Technical Brief October 2017

SEARCH
The National Consortium for Justice Information and Statistics

Tips and Tricks

Implementing the Global Federated Identity and Privilege Management Framework in Microsoft's Active Directory Federation Services

By James Douglas and Michael Jacobson
Information Sharing Specialists
SEARCH

Introduction

This *Technical Brief* provides guidance and "tips and tricks" justice stakeholders can use to implement the Global Federated Identity and Privilege Management (GFIPM)[1] framework using Microsoft's Active Directory Federation Services (AD FS)[2] as an identity provider. This guidance is based on actual implementations of GFIPM on Microsoft Windows Server 2012, and it addresses the following: differences in nomenclature used in GFIPM and by Microsoft, how to configure AD FS to enable GFIPM, and how to manage digital certificates when implementing GFIPM in a Microsoft AD FS environment.

Overview of GFIPM

GFIPM is the national justice standard for cryptographically-secure federated identity management and secure single sign-on. It is based on the Security Assertion Markup Language (SAML) 2.0 specification[3] and was developed by the Global Advisory Committee.[4] GFIPM provides justice organizations a means to establish the trust required to share information and reduces the burden of user management.

[1] The GFIPM framework provides the justice community and partner organizations with a standards-based approach to implement federated identity. https://it.ojp.gov/initiatives/gfipm

[2] Microsoft developed AD FS for Windows Server operating systems to provide users with single sign-on access to systems and applications located across organizational boundaries. https://en.wikipedia.org/wiki/Active_Directory_Federation_Services

[3] Security Assertion Markup Language is an XML-based open standard used to exchange authentication and authorization messages between federation partners. https://en.wikipedia.org/wiki/Security_Assertion_Markup_Language

[4] https://it.ojp.gov/global/gac-membership

Four vital components within GFIPM enable users to securely interact with multiple federation resources:

- **Assertions:** GFIPM is based on the industry standard, SAML, which is an XML-based language that provides a set of protocols and profiles to identify users.
- **Identity Providers (IdP):** Identity providers are the authoritative entity responsible for authenticating end users and creating the assertion used throughout the session to identify the user to trusted partners in a federation. The IdP is responsible for verifying identities, creating accounts, managing passwords and credentials, general account management, and creating the GFIPM assertion. Products like Microsoft's AD FS or an open source tool such as Shibboleth's Identity Provider[5] enable SAML and, therefore, GFIPM conformance.
- **Service Providers (SP):** Service providers share resources with trusted partners. The SP relies on the assertion created for the user by the IdP to make access control and dissemination decisions based on the attributes contained in the assertion.
- **Cryptographic Trust Fabric (CTF):** The CTF defines the security context of the federation. This serves as a roster of the trusted entities (i.e., identity and service providers) within the federation, including the digital certificates used by the entities to sign and encrypt messages.

GFIPM uses SAML assertions produced by the IdP to provide the SP with facts about a user. The SP can then make authorization and access control decisions based on the assertion. Figure 1 illustrates a common scenario for GFIPM in a justice information exchange.

