OJ user's browser.
- The OJ user is able to browse the SharePoint site and use the functionality they have access to.

Federated Security notes

Model 3 agency will need to implement AD FS and have trust enabled between the CISS AD FS service and its own AD FS service. CISS has developed a policy for any Model 3 agency that connects to the CISS environment consisting of attributes including password length, password age, password failure attempts, etc.

Second Factor Authentication

- Use Case 1, 2, and 3 use a second authentication factor with certificates: certificates will be issued to users for client authentication purposes. The web site will be configured to require client authentication over SSL/TLS, using certificates issued by a small set of Certificate Authorities (CAs), for example, self-signed, CT CA or third party CA, but no others than those required to boot the operating system. When the user connects, they are automatically prompted to select a certificate. The user selects the certificate, and assuming everything with the selected certificate is correct, the connection is made. The two factors in this case are the user's name and password and then the certificate.

- Use case 3 also uses certificates to provide claims. For example, if a user is authenticated to the local system using AD, a claim can be added to the SAML token indicating that the user was authenticated in that manner rather than using only a username and password.

Active Directory Federation Services v 2.0

Microsoft Active Directory Federation Services (AD FS) is a core architecture component in the Enterprise Federated Identity solution. AD FS provides the interoperability required to simplify the federated sharing of digital identities and policies across organizational boundaries.

Agencies' employees can all use these security tokens to gain access to the information they need, when they need it once the trust relationships between the federation services have been made and sharing policies established. Trust for example is trust between SharePoint and AD FS and/or AD FS to a relay party (another SAML based authentication provider).

Security Token Service

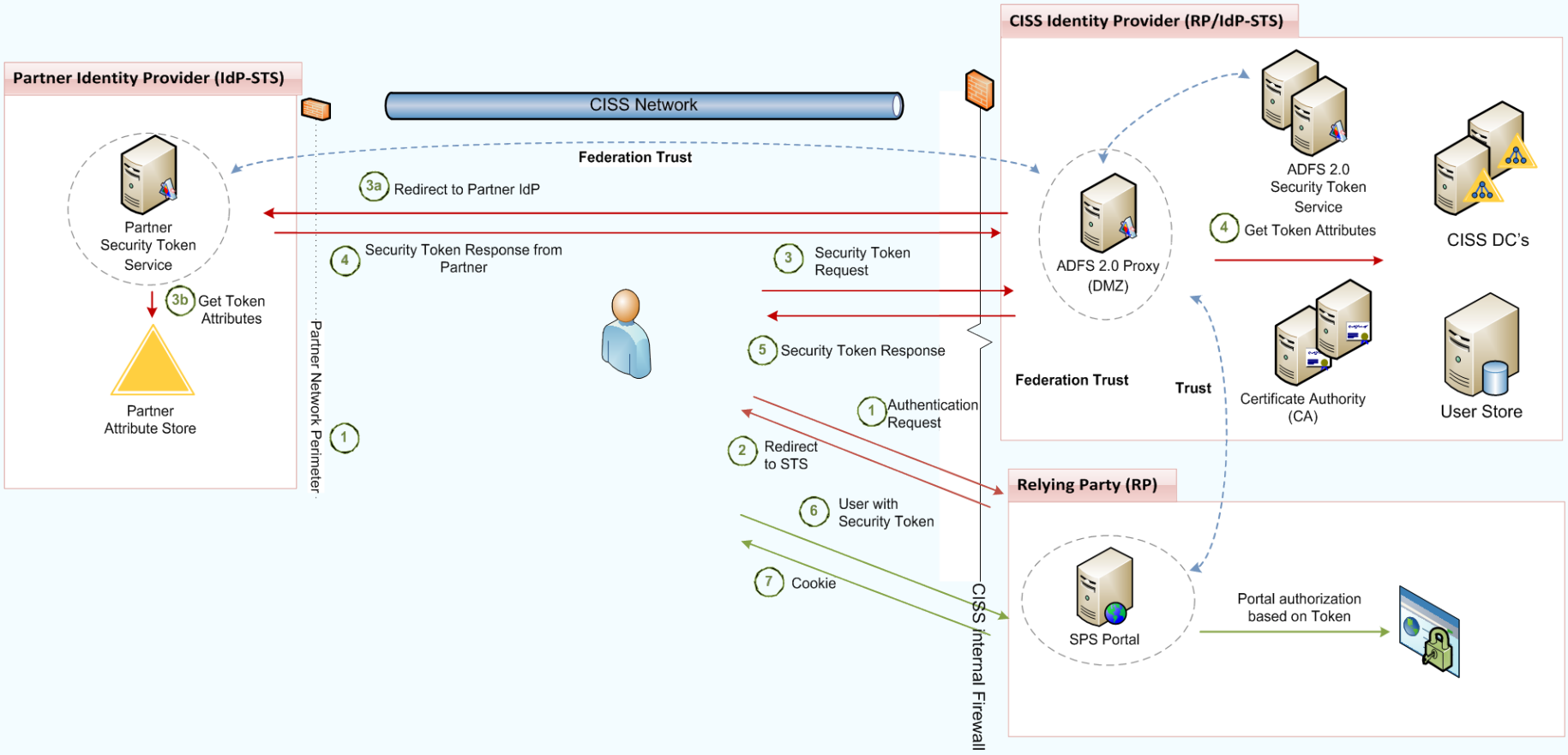
- The Security Token Service (STS) component of AD FS 2.0 issues and consumes tokens that contain claims about authenticated users. A STS can be configured to act as a claims provider or in a relying party role.
- In the three models, both model 1 and 2 share the same AD FS instance with slight differences in the page that is shown to the user based on selected entry option. Model 3 would have its own AD FS and ADFS in that model will host its own STS to authenticate end users.
- A claims provider is a STS that processes requests for trusted identity claims. A federation server processes requests to issue, manage, and validate security tokens. Security tokens consist of a collection of identity claims about the user, such as a user's name, ORI, and other credentials. A federation server can issue tokens in various formats, such as the Security Assertions Markup Language (SAML). In addition, a federation server can protect the contents of security tokens in transit with an X.509 certificate, which makes it possible to validate trusted issuers.

