



DSA1.1 REPORT ON BGCA AND RA NETWORK

REPORT ON IMPLEMENTATION OF CERTIFICATION
AUTHORITY OF BG AND THE NETWORK OF RAS

Document Filename:	BG-DSA1.1-v1.0-EENet-CA_RA.doc
Activity:	SA1
Partner(s):	EENet, NICPB, LATNET, VU
Lead Partner:	EENet
Document classification:	PUBLIC

Abstract: (Must not go beyond this first page)

The Certification Authority and the network of Registration Authorities is a crucial part of the grid infrastructure. This document describes the creation and operations of Baltic Grid CA and its RA network.





Document review and moderation

	Name	Partner	Date	Signature
Released for moderation to				
Approved for delivery by				

Document Log

Version	Date	Summary of changes	Author
0.1	16/12/2005	Draft version 1	Lauri Anton
0.2	6/1/2006	Draft version 2	Lauri Anton
0.3	10/1/2006	Draft version 3	Lauri Anton
0.4	11/1/2006	Draft version 4	Lauri Anton
0.5	18/1/2006	Draft version 5	Lauri Anton, Per Öster
0.6	23/1/2006	Draft version 6	Lauri Anton, Hardi Teder
0.7	24/1/2006	Draft version 7	Lauri Anton, Hardi Teder
0.8	31/1/2006	Draft version 8	Lauri Anton, Zofia Mosurska, Pawel Wolniewicz
0.9	8/2/2006	Draft version 9	Lauri Anton, Marcin Radecki



CONTENTS

1. ACRONYMS AND ABBREVIATIONS LIST	4
2. INTRODUCTION.....	5
3. BALTIC GRID CERTIFICATION AUTHORITY	6
3.1. CERTIFICATION AUTHORITY	6
3.2. NETWORK OF REGISTRATION AUTHORITIES	6
3.3. BALTIC GRID CA CP/CPS	7
3.4. EUGRIDPMA	7
4. OPERATIONS OF BALTIC GRID CA AND RA NETWORK.....	9
4.1. BGCA OPERATIONS	9
4.2. RA OPERATIONS.....	10
4.3. JOINING WITH VIRTUAL ORGANISATION.....	10
5. FUTURE OF BALTIC GRID CA AND RA NETWORK.....	11
5.1. BALTIC GRID CA	11
5.2. RA.....	11
5.3. PARTICIPATION IN INTERANTIONAL COLLABORATION.....	11
6. LINKS	12



1. ACRONYMS AND ABBREVIATIONS LIST

CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
BG	Baltic Grid
BGCA	Baltic Grid Certification Authority
EENet	Estonian Educational and Research Network
EUGridPMA	European Policy Management Authority for Grid Authentication in e-Science
IMCS UL	Institute of Mathematics and Computer Science, University of Latvia
NICPB	National Institute of Chemical Physics and Biophysics
PGP	Pretty Good Privacy
PKC	Public Key Cryptography
PKI	Public Key Infrastructure
PSNC	Poznan Supercomputing and Networking Center
RA	Registration Authority
VO	Virtual Organisation
VU	Vilnius University



2. INTRODUCTION

To rely on someone, there must be mutual trust between parties. One of the basic requirements is to know the other's identity. In the physical world, someone's identity can be checked by comparing the person's identification document with a picture, may it be passport, ID-card or drivers license, to the bearer of the document. That ID-document has been issued by some national institution, which is trusted by wide audience and which takes care of the initial authentication of the person. To get an ID-document, the person has to go to that national institution and has to prove his/her identity based on previous documents.

In the virtual world, one possible solution is to use certificates based on public key cryptography, where Certification Authority (CA) certifies the identity of the certificate holder.

Typically there is one CA setup per country, region or an organisation. In BalticGrid project there are five countries. Poland is running Polish Grid CA operated by PSNC, people in Sweden can obtain certificates from NorduGrid CA operated by Niels Bohr Institute and EENet in Estonia operates Estonian Grid CA. The only remaining countries were Latvia and Lithuania. It was decided, that there will be the new Baltic Grid CA and it will issue certificates for all three countries – Estonia, Latvia and Lithuania. This new CA created as a part of Baltic Grid project is described in detail in this document.