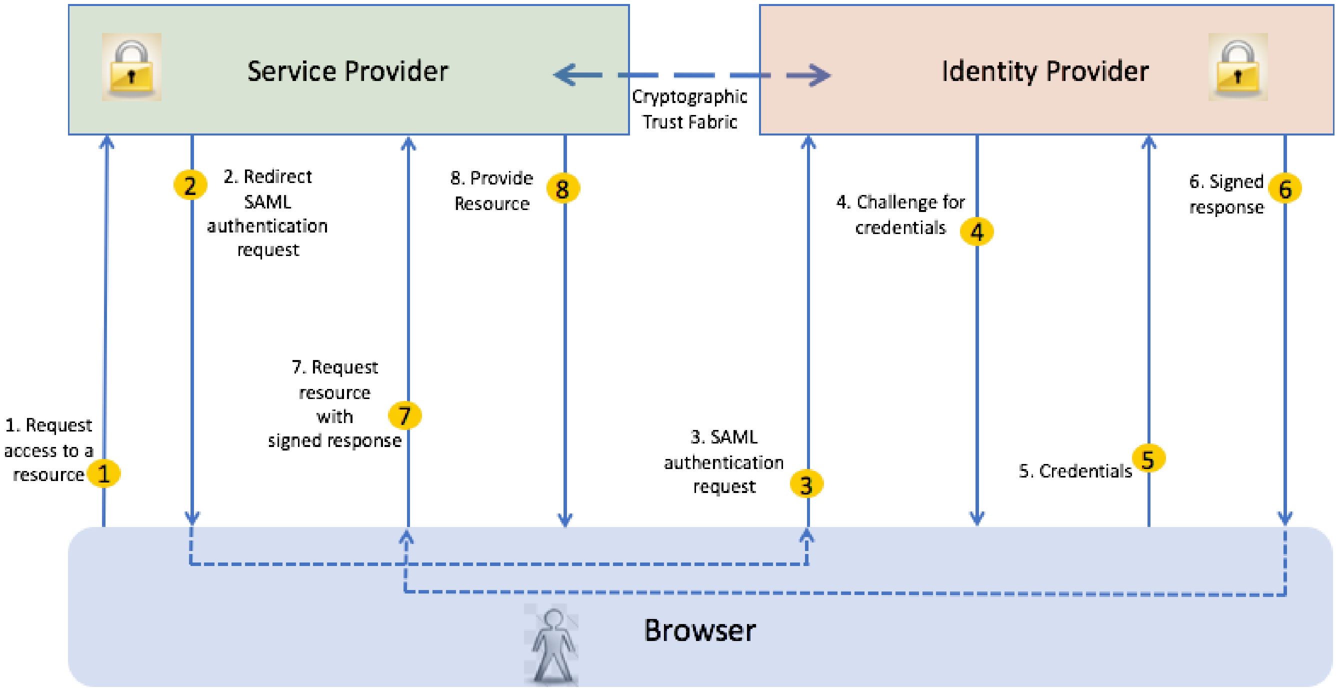

Service Provider
Identity Provider
Cryptographic Trust Fabric
1. Request access to a resource 1
2 2. Redirect SAML authentication request
3. SAML authentication request 3
4. Challenge for credentials 4
5. Credentials 5
6. Signed response 6
7. Request resource with signed response 7
8. Provide Resource 8
Browser

Figure 1: GFIPM components in a typical justice information exchange

[5] https://www.shibboleth.net/products/identity-provider/

The following steps, as illustrated in Figure 1, outline a user-to-system interaction:

1. Using a browser, the user requests access to a federation resource secured by an SP. Typically, the first resource is a federation web page or web application.
2. The SP redirects the user authentication request to the IdP.
3. The IdP receives the user authentication request.
4. The IdP challenges the user for credentials.
5. The user is authenticated on the IdP.
6. The IdP provides the SP with a signed response — the SAML assertion.
7. The SP receives the SAML assertion.
8. Based on the values of the attributes in the response, the SP decides whether to allow the user access the requested resource, in this example, the federation web site.

From this point forward and throughout the current session, the assertion provides access to other federation resources, such as a criminal history query.

A significant benefit of GFIPM is that it creates a single sign-on environment where users do not have to maintain separate credentials to access other federation resources. Rather, the assertion is trusted by the resources and provides sufficient information to each resource to make individual authorization and access control decisions.

Tips to Make it Easier to Implement an AD FS IdP

Microsoft's AD FS employs SAML and, therefore, can conform to GFIPM. However, it can be challenging to configure AD FS to implement GFIPM in an environment with a mix of Microsoft and open source IdPs. Below are three tips to help make implementing an AD FS IdP in an environment with both Microsoft and open source components a little easier.

