



LCG Security Group

Approval of LCG-1 Certificate Authorities

<i>Date:</i>	2nd June 2003
<i>Version:</i>	1.0
<i>Status:</i>	Final
<i>Author:</i>	David Kelsey



Document Log			
Issue	Date	Author	Comment
1.0	2 June 2003	David Kelsey	For approval at 10 th June 2003 GDB



1 Introduction

The LCG Security Group has proposed a procedure by which the list of trusted Certificate Authorities for use in LCG-1 should be created and maintained. This was presented to the LCG GDB meeting of 8th May 2003. The proposal has been updated following the discussion at that meeting.

This paper presents the revised procedure and the current list of Certificate Authorities to be used in LCG-1 from July 2003 for the rest of this year. The procedure will be reviewed before the end of 2003 at which time it should be clearer what body will replace the EDG CA Managers Group.

2 Procedure for approving and implementing trusted Certificate Authorities during 2003

- 1) The LCG-1 Security Group proposes the list of accepted CA's from two sources:
 - a) The list of "traditional" CA's, issuing long-lived (12 months or more) certificates, comes from the EDG CA Group
 - b) The list of additional CA's (online short-lived, special cases, etc.) is generated by the LCG-1 Security Group
- 2) Proposed additions to these lists above will be circulated to the GDB and to the LCG-1 site security contacts for objection prior to implementation
- 3) The LCG-1 operations team maintains the necessary information (certificates, signing policy, CRL's) and distribution mechanisms for CA's on both sub-lists
- 4) All LCG-1 resources will install the full list of approved CA's

3 The initial list of trusted CA's for LCG-1

The current list of EDG-trusted CA's, consisting of DataGrid and CrossGrid CA's, are presented in 3.1 and 3.2. Some CA's appear on both lists. The union of 3.1 and 3.2 is the current EDG list. These are the CA's deemed to have met the minimum requirements specified in <http://hepwww.rl.ac.uk/edgwp6ca/docs/CAminreqsv2.txt>

This combined list results in the following 18 approved CA's:

Canada, CERN, Cyprus, Czech Republic, France, Germany, Greece, Ireland, Italy, Netherlands, Nordic countries, Poland, Portugal, Russia, Slovakia, Spain, UK, and USA.

The "catch-all" CA able to issue certificates to users, hosts and services without access to a local national CA is currently France/CNRS. This requires the satisfactory negotiation and agreement of an appropriate Registration Authority to check and confirm identities. This service will be reviewed before the end of 2003 to decide an appropriate "catch-all" for 2004 and onwards (or perhaps earlier).

The next meeting of the EDG CA group will be held at CERN on 12th/13th June 2003. Several new CA's will be considered at that meeting and may therefore also be available for use in July 2003.

An additional online CA from FNAL, issuing short-lived certificates, is listed in 3.3. This will not be added to the list of trusted "traditional" CA's as both EDG and LCG have decided to treat online (short-lived certificates) CA's separately. The best practice and minimum requirements for this type of service, different in nature from the "traditional" CA's, will be worked on during the rest of the year.

3.1 DataGrid Certificate Authorities

See <http://marianne.in2p3.fr/datagrid/ca/>

CA	CA Certificate	CA CRL	CP/CPS
CERN	bc870044.0	bc870044.r0	X
Czech Republic - CESNET	ed99a497.0	ed99a497.r0	X
France - CNRS	cf4ba8c8.0	cf4ba8c8.r0	X <i>in French</i>
France - CNRS-Projets	34a509c3.0	34a509c3.r0	.
France - CNRS Datagrid-fr	6b4ddd18.0	6b4ddd18.r0	X <i>in English</i>
Germany - GermanGrid	6df70cb1.0	6df70cb1.r0	X
Ireland - Grid-Ireland	1e43b9cc.0	1e43b9cc.r0	X
Italy - INFN	df312a4e.0 <i>Php script</i>	df312a4e.r0 <i>DER format</i>	X
Netherlands - NIKHEF	16da7552.0	16da7552.r0	X
Nordic countries - NorduGrid	1f0e8352.0	1f0e8352.r0	.
Portugal - LIP	41380387.0	41380387.r0	X
Russia - Russian DataGRID	d64ccb53.0	d64ccb53.r0	X
Spanish - DATAGRID-ES	90e2484f.0	90e2484f.r0	X
United Kingdom - GridPP	0ed6468a.0	0ed6468a.r0	.
United Kingdom - UK e-Science <i>New UK CA</i>	01621954.0	01621954.r0	X
US - DOE Root CA	6349a761.0	6349a761.r0 <i>DER format</i>	.
US - DOE Sub CA	9d8753eb.0	9d8753eb.r0 <i>DER format</i>	X
Canada CA	5f54f417.0	5f54f417.r0	X

3.2 CrossGrid Certificate Authorities

<http://grid.ifca.unican.es/crossgrid/wp4/ca/>

COUNTRY 	CPS	CA Cert	CA CRL	TEST	CENTER	Contact Person
 Slovakia	CPS	CA Cert	CA CRL	CERT CRL	II SAS	Jan Astalos
 Cyprus	pdf,ps	CA Cert	CA CRL	CERT CRL	UCY	Wei Xing
 Germany	CPS	CA Cert	CA CRL	CERT CRL	FZK	Ursula Epting
 Greece	CPS	CA Cert	CA CRL	CERT CRL	AUTH	Christos Kanellopoulos
 Netherlands	CPS	CA Cert	CA CRL	CERT CRL	NIKHEF(*)	David Groep
 Ireland	CPS	CA Cert	CA CRL	CERT CRL	TCD	Brian Coghlan
 Poland	CPS	CA Cert	CA CRL	CERT CRL	PSNC	Pawel Wolniewicz
 Portugal	CPS	CA Cert	CA CRL	CERT CRL	LIP	Jorge Gomes
 Spain	CPS	CA Cert	CA CRL	CERT CRL	IFCA	Rafael Marco

3.3 Additional LCG-1 CA's

The additional online CA, issuing short-lived certificates, for LCG-1 is the FNAL Kerberos CA (KCA) and its root CA. See <http://computing.fnal.gov/security/pki/>

- GC - Globus-based clients
- GS - Globus-based services
- WB - Web browsers
- WS - Web servers

Who?	File	Description
GC	7a15b590.0	FNAL Root CA certificate (store it under this name for Globus)
GC	7a15b590.signing_policy	FNAL Root CA signing policy
GS, WS	e1fce4e9.0	New FNAL KCA certificate (store it under this name for Globus or in Apache's SSLCACertificatePath)
GS	e1fce4e9.signing_policy	New FNAL KCA signing policy
GC, GS	fnal-certs-2.tar	All four of the above files (and two related to the previous KCA format).
WS	fnal-kca-cert-2.pem	New FNAL KCA certificate - the same contents as e1fce4e9.0, but MIME tagged for easy import into a web browser
WB	fnal-root-ca.pem	FNAL root CA certificate - the same contents as 7a15b590.0, but MIME tagged for easy import into a web browser
WB	fnal-root-crl.crl	The CRL (Certificate Revocation List) for the FNAL Root CA
GC	fnal-root-crl.base64	The same CRL in Base64 (or "PEM") format

4 Approval by GDB

The LCG GDB is asked to approve both the procedure (section 2) and the initial list of trusted CA's (sections 3.1, 3.2 and 3.3).