Information about Polish Grid CA can be found at <http://www.man.poznan.pl/plgrid-ca>, information about NorduGrid CA can be found at <http://hep.nbi.dk/CA/>.

In first part this document gives an overview about Baltic Grid Certification Authority, Network of Registration Authorities, policy document and EUGridPMA. Second part describes BGCA operations and the last part describes the future of the Baltic Grid CA.



3. BALTIC GRID CERTIFICATION AUTHORITY

3.1. CERTIFICATION AUTHORITY

In cryptography, a certification authority (CA) is an entity which issues digital certificates for use by other parties. It is an example of a trusted third party. CA is part of various public key infrastructure (PKI) schemes.

In the virtual world, the X.509 certificates based on public key cryptography are used as ID-documents for persons and computers. To obtain a certificate, the person has to be validated by some trusted institution. CA is an institution that checks the identity of the certificate requester, and by signing the certificate approves to the Relaying Parties, that the certificate identifies that person.

The scope of the Baltic Grid Certification Authority (BGCA) is to provide authentication and certification service for grid initiatives in the Baltic States (Estonia, Latvia and Lithuania).

Estonian Educational and Research Network (EENet) has experience in operating a grid CA since 2004 when the Estonian Grid Project started. The Estonian Grid CA, which is being run by EENet, got accreditation from EUGridPMA on September 24th in 2004.

Performing the everyday activities of a CA is not a big economic burden on an institution, but the participation in various international bodies (like EUGridPMA) demands some resources. When the Baltic Grid initiative started, EENet proposed that it may run one CA for all Baltic Countries, because EENet was already running Estonian Grid CA and it had the necessary knowledge. The proposal was accepted and a single CA that would serve the whole Baltic region was set up. It was established before the November 1st in 2005, the starting date of the Baltic Grid project, because a CA is the crucial part of grid infrastructure and without it, current grid software is not able to work.

The Estonian Grid CA is being phased out and new certificates for Estonian entities are issued by BGCA.

The Baltic Grid CA is operated by EENet employees Lauri Anton and Hardi Teder.

BGCA has a web page <http://ca.balticgrid.org/>

3.2. NETWORK OF REGISTRATION AUTHORITIES

A person requesting a personal certificate needs to be securely validated. This can be achieved via face-to-face meetings or via some governmental PKI system. Such system is currently available only in Estonia (Estonian ID-card, <http://www.id.ee/pages.php/0303>).

If governmental PKI cannot be used, then the face-to-face meeting has to be used. In order to reduce the travelling to the Certification Authority by all requestors a network of Registration Authorities is set up. Registration Authority (RA) is a person authorized by the CA to act as an identity checker. He or she typically works in one of the institutions participating in grid activities.

RA network expands to all Baltic States, currently there are 10 persons acting as a RA.

Country	Institution	RAs Name
Estonia	EENet	Lauri Anton
	EENet	Hardi Teder
	NICPB	Mario Kadastik
	NICPB	Andi Hektor
	Tartu Observatory	Tõnis Eenmäe
Latvia	LATNET	Mārtiņš Freivalds



	LATNET	Uldis Koškins
Lithuania	VU	Rolandas Naujikas
	VU	Eduardas Kutka
	KTU	Kęstutis Paulikas

In the future, there should be at least one RA in every major institution that takes part in grid activities at Baltic countries.

The trust network between CA and RAs is established in face-to-face meetings between CA representative and RAs. On those meetings, CA representative and a RA exchange PGP key fingerprints and other information in order to establish secure communication methods using electronic channels. After that, CA and RAs can communicate with each other in trustful manner.

3.3. BALTIC GRID CA CP/CPS

The operations and procedures of a CA are described in a policy document called Certificate Policy and Certification Practice Statement (CP/CPS). In that document are described all procedures needed for establishing, running and closing the CA. BGCA CP/CPS was based on the Estonian Grid CA CP/CPS with necessary modifications.