1. Nomenclature Differences

Microsoft uses its own nomenclature to describe the components defined in GFIPM. For the most part, GFIPM uses SAML terms as defined in the OASIS standard.[6] However, these naming differences may cause some confusion for administrators that use AD FS to implement GFIPM. Microsoft AD FS uses the following key terms, which differ from those used in GFIPM:

This GFIPM component term:		***…is called this in AD FS:***
Identity Provider (IdP)		**Claims Provider** (CP)
Service Provider (SP)	➡	**Relying Party** (RP)
GFIPM metadata **attributes**		GFIPM metadata **claims**

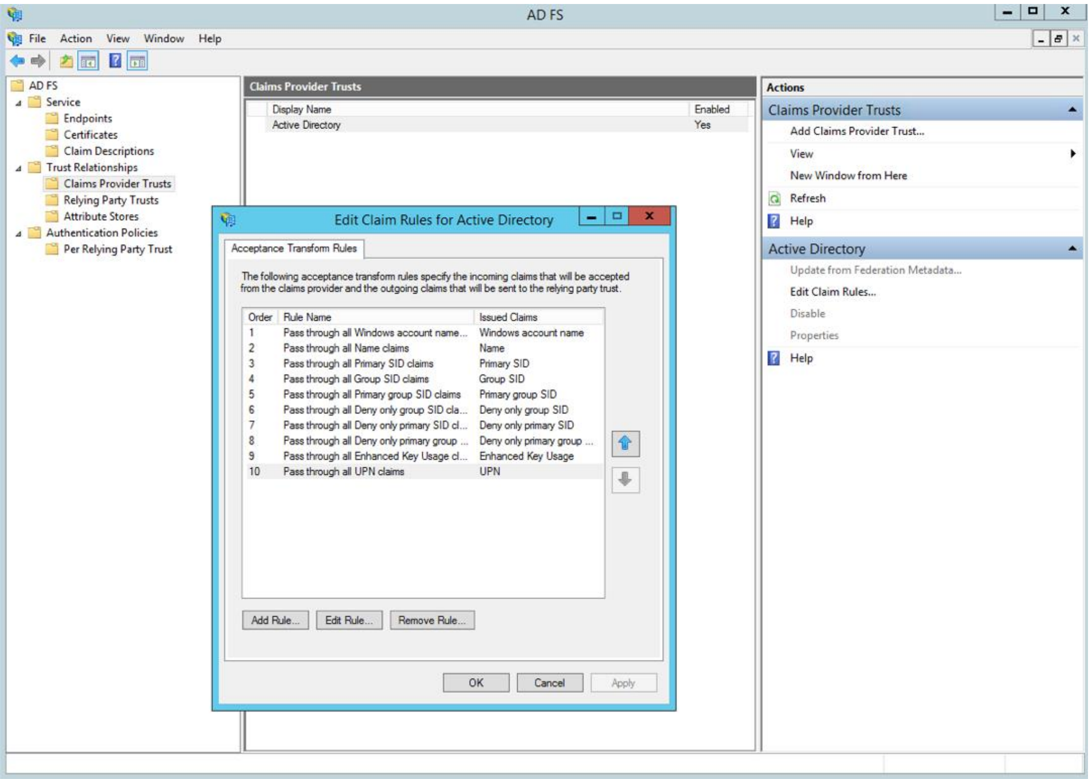
Both Microsoft and GFIPM provide comprehensive terminology definitions:

- Microsoft: https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/technical-reference/understanding-key-ad-fs-concepts
- GFIPM: https://www.it.ojp.gov/GIST/78/Federated-Identity-and-Privilege-Management--GFIPM---Terminology-Matrix

[6] Glossary for the OASIS SAML v2.0. https://www.oasis-open.org/committees/download.php/21111/saml-glossary-2.0-os.html

2. *Configuring AD FS to enable GFIPM*

When configuring AD FS as a GFIPM IdP, the administrator sets claim rules as established by the federation that are used when creating the SAML assertion. Microsoft provides some claim rules in a set of templates included in AD FS, and also provides a graphical user interface (GUI) tool to help administrators edit or develop new claims rules. Figure 2 shows the AD FS configuration tool and how to edit or add rules.



