EGI-InSPIRE

NOTE ON MIGRATION TO SHA-2 CERTIFICATES

Document identifier:	EGI-docid-V9.doc
Date:	**23/08/2012**
Document Status:	**v 1.1**
Dissemination Level:	**PUBLIC**
Document Link:	https://documents.egi.eu/document/1291

Authors

Peter Solagna/EGI.eu, David Groep/NIKHEF

TABLE OF CONTENTS

1 INTRODUCTION

The EGI Public Key Infrastructure (PKI) for the authentication of users and service hosts is based on the IGTF PKI implementation[1]. The IGTF is currently scheduling a migration from the SHA-1 hash algorithm to the newer version SHA-2 - for newly-issued certificates only - and this will probably happen during 2013.

This document provides a brief introduction to the subject, a description of the impact of these planned changes on the EGI infrastructure and an EGI action plan.

2 X.509 CERTIFICATES

The user and host certificates used in the EGI infrastructure for identity management and authentication purposes are released by the Certification Authorities (CA) that are members of the International Grid Trust Federation (IGTF).

When a certificate is issued, the issuer – the CA in the EGI PKI - includes a signature which is based on a digest of the certificate content, currently generated using the SHA-1 hash algorithm, computed from the relevant information contained in the certificate and encrypted with the CA private key. To validate the certificate a relying party must:

1. Decrypt the CA signature attached to the certificate using the CA public key, obtaining the hash value calculated by the CA.
2. Calculate the hash value for the rest of the certificate using the same hash algorithm (currently SHA-1).

[1] http://www.igtf.net/

3. Compare the two hash values; if they match the certificate has been confirmed as having been issued by the CA.

This is the core validity check on a certificate; there are of course many others, e.g. certificate expiration, syntax and validity of extensions.

The CA public keys are available together with the CA certificates as part of the IGTF Trust Anchors releases, and should be installed by all EGI services which require authentication of users and/or hosts. For more information about the X.509 infrastructure, please see [R2].

3 SHA-1 COLLISION RESISTANCE

A PKI can be compromised by generating a false certificate which uses the CA signature of an existing certificate. In order to do so, the attacker needs to build a certificate such that its hash value is identical to the hash value in the signature of the original certificate. This is known as a hash collision.

The SHA-1 hash algorithm was originally estimated to have 80 collision resistance bits: this means that finding a collision (more specifically, another valid certificate body that generates the same hash value) requires a number of operations of the order of 2^{80}.

The number of operations to identify a collision has been estimated to be on the order of 2^{58} (2010 estimation), which would require approximately 544 CPU-years.

The strength of the SHA-1 algorithm relies on the computing capacity required to find a hash collision, and hence the algorithm becomes weaker as computing power increases. Any weaknesses found in the algorithm in the near future may reduce the number of resistance bits and further weaken the algorithm.

4 TRANSITION TOWARDS SHA-2

Because of the progressive reduction in the strength of the SHA-1 algorithm, the National Institute of Standards and Technology (NIST) have planned to phase out the algorithm in favour of the stronger hash function family SHA-2 (SHA-224, SHA-256, SHA-384 and SHA-512). Although the endorsers of SHA-1 (NIST and NSA) recommended an end-of-life date for SHA-1 in 2010, there are no strong indications at this point in time that SHA-1 is severely broken, or will be before mid-2014, although such an event cannot be excluded.

Starting from these recommendations, the IGTF and the European Policy Management Authority for Grid Authentication (EUGridPMA) have drafted a timeline for the migration of Grid certificates from the SHA-1 algorithm to SHA-2.

The timeline will be defined with more precision during the next EUGridPMA meeting (Lyon, September 2012). There are two milestones:

1. All the CAs **must** be able to issue SHA-2 signed certificates by October 2012.
2. EUGridPMA member CAs will **not be allowed** to release SHA-2 certificates before 1st January 2013:
    a. This does **not** mean that all certificates issued after January 2013 must be SHA-2

b. The **exact date** from which CAs will be allowed to release SHA-2 certificates will not be before January 2013, and is to be determined based on a comprehensive risk assessment [R 1] including any operational issues for the Grid infrastructure. That **may** result in a limited (a few months) rescheduling of the recommended introduction of SHA-2 for general availability.

Point 1 should not imply any change for relying parties, since it is purely an internal re-structuring for the CAs.

Point 2 will however affect the infrastructure, and this step needs to be carefully scheduled considering the readiness of the Grid infrastructure to accept SHA-2 certificates. For this reason the initially proposed date – the 1st of January 2013 – may be reconsidered, depending on the outcome of the risk analysis.

Currently the certificates used in the EGI infrastructure have a lifespan from 13 to 18 months, which means that SHA-2 certificates must be in widespread use at least one year in advance of the time when SHA-1 is considered to be compromised. If SHA-1 is demonstrated to be insecure, all existing SHA-1 certificates will have to be re-issued with a SHA-2 signature. If, at that point, the majority of certificates are still SHA-1, the upgrade could be a challenging task (if not disruptive) for the whole infrastructure.

