# After Action Review: UMBC IdP unintentional removal from metadata 2020-07-30

**Date**: 2020-07-31
**Prepared by**: Nic Roy, Internet2 Trust and Identity Services



# Summary


During routine InCommon federation metadata publication on Thursday, July 30, 2020, the metadata for the University of Maryland Baltimore County (UMBC) Identity Provider (IdP) with entityID urn:mace:incommon:umbc.edu was unintentionally removed from metadata. This appears to be due to a defect in the metadata state machine in the InCommon Federation Manager. The issue was identified by UMBC staff on the morning of July 31, 2020, and they

contacted InCommon operations, which forced publication of the IdP and immediately re-signed and re-published metadata.

# Timeline

2020-07-30 14:08:44 EDT Paul Riddle, UMBC InCommon Site Administrator, submits updated metadata for the UMBC IdP with entityID urn:mace:incommon:umbc.edu. The change contains a certificate update, some endpoint updates and an error URL update. The change is auto-approved by the Federation Manager application

2020-07-30 14:08:46 EDT The new copy of the entity descriptor for this IdP is set to “Canceled” state by the FM state machine, which is an incorrect behavior. This is what caused the entity descriptor to drop out of the published InCommon metadata.

2020-07-30 ~14:45:10 EDT Shannon Roddy, the TI L2 on-call person, begins signing metadata per documented procedure.

2020-07-30 15:02:00 EDT Signed metadata is published. The signing process does not show any signs of problems, as would be expected from a normal entity descriptor deletion. Paul Riddle does not receive a confirmation that his IdP has been published.

2020-07-30 16:25:40 EDT UMBC receives first reports that its IdP is not working for federated transactions.

2020-07-31 08:28:00 EDT Paul Riddle contacts the InCommon Security hotline via phone call and leaves a voicemail about the issue. Shannon Roddy, the on-call person, received a transient notification from OpsGenie on his lock screen but the notification disappeared when he looked in the app.

2020-07-31 08:32:00 EDT Paul Riddle contacts Bill Kaufman on Internet2’s Slack instance about the issue. Bill Kaufman posts in the #ti-operations channel to get in contact with the on-call person.

2020-07-31 08:36:00 EDT Shannon Roddy logs into FM to begin triaging the issue.

2020-07-31 08:50:00 EDT Shannon Roddy tries to retrieve the voicemail from OpsGenie.

2020-07-31 09:08:00 EDT The entire L2 ops team is notified by OpsGenie of the alert. Nic Roy responds, acks the alert, listens to the voicemail and calls Paul Riddle. Nic looks at the FM RA interface and sees that the entity descriptor for the UMBC IdP is in an auto-approved but

unpublished state. Nic clicks the “Publish” button in the FM RA interface and begins signing metadata.

2020-07-31 09:21:00 EDT Nic Roy notifies the #ti-operations channel of the status of his work on the issue and starts to catch up with the thread between Bill and Shannon.

2020-07-31 09:32:00 EDT Signing and publication of metadata completes. Nic reports this in the #inc-ops-ra-hotline channel and the #ti-operations channel. Nic confirms with Paul Riddle that the IdP is back in metadata. Nic and Shannon discuss approach to forensics to determine root cause. Nic closes the issue in OpsGenie.

2020-07-31 11:00:00 EDT The FM development team meets and discusses the issue and investigates root cause. More information on this below.

# Scope/impact of the outage

Single sign-on to several federated services at UMBC was impacted, with some displaying an “Unknown or unusable identity provider” message. Some providers were unaffected, as the outage was under 24 hours, and staff at UMBC, working with InCommon, caught and remediated the issue before those SPs updated their copy of metadata.

Once the entity descriptor was restored to the InCommon metadata aggregate, staff at UMBC contacted two or three vendors and requested that they manually reload the InCommon metadata, which restored service. Service to most frequently-used providers was restored by around 10:00am EDT on 2020-07-31.

