

EGI.eu

EGI CSIRT OPERATIONAL PROCEDURE FOR COMPROMISED CERTIFICATES AND CENTRAL SECURITY EMERGENCY SUSPENSION

Document identifier	EGI-CSIRT-Compromised-Certificate
Document Link	https://documents.egi.eu/document/1018
Last Modified	24/09/2013
Version	(For approval)
Policy Group Acronym	EGI CSIRT
Policy Group Name	EGI Computer Security Incident Response Team
Contact Person	Linda Cornwall
Document Type	Procedure
Document Status	DRAFT
Approved by	To be approved by OMB
Approved Date	DD/MM/YYYY



Procedure statement

This procedure describes what should be done by the EGI CSIRT in the event of a compromised identity certificate, including long lived certificates and proxies. This applies to robot certificates and service certificates as well as user certificates. This also includes what is done when certificates are linked to security incidents. This procedure also addresses usage of Central Security Emergency suspension. The implications of a CA compromise are also briefly described.

I. AUTHORS LIST

	Name	Organisation	Date
From	Linda Cornwall + EGI CSIRT	STFC	

II. DELIVERY SLIP

	Body	Date
Reviewed by	TCB	DD/MM/YYYY
Reviewed by	OMB	DD/MM/YYYY
Reviewed by	UCB	DD/MM/YYYY
Approved by	EGI.eu Director	DD/MM/YYYY
Approved by	EGI.eu Executive Board	DD/MM/YYYY

III. DOCUMENT LOG

Version	Date	Comment	Author/Organization
0.1	4th March 2013	Draft for discussion	Linda Cornwall/ STFC
0.2	26th March 2013	Modified on the assumption that Central Security Emergency suspension using Argus is available.	Linda Cornwall/STFC
0.3	18th April 2013	Modified after result of comments plus discussions at the EGI CF	Linda Cornwall/STFC
0.4	1st May 2013	Modified after discussions at EGI CSIRT F2F meeting, including some re-structuring	Linda Cornwall/STFC
0.5	23rd May 2013	Addressed Ursula Epting's comments	Linda Cornwall/STFC
0.6	28th May 2013	Minor edit	Linda Cornwall/STFC
0.7	31st May 2013	Addressed Leif Nixon's comments	Linda Cornwall/STFC
0.8	7th June 2013	Addressed Dave Kelsey's comments	Linda Cornwall/STFC
0.9	15th July 2013	Addressed Alessandro Usai and Goncalo Borges comments.	Linda Cornwall/STFC
0.10	1st August 2013	Addressed comments from Sven Gabriel, Leif Nixon, Alessandro Usai. Separated to a greater extent revocation and central security emergency suspension.	Linda Cornwall/STFC
Alt-0_1	3rd September2013	Alternative structure, providing short procedures and referring to explanations	Linda Cornwall/STFC
Version for appr	24th September 2013	Same as 'alt' but to avoid confusion document server	Linda Cornwall/STFC
1.0			
2.0			
3.0			
4.0			

IV. APPLICATION AREA

This document is a formal EGI.eu policy or procedure applicable to all participants and associate participants, beneficiaries and Joint Research Unit members, as well as its collaborating projects.

V. POLICY/PROCEDURE AMENDMENT PROCEDURE

Reviews and amendments should be done in accordance with the EGI.eu "Policy Development Process" (https://documents.egi.eu/document/169).

VI. ORGANISATION SUMMARY

To support science and innovation, a lasting operational model for e-Infrastructure is needed – both for coordinating the infrastructure and for delivering integrated services that cross national borders. The objective of EGI.eu (a foundation established under Dutch law) is to create and maintain a pan-European Grid Infrastructure in collaboration with National Grid Initiatives (NGIs) in order to

guarantee the long-term availability of a generic e-infrastructure for all European research communities and their international collaborators.

In its role of coordinating grid activities between European NGIs, EGI.eu will:

- Operate a secure integrated production grid infrastructure that seamlessly federates resources from providers around Europe
- Coordinate the support of the research communities using the European infrastructure coordinated by EGI.eu
- Work with software providers within Europe and worldwide to provide high-quality innovative software solutions that deliver the capability required by our user communities
- Ensure the development of EGI.eu through the coordination and participation in collaborative research projects that bring innovation to European Distributed Computing Infrastructures (DCIs)

The EGI.eu is supporting 'grids' of high-performance computing (HPC) and high-throughput computing (HTC) resources. EGI.eu will also be ideally placed to integrate new Distributed Computing Infrastructures (DCIs) such as clouds, supercomputing networks and desktop grids, to benefit the user communities within the European Research Area.

