

NACO, the "N" Attribute Conformity Checker

Thursday, 19 March 2026 11:00 (20 minutes)

NACO is a comprehensive Python-based validation tool designed to ensure compliance with attribute requirements, such as NFDI or AARG-G056. The system provides dual interfaces - a command-line tool (naco) and a web service (naco-web) - for validating OIDC tokens and SAML assertions against configurable attribute specifications.

The tool supports flexible attribute checking through JSON-based configuration files that define both mandatory and optional attribute sets (basic and extended). NACO can validate against multiple OpenID Connect providers simultaneously, with each provider having its own configuration section including credentials, mytokens, and administrative contacts.

Key capabilities include external and community scope validation, and comprehensive email notification systems for administrators. The architecture is built around core components including a spec checker for validation logic, token handling utilities for OIDC operations, and a robust configuration system. This makes NACO suitable for research data infrastructure environments where consistent attribute validation across federated identity providers is critical for access control and compliance.

Primary author: HARDT, Marcus (KIT)

Presenter: HARDT, Marcus (KIT)

Session Classification: Networking, Security & Operationws - I (11:00 - 12:40)

Track Classification: Track 7: Network, Security, Infrastructure & Operations