Better security for maintainers

Piotr Strzyżewski
Silesian University of Technology, Computer Centre

Reason

- Majority (almost all) of objects use password authentication
- Current implementation supports only MD5
- MD5 is not collision resistant
- MD5 is considered as not suitable for further use
- Objects are not well protected

Idea

- Modify the DB software and introduce new, stronger hash algorithms:
  - SHA-2 family
  - GOST
  - Others?
- Remove support for MD5 within 1-2 years from introduction of new alghoritms

Pros and cons

- (+) Objects will be better protected against abuse
- (-) LIRs have to change their maintainer objects
- (-) Some objects will be locked after MD5 removal (lesson from history)

Questions?