EGI will collect user requirements and provide support for the current and emerging user communities. Support will also be given to the current heavy users of the infrastructure, such as high energy physics, computational chemistry and life sciences, as they move their critical services and tools from a centralised support model to one driven by their own individual communities.

The EGI community is a federation of independent national and community resource providers, whose resources support specific research communities and international collaborators both within Europe and worldwide. EGI.eu, coordinator of EGI, brings together partner institutions established within the community to provide a set of essential human and technical services that enable secure integrated access to distributed resources on behalf of the community.

The production infrastructure supports Virtual Research Communities − structured international user communities − that are grouped into specific research domains. VRCs are formally represented within EGI at both a technical and strategic level.

TABLE OF CONTENTS

1 INTRODUCTION

1.1 Purpose of this document

The purpose of this document is to define what should be done operationally in the event of a compromised certificate and security incident where certain identity certificates may be involved. It addresses Central Security Emergency Suspension from the EGI infrastructure and some of the criteria for carrying it out.

The following types of identity certificate compromise are described:

1. Standard user certificate or proxy of a user certificate.
2. User certificate which is also used for the submission of pilot jobs
3. Robot certificate
4. Host or service certificate
5. CA compromise

In all cases, certificates which are part of the International Grid Trust Federation (IGTF) [R 1] are primarily being referred to. This may apply to certificates from other sources, but communication with other certificate providers may be less relevant and is at the EGI CSIRT's discretion.

It is also noted that there may be situations which we have not thought of, and members of the EGI CSIRT team will have to use discretion. This document aims to provide a clear view of what needs to be done in most cases, to help the team take appropriate action in any other cases which may occur.

Compromise of a VO is outside the scope of this document. This does not exclude the need for a procedure in the future for the handling of compromised VOs.

1.2 What is meant by a compromised certificate

A user, host, robot or service certificate is usually considered compromised if the private key has been exposed outside normal usage and policy. This includes both the private key and proxies of the CA signed certificate which have been exposed outside normal usage and policy. This includes if a password protected private key is accessible, and there is the possibility that it could be usable, e.g. if the password may also be accessible. The EUGrid PMA provides Guidelines on Private Key protection [R 8]

A certificate may also be treated as compromised if it is involved in a security incident on the grid.

There is also the (unlikely) case where a CA itself is compromised.

1.3 Suspending a DN using central security emergency suspension

This procedure describes the meaning of central security emergency suspension, which allows the rapid blacklisting of a specific DN to protect the infrastructure without the need for manual intervention at each site, or action from others such as a CA. This may be carried out using the Argus framework [R 4]. Some of the types of criteria for the application of central security emergency suspension are also discussed.

1.4 Why a procedure for compromised certificates

A procedure is necessary for the following main reasons:

1. EGI CSIRT should act in an agreed and expected manner
2. EGI CSIRT people know what to do, this saves time and allows actions to be carried out relatively quickly

3. Sites are protected, as quickly and efficiently as possible

Note that central security emergency suspension is NOT the same as certificate revocation. Central security emergency suspension may be carried out by EGI CSIRT but certificate revocation is not. Certificate revocation is carried out by the Certificate Authorities (CAs). This is explained in more detail in 5.7

1.5 Why not compromised general credential

The question has been asked "why not produce a procedure for more general compromise of credentials?" The reason is this procedure is defined for the current way in which the EGI Grid infrastructure is used, where certificates are used to submit jobs. Even if a user does not actually have a certificate, a robot certificate is used to submit the job when the user initiates a job via a portal. It is beyond the scope of this document to define how portal owners investigate mis-use or compromise of user credentials used to submit jobs via the portal.

1.6 Structure of this document

The following 3 sections contain the main procedures which may be carried out in appropriate circumstances. Section 2 provides the compromised user certificate operational procedure, which may be carried out for any type of certificate which is able to submit jobs, whether standard user certificates, user certificates used for pilot job submission or robot certificates. Section 3 provides the procedure for compromised host or service certificates. Section 4 provides the procedure in the event of a compromised CA. Section 5 describes central emergency suspension in detail and the types of situation where emergency suspension is envisaged. Subsequent sections provide more information and explanations.

1.7 Who should approve this procedure

This procedure should be formally approved by the EGI Operations Management Board (OMB). It should also be agreed by the EGI CSIRT team as well as the EGI representative of the EUGridPMA.

2 COMPROMISED USER CERTIFICATE OPERATIONAL PROCEDURE

This is the procedure to be carried out in case of compromise of any certificate able to be used to submit jobs. This includes single user certificates and multi user certificates (Robot and pilot jobs).

