Known Metadata Operational Issues

This page lists entity metadata values that are well known as source of operational issues affecting SAML2 implementations in eduGAIN. The eduGAIN OT will take all the possible measures to limit the damages caused by the issue according to its severity, rejection of the feed included.

Whatever the action the eduGAIN OT will undertake, it will promptly contact the Identity Federation responsible for the feed and it will try to solve the issue without any service interruption whenever possible.

When the rejection of the feed is unavoidable, the eduGAIN OT will support the Identity Federation to restore the feed as soon as possible. Please note that even in the case of rejection, the last usable feed will continue to be published as part of the eduGAIN metadata aggregate until its validity (set by the ValidUntil attribute) expires which according to the eduGAIN SAML profile will give the Federation a minimum of 5 days to react.

Known Metadata Operational Issues table

Code	Upstream Conditions	Downstream Conditions	Know Operational Issues	Actions
CR	The upstream metadata feed of an eduGAIN member contains a CR (Carriage Return) as a literal character reference ("
" or "
").	An eduGAIN member picks up the eduGAIN metadata aggreagate and republishes it to its own parties leaving untouched the CR literal character reference.	(2016) Relying parties not able to validate the metadata. (2019-08-21) .NET based signature validation fails (ADFSToolkit and other Powershell aggregate handlers impacted) - signaled by InCommon member to ADFSToolkit team via ADFSToolkit issue tracker, escalated and resolved by InCommon support. (2020) .NET based signature validation fails (ADFSToolkit and other Powershell aggregate handlers not able to validate the metadata).	▪ Reject the upstream feed containing the CR. ▪ Immediately notify the Identity Federation responsible for the feed in order to fix it.

Notes

2020-10-15 side note on Code **CR** from Chris Phillips:

This .Net parsing issue was seen Sept 2019 and was submitted to the Microsoft Security Center (msrc.microsoft.com) on Sept 12, 2019. Including a full test harness with fabricated data illustrating the failure with the following description upon submission:

> *User entered data could trigger improper XML validation and thus improper failure in validating trust in properly signed XML documents wherever . net/powershell library is used*
>
> MSRC assigned a tracking #VULN-009799 to the submission at the time. A reply by MSRC came October 28,2019 to Chris Phillips after MSRC completed their assessment and said:
>
> > "The engineering team has finished their investigation and determined it does not meet the bar for servicing. They were not able to determine a situation where this would be exploitable, and at worst the system returns a 'not valid' response when it should return 'valid' meaning it's failing in a more secure direction."