Global Federated Identity and Privilege Management (GFIPM)

Global Federated Identity and Privilege Management (GFIPM) (gee-fip-um)

- AD FS 2.0 will leverage industry-standard metadata formats such as GFIPM for encoding user claims. GFIPM enables information sharing for state and local agencies through a federated model that is secure, scalable, and cost-effective. At the core of GFIPM is the GFIPM metadata standard which defines a collection of information attributes (claims) about users and the mechanism for sharing them with systems and applications in a trusted manner. For more information on GFIPM, go to http://www.gfipm.net/.
- CISS will implement GFIPM attributes in a SAML 1.1 claim token provided to SharePoint. ADFS will implement the capability to provide a GFIPM claim token provided to any endpoint that requests such a token.
- Using Active Directory Federation Services (AD FS 2.0), the CISS will be constructed as shown below:

Active Directory Federation Services



Minimum GFIPM attributes

The Following are the minimum GFIPM attributes required for the CISS Federation:

- First Name (gfipm:2.0:user:GivenName) – The first name of the user
- Last Name (gfipm:2.0:user:SurName) – The last name of the user
- Federation ID (gfipm:2.0:user:FederationId) – The unique identifier of the user within the CISS Federation
- Telephone Number(gfipm:2.0:user:TelephoneNumber) – The telephone number for a telecommunication device by which the user may be contacted.
- Email Address (gfipm:2.0:user:EmailAddressText) – The email address of the user.
- Employer Name (gfipm:2.0:user:EmployerName) – The name of the organization that is the user's primary employer
- Employer ORI (gfipm:2.0:user:EmployerORI) – Unique identifiers assigned to the organization or agency to which the user is assigned. Users who are assigned to multiple agencies will include additional Assignment Agency ORI attributes (gfipm:2.0:user:AssignmentAgencyORI)
- Identity Provider ID (gfipm:2.0:user:identityProviderId) – The unique identifier within the federation that identifies the identity provider (IdP) of the user within the federation.
- Local Id (gfipm:2.0:user:LocalId) – The unique local identifier (Windows account) associated with the user for internal purposes within the user's identity provider (IdP).