EGI CSIRT may decide when the exposure of credentials requires the application of this procedure. When a compromise comes to the attention of EGI CSIRT, it will be for EGI CSIRT to consider whether no action is necessary, whether all actions in this section are necessary, or whether more limited action is necessary. Assessing the situation is discussed in 6.1

Further information on multi user certificate compromises and the implications is given in section 7. All the steps are at the discretion of the EGI CSIRT members and will depend on the circumstances of the incident. Criteria are discussed in sections 5 and 6 of this document. Cross references for further information for various steps are provided in this procedure.

2.1 Carry out central security emergency suspension of the user DN(s)

The central security emergency suspension may be carried out using the central security emergency suspension framework. Details of some types of situation where emergency suspension is likely to be necessary are in section 5.4. Information on Argus Authorization framework which may be used to suspend DN(s) is in [R 4]

2.2 Inform sites and NGIs of suspension of DN(s)

Sites and NGI security contacts should be informed by e-mail to site-security-contacts@mailman.egi.eu and ngi-security-contacts@mailman.egi.eu that a certificate has undergone emergency suspension. The e-mail should include the user's DN(s), and a brief reason why the DN(s) has/have been suspended. See section 6.3.1

2.3 Inform the VOs of security emergency suspension of DN(s)

VOs may be informed of the emergency suspension of the DN(s).

See Voms operational portal [R 9]

See section 6.3.2

2.4 Inform the IGTF of security emergency suspension

Inform the IGTF of emergency suspension of the DN(s), including the reasons.

This can be done by e-mail to igtf-general@gridpma.org

See section 6.3.3

2.5 The certificate may need to be revoked

See section 6.3.4, and section 5.7

2.6 Contact long term proxy storage providers

EGI CSIRT may contact long term proxy storage providers, such as those running 'Myproxy' stores.

See section 6.3.5

2.7 Carry out incident response and any further investigation

In most cases it is expected that the central security emergency suspension will be due to a security incident, and this will be handled by EGI CSIRT according to the EGI CSIRT incident handling procedure [R 2]. Most of the communication will be according to the workflow contained in the incident handling procedure, which are not repeated in this document.

2.8 Remove security emergency suspension of user

The emergency suspension of the user may be removed by the EGI CSIRT team using the Central Emergency Suspension Framework, when it is considered appropriate. This will be considered on a case by case basis. See section 6.3.7

2.9 Inform sites and NGIs if security emergency suspension is removed

Sites and NGI security contacts should be informed by e-mail to site-security-contacts@mailman.egi.eu and ngi-security-contacts@mailman.egi.eu when DN(s) are no longer under emergency suspension. See section 6.3.8

2.10 Inform the IGTF if security emergency suspension is removed

If the IGTF was informed of emergency suspension, the IGTF should be informed when emergency suspension is removed. See section 6.3.9

This can be done by e-mail to igtf-general@gridpma.org

2.11 Inform the VOs if security emergency suspension is removed

Affected VOs should be informed if emergency suspension of DNs has been removed.

2.12 Report to the OMB

When investigations are complete, the OMB will receive a report of the incident as part of the incident handling procedure [R 2].

See section 6.3.10

3 COMPROMISED HOST OR SERVICE CERTIFICATE OPERATIONAL PROCEDURE

This defines the steps of the procedure which are normally carried out when a host or service Certificate or proxy has been found or suspected to be compromised. Host and service certificates are normally not password protected, but protected by system permissions. The most likely cause of a compromised host or service certificate is likely to be due to a security incident at the site. Since a host or service certificates cannot normally be used to submit jobs, and cannot be used to obtain VOMS credentials then there is no user, emergency suspension is not applicable. However, the certificate should be revoked and a new one obtained, as it is possible that the compromised certificate could be used to host a malicious service.

Normally the revocation of the certificate is expected to be carried out by the system administrator of the service, as it is most likely that the host or service certificate is compromised due to an incident at the site, and the system administrator will be dealing with it.

3.1 Service provider should shut down the service

The site administrator for the services should shut down the service. This includes putting the service into downtime, stating security operations.

If EGI CSIRT becomes aware of a possible compromise of a service certificate, EGI CSIRT should inform the site and ask them to put the service in downtime.

3.2 Request certificate revocation

Normally the certificate owner/site admin should revoke the certificate, assuming they have the private key or their private key is managed via a system they are able to access. If not, for example if they have lost the only copy of the private key, they should contact the CA to arrange its revocation.

Otherwise, the EGI CSIRT should request revocation by the CA(s). For example, if a system storing private keys has had a root compromise then it is likely that the CA(s) will revoke certificates on the request of EGI CSIRT IRTF.

3.3 Users should be advised not to use the service

This may be done either by EGI CSIRT, or by the service provider.

3.4 If necessary, carry out security emergency site suspension

If necessary, EGI CSIRT should carry out emergency site suspension, if the owner cannot be contacted to put the service into downtime, or other reasons.

