CoCo v1 vs v2

This page summarises the key commonalities and differences of GEANT CoCo ver 1.0 and 2.0 draft (as per 10 Jan 2019).

Note that this document is historical and does not cover the final CoCo ver 2.0

This page is non-normative and does not present exhaustive analysis of the CoCo versions. For complete analysis, the reader is encouraged to study the CoCos in detail. It is still believed this page is useful as a quick overview.

Commonalities of CoCo 1.0 and 2.0 (draft)

- Both are binding agreements for the Service Provider that has committed to it.
- They both consist of 17-18 clauses which express the what the service provider is committing to. The reader can observe many similarities between the clauses.
- They both use similar SAML metadata constructs (Entity category, RequestedAttributes, mdui:PrivacyStatementURL, mdui:DisplayName, mdui: Description)

Differences between CoCo 1.0 and 2.0 (draft)

- CoCo 1.0 is based on the Data Protection Directive and CoCo 2.0 on the GDPR which replaced the directive in 25 May 2018.
- CoCo 2.0 is more descriptive, it explains how the law should be interpreted in the context of attribute release in an R&E identity federation (e.g. what the attributes can be used for, how long they can be stored, etc)
- CoCo 2.0, after having been approved by the data protection authorities, justifies attribute release out of EU, if the SP has committed to it properly. This means also non-EU/EEA SPs can commit to it.
- CoCo 2.0 better serves the needs of international organisations (such as CERN and EMBL)
- CoCo 2.0 introduces a CoCo monitoring body, as required by GDPR
- CoCo 2.0 requires the SP to commit to SIRTFI, too
- Some of the material that is non-normative in CoCo 1.0 is made normative in CoCo 2.0, as suggested by the authorities (e.g. Privacy Policy template, handling non-compliance)
- SPs can make use of the CoCo also for receiving attributes from Attribute Providers (not only Identity Providers)