

# TLS Authorization

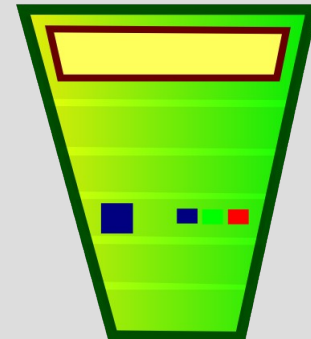


Client



Authorization data

- X.509 Attribute Certificate
- SAML assertions
- ...



Server

- Standard TLS is about authentication.
  - Using X.509 Certificates, Pre-Shared-Keys, OpenPGP keys, SRP, ...
- RFC 4680 and draft-housley-tls-authz-extns-07 adds authorization.
  - During TLS handshake, authorization data is transmitted to server.
- Enables clean separation of authentication and authorization.
  - Allows more modular use of authorization mechanisms.
- Implemented in GnuTLS 1.7.7 available from <http://www.gnutls.org/>.
  - Experimental branch.
  - Released 2007 Feb 22.