3.5 Investigate incident

EGI CSIRT should follow the Incident handling procedure [R 2] in conjunction with the site administrators at the compromised site.

3.6 Service provider may apply for a new certificate

The service site administrator will need to apply for a new certificate.

3.7 Service provider may restore the service

The service may then be restored. This may be announced to the community.

4 COMPROMISED CA

This will be handled mainly by the IGTF [R 1], and not by EGI CSIRT. However EGI CSIRT should be aware of what to do in case they suspect a compromise, and the consequences of a compromise.

4.1 If EGI CSIRT member suspects a CA has been compromised

4.1.1 Alert the CA

The EGI CSIRT member should alert the CA of the suspicion that the CA has been compromised, including stating why with as much information as available.

4.1.2 Alert the IGTF

The EGI CSIRT member should slert the IGTF [R 1] of the suspicion that a CA has been compromised, including stating why with as much information as is available. This can be done by e-mail to igtf-general@gridpma.org

See http://www.igtf.net/

4.1.3 Alert the EUGridPMA or other regional authority

The regional appropriate PMA authority should also be alerted, again with as much information as available. For EUGridPMA this may be carried out by e-mail to

concerns@eugridpma.org

concerns@apgridpma.org or

concerns@tagpma.org

(More information at http://www.eugridpma.org/ , http://apgridpma.org, http://tagpma.org)

4.2 CA or IGTF informs of or confirms a compromise

The CA or IGTF may confirm the compromise as reported in 4.1, or discovered from another source. The IGTF will carry out all the handling, including informing site-security-contacts.

4.3 Emergency release of Trust Anchor

It is possible to request an emergency release of the Trust Anchor. [R 7]

4.4 Consequences of a CA Compromise

If a CA is compromised all service providers which authenticate with certificates from that CA will be in downtime until the CA is restored. Also, all users who authenticate with certificates from that CA will not be able to submit jobs. After the CA is restored all services and users who authenticate with that CA will need to re-apply for certificates, and services will need to be restored.

5 CENTRAL SECURITY EMERGENCY SUSPENSION

5.1 What is meant by central security emergency suspension

The Central Security Emergency Suspension Framework allows for a central, infrastructure wide blacklisting of a DN. Central security emergency suspension means that DNs are entered in the security emergency suspension framework. This framework serves plain text files and Argus policy files containing the suspension information (DNs) in plain text, to be fetched and processed by the Resource Centres (RC). This allows sites to guarantee fast reaction during incident response to automatically suspend or reject all authorization requests for a given DN. This avoids sites needing to take urgent action to protect their sites outside office hours. Sites may run an Argus server, or alternatively sites may download a list of DNs which are suspended from the Argus server and deploy an alternative mechanism to manage authorization at their sites which they know and control.

DNs suspended via the central security emergency suspension are in clear text in the deployed files (whether in Argus policies or text files.

Central security emergency suspension helps containing the incident by preventing further access to systems using pki.

At the time of writing not all services are able to be integrated with the central security emergency suspension framework, and this integration is in work.

Jobs which are already executing which are owned by the DN still have to be stopped by the local admin teams as there is no automated way at present of stopping jobs which are already running.

5.2 Policy and user suspension

Service providers are required to obey the Service Operations Security Policy [R 5].

This includes the statement “You must implement automated procedures to download the security emergency suspension lists defined centrally by security operations and should take appropriate actions based on these lists, to be effective within the specified time period”.

Sites are obliged to consume this list; but they may choose to give local policies priority over it, thereby overriding it partly or entirely. EGI CSIRT is responsible for the security emergency suspension list, and sites will be held accountable if they overrule it.

5.3 Reason why EGI CSIRT may carry out central security emergency suspension

The reason why EGI CSIRT may carry out central security emergency suspension is to protect resources against mis-use, and/or to protect external resources against on-line attack. The most likely reason is that a certificate is linked to an incident, including attacks against sites external to the EGI infrastructure.

EGI-CSIRT is well aware of the consequences of suspending a user certificate, in particular the implications of robot certificates and certificates used in multi-user-pilot-job frameworks. Based on the severity of the security incident and the impact of suspending a particular DN EGI-CSIRT will decide on a per case basis, whether a DN will be suspended or not.

The examples given in section 5.4 are only for illustration purposes, there might be more situations where suspending a DN is needed.

If a certificate has been used to submit jobs which are causing problems to the EGI infrastructure, but not due to a security incident, then emergency suspension is not permitted by this procedure.

