

# Macaroons: looking back and looking forward

*Tuesday 10 July 2018 15:30 (15 minutes)*

X.509 is the dominate security infrastructure used in WLCG. Although this technology has worked well, it has some issues. One is that, currently, a delegated proxy can do everything the parent credential can do. A stolen “production” proxy could be used from any machine in the world to delete all data owned by that VO on all storage systems in the grid.

Generating a delegated X.509 credential is also computationally expensive. As a result, credentials tend to be cached and reused, potentially increasing the likelihood of theft.

In October 2017, dCache v3.2 was released, which introduced support for macaroons: a pure authorisation, bearer token that supports delegation with autonomous attenuation.

In contrast to X.509, minting a macaroon is much faster, so that creating a macaroon per request is feasible. Macaroons also support attenuation when delegating: the delegated macaroon can be limited to a specific task and to a specific machine.

This paper reviews the current state of this support in dCache and present the different use-cases and projects that are using or are evaluating macaroons. It also compares macaroons to other pure bearer token solutions, such as the OAuth2 approach in SciToken, highlighting the relative strengths and weaknesses of each.

**Primary authors:** MILLAR, Paul (DESY); Dr ADEYEMI, Olufemi (DESY); BEHRMANN, Gerd (NEIC); FUHRMANN, Patrick (DESY); GARONNE, Vincent (University of Oslo (NO)); LITVINTSEV, Dmitry (FNAL); MKRTCHYAN, Tigran (DESY); Dr ROSSI, Albert (FNAL); Dr SAHAKYAN, Marina (DESY); Mr STAREK, Juergen (DESY); BOCK-ELMAN, Brian Paul (University of Nebraska Lincoln (US))

**Presenter:** MILLAR, Paul (DESY)

**Session Classification:** T3 - Distributed computing

**Track Classification:** Track 3 –Distributed computing