Table of Contents

RFC proxy and SHA-2 signature support in WLCG middleware

Introduction

IGTF would like CAs to move from SHA-1 to SHA-2 signatures ASAP, to anticipate concerns about the long-term safety of the former.

- See Secure Hash Algorithms

For WLCG this originally implied using RFC proxies instead of the Globus legacy proxies in use today, but that constraint has been avoided since Jan 2013:

- Jan 2013 pre-GDB agenda
- SHA-2 presentation

The latest IGTF timeline aims to allow SHA-2 certificates to be introduced by **Dec 1, 2013**. See the minutes of the Sep 19 WLCG Operations Coordination meeting.

EGI and EMI have assessed per product which version is supposed to be ready for SHA-2 certificates:

- SHA-2 support middleware baseline

EGI will pursue the uptake of the required versions in the EGI infrastructure and OSG will do the same for their products in their infrastructure.

The LHC experiments are asked to check their own services and clients explicitly:

- SHA-2 readiness testing

This topic: LCG > RFCproxySHA2support
Topic revision: r5 - 2013-09-26 - MaartenLitmaath