5.4 Examples of when a DN may be subject to central security emergency suspension

It is a matter of the judgement of the EGI CSIRT Incident Response Task Force (IRTF) to decide whether it is necessary to suspend a DN. This is not done lightly, and is done to protect the infrastructure from mis-use, or from jobs which represent a security threat to EGI, or to protect external resources from attack. Here we provide some examples of the type of cases where the EGI CSIRT is likely to consider the suspension of a DN. This is not an exhaustive list, but guides the reader to indicate the types of cases where central security emergency suspension may be carried out.

If a private key has been exposed outside policy, this may result in emergency suspension of a DN. For example

- A system containing proxies and/or private keys has been compromised
- A user private key was shared by the user with others
- A user copied a private key which is not protected by a password or a proxy to a location readable by others. This could include uploading to a web page or copying to a world readable directory.
- A user private key protected by a password is on a compromised device, where there is the possibility that the private key is usable.
- The user e-mailed a proxy to a mailing list with a world readable archive
- A device was stolen which contains a non-protected private key, or a private key that may be usable (e.g. there is the possibility that the password is on the device).
- A software vulnerability or a mis-configured site exposed private keys or proxies publicly
- The CA itself has revoked a certificate

It is likely that a user or robot certificate will undergo emergency suspension if a DN is associated with any sort of security incident or mis-use.

For example

- If a security incident takes place, which can be linked to a particular certificate.
- Jobs have been submitted which appear to be a security threat to EGI.
- The certificate has been linked to any sort of on-going security incident.
- The certificate is linked to any sort of attack on a 3rd party, this could include a DoS on a bank or an attempt to attack a government or other organisation.

These events by themselves will not automatically provide sufficient reason for security emergency suspension. In many cases these events by themselves are only likely to lead to certificate revocation, not to emergency suspension. If a certificate is compromised through any of these events, and there is sufficient evidence that the identity is being used for activities outside policy then there would be a case for emergency suspension. If there is a substantial expectation that a certificate may become mis-used; for example if a private key has been inadvertently exposed through a website, and the web server logs indicate that the key has been downloaded from suspect IP addresses then this would be a reason for emergency suspension.

In the security risk assessment carried out in 2012, the threat with the second highest impact was judged to be ‘resources used for on-line attacks to a 3rd party’. The ability to quickly prevent further jobs being successfully submitted to further the attack using a particular certificate is an important mitigation of this threat.

A security incident, defined as the act of violating an explicit or implied security, is likely to lead to security emergency suspension.

Not all cases where a DN may be subject to emergency suspension can be defined in this document. The EGI CSIRT IRTF must be allowed discretion to decide if it is necessary to carry out emergency suspension to protect the infrastructure.

5.5 Suspension does not imply certificate owner is at fault

It should also be made clear that the fact that a certificate is compromised and that there is a need for emergency suspension does not imply that the owner of the certificate is at fault. The certificate could have been compromised due to a mis-configured site, a vulnerability exposing a certificate publicly, or error of a 3rd party. Similarly, a security incident involving a DN does not imply fault on the user's part, again the certificate could have been exposed due to a mis-configured site, a vulnerability, or error of a 3rd party. However, the reason why the certificate was compromised needs to be investigated and understood if possible in order to prevent a re-occurrence.

There is also the possibility that a DN may be suspended if a security incident occurs on a host, but it is not possible to quickly find which DN is responsible. In this case, EGI CSIRT must have the ability to suspend all the suspect identities, even if some of them are innocent, to stop the incident from spreading through the infrastructure.

It is not an especially contrived scenario that malicious activity from a host is observed (say, denial-of-service attacks against American media sites), that it is possible can tell from third-party logs that a small number of identities are running processes on that host, but it is not possible to tell exactly which of them are engaging in the bad activities without manual intervention from the local site admin, which may take hours. In such as case EGI CSIRT must have the ability to suspend all suspect identities, even though some are likely to be innocent, to stop the incident from spreading through the infrastructure.

Suspension is a quickly revertible action that is designed for stabilizing the situation in an on-going, serious incident.

5.6 Re-instating a DN

If a DN has undergone emergency suspension, when the problem has been resolved, re-instatement (or white listing) can happen very quickly via the central emergency suspension framework (Argus server). Unless the site has its own manual mechanism for carrying out emergency suspension, no manual site action is needed to undo the emergency suspension.

5.7 Emergency Suspension vs Certificate Revocation

Emergency suspension of a DN is carried out using procedures available to the EGI CSIRT.

Emergency suspension is separate from certificate revocation by a CA, and EGI CSIRT does not control certificate revocation.

A Certificate is issued as a result of a contract between an individual user and the CA, and involves vetting the users' identity. It is proof of a users' identity. EGI CSIRT does not revoke certificates.

