Recipe for a Home Organisation

The Data protection Code of Conducts (CoCo) enables safe attribute release between Identity and Service Providers within EU.

This page explains how an Identity Provider can implement the GÉANT Data Protection Code of Conduct in order to safely release attributes about its users.

1. Read and understand the GÉANT Data Protection Code of Conduct for SPs:
    - GÉANT Data Protection Code of Conduct for Service Providers
    - For a more complete elaboration: TNC2013 Code of Conduct Presentation
2. Develop a maximum list of attributes that the Home Organisation (the organization responsible for the IdP server) is willing to release to an SP committed to the Code of Conduct
    - An approach to limit the Home Organisation's data protection risks is to release only innocuous attributes to the SP
    - The list is a maximum list of attributes. If the SP requests fewer attributes, it is going to receive only those requested
    - Especially, the Home Organisation should not release personal data the data protection laws define sensitive (attributes revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and attributes concerning health or sex life)
    - On the other hand, releasing too few attributes may lead to the end user being denied access to the SP
    - c.f. the eduGAIN attribute profile recommends Home Organisations to populate the following attributes: displayName, cn, mail, eduPersonAffiliation, eduPersonScopedAffiliation, eduPersonPrincipalName, SAML2 Persistent NameID (eduPersonTargetedID), schacHomeOrganization and schacHomeOrganizationType
3. Find out if your Home Organisation is willing to release attributes to an SP committed to the CoCo
    - You need to identify the person to make that decision. The person must have the right to do the decision.
    - The person needs to be able to balance the risks (attribute release leading to a data protection problem) with the benefits (the potential of easier scientific collaboration which may lead to an increased scientific output of the institution)
    - The person can be for instance a CIO or information manager responsible for identity management
    - The person may need security consultation by the security manager and legal consultation by a lawyer or other person familiar with the data protection laws
4. Consider deploying an attribute release UI to the IdP server for informing the end user
    - The CoCo does not strictly require it but recommends it as a good practice for reducing Home Organisations' risks of non-compliance with the data protection laws
    - See Data Protection Good Practice for Home Organisations
5. Configure your Home Organisation's IdP server to
    - Release attributes to the SPs asserting conformance to the Code of Conduct
    - Release at most the maximum list of attributes, as requested by the SPs
    - How these configurations are done depends on your federation and on your IdP product
        - SWAMID's instructions for Shibboleth IdP
        - DFN-AAI examples for Shibboleth IdP 3.4.x (explanations in German)
        - IDEM GARR AAI IdP Config example