EGI-InSPIRE

INFORMATIVE NOTE ON MIGRATION TO SHA-2 CERTIFICATES

Document identifier:	EGI-docid-V9.doc
Date:	**03/08/2012**
Document Status:	**DRAFT**
Dissemination Level:	**PUBLIC**
Document Link:	

Authors

….

Abstract

TABLE OF CONTENTS

1 INTRODUCTION

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

This document will provide a brief introduction to the subject, and a description of the impact of these planned changes in the EGI infrastructure.

2 X.509 CERTIFICATES

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

As a certificate is released, the issuer – the CA in the EGI PKI- includes a signature, which is based on a digest of the certificate content, currently done using the SHA-1 algorithm, computed on the relevant information contained in the certificate and encrypted with the CA private key. To validate the certificate a third entity must:

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

1. Decrypt the CA signature of the certificate using the CA public key, obtaining the hash value calculated by the CA
2. Calculate the hash value on the rest of the certificate using the same hash algorithm (currently SHA-1)
3. Compare the two hash values, if they match the certificate has been confirmed as issued by the CA

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

The CA public keys are available in the CA public certificates available from the IGTF Trust Anchors release, and should be deployed by all the EGI services which request authentication of users and hosts.

For more information about the X.509 infrastructure, please see [R 2]

3 SHA-1 COLLISION RESISTANCE

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 which hash code collides with the hash code in the signature of the original certificate.

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

The number of operations to identify a collision is estimated to be in the order of 2^{58} (2010 estimation), this requires approximately ~544 CPU-years.

The strength of the SHA-1 algorithm relies on the computing capacity required to find an hash collision. A weaknesses found in the collision in the near future may reduce the current amount of resistance bits.

4 TRANSITION TOWARDS SHA-2

Because of the reduction in the number of collision resistance bits, the National Institute of Standards and Technology (NIST) have planned to phase out SHA-1 algorithm in favour of the stronger hash functions family SHA-2 (SHA-224, SHA-256, SHA-384 and SHA-512). Although the endorsers of SHA-1 (NIST and NSA) have 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 IGTF and the European Policy Management Authority for Grid Authentication (EUGridPMA) have drafted a timeline for the migration of the 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), the two milestones are:

1. All the CAs **must be able** to deliver SHA-2 signed certificates by the October 2012
2. EUGridPMA member CAs will be **allowed** to release SHA-2 certs not before 1st January 2013
    a. This does not mean that all the certificates released 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 the operational issues in the infrastructure. That may result in limited (few months) rescheduling of the recommended general availability introduction.

Point 1) should not change anything for the relying parties, being an internal re-structuration for the CAs.

Point 2) will instead 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 initial proposed date – the 1st of January 2013 – could be reconsidered depending on the risk analysis.

Currently the certificates used in the infrastructure have a lifespan from 13 to 18 months, this means that SHA-2 certificates should be widely used one year in advance the moment when a SHA-1 vulnerability is discovered. As the previous hash algorithm will be demonstrated to be no more reliable, all the SHA-1 certificates have to be re-issued with a SHA-2 signature. If, in that moment, the majority of the 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 i.e. describing limitation or enumeration of rights. The RFC proxies (compliant to RFC 3820) are structured in a different format, therefore the RFC must be implemented in the authentication libraries used by the software to handle these certificates.

Two middleware components: **dCache** and **BestMan** (the latter deployed in the OSG infrastructure) are using (or will use) jGlobus2 as 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 the middleware components will have to support them.

Currently the middleware readiness to support RFC proxies has to be 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 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) is a new product released in EMI-2 that aims at supporting authentication and other X.509 PKI related operations of the components maintained by the EMI project. The target for EMI is to implement the use of the CANL in all the 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, missing 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 defined a plan for the assessment of the readiness of the deployed services, and the new releases produced by the technology providers.

The EGI 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 to SHA-2 certificates and proxies during the UMD software provisioning process. In case of a component is identified as not being able to handle SHA-2, the developers will be notified and the product released with UMD. The inability to handle SHA-2 certificates won't be considered a bug in the near future.
- **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 EGI CSIRT. The extension of the security nagios framework is being discussed for this. For the components not supporting SHA-2 an upgrade plan to a newer version of the software SHA-2 enabled, must be defined.
- **ACTION 4 Assessment of impact on users**. Users need to be ready for changes in the certificate format supported by the infrastructure, this concerns 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 to 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.

  Application using authentication common libraries, such as the OS libraries, or based on web servers and servlet containers like Apache and Apache Tomcat, automatically inherit the

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 assess the readiness of user application frameworks.

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

The implementation of ACTION 3 is being discussed with 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 because of insufficient reliability of the SHA-1 algorithm.

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

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

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

7 REFERENCES

R 1	Risk assessment on Hash Function Vulnerabilities - IGTF HASHRAT
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