If a certificate has been implicated in a security incident, this does not affect the contract between the User and the CA which established the Users identity. But it may mean that the user has acted in a way which means they are prohibited from using the EGI infrastructure. It may also mean that the Certificate has been exposed or actions have been carried out by a person other than the rightful owner of the certificate, in this case it will be necessary to revoke the certificate and for the user to obtain a new one before they are permitted to use the EGI infrastructure.

If an incident exposes DNs, or an incident is associated with a DN, then the DN(s) will be suspended. EGI CSIRT cannot distinguish between (malicious) jobs submitted by a regular user or a person that uses a stolen certificate. EGI CSIRT can only say that a certain action connected to certain identity (certificate proxy) is outside the permissive usage of our resources, and in that case the DN will need to be suspended. After investigations have proceeded it may not be necessary to revoke the certificate, and it may be appropriate to quickly re-instate the DN.

EGI CSIRT cannot and does not revoke certificates, even in the case where they have an unprotected private key. However if EGI CSIRT does have an unprotected private key which has been exposed outside policy they may send it to the CA suggesting the certificate is revoked.

6 COMPROMISED USER CERTIFICATES

6.1 Assessing the situation when user certificate(s) are compromised

Not all user certificate compromises will need the procedure described in section 2 which includes security emergency suspension.

Information on storage of private keys is available in [R 8].

The user certificate private key must be protected by a password, but this is not generally enforced; also the passphrase may be stored on the device. For example, if an ordinary user mislays a memory stick, which contains their user private key without a password or with the password on the device the chance of that stick being found by someone who knows what it is for, how to use it, and chooses to use it is quite low. The appropriate action would probably be for the user to simply revoke their certificate and apply for a new one as a precaution, carrying out the steps in 6.2. Cases like this are probably handled by users from time to time and do not come to the attention of EGI CSIRT. If the memory stick contains an unencrypted private key which allows administration of a database, and the stick is in a bag which has been stolen, it may be necessary to carry out the procedure described in section 2 which includes central security emergency suspension.

Similarly if a mis-configured site or software vulnerability exposes proxies in a limited way to other authorized users EGI CSIRT may decide it is not worth doing anything, that the chance of any authorized user both finding the problem and exploiting it is not sufficient to consider the certificates to be compromised.

Types of cases where the procedure including central security emergency suspension is necessary are described in sections 5.3 and 5.4

When a compromise comes to the attention of EGI CSIRT, it will be for EGI CSIRT to consider whether no action is necessary, whether actions in 6.2 are appropriate, or whether the procedure in section 2 is appropriate.

6.2 Simple revocation and request for a new certificate

This is a simple procedure which the user may carry out if they have, for example, lost a device containing their private key, or accidentally exposed their private key in a limited way. This is if there is no evidence that anyone has used the private key. It should be noted that a user may revoke a certificate at any time for a variety of reasons, including following the end of their association with their home institution. If a compromise comes to the attention of EGI CSIRT, and EGI CSIRT think this is the appropriate procedure then they may instruct the user to carry out this procedure.

6.2.1 The certificate should be revoked

The user should revoke their certificate. This may be simply done by the user if they have their private key or their private key is managed via a system they are able to access. If not, for example if they have lost the only copy of the private key, they should contact the CA to arrange its revocation.

6.2.2 Any proxies from long term storage should be removed

The user should remove any proxies from long term storage, such as MyProxy.

6.2.3 The user may request a new certificate

The user will need to apply for a new certificate in order to resume usage of the Grid.

6.2.4 The user may ask to re-join VOs

The user will need to re-join VOs once again signing the Acceptable Use Policy using the new certificate in order to resume their work.

The user should see the info for their VOs from the VO operations portal [R 9]

6.3 Notes on procedure including central security emergency suspension for compromised or mis-used user certificate

This provides notes on some of the steps of the procedure defined in section 2 to be carried out in the case where a user certificate or proxy of a user certificate has been found to be or suspected of being compromised. These are the type of cases described in 5.4 where emergency suspension is needed as part of the procedure.

If the need for this procedure is due to an on-going incident, then most of the communication will take place as part of the on-going EGI security incident response procedure as [R 2].

Note that it is not compulsory to carry out all steps, but are at the discretion of the IRTF member handling the situation, and most will be carried out in most cases unless there is good reason not to.

Note that all information should be sent as 'Amber' information [R 6].

6.3.1 Informing sites and NGIs of suspension of DN(s)

Sites and NGI security contacts should be informed of emergency suspension by e-mail to site-security-contacts@mailman.egi.eu and ngi-security-contacts@mailman.egi.eu that a certificate has undergone emergency suspension. The e-mail should include the user's DN(s), and a brief reason why the DN(s) has/have been suspended.