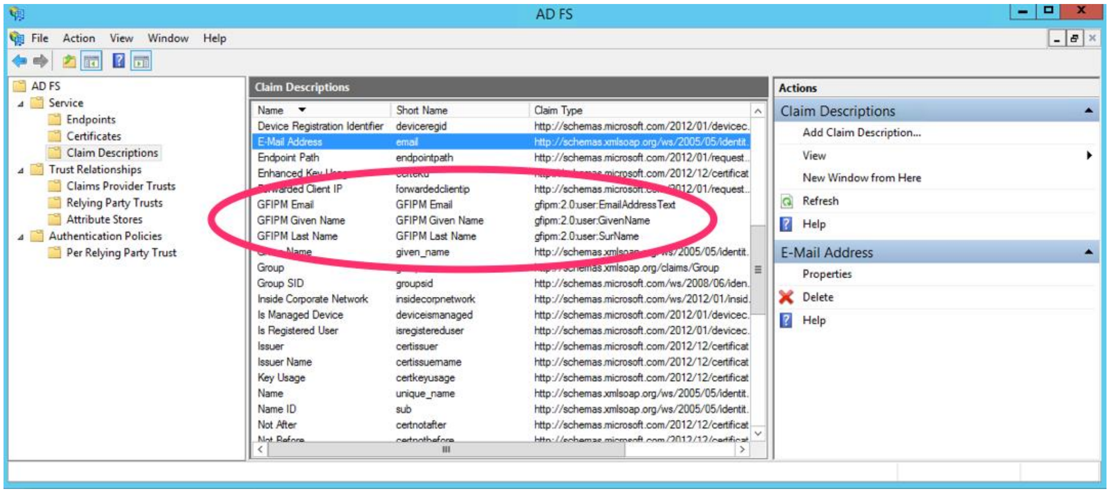
Display Name	Enabled
Active Directory	Yes

The following acceptance transform rules specify the incoming claims that will be accepted from the claims provider and the outgoing claims that will be sent to the relying party trust.

Order	Rule Name	Issued Claims
1	Pass through all Windows account name...	Windows account name
2	Pass through all Name claims	Name
3	Pass through all Primary SID claims	Primary SID
4	Pass through all Group SID claims	Group SID
5	Pass through all Primary group SID claims	Primary group SID
6	Pass through all Deny only group SID cla...	Deny only group SID
7	Pass through all Deny only primary SID cl...	Deny only primary SID
8	Pass through all Deny only primary group ...	Deny only primary group ...
9	Pass through all Enhanced Key Usage cl...	Enhanced Key Usage
10	Pass through all UPN claims	UPN

Figure 2: Microsoft AD FS Configuration Tool

When administrators establish claim rules in AD FS, they can add GFIPM-specific attributes as new claims to be included in the SAML assertion. Figure 3 shows where to make these changes.



Name	Short Name	Claim Type
Device Registration Identifier	deviceregid	http://schemas.microsoft.com/2012/01/devicec.
E-Mail Address	email	http://schemas.xmlsoap.org/ws/2005/05/identit.
Endpoint Path	endpointpath	http://schemas.microsoft.com/2012/01/request.
Enhanced Key Usage	certeku	http://schemas.microsoft.com/2012/12/certificat
Forwarded Client IP	forwardedclientip	http://schemas.microsoft.com/2012/01/request.
GFIPM Email	GFIPM Email	gfipm:2.0:user:EmailAddressText
GFIPM Given Name	GFIPM Given Name	gfipm:2.0:user:GivenName
GFIPM Last Name	GFIPM Last Name	gfipm:2.0:user:SurName
Given Name	given_name	http://schemas.xmlsoap.org/ws/2005/05/identit.
Group	[illegible]	http://schemas.xmlsoap.org/claims/Group
Group SID	groupsid	http://schemas.microsoft.com/ws/2008/06/iden.
Inside Corporate Network	insidecorpnetwork	http://schemas.microsoft.com/ws/2012/01/insid.
Is Managed Device	deviceismanaged	http://schemas.microsoft.com/2012/01/devicec.
Is Registered User	isregistereduser	http://schemas.microsoft.com/2012/01/devicec.
Issuer	certissuer	http://schemas.microsoft.com/2012/12/certificat
Issuer Name	certissuername	http://schemas.microsoft.com/2012/12/certificat
Key Usage	certkeyusage	http://schemas.microsoft.com/2012/12/certificat
Name	unique_name	http://schemas.xmlsoap.org/ws/2005/05/identit.
Name ID	sub	http://schemas.xmlsoap.org/ws/2005/05/identit.
Not After	certnotafter	http://schemas.microsoft.com/2012/12/certificat
Not Before	certnotbefore	http://schemas.microsoft.com/2012/12/certificat