Certificates

Public Key X.509 Certificates play a critical role in securing this solution. The two main categories or use are:

- Securing communications channels and
- Providing authentication, mostly for two-factor authentication.

In the case of securing communications between federation servers, federation server proxies, claims-aware applications, and web-based clients, the requirements for certificates vary depending on whether the machine is serving as a federation server or proxy server. The following certificates are required for the ADFS installation:

- Token-Signing Certificate
- Token-Encryption Certificate
- AD FS 2.0 Service communication certificate (for SSL)

The second use of certificates is to provide a second authentication mechanism. In Windows, this can either be at logon (username, smartcard and PIN) or for application authentication by requiring a username and PIN (and optionally a smartcard) during web site access. In the case of OS logon, the policy and infrastructure is pushed out using AD policy automatically. In the case of application authentication, this policy is pushed to the web servers, and the policy is then enforced automatically.

There are three options for creating certificates.

- Self-signed certificates
- Certificates issues using AD Certificate Services (AD CS)
- Third Party Certificate provider

Attribute Store

AD FS 2.0 requires at least one attribute store for authenticating users and maintaining security claims. By default, AD FS 2.0 creates an Active Directory attribute store. For this project the attribute store will be stored in SQL server and kept up to date via FIM (Forefront Identity Management) that will keep both the attribute store and SharePoint's UPS up to date. The attribute store can be managed via SharePoint BCS service by exposing the data as Lists and maintained by administrators with access.

AD FS 2.0 uses the term "attribute stores" to refer to directories or databases that an organization uses to store its user accounts and their associated attribute values. Once configured in an identity provider organization, AD FS 2.0 retrieves attribute values from the store to create a security token. This token enables a Web application or service that is hosted in a relying party organization to make the appropriate authorization decisions whenever a federated user (a user whose account is stored in the identity provider organization) attempts to access the application or service.

Supported Protocols & Token Formats

ADFS 2.0 is an enterprise-ready federation and single sign-on solution that supports both active (WS-Trust) and passive (WS-Federation and SAML 2.0) scenarios. The Security Token Service (STS) in AD FS 2.0 can issue security tokens to the caller using various protocols including WS-Trust, WS-Federation and SAML 2.0. The AD FS 2.0 STS also supports both SAML 1.1 and SAML 2.0 token format.