This allows sites to monitor for unexpected activity related to suspended DN(s), and to stop any jobs associated with that particular DN. This is also useful if they are not automatically rejecting DNs suspended by the central security emergency suspension tool, or for any software which is not yet integrated with the central emergency suspension.

6.3.2 Informing VOs of security emergency suspension of DN(s)

VOs may be informed of the emergency suspension of the DN(s). This may be confined to affected VO(s) where the user DN is known to be associated.

6.3.3 Informing the IGTF of security emergency suspension

If appropriate, the IGTF should be informed of security emergency suspension.

This can be done by e-mail to igtf-general@gridpma.org

This is not appropriate in all circumstances.

In the case where emergency suspension is due to a root compromise at a site exposing usable certificates then it is very appropriate to contact the IGTF.

In the case where a certificate is NOT an IGTF certificate, obviously informing the IGTF would not be appropriate, but other CAs may be informed if EGI CSIRT considers it appropriate.

6.3.4 Certificate revocation

If it is clear that certificates have been exposed, unless only short lived proxies (proxy life less than 24 hours) have been exposed, then the certificate(s) should be revoked to prevent it's further usage on the EGI and other infrastructures, and at least prior to the lifting of emergency suspension.

This is not carried out by the EGI CSIRT.

This may be simply done by the user, if it is possible to contact them and if they have their private key or their private key is managed via a system they are able to access. If not, for example if they have lost the only copy of the private key, they should contact the CA to arrange its revocation.

In the case of IGTF certificates which are confirmed to be exposed, EGI CSIRT should request revocation by the CA(s) indicating any exposure of the credential. For example, if a system storing private keys has had a root compromise then it is likely that the IGTF CA(s) will revoke certificates on the request of EGI CSIRT IRTF.

If the user is identified using a commercial CA then it is likely that only the user can revoke their certificate, if this is appropriate.

6.3.5 Contacting long term proxy storage providers

EGI CSIRT may contact long term proxy storage providers, such as those running 'Myproxy' stores, if appropriate. It is not possible for EGI CSIRT to ensure all long term proxies are removed, and the certificate owner will need to confirm this as one of the steps in 6.3.7.

6.3.6 Carrying out incident response and any further investigation

In most cases it is expected that the emergency suspension will be due to a security incident, and this will be handled by EGI CSIRT according to the EGI CSIRT incident handling procedure [R 2]. Most of the communication will be according to the workflow contained in the incident handling procedure, which are not repeated here.

This may include contacting the certificate owner if appropriate.

6.3.7 Removing security emergency suspension of user

The emergency suspension of the user may be removed by the EGI CSIRT team using the Central Emergency Suspension Framework, when it is considered appropriate. This will be considered on a case by case basis.

The following will be taken into account:

- The user has been contacted and co-operated
- The certificate has been revoked, if appropriate
- Any proxy which has been exposed has expired
- The user has confirmed that all long term proxies from MyProxy or any other system for storage of long term proxies in use have been removed
- Investigations are complete, or have progressed sufficiently for the users' access to be restored
- In the case where the certificate was mis-used, that this action has been understood and steps have been taken to ensure that it is unlikely the action will be repeated.
- If a number of DNs were suspended during an incident, and investigations showed that the DN was not be involved

6.3.8 Informing sites and NGIs if security emergency suspension is removed

Sites and NGI security contacts should be informed by e-mail to site-security-contacts@mailman.egi.eu and ngi-security-contacts@mailman.egi.eu when DN(s) are no longer under emergency suspension. This may be done separately, before the final report on the incident investigation, or if the incident investigation is complete this may be as part of the incident report.

6.3.9 Inform the IGTF if security emergency suspension is removed

The IGTF should be informed when emergency suspension is removed, if previously IGTF was informed of the emergency suspension. EGI CSIRT may wish to state it is appropriate to allow the user access to the EGI infrastructure. It may be appropriate to say something of the results of the investigation. This can be done by e-mail to igtf-general@gridpma.org

6.3.10 Report to the OMB

When investigations are complete, the OMB will receive a report of the incident as part of the incident handling procedure [R 2]. This will include information on suspended DN(s) and the outcome. EGI CSIRT should respond to any questions on this report. Interim information may also be reported to the OMB at EGI CSIRT's discretion. Note that normally when an incident is taking place, EGI CSIRT will need to concentrate on dealing with the incident, rather than answering questions from OMB members – however they will answer questions during the incident if it does not interfere with handling the incident.