# Results of the investigation

The FM development team investigated the issue but reproduction is impossible with the information at hand. From the audit records available in the Federation Manager (included as Appendix A and B) it appears that the issue was caused by a timing or connectivity issue within the Federation Manager during creation of a new instance of the updated UMBC IdP entity descriptor. The development team believes it can introduce tests within the codebase to check that the actions that should be taken during this process actually are taken each time the process executes, and raise an error if things do not work correctly. The entity update code is complex and the dev team has been reluctant to change it much, if at all, due to the complexity and relative lack of understanding of the process.

Recommendations:

1) Introduce checks in the /siteadmin/ops process which generates unsigned aggregates, to warn the person generating unsigned aggregates that there are problems with expected versus actual numbers of metadata cancellations/etc.
2) Update the metadata signing procedure to require L2 on-call staff to check the metadata approval queue and list of recently published metadata both before and after signing, to ensure there are no “dangling” approved entity descriptors in an unpublished state after signing.
3) Revisit the FM code which cancels old entity descriptors when entity descriptors are approved or auto-approved, to ensure that the cancellation only happens if the new copy of the entity descriptor was successfully created and put in a pending publication state.
4) Longer-term, as part of the work to automate metadata publication, refactor how FM stores metadata to reduce the complexity of the state machine, and how much of the state machine/metadata maintenance code actually has to reside within the FM application. It may make sense to check individual entity descriptors into GitHub Enterprise, tag them with various state tags, and use post-commit hooks to generate metadata signing/publication events on a message bus.
5) Revisit OpsGenie as an alerting platform, since it continues to fail to alert staff in a reliable way.

# Appendix A: FM Status Records (18 month retention period) for urn:mace:incommon:umbc.edu

## Entity Analysis

### Provider Status:

Submitted

2020-07-31 12:21:33 UTC

### Entity 34854

Auto Approved

2020-07-31 12:21:33 UTC

Published

2020-07-31 13:11:28 UTC

### Entity 34851

Auto Approved

2020-07-30 18:08:44 UTC

Canceled

2020-07-30 18:08:46 UTC

### Entity 34782

Auto Approved

2020-07-23 15:44:28 UTC

Published

2020-07-23 18:49:01 UTC

Inactive

2020-07-30 18:08:44 UTC

### Entity 34752

Auto Approved

2020-07-17 21:47:42 UTC

Published

2020-07-20 18:57:34 UTC

Inactive

2020-07-23 15:44:28 UTC

### Entity 33646

Auto Approved

2020-03-27 20:37:17 UTC

Published

2020-03-30 19:25:39 UTC

Inactive

2020-07-17 21:47:42 UTC

### Entity 32514

Approval Pending

2019-11-21 22:33:02 UTC

Publish Pending

2019-11-22 19:39:17 UTC

Published

2019-11-22 20:08:06 UTC

Inactive

2020-03-27 20:37:17 UTC

### Entity 20107

Approval Pending

2017-12-09 17:33:39 UTC

Publish Pending

2017-12-11 19:35:55 UTC

Published

2017-12-11 20:09:16 UTC

Inactive

2019-11-22 19:39:17 UTC

# Appendix B: FM Audit Records for urn:mace:incommon:umbc.edu

| Action | User | Changes | Date |
|---|---|---|---|

| | | | |
|---|---|---|---|
| create | paulr@umbc.edu | • organization_id set to "10032"<br>• entity_name set to "urn:mace:incommon:umbc.edu"<br>• status set to "auto_approved"<br>• metadata set to "<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:shibmd="urn:mace:shibboleth:metadata:1.0" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" entityID="urn:mace:incommon:umbc.edu"> <Extensions xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute" xmlns:mdrpi="urn:oasis:names:tc:SAML:metadata:rpi"> <mdrpi:RegistrationInfo registrati..."<br>• last_submitter_id set to "85"<br>• provider_id set to "19"<br>• provider_type set to "Idp"<br>• federation set to ""<br>• replaced_by_id set to ""<br>• submitted_at set to ""<br>• metadata_preview set to "<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:shibmd="urn:mace:shibboleth:metadata:1.0" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" entityID="urn:mace:incommon:umbc.edu"> <Extensions xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute" xmlns:mdrpi="urn:oasis:names:tc:SAML:metadata:rpi"> <mdrpi:RegistrationInfo registrati..."<br>• metadata_fallback set to "<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:shibmd="urn:mace:shibboleth:metadata:1.0" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" entityID="urn:mace:incommon:umbc.edu"> <Extensions xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute" | 2020-07-31 12:21:33 PM UTC |