Timeline of the Baltic Grid CA CP/CPS.

22.05.2005	Baltic Grid CA CP/CPS v0.1
26.05.2005	First presentation of BGCA on EUGridPMA
21.09.2005	Baltic Grid CA CP/CPS v1.0, new namespace
28.09.2005	Baltic Grid CA CP/CPS got accreditation from EUGridPMA
10.01.2006	Baltic Grid CA CP/CPS v1.1, bugfix release

The BGCA issues certificates to natural persons, computer and service entities. The entities eligible for certification from the BGCA are all those related to organizations, that are involved in research or deployment of multidomain distributed computing infrastructure, intended for cross-organizational sharing of resources, formally based in and/or having offices in Estonia, Latvia or Lithuania. The focus of these organizations should be in research or education, but certificate requests from commercial companies involved in grid development are also accepted.

The enforceability, construction, interpretation and validity of the policy of the BGCA are governed by the Laws of the Republic of Estonia. Legal disputes arising from the operation of the BGCA will be handled according to Estonian laws, legal disputes arising from the operation of the Registration Authorities (RAs) will be handled according to the law of the hosting country, respectively.

The latest BGCA CP/CPS is available on BGCA web page (<http://ca.balticgrid.org>).

3.4. EUGRIDPMA

For coordinating the work of the CA-s and their policies, the policy management authorities have been set up.

The European Policy Management Authority for Grid Authentication in e-Science (hereafter called EUGridPMA) is a body to establish requirements and best practices for grid identity providers to enable a common trust domain applicable to authentication of end-entities in inter-organisational access to distributed resources. As its main activity the EUGridPMA coordinates a Public Key



DSA1.1 REPORT ON BGCA AND RA NETWORK
Report on implementation of Certification Authority of BG and
the Network of RAs

Infrastructure (PKI) for use with Grid authentication middleware. The EUGridPMA itself does not provide identity assertions, but instead asserts that - within the scope of this charter - the certificates issued by the Accredited Authorities meet or exceed the relevant guidelines.

EUGridPMA Minimum Requirements states that there should be a single Certification Authority (CA) organisation per country, large region or international organization. The goal is to serve the largest possible community with a small number of stable CAs. To achieve sustainability, it is expected that the CAs will be operated as a long-term commitment by institutions or organisations rather than being bound to specific projects.

The accreditation from EUGridPMA gives acceptance for certificates issued by Baltic Grid CA for use in international grid projects like EGEE and NorduGrid.

EENet have been participated regularly on EUGridPMA meetings since 2004. BGCA got accredited by EUGridPMA on September 28th, 2005.

BGCA has to keep its policy in compliance with standards and requirements set by EUGridPMA and other international organisations. BGCA may be audited by members of EUGridPMA or by Relaying Parties.



4. OPERATIONS OF BALTIC GRID CA AND RA NETWORK

Operating a CA consists of various operations, of which some are purely technical, others include many legal and administrative issues. All the policies and procedures described below are fully defined in Baltic Grid CA CP/CPS.

4.1. BGCA OPERATIONS

The BGCA is responsible for all aspects of the issuance and management of a certificate referencing the CP/CPS, including:

1. Certificate application/enrolment process;
2. Verification of the identity of the applicant;
3. Certificate signing process;
4. Revocation of the certificate;
5. Certificate renewals;
6. Issuing and publishing certificate revocation lists;
7. Ensuring that all aspects of the CA services and CA operations and CA infrastructure related to certificates issued under this policy are performed in accordance with the requirements, representations, and warranties of the CP/CPS;
8. Auditing periodically the work of RAs.

The software of the BGCA is based on OpenSSL wrapped with BASH shell and Perl scripts. Knoppix Linux is used as the operating system.

BGCA hardware consists of 2 USB memory sticks and a laptop computer with no network connection. One of the USB memory sticks contains all the CA scripts and databases. The other is for transporting requests and other data to and from CA. USB sticks and the CDROM with Knoppix Linux are kept in safe.