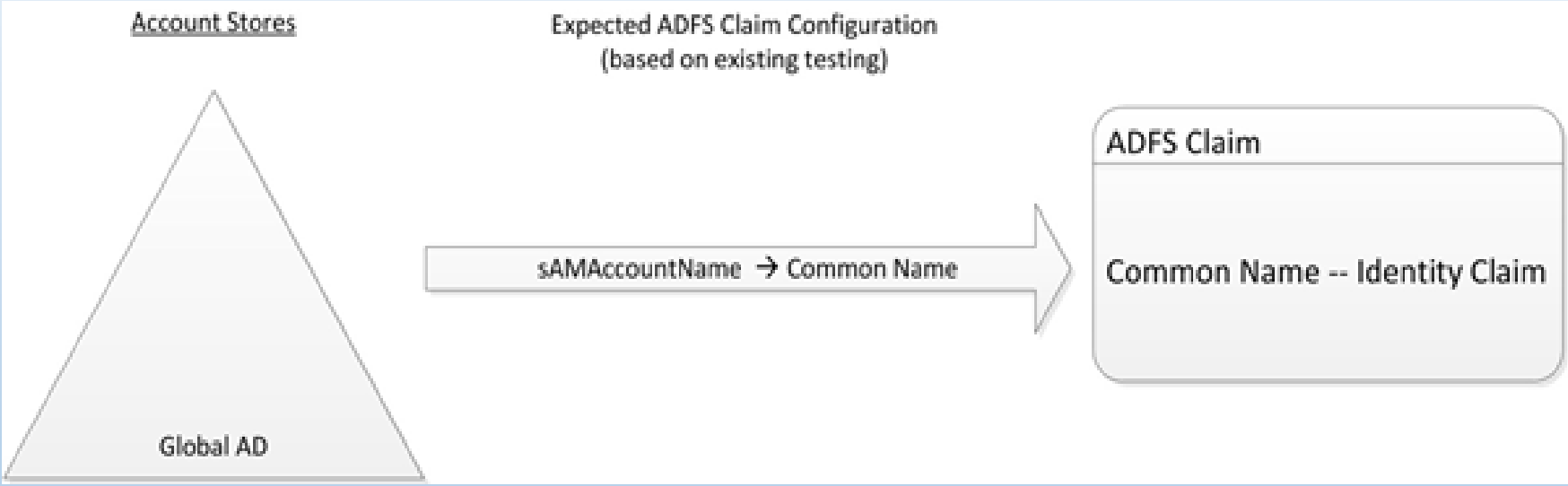
Conceptually, WS-Federation and the SAML protocol are similar even though they have different wire representations. The WS-Federation wire format is closely related to WS-Trust protocol and is suitable for serving both active and passive (browser-based) clients. The SAML protocol has better interoperability across different vendors. AD FS 2.0 natively supports both of these protocols. Within CISS, the AD FS 2.0 federation implementation uses WS-Federation with SAML 1.1 token formats as SharePoint natively understands these formats. It is recommended that internal relying parties use this protocol and token format. The SAML 1.1 token format will leverage claims-based on the GFIPM Metadata Specification. For external federation trust, GFIPM 2.0 attributes and SAML 2.0 token format will be leveraged. ADFS 2.0 will provide the required transformation of the SAML 2.0 token format to SAML 1.1 in order for SharePoint to consume those claims.

The WS-Federationws-Federation 1.1 token will contain URI GFIPM token attributes that match the GFIPM 2.0 URN Token attributes. That way the components that are developed will use the same named attributes regardless of the token format.

Federated Trusts & Claims Rules

An Identity Provider Trust between CISS and other agencies will be established when an agency wants to manage their own users within their own domain. Under this model, external agencies will be required to install, setup, configure and manage their own AD FS server which is in turn trusted by CISS. A setup and configuration document will be provided as a template to allow an agency to implement their own Model 3 scenario.

For each Federated Trust within an organization, claims rules can be used to control the flow of claims from attribute stores or other sources to the Security Token Service at the receiving end of the Federated Trust.



Federated Trusts & Claims Rules

Claims Configuration

Claims rules can be used in one or more of the following scenarios:

- To retrieve data values from an attribute store and make them part of an outgoing claim.
- To transform an incoming claim type or value to an outgoing claim type or value.
- To pass-through an incoming claim as an outgoing claim.

To allow for more complex logic to form a new claim or transform an existing claim (Custom Rules). Custom Rules are based on the Claim Rule Language. For more information, refer to the following: http://technet.microsoft.com/en-us/library/dd807118%28WS.10%29.aspx.

Data Security & Trimming

Through the use of claims-based security and standardized token formats, the CISS security solution allows for filtering and trimming of sensitive data throughout all tiers of the application. All application services within CISS require a valid, trusted security token and, consequently, these application services have full access to the security claims and metadata describing the user or system making the request. This information can be used to perform security trimming of sensitive data as part of the search and publishing processes.

Detailed data security requirements and policies have been formalized yet continue to be a point of discussion between Xerox and the CISS team.

Record Security

FAST Search provides record-level filtering of search results by integrating with the SharePoint security model. Security descriptors and access control information are indexed as part of the crawling process. Upon performing a search, the security claims included in a user's token are compared to the security metadata stored in the search index to determine which records are included in search results. In this way, entire records or groups of records can be restricted from appearing in search results based on the security claims of an individual user. Note that this is a native feature of SharePoint and FAST Search.

Because security metadata is part of the search index, this type of security trimming does not add any significant performance overhead to the search experience. Additionally, features such as refiners, sorting, and saved searches apply security trimming uniformly and accurately throughout the application.