4.1 Legacy vs RFC proxies

Legacy proxy certificates are the proxies currently used in the infrastructure. RFC 3820 [R 4] introduced a framework for carrying policies in Proxy Certificates, e.g. describing limitations or enumerations of rights. The RFC proxies (compliant to RFC 3820) are structured in a different format to the legacy proxies, and therefore support for RFC proxies must be implemented in the authentication libraries used by all software which handles these certificates.

Two middleware components, **dCache** and **BeStMan** (the latter deployed in the OSG infrastructure), are using (or will use) jGlobus2 as an authentication library, which supports SHA-2 but does **not** support legacy proxies. Currently the dCache team is looking into solutions to support both legacy proxies and SHA-2. If some components will require RFC proxies for SHA-2 support, certificates will have to be issued in the RFC format, and therefore **all** middleware components will have to support them.

Currently the readiness of the middleware to support RFC proxies has yet to be fully assessed. To our knowledge, all the **IGE** products and the EMI components released in the **EMI-2** (major release and subsequent updates) should be able to handle RFC proxies.

EGI-InSPIRE SA2 will implement a quality verification criterion to test all the new components entering the UMD with RFC proxies.

4.2 EMI CANL

The EMI Common AuthenticatioN Library (CANL) [R6] is a new product released in EMI-2 that aims to support authentication and other X.509 PKI-related operations for the components maintained by the EMI project. The target for EMI is to implement the use of the CANL in all products by EMI-3.

EMI CANL will support SHA-2 signed certificates and RFC proxies (see **Error! Reference source not found.**), but it has not be tested in a production environment, in the absence of products that use it.

5 EGI ACTION PLAN

To handle certificates and proxies signed using a SHA-2-family algorithm, the authentication libraries used by the Grid middleware must support these algorithms.

The critical point is that in order to allow users to access the Grid infrastructure at large, by the time the first CA starts to issue SHA-2 certificates, all the production Grid services must be able to handle SHA-2 signed credentials.

EGI Operations has defined the following plan for the assessment of the readiness of the deployed services, and new releases produced by the technology providers. The plan includes the following actions:

- **ACTION 1: SHA-2 readiness matrix.** The technology providers relevant to UMD will be requested to produce a table identifying the capability to handle SHA-2 certificates for all supported product versions.
- **ACTION 2: SHA-2 compliance software validation**. Starting from September 2012 new middleware products will be tested for compliance with SHA-2 certificates and proxies during the UMD software provisioning process. In the case that a component is identified as not being able to handle SHA-2, the developers will be notified and the product released within UMD. The inability to handle SHA-2 certificates will not be regarded as a bug in the near future. A timeline for mandatory compliance with SHA-2 will be discussed after the EUgridPMA September meeting.
- **ACTION 3: SHA-2 readiness of the production infrastructure**. The production infrastructure (services already deployed in production in EGI) will be tested with SHA-2 signed credentials. This will be carried out in collaboration with the EGI CSIRT. An extension of the security nagios framework is being discussed to facilitate this. For any components not supporting SHA-2, an upgrade path to a newer version of the software which is SHA-2 enabled must be defined.
- **ACTION 4: Assessment of the impact on users**. Users need to be ready for changes in the certificate format supported by the infrastructure. This concerns any application software, frameworks and portals that use X.509 certificates for user or host authentication.

  The developers of such tools **must** test their code for compliance with SHA-2 and RFC proxies. If there is any blocking issue that prevents the support for SHA-2 and RFC proxies in the applications, developers should contact EGI Operations.

  Applications using common authentication libraries, such as libraries distributed with the OS or provided with web servers or servlet containers like Apache and Apache Tomcat, automatically inherit support for SHA-2 as it is already implemented in these tools. No development should be needed in this case, but testing SHA-2 certificates and proxies is still recommended.

  EGI will collect assessments of the readiness of user application frameworks.

ACTION 2 is technically feasible, as the verification of the capability of new software releases is already part of the EGI software provisioning process.

The implementation of ACTION 3 is being discussed with the EGI CSIRT.

ACTION 4 will be implemented in collaboration with the User Community Board (UCB).

This action plan will be reviewed after the September EUgridPMA meeting and new actions will be defined accordingly.

6 CONCLUSIONS

SHA-2 certificates will probably become mandatory during 2014 as a result of the insufficient strength of the SHA-1 algorithm.

Considering the lifespan of the certificates used in the EGI infrastructure (13 to 18 months), CAs will probably start to release SHA-2 signed credentials during 2013, following the policies defined by the IGTF and according to the risk assessment conducted by the EUgridPMA.

The readiness of all deployed middleware, application software and future releases of software making use of certificates and user proxies will be assessed. An action plan has been defined for this.

EGI Operations are monitoring the evolution of SHA-2 support (together with RFC proxy support) to define the middleware upgrade guidelines.

7 REFERENCES

R 1	EUgridPMA Risk assessment on Hash Function Vulnerabilities, July 2012 (https://www.eugridpma.org/documentation/hashrat/SHA1Risk.pdf)
R 2	ITU Public-key and attribute certificate frameworks
R 3	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
R 4	Internet X.509 Public Key Infrastructure (PKI) Proxy Certificate Profile
R 5	Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
R 6	Common Authentication Library Manual, EMI Project (http://unicore-dev.zam.kfa-juelich.de/documentation/canl-1.0.1/manual.pdf)