| | | | |
|---|---|---|---|
| | | xmlns:mdrpi="urn:oasis:names:tc:SAML:metadata:rpi"> <mdrpi:RegistrationInfo registrati..."<br>• note set to ""<br>• allow_export set to "true"<br>• metadata_export set to "<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:shibmd="urn:mace:shibboleth:metadata:1.0" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" entityID="urn:mace:incommon:umbc.edu"> <Extensions xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute" xmlns:mdrpi="urn:oasis:names:tc:SAML:metadata:rpi"> <mdrpi:RegistrationInfo registrati..."<br>• by_steward set to "false" | |
| update | nroy@internet2.edu | • status changed from "auto_approved" to "published" | 2020-07-31 01:11:28 PM UTC |

| Action | User | Changes | Date |
|---|---|---|---|

| | | | |
|---|---|---|---|
| create | paulr@umbc.edu | • organization_id set to "10032"<br>• entity_name set to "urn:mace:incommon:umbc.edu"<br>• status set to "auto_approved"<br>• metadata set to "<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:shibmd="urn:mace:shibboleth:metadata:1.0" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" entityID="urn:mace:incommon:umbc.edu"> <Extensions xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute" xmlns:mdrpi="urn:oasis:names:tc:SAML:metadata:rpi"> <mdrpi:RegistrationInfo registrati..."<br>• last_submitter_id set to "85"<br>• provider_id set to "19"<br>• provider_type set to "Idp"<br>• federation set to ""<br>• replaced_by_id set to ""<br>• submitted_at set to ""<br>• metadata_preview set to "<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:shibmd="urn:mace:shibboleth:metadata:1.0" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" entityID="urn:mace:incommon:umbc.edu"> <Extensions xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute" xmlns:mdrpi="urn:oasis:names:tc:SAML:metadata:rpi"> <mdrpi:RegistrationInfo registrati..."<br>• metadata_fallback set to "<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:shibmd="urn:mace:shibboleth:metadata:1.0" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" entityID="urn:mace:incommon:umbc.edu"> <Extensions xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute" | 2020-07-30 06:08:44 PM UTC |

| | | | |
|---|---|---|---|
| | | xmlns:mdrpi="urn:oasis:names:tc:SAML:metadata:rpi"> <mdrpi:RegistrationInfo registrati..."<br>• note set to ""<br>• allow_export set to "true"<br>• metadata_export set to "<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:shibmd="urn:mace:shibboleth:metadata:1.0" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" entityID="urn:mace:incommon:umbc.edu"> <Extensions xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute" xmlns:mdrpi="urn:oasis:names:tc:SAML:metadata:rpi"> <mdrpi:RegistrationInfo registrati..."<br>• by_steward set to "false" | |
| update | paulr@umbc.edu | • status changed from "auto_approved" to "canceled" | 2020-07-30 06:08:46 PM UTC |

