

# DataGrid WP6/CA Passing the Default Ruleset

Trinity College Dublin (TCD)

Brian Coghlan



default LOW ruleset	CERNO	CESNET	CNRS	CNRS . Projets	СУСА	DATAGRIDIES	DOMS of enceGrid	Datagrid . fr	N-KHEF O	FZK - Grid - CA	GermanGrid	Grid. Ireland	HellasGrid	-NFN -CA	LIPO	Z O L D U G L i D	P L G R I D	RDGRID.CA	SIOVAKGrid	ASGCCA	K H E P	UKesciencecA
Atlas VO		1	0	b		0		0	0	Ю	0		0		Ю	0	0	0				0
CMS VO	2	F	0	6	F	0		6	0	0	0	F	0	F	6	0	0	0			33.	ō
DO VO	2	F	ō	6	F	0		0	0	0	0	F	0	F	0	0	0	0	F	-	22.	ō
LHCb VO	20	F	o	6	F	0		ō	0	0	0	T	0	Г	0	0	0	O	Г	1	22.	ō
Switzerland(CERN)	X	F	o	6	F	0		ō	0	o	0	1	0	F	6	0	o	ō			33.	ō
Czech(CESNET)		X	o	0	Г	0	Г	0	0	o	o	2	ō	ō	ō	0	o	ō	Г	o	0	o
France(CNRS)	-	Γ	X	ō	Г	o	Г	ō	0	0	0	Г	ō	Γ	ō	o	0	o	Г	o	o	o
France(CNRS-Projets)	440	Γ	o	X	Г	o	Г	0	0	0	0	Г	o	Г	ō	o	0	o	Г	o	o	o
Cyprus(CyCA)	100	Γ	o	ō	X	o	Г	0	0	0	0	Г	o	Г	ō	o	0	o	Г	o	o	o
Spain(DATAGRID-ES)		Γ	o	ō	F	X	Г	ō	0	0	0	Г	o	Γ	ō	o	0	0	Г	o	0	o
America(DOEScienceGrid)	o	Γ	0	0	Γ	0	X	ō	0	0	0	Γ	0	Γ	ō	0	0	0	Г	0	o	o
France(Datagrid-fr)	o		0	0	Γ	0	Γ	X	0	0	0	Г	0	Γ	0	0	0	0	Г	0	o	o
Netherlands(NIKHEF)	o	3	0	0	Γ	0	Г	o	X	0	0	1	0	0	0	0	0	0		0	0	o
Germany(FZK-Grid-CA)	o		0	0		0		0	0	X	0	3	0	1	0	0	0	0		0	0	0
Germany(GermanGrid)	o	Γ	0	0		0		0	0	0	X		0	Г	0	0	0	0		0	0	0
Ireland(Grid-Ireland)	0		0	0		0		0	0	0	0	X	0	2	0	0	0	0				0
Greece(Hellas Grid)	100		0	0		0		0	0	0	0		X		0	0	0	0			_	0
Italy(INFN-CA)	-		0	0		0		0	0	0	0		0	X	0	0	0	0		_	_	0
Portugal(LIP)	_		0	0		0		0	0	0	0		0		X	0	0	0				0
Scandinavia(NorduGrid)	100		0	0		0		0	0	0	0		0		0	X	0	0		_		0
Poland(PLGRID)	-		0	0		0		0	0	0	0		0		0	0	X	0			_	0
Russia(RDGRID-CA)	-		0	0		0		0	0	0	0		0		0	0	0	X				0
Slovakia(SlovakGrid)	1/22		0	0		0		0	0	0	0		0		0	0	0	0	X			0
Tai wan(ASGCCA)	_	_	0	0		0		0	0	0	0		0		0	0	0	0			-	0
UK(UKHEP)	-	•	0	0		0		0	0	0	0		0		0	0	0	0			X	
UK(UKeScienceCA)	0		0	0		0		0	0	0	0		0		0	0	0	0	1	0	0	X

### 16/22 FAIL !!!

- Since: (condition) → (graded issue)
- then must define condition per feature → {rules}
  - e.g.: (name eq 'NIL') → (graded issue)
    - thus: if (name eq 'NIL') (graded issue) == (coefficient @ class)
    - per class: (severity) ==  $\Sigma$ (graded issues) limit=1.0
- Allow for classes: [minor | major | severe]
  - Allow for security levels: [high | medium | low]
- Syntax: (condition) severity = (level, class, weight)

```
CA_key_lifetime
if_gt ( 1825 ) severity = (low, severe, 100%)
```