Search Engine

Individual data elements may be filtered from the search results based on a user's security claims. That is, there may be records that the user is permitted to view, but specific data elements of those records that must be hidden.

In practice, this is typically implemented as a custom software component responsible for converting a user's token and a security policy into a dynamically-generated style sheet. Using the security claims, this style sheet is able to show and/or hide individual fields of search results from the user interface (note that these style sheets are generated and applied on the server).

Similarly, a custom software component can be created to hide specific search fields (on the advanced search form) based on a user's security claims. This would be implemented as an extension to the advanced search SharePoint web part and execute server-side before being displayed to the user.

Finally, custom search request processing can be implemented within the FAST query engine to ensure that carefully-crafted search strings (entered by the user) do not expose sensitive information. This is accomplished by internally adjusting the user-entered query parameters before executing the search. In this manner the system is secured against client-side URL, form, and other HTTP-related tampering.

Detail Information View

This type of security trimming is implemented at the service-provider level (i.e. within the ESB process that generates detailed responses). Because this service requires the caller to present a trusted and valid security token, the ESB process is able to make filtering decisions based on a user's security claims. Furthermore, since the ESB process is the only mechanism to retrieve a detailed response, policy enforcement is centralized for all CISS client components (e.g. portal or external systems).

As an example, a rule may be included that requires a specific claim to see the name and date of birth on a record when the individual is a juvenile. By filtering at the service layer, the ESB provides a centralized policy enforcement point and only returns those data elements that a user is permitted to see. In this case, the name and date of birth would not be returned to the user interface unless the user had an appropriate set of security claims.

Policy Definition and Enforcement

There are several methods for defining, maintaining, and applying data security policies, for instance:

- Defining and enforcing rules directly inside code
- Use of a shared database or configuration file for storing rules
- Centralized policy enforcement points
- Shared libraries or code implementing policy enforcement
- Standards-based policy definitions such as eXtensible Access Control Markup Language (XACML)

Each of these approaches includes varying degrees of effort, performance tradeoffs, maintenance concerns, and training requirements. For instance, ad-hoc rules implemented in custom code are easy to create, yet difficult to maintain. Centralized policy enforcement services include the overhead of a web service call for every single policy decision. Standards such as XACML can be difficult to learn for developers and administrators. Ultimately, the chosen solution must balance these factors to minimize policy maintenance costs while meeting requirements for security and performance.

Active Directory Federation Services (ADFS)

AD FS is an identity access solution that provides browser-based clients (internal or external to your network) with seamless, "one prompt" access to one or more protected Internet-facing applications, even when the user accounts and applications are located in different networks or organizations.

When an application and user accounts are in different networks, it is typical for users to encounter prompts for secondary credentials when they attempt to access the application. These secondary credentials represent the identity of the users in the realm in which the application resides. The web server that hosts the application usually requires these credentials so that it can make the most appropriate authorization decision.

AD FS provides federated trust relationships that you can use to project a user's digital identity and access rights to trusted partners, thus making secondary accounts and their credentials unnecessary. In a federated environment, each organization continues to manage its own identities, but each organization can also securely project and accept identities from other organizations.

Active Directory Federation Services (ADFS) cont'd.

Furthermore, you can deploy federation servers in multiple organizations to facilitate business-to-business (B2B) transactions between trusted partner organizations. Federated B2B partnerships identify business partners as one of the following types of organization:

- **Resource organization:** Organizations that own and manage resources that are accessible from the Internet can deploy AD FS federation servers and AD FS-enabled web servers that manage access to protected resources for trusted partners. These trusted partners can include external third parties, or other departments or subsidiaries that are in the same organization.
- **Account organization:** Organizations that own and manage user accounts can deploy AD FS federation servers that authenticate local users, and create security tokens that federation servers in the resource organization can use later to make authorization decisions.

Feedback

We need your feedback —

please send us your comments, questions & suggestions.

Sean Thakkar — Sean.Thakkar@ct.gov

Mark Tezaris — Mark.Tezaris@ct.gov

Rick Ladendecker — Rick.Ladendecker@ct.gov

Nance McCauley — Nance.McCauley@ct.gov

Thank you.