The private key of the CA must be protected from unauthorized use or compromise at all times. If the CA's private key is compromised, then all certificates signed with that key will be treated as invalid. Therefore the protection of the CA's private key is one of the main obligations of a CA.

The private key of the BGCA is only available in encrypted form on a USB memory stick stored in a safe box. The key used for encryption is at least 15 characters long. The computer used to activate private key is every time booted up with fresh operating system from the Knoppix CDROM.

The backup copy of the private key is kept in another safe on CDROM and on paper media.

CA operations are logged on paper. Types of events recorded:

1. Boot and shutdown of CA machine;
2. Interactive system logins;
3. Certification requests;
4. Revocation requests;
5. Issued certificates;
6. Issued CRLs.



If the end entity's secret key is lost or compromised, the CA must be notified. CA will revoke the certificate and issue a new Certificate Revocation List.

BGCA's goal is to have response time of one day in certificate issuance and revocation operations.

Until 17.01.2006 Baltic Grid CA has issued 87 certificates, of which 31 are personal and 56 host or service certificates.

4.2. RA OPERATIONS

The RA checks the identity of a person in face-to-face meeting with the requester or via using national PKI. It collects various data from the requester:

1. copy of the photo-ID;
2. Requestor's name with diacritical marks
3. Requestor's name without diacritical marks;
4. Postal address
5. Telephone
6. E-mail address

The requester has to deliver the certificate request to a RA. The RA checks that the request is valid and is compatible with BGCA's policy document. If the request is correct, then the RA sends it to the CA using secure communication methods, for example using e-mail encrypted with the RA's own certificate or PGP key.

In all operations, RA has to follow the policies and procedures described in BGCA CP/CPS.

4.3. JOINING WITH VIRTUAL ORGANISATION

Certificate is needed, because it allows a user to start applying for grid resources. Virtual Organisations (VO) join together those, who are allowed to use certain resources, like resources in one institute or in one country.

Most resources made available via Baltic Grid Project can be accessed, when user joins the Baltic Grid VO. Description of the VO and the guide for registration can be found from http://www.balticgrid.org/SA1_Activity/bgvoregistration



5. FUTURE OF BALTIC GRID CA AND RA NETWORK

BGCA is a fully functional CA: it issues certificates, maintains the CRL and has the network of RA-s. Still BGCA needs further development.

5.1. BALTIC GRID CA

BGCA is organisationally tied to EENet and it should give to the BGCA reasonable organisational stability. One of the objectives of EENet is developing grid in Estonia and it includes running a CA.

The software used for CA operations must be developed further, it has to include network-accessible databases. The BGCA webpage has to be enhanced and developed, separate page for certificate users has to be created. The interface for signing certificates is currently not very convenient and needs development. Also there should be created automatic system for sending expiration warnings to certificate holders.

5.2. RA

In the future, there should be at least one RA in every major institution that takes part in grid activities. The web-based interface for RA operations must be developed, where information may be gathered at central database and the requests can be posted for signing.

5.3. PARTICIPATION IN INTERANTIONAL COLLABORATION

Running a CA itself is not a big economical burden on an institution. Significant amount of financial resources is used for communication and taking part of the work of the EUGridPMA and other international resources. It is not economically feasible that each Baltic State has its own CA before the number of active certificates reaches a couple of thousands.

BalticGrid has to continue its membership in EUGridPMA, because therefore certificates issued by members of EUGridPMA are internationally acknowledged and can be used as ID in grid projects globally.

Baltic Grid CA is in process to join the TERENA TACAR repository.



6. LINKS

Baltic Grid CA	http://ca.balticgrid.org/
Baltic Grid Project	http://www.balticgrid.org/
Estonian ID-card	http://www.id.ee/pages.php/0303
EUGridPMA	http://www.eugridpma.org/
NorduGrid CA	http://hep.nbi.dk/CA/
Polish Grid CA	http://www.man.poznan.pl/plgrid-ca
TERENA TACAR	http://www.tacar.org/
Statute of EENet	http://www.eenet.ee/EENet/statutes2004.html