To better serve the needs of multiple independent GFIPM federations, and also to more adequately meet the needs of GFIPM federations that include one or more trusted identity broker (TIB) entities, the following changes have been made to the GFIPM Metadata 2.0 Spec as of January 18, 2011.

1. Change attribute "gfipm:2.0:user:IdentityProviderId" as follows.

   Old Definition:

   > The unique identifier within the federation that identifies the identity provider (IDP) of the user within the federation.

   New Definition:

   > The unique identifier within the federation that identifies the identity provider (IDP) of the user within the federation. Comprises a federation part, an optional trusted identity broker (TIB) part, and an identity provider (IDP) part. The general format of an identity provider ID is: "{Federation}:[TIB:{TIB}:]IDP:{IDP}".
   >
   > {Federation} is required, and is a globally unique federation identifier. It must contain only alphanumeric characters and dashes. Federation identifiers are managed via the GFIPM Federation Name Registry. Information about this registry is available at the following URL.
   >
   > http://gfipm.net/fed-registry.html
   >
   > "TIB" and {TIB} are required only for identity providers that are brokered by a trusted identity broker. {TIB} must uniquely identify a trusted identity broker within the federation. It must contain only alphanumeric characters and dashes.
   >
   > "IDP" and {IDP} are required. If preceded by a TIB part, {IDP} must uniquely identify an identity provider that is brokered by the TIB within the federation. If not preceded by a TIB identifier, {IDP} must uniquely identify an identity provider that is NOT brokered by a TIB within the federation. {IDP} must contain only alphanumeric characters and dashes.

   Old Usage Information:

   > This identifier MUST be equal to the value of the "Entity Id" attribute used by the IDP within the federation's cryptographic trust fabric, and MUST be consistent with the IDP ID denoted within the user's

FederationId attribute. The general format of an identity provider ID is: “GFIPM:IDP:{Unique IDP String}”.

New Usage Information:

This identifier MUST be consistent with the federation identifier, IDP identifier, and (if applicable) TIB identifier denoted within the user's FederationId attribute.

Old Example Content:

“GFIPM:IDP:JNET”

New Example Content:

“NIEF:IDP:JNET”,
“DOJTB:IDP:RISS”,
“NIEF:TIB:CJIS-Portal:IDP:RISS”,
“CONNECT:IDP:XYZ”

2. Change attribute “gfipm:2.0:user:FederationId” as follows.

Old Definition:

The persistent, federation-unique identifier for the user, comprising a federation part and a local part. The federation part includes the federation name and the name of the user's identity provider (IDP). The namespace for IDP names is governed by the federation. The local part is in a format specified by the IDP. All parts of the identifier are delimited by colons. The general format of a federation ID for a user is: “GFIPM:IDP:{Unique IDP String}:USER:{IDP-Unique User ID}”.

New Definition:

The persistent, federation-unique identifier for the user, comprising a federation part, an optional trusted identity broker (TIB) part, an identity provider (IDP) part, and a local ID. All parts of the identifier are delimited by colons. The general format of a federation ID for a user is: “{Federation}:[TIB:{TIB}:]IDP:{IDP}:USER:{User ID}”.

{Federation} is required, and is a globally unique federation identifier. It must contain only alphanumeric characters and dashes. Federation identifiers are managed via the GFIPM Federation Name Registry. Information about this registry is available at the following URL.

http://gfipm.net/fed-registry.html

"TIB" and {TIB} are required only for identities asserted by trusted identity brokers. {TIB} must uniquely identify a trusted identity broker within the federation. It must contain only alphanumeric characters and dashes.

"IDP" and {IDP} are required. If preceded by a TIB part, {IDP} must uniquely identify an identity provider that is brokered by the TIB within the federation. If not preceded by a TIB identifier, {IDP} must uniquely identify an identity provider that is NOT brokered by a TIB within the federation. {IDP} must contain only alphanumeric characters and dashes.

"USER" and {User ID} are required, and must uniquely identify a user from the identity provider indicated in the IDP part. The format of {User ID} is undefined, and is intended to match the format in which the IDP stores local user IDs. Typical format choices may include email address or X.509 common name.

Old Example Content:

"GFIPM:IDP:JNET:USER:johndoe@jnet.net"

New Example Content:

"DOJTB:IDP:XYZ:USER:johndoe@example.org",
"NIEF:IDP:RISS:USER:riss.user@rissnet.net",
"NIEF:TIB:CJIS-Portal:IDP:RISS:USER:riss.user@rissnet.net",
"CONNECT:IDP:XYZ12:USER:johndoe99"

3. Change attribute "gfipm:2.0:entity:EntityId" as follows.

Old Definition:

The federation-unique identifier by which the entity is denoted, comprising a federation type identifier ("GFIPM"), a technical role identifier (e.g. "IDP", "SP", etc.), and a 3rd-level identifier denoting the unique ID of the entity within the scope of the other identifiers. All parts of the identifier are delimited by colons. The general format of an entity ID is: "GFIPM:{Technical Role}:{Unique Identifier}".

New Definition:

The unique identifier by which the entity is denoted, comprising a federation part, a technical role identifier (e.g. "IDP", "SP", "TIB", etc.), and a 3rd-level identifier denoting the unique ID of the entity within the scope of the other identifiers. All parts of the identifier are required, and they are delimited by colons. The general format of an entity ID is: "{Federation}:{Technical Role}:{Unique Entity ID}". {Federation} and {Unique Entity ID} must contain only alphanumeric characters and dashes. Federation identifiers are managed via the GFIPM Federation Name Registry. Information about this registry is available at the following URL.

http://gfipm.net/fed-registry.html

Old Example Content:

"GFIPM:IDP:JNET",
"GFIPM:SP:CISA",
"GFIPM:WSP:ARJIS"

New Example Content:

"NIEF:IDP:JNET",
"CONNECT:SP:ABC",
"DOJTB:WSP:123",
"NIEF:TIB:CJIS-Portal"