6.3.11 User may resume their work

In most cases, the certificate will have been revoked. The user will need to apply for a new certificate in order to restore access. The user will then need to re-join VOs once again signing the Acceptable Use Policy (AUP) using the new certificate. The user should see the info for their VOs from the VO operations portal [R 9]

6.4 Effects of security emergency suspension for compromised user certificates

In cases of a regular user certificate this will affect only one person. If a number of certificates are compromised (for example if an incident exposes a number of proxies) this will affect the owners of all compromised certificates.

7 NOTES MULTI USER CERTIFICATES

7.1 Types of multi user certificate

There are two main types of multi user certificates in use in the EGI infrastructure at present; these are Robot certificates and Multi User pilot job certificates.

In both these cases actions are taken operationally by EGI CSIRT as in section 2 including emergency suspension. Here we note some specific points associated with multi user certificates.

7.2 Robot certificates

Robot certificate usage is increasing, including for the authentication of users who do not have personal certificates but use various services through the use of portals. Guidelines for use of Robot certificates are provided by the EUGridPMA [R 3]. Usually, there is no easy physical way to get to the hardware tokens, also the proxy creation and storage process is not accessible to the users. Other set-ups have the hardware tokens plugged into the portal, which is probably the weakest point in that technology, since users have to be able to access it.

Hopefully, a compromised Robot Certificate should be a rare event but the possibility cannot be ignored.

7.2.1 Procedure notes for compromised robot certificates

If a robot certificate has been compromised it is quite likely that the owner of the certificate discovers the problem, e.g. an incident concerning the hardware on which the key is installed or loss or theft of the hardware device.

The procedure for a compromised robot certificate will be that in section 2. As far as the EGI CSIRT is concerned, it will be treated in a similar way to a compromised user certificate, only further investigation will need to be carried out by the robot owner, to find out how the abuse happened. Emergency suspension will be carried out in all cases.

In parallel to the incident response investigation the owner of the certificate involved will need to contact the users to let them know that services are temporarily suspended. After restoration of the service the owner will again need to contact the users to inform them that service is available again.

7.2.2 Effect of security emergency suspension of compromised robot certificates

As a robot normally allows a number of users to submit jobs via a portal, until investigation is complete and the portal is restored emergency suspension will affect all users depending on the portal which uses the certificate to submit jobs to the infrastructure.

The impact would be higher for robot certificates on which the Nagios system is based, as the entire infrastructure is dependent on this.

7.3 Compromises concerning pilot job frameworks

Pilot job frameworks are used whereby the pilot owner submits jobs which allow other users jobs to be executed on the infrastructure.

7.3.1 Procedure notes for certificates associated with pilot jobs

Operationally, from the EGI CSIRT point of view this is similar to a user certificate compromise, and the steps in section 2 will be carried out.

It will also be necessary to contact the pilot owner.

In cases of multi-user pilot jobs which DN is suspended depends on the particular set-up. If only the pilot-submitter appears in the logs, this DN has to be suspended (affecting many users), if it is possible to operate on the pilot user, and only the pilot user is implicated in the incident, then the DN for that particular user will be suspended. The EGI-CSIRT is aware of the particularities of multi-user pilot jobs and will try to minimize the impact on the VOs production.

7.3.2 Effect of security emergency suspension associated with pilot jobs

If it is clear that one pilot user is carrying out the inappropriate activity, then it may be possible to suspend the one pilot user.

If this is not possible, and it is necessary to suspend the pilot job submitter, then all users who rely on that pilot job submitter will effectively be suspended from this activity.

8 REFERENCES

R 1	The International Grid Trust Federation (IGTF) http://www.igtf.net/
R 2	The EGI security incident handling procedure https://documents.egi.eu/secure/ShowDocument?docid=710
R 3	EU Grid PMA guidelines for robot certificates http://www.eugridpma.org/guidelines/robot/
R 4	The Argus Authorization Service https://twiki.cern.ch/twiki/bin/view/EGEE/AuthorizationFramework
R 5	The Service operations security policy https://documents.egi.eu/public/ShowDocument?docid=1475
R 6	Distribution Restrictions Traffic light protocol https://wiki.egi.eu/wiki/EGI_CSIRT:TLP
R 7	Emergency release of IGTF trust anchor https://wiki.egi.eu/wiki/EGI_IGTF_Release_Process
R 8	EU Grid PMA Guidelines on Private key protection https://www.eugridpma.org/guidelines/pkp/
R 9	VO operations portal http://operations-portal.egi.eu/vo

APPENDIX A FURTHER INFORMATION

A.1 FURTHER INFORMATION ON CONTACTING IGTF

If there a risk or incident to be assessed by the IGTF, there is the IGTF-RAT for that:
<igtf-rat@eugridpma.org>

For generic concerns about the IGTF distribution:
<concerns@eugridpma.org>

For the EGI specific trust anchor distribution:
<egi-igtf-liaison@nikhef.nl>