| Action | User | Changes | Date |
|---|---|---|---|

| | | | |
|---|---|---|---|
| create | paulr@umbc.edu | • organization_id set to "10032"<br>• entity_name set to "urn:mace:incommon:umbc.edu"<br>• status set to "auto_approved"<br>• metadata set to "<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:shibmd="urn:mace:shibboleth:metadata:1.0" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" entityID="urn:mace:incommon:umbc.edu"> <Extensions xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute" xmlns:mdrpi="urn:oasis:names:tc:SAML:metadata:rpi"> <mdrpi:RegistrationInfo registrati..."<br>• last_submitter_id set to "85"<br>• provider_id set to "19"<br>• provider_type set to "Idp"<br>• federation set to ""<br>• replaced_by_id set to ""<br>• submitted_at set to ""<br>• metadata_preview set to "<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:shibmd="urn:mace:shibboleth:metadata:1.0" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" entityID="urn:mace:incommon:umbc.edu"> <Extensions xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute" xmlns:mdrpi="urn:oasis:names:tc:SAML:metadata:rpi"> <mdrpi:RegistrationInfo registrati..."<br>• metadata_fallback set to "<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:shibmd="urn:mace:shibboleth:metadata:1.0" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" entityID="urn:mace:incommon:umbc.edu"> <Extensions xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute" | 2020-07-23 03:44:28 PM UTC |

| | | | |
|---|---|---|---|
| | | xmlns:mdrpi="urn:oasis:names:tc:SAML:metadata:rpi"> <mdrpi:RegistrationInfo registrati..."<br>• note set to ""<br>• allow_export set to "true"<br>• metadata_export set to "<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:shibmd="urn:mace:shibboleth:metadata:1.0" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" entityID="urn:mace:incommon:umbc.edu"> <Extensions xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute" xmlns:mdrpi="urn:oasis:names:tc:SAML:metadata:rpi"> <mdrpi:RegistrationInfo registrati..."<br>• by_steward set to "false" | |
| update | chubing@internet2.edu | • status changed from "auto_approved" to "published" | 2020-07-23 06:49:01 PM UTC |
| update | paulr@umbc.edu | • status changed from "published" to "inactive" | 2020-07-30 06:08:44 PM UTC |

| Action | User | Changes | Date |
|---|---|---|---|

| | | | |
|---|---|---|---|
| create | paulr@umbc.edu | • organization_id set to "10032"<br>• entity_name set to "urn:mace:incommon:umbc.edu"<br>• status set to "auto_approved"<br>• metadata set to "<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:shibmd="urn:mace:shibboleth:metadata:1.0" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" entityID="urn:mace:incommon:umbc.edu"> <Extensions xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute" xmlns:mdrpi="urn:oasis:names:tc:SAML:metadata:rpi"> <mdrpi:RegistrationInfo registrati..."<br>• last_submitter_id set to "85"<br>• provider_id set to "19"<br>• provider_type set to "Idp"<br>• federation set to ""<br>• replaced_by_id set to ""<br>• submitted_at set to ""<br>• metadata_preview set to "<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:shibmd="urn:mace:shibboleth:metadata:1.0" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" entityID="urn:mace:incommon:umbc.edu"> <Extensions xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute" xmlns:mdrpi="urn:oasis:names:tc:SAML:metadata:rpi"> <mdrpi:RegistrationInfo registrati..."<br>• metadata_fallback set to "<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:shibmd="urn:mace:shibboleth:metadata:1.0" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" entityID="urn:mace:incommon:umbc.edu"> <Extensions xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute" | 2020-07-17 09:47:42 PM UTC |

| | | | |
|---|---|---|---|
| | | xmlns:mdrpi="urn:oasis:names:tc:SAML:metadata:rpi"> <mdrpi:RegistrationInfo registrati..."<br>● note set to ""<br>● allow_export set to "true"<br>● metadata_export set to "<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:shibmd="urn:mace:shibboleth:metadata:1.0" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" entityID="urn:mace:incommon:umbc.edu"> <Extensions xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute" xmlns:mdrpi="urn:oasis:names:tc:SAML:metadata:rpi"> <mdrpi:RegistrationInfo registrati..."<br>● by_steward set to "false" | |
| update | chubing@internet2.edu | ● status changed from "auto_approved" to "published" | 2020-07-20 06:57:34 PM UTC |
| update | paulr@umbc.edu | ● status changed from "published" to "inactive" | 2020-07-23 03:44:28 PM UTC |