- EDG can define its <u>default ruleset</u>
- each VO can define its own VO-specific ruleset overloadings
- each CA can define its own <u>CA-specific ruleset</u> overloadings

```
# Default Ruleset
inspecting CA:
 name = "default LOW ruleset"
                                           # " < name > "
  if eq ("NIL") severity = (low, severe, 100%)
 alias = default-low
                                           \# < alias >
  if eq ("NIL") severity = (low, severe, 100%)
                                           # < country >
 country =
  if eq ("NIL") severity = (low, severe, 100%)
 country ID =
                                           # < US | IT | CH | IE | ... >
 if_eq ("NIL") severity = (low, severe, 100%)
 CP and CPS:
  RFC2527 compliant = # < true | false >
  #if ne ("true") severity = (low, minor, 20%)
  OID identifier =
                                           \# < OID >
  #if eq ("NIL") severity = (low, minor, 20%)
  OID in cert =
                                  # < true | false >
   #if_ne ("true") severity = (low, minor, 20%)
```

```
# Default Ruleset [CONTINUED]
# CA_web_server:
```

```
publishes CA cert = # < true | false >
if ne ("true") severity = (low, severe, 100%)
publishes CRL =
                                       # < true | false >
if ne ("true") severity = (low, severe, 100%)
publishes CP =
                                       # < true | false >
if ne ("true") severity = (low, severe, 100%)
cert publication max latency = # < days >
if gt(7) severity = (low, severe, 100%)
CRL publication min freq = # < freq in days >
if gt(23) severity = (low, severe, 100%)
CRL publication max latency = # < days >
if gt(0) severity = (low, severe, 100%)
```

```
# Default Ruleset [CONTINUED]
cert issuance:
  CA obtains proof of key possession = # < true | false >
   #if ne ("true") severity = (low, minor, 100%)
  subject keys generated by CA =
                                                   # < true | false >
   if ne ("false") severity = (low, severe, 100%)
 CRLs:
                                           # < period in days >
  lifetime =
   if gt (30) severity = (low, severe, 100%)
  lifetime after revocation = # < period in hours >
   if gt(1) severity = (low, severe, 100%)
 cert signing host:
  controlled physical access = # < true | false >
   if ne ("true") severity = (low, severe, 100%)
 CA private keys:
  backed up =
                                  # < true | false >
   #if ne ("true") severity = (low, major, 50%)
```

```
# Default Ruleset [CONTINUED]
# certs:
```

```
CA_key_size = # < key size in bits >
  if_lt ( 2048 ) severity = (low, severe, 100%)

CA_key_lifetime = # < duration in days >
  if_gt ( 1825 ) severity = (low, severe, 100%)

minimum_subject_key_size = # < key size in bits >
  if_lt ( 1024 ) severity = (low, severe, 100%)

maximum_subject_key_lifetime = # < duration in days >
  if_gt ( 420 ) severity = (low, severe, 100%)
```

```
# Default Ruleset [CONTINUED]
cert profile:
                                           # < X.509v1 | X.509v2 | X.509v3
  version = X.509v3
   if ne ("X.509v3") severity = (low, severe, 100%)
  cert extensions:
   SubjectKeyIdentifier =
                                           # < present | absent >
    #if ne ("present") severity = (low, minor, 20%)
   AuthorityKeyIdentifier =
                                           # < present | absent >
    #if ne ("present") severity = (low, minor, 20%)
   BasicConstraints =
                          # < absent | critical | non critical >
    if_ne ( "critical" ) severity = (low, severe, 100%)
     BasicConstraints value = # < notCA | CA | yet to be defined >
      if ne ("CA") severity = (low, severe, 100\%)
                                  # < absent | critical | non critical >
   KeyUsage =
    if ne ("critical") severity = (low, severe, 100%)
CRL profile:
                                           \# < X.509v1 >
  version =
```

#if ne ("X.509v1") severity = (low, severe, 100%)