Figure 3: Where to add GFIPM-specific attributes as new claims in AD FS

3. Managing Digital Certificates

GFIPM implementations require justice organizations to create a Cryptographic Trust Fabric (CTF) that defines the security context of the federation, which is comprised of the trusted IdPs, SPs, and other endpoints within the federation. The CTF provides the foundation for secure communications. By having the message sender digitally sign the message, the recipient can authenticate that the sender is a member of the federation and verify that the message has not been tampered with or altered. Additionally, the use of digital certificates allows messages to be encrypted and ensures that only the intended recipient can decipher the message and gain access to any confidential information it may contain. Administrators can purchase digitally signed certificates commercially or create them independently. Within GFIPM, there is no requirement to use commercial digital certificates; self-signed digital certificates are perfectly suitable for this purpose. There are many tools available to generate self-signed certificates for federation members.

Implementing the certificates on the Windows server requires the administrator to run the import wizard and be familiar with how Windows organizes its security items. Administrators must ensure that they are applying the certificate to the correct machine in the correct domain.

One consideration when using certificates is the requirement to renew the certificates before they expire, which would prevent users from accessing resources over time. Microsoft has addressed this issue by offering a feature that ensures AD FS always uses a valid signing certificate. This service is called AD FS Auto Certificate Rollover (ACR). The ACR service detects when a signing certificate is nearing expiration, then it creates a new certificate and deletes the old one. Within a federation, this feature can create problems because service providers are not informed of the certificate change. The SP will start to receive SAML assertions that are signed by an untrusted certificate, resulting in blocked access. The solution is as follows:

- The administrator configures AD FS to create a new certificate several days before the current certificate is due to expire and has AD FS set this new certificate as the “secondary signing certificate.”(This is an AD FS concept, but translates nicely to SAML because SAML metadata can contain multiple signing certificates for an IdP.)
- This gives the AD FS administrator time to notify the federation members that a new certificate was created. In turn, this allows federation members to update the SAML metadata and trust stores to include this new certificate, while keeping the current one active.
- Prior to expiration of the current certificate, AD FS will assign the new certificate as the “primary signing certificate,” which should have no downstream impacts because enough time was allowed for federation members to update their SAML metadata and trust stores within the CTF.
- After the new certificate is enabled, federation members can remove the old/expired one from the CTF.

Conclusion

Microsoft’s Active Directory is a commonly used identity management product that has the ability to authenticate users for secure access to distributed services. This is possible via Active Directory Federation Services (AD FS), the SAML implementation for Active Directory. Users can easily incorporate AD FS into a GFIPM federated environment where other identity management tools and products are used. This brief outlines some considerations when using AD FS that further simplify this integration.

Microsoft AD FS provides step-by-step wizards to assist network administrators to configure AD FS to provide single sign-on that improves usability and privacy and security. The administrator can take advantage of these configuration wizards to include GFIPM attributes in the SAML assertion; however, the administrator needs to be aware of the different terms used to describe the IdPs (Claims Provider), SPs (Relying Party), and attributes (claims).

The GFIPM CTF requires digital certificates to ensure secure communications. There are several tools to establish and maintain certificates. Administrators need to be diligent to ensure the certificates do not expire, thereby preventing user access to critical information. This brief explains how to take advantage of Microsoft's Auto Certificate Rollover (ACR) capability while still ensuring the continuous availability of federation resources.

Have a question for the authors? Contact them at jdouglas@search.org or mjacobson@search.org.

This project was supported by Grant No. 2012-DP-BX-K006 awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, the SMART Office, and the Office for Victims of Crime. Points of view or opinions in this document are those of the author and do not represent the official position or policies of the United States Department of Justice.

Mr. Brad Truitt
Chair

Mr. Timothy M. Lott
Interim Executive Director

SEARCH
1900 Point West Way, Suite 275 • Sacramento, CA 95815
(916) 392-2550 • www.search.org