Oublin DEC-2003

default LOW ruleset	CERNO	E	CNRS	CNRS . Projets	СУСА	DATAGRIDIES	DOMScienceGrid	Datagrid . fr	NIKHEFO	FZK . Grid . CA	GermanGrid	Grid. Ireland	HellasGrid	-NFN -CA	LIPO	Z O L D U G L i D	PLGRID	RDGRID . CA	SlovakGrid	ASGCCA	KHE	UKesciecceca
Atlas VO			0	Ю		0		0	0	0	0	10	0		Ю	0	0	0				D D
CMS VO	200	_	0	6	F	0		6	0	0	0		0	F	6	0	0	o	r	o		ō
D0 V0	o	F	0	6	F	0		0	0	0	0	İ	0		0	o	o	o	F	o	<u> </u>	o
LHCb VO	0	F	0	6	F	0		0	0	0	0	T	0		0	0	0	o	F	o	o	o
Switzerland(CERN)	X	F	0	ō	F	0	F	0	0	0	0		0	F	0	0	0	o	F	o.	o	ō
Czech(CESNET)	_	X	o	0	Г	0	Г	0	0	0	0	2	ō	o	ō	o	0	o	T	ō	o	ō
France(CNRS)	o	Γ	X	ō	Г	0	Г	0	0	0	0	Г	o	Г	ō	o	0	o	F	o	o	ō
France(CNRS-Projets)	o	Γ	o	X	Г	o	Г	0	0	0	0	Г	o	Г	ō	0	0	o	Г	o	o	ō
Cyprus(CyCA)	o	Γ	0	0	X	0	Г	0	0	0	0	Г	o	Г	o	0	0	0	Г	o	0	ō
Spain(DATAGRID-ES)	o	Γ	0	0	Γ	X	Γ	ō	0	0	0	Γ	0	Γ	ō	0	0	0	Г	0	o	ō
America(DOEScienceGrid)	o	Γ	0	0	Γ	0	X	0	0	0	0	Γ	0	Γ	0	0	0	0	Г	0	0	o
France(Datagrid-fr)	0	Γ	0	0	Γ	0	Γ	X	0	0	0	Г	0	Γ	0	0	0	0	Г	0	0	o
Netherlands(NIKHEF)	0	3	0	0	Γ	0	Г	0	X	0	0	1	0	0	0	0	0	0	Г	0	0	o
Germany(FZK-Grid-CA)	o	Γ	0	0	Γ	0	Г	0	0	X	0	3	0	1	0	0	0	0	Г	0	0	o
Germany(GermanGrid)	0	Γ	0	0	F	0	Г	0	0	0	X	Г	0	Γ	0	0	0	0		0	0	o
Ireland(Grid-Ireland)	o	Γ	0	0	Γ	0		0	0	0	0	X	0	2	0	0	0	0		0	0	o
Greece(HellasGrid)	0	Γ	0	0	Γ	0		0	0	0	0		X		0	0	0	0		0	0	o
Italy(INFN-CA)	0	Γ	0	0	Г	0		0	0	0	0		0	X	0	0	0	0		0	0	o
Portugal(LIP)	0		0	0	Г	0		0	0	0	0		0	Γ	X	0	0	0		0	*	0
Scandinavia(NorduGrid)	100	•	0	0	Г	0		0	0	0	0		0	Г	0	X	0	0			*	o
Poland(PLGRID)	0	_	0	0	Г	0		0	0	0	0		0	Г	0	0	X	0			200	o
Russia(RDGRID-CA)	-		0	0		0		0	0	0	0		0		0	0	0	X				0
Slovakia(SlovakGrid)	144		0	0		0		0	0	0	0		0		0	0	0	0	X	0	_	0
Tai wan(ASGCCA)	0		0	0		0		0	0	0	0		0		0	0	0	0		X	-	0
UK(UKHEP)	440	_	0	0		0		0	0	0	0		0		0	0	0	0		0	X	0
UK(UKeScienceCA)	0		0	0		0		0	0	0	0	1	0		0	0	0	0	1	0	0	Х

## 16/22 FAIL Default Ruleset!



#### **Autoevaluation Report:**

```
inspecting_CA=default LOW ruleset
inspected_CA=CNRS
inspected_CA:
```

```
publishes_CA_cert=
  issue with default rule: if_ne ( true ) severity = (low,severe,100%)
publishes_CRL=
  issue with default rule: if_ne ( true ) severity = (low,severe,100%)
publishes_CP=
  issue with default rule: if_ne ( true ) severity = (low,severe,100%)
```

IGNORE (doesn't work)



#### **Autoevaluation Report** [CONTINUED]

#### cert\_signing\_host:

```
controlled_physical_access=
    issue with default rule: if_ne ( true ) severity = (low,severe,100%)

CA_key_lifetime=7300
    issue with default rule: if gt ( 1825 ) severity = (low,severe,100%)

minimum_subject_key_size=
    issue with default rule: if lt ( 1024 ) severity = (low,severe,100%)

_BasicConstraints=non_critical
    issue with default rule: if ne ( critical ) severity = (low,severe,100%)

_KeyUsage=non_critical
    issue with default rule: if ne ( critical ) severity = (low,severe,100%)
```

CA	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
CERN		X	X													
CNRS				X	X	X	X	X	X		X		X		X	
CNRS_projet				X	X	X	X	X	X		X		X		X	
datagrid_ES				X	X	X	X	X			X		X		X	
datagrid_fr	X						X		X		X		X		X	
NIKHEF															X	
FZK																X
GermanGrid				X	X	X	X	X		X	X			X	X	
HellasGrid	X								X							
LIP														X	X	
NorduGrid				X	X	X	X	X		X	X		X		X	
PolishGrid		X							X							
Russia										X	X		X	X	X	
Taiwan				X	X	X	X	X		X	X	X	X	X	X	
UK HEP						X	X	X		X	X	X	X	X	X	
UK eScience						X	X	X			X				X	

FAILURES

CRL Web key server gen

cert details

empty entries

CA	1	2	3	4	5	6	7	8	
CERN		X	X						
CNRS				X	X	X	X	X	
CNRS_projet				X	X	X	X	X	
datagrid_ES				X	X	X	X	X	
datagrid_fr	X						X		
NIKHEF									<b>1</b>
FZK									<b>V</b>
GermanGrid				X	X	X	X	X	
HellasGrid	X								
LIP									<b>1</b>
NorduGrid				X	X	X	X	X	
PolishGrid		X							
Russia									<b>1</b>
Taiwan				X	X	X	X	X	
UK HEP						X	X	X	
UK eScience						X	X	X	

(a) extracting from cert helps a lot

(b) talk to D.Chadwick

CRL Web key server gen

empty entries