



---

29/1/2010

## WS-ARC SERVICE CONFIGURATION MANUAL

Martin Skou Andersen\*

---

\*skou@nbi.dk

# Contents

<b>1</b>	<b>Introduction</b>	<b>3</b>
1.1	How to read this manual . . . . .	3
<b>2</b>	<b>INI configuration</b>	<b>3</b>
2.1	Examples . . . . .	4
2.1.1	Echo service . . . . .	4
2.1.2	Other service . . . . .	4
2.2	Limitations . . . . .	4
<b>3</b>	<b>XML configuration</b>	<b>5</b>
3.1	Overview . . . . .	5
3.2	Service configuration . . . . .	5
3.3	Message Chain . . . . .	5
3.3.1	TCP MCC . . . . .	6
3.3.2	TLS MCC . . . . .	7
3.3.3	HTTP MCC . . . . .	7
3.3.4	SOAP MCC . . . . .	8
3.3.5	Plexer . . . . .	8
3.4	Security Handlers . . . . .	8
3.4.1	Identity Mapping . . . . .	8
3.4.2	ARC Authorization . . . . .	8
3.4.3	Delegation Collector . . . . .	8
3.4.4	Username Token . . . . .	8
3.5	General Daemon Configuration . . . . .	8
3.6	Examples . . . . .	9
3.6.1	Echo Service . . . . .	9
<b>4</b>	<b>Profiles</b>	<b>10</b>
<b>5</b>	<b>The arched daemon</b>	<b>12</b>
<b>A</b>	<b>List of standard profiles in WS-ARC</b>	<b>12</b>
A.1	A-REX . . . . .	12
A.2	Chelonia . . . . .	12
A.3	ISIS . . . . .	13
A.4	Charon . . . . .	13
A.5	Hopi . . . . .	13
A.6	Combined services . . . . .	13
A.7	Testing . . . . .	13
<b>B</b>	<b>Profile attributes naming convention</b>	<b>14</b>

<b>C XML Schemas</b>	<b>14</b>
C.1 General Daemon Schema . . . . .	14
C.2 Loader Schema . . . . .	17
C.3 TCP Schema . . . . .	20
C.4 TLS Schema . . . . .	22

# 1 Introduction

The Web Service (WS) Advanced Resource Connector (ARC) provides a great deal of services which all share a common configuration interface. One or more services can be specified in a configuration and the **arched** daemon should then be used for starting the service(s). The configuration should be specified in a file using either the relatively simple INI format, or the more complex XML format.

INI configuration is the recommended way of configuring services for people who are new to ARC or unfamiliar with WS-ARC configuration. However it is limited in the sense that it relies on profiles. A profile is a configuration template setup for one or more services, and common use case profiles exist for most services and are installed per default. The limitation lies in the fact that only services and options which are specified in the profile can be configured in INI configuration, however the installed profiles should give enough flexibility for common use cases. For a detailed description on INI configuration see section 2. Profiles are further discussed in section 4.

XML configuration is the core format of WS-ARC configuration – it is used internally – and thus it gives full flexibility when configuring services. A detailed description of XML configuration can be found in section 3.

The **arched** daemon, which is used to start WS-ARC services according to the configuration is briefly discussed in section 5.

## 1.1 How to read this manual

This manual is divided into the three independent sections INI configuration, XML configuration and Profiles, and these can be read independent of each other. Additionally the **arched** section describe the command with the same name.

It should be noted that words typeset with the **typewriter** font should be typed as written.

# 2 INI configuration

As mentioned in the introduction, INI configuration directly relies on profiles, and a profile is a configuration template setup for one or more services. So when creating a INI configuration file a choice of profile must be made. Only one profile can be used in a given INI configuration. A standard WS-ARC installation comes with a set of profiles and the list in appendix A gives a short description of these. The profiles will per default be installed into the `/usr/share/arc/profiles` folder, where it is also possible to find an example INI configuration file for each of the profiles.

A INI configuration file basically consist of sections, attribute-value pairs and maybe comments and blank lines. In the following code-listing the syntax of an INI configuration file is shown:

```
# A comment
[ common ]
profile = <path-to-profile>

<attribute> = <value>
...
...

# Another comment
[ <section-name> ]
<attribute> = <value>
...
...
[ <another-section> ]
<attribute> = <value>
...
...
```

A section is specified by putting the name of the section inside brackets ([ and ]), where the left bracket ([) must be the first non white space character on the line. Any white space character after the left bracket and before the right will not be part of the section name. Every attribute-value pair belongs to the section which has been defined previously. If the file starts without declaring a section, then following attributes will belong to the common section. Multiple sections with identical names are different sections, except for the common section, which is special in this respect and if multiple common sections exist these will be considered as one.

The **profile** attribute is also a special, as it is used to indicate which profile the INI configuration uses, and its value should be the absolute path to the profile file. The **profile** attribute must be located in the common section. If multiple **profile** attributes exist only the first attribute will be used.

Attribute-value pairs are defined by specifying the name of the attribute followed by an equal sign and then the value the attribute should take. It is the first equal sign which separates the attribute from the value. If a line, not defining a section, does not contain an equal then it will be ignored and if it contains multiple equal signs then all but first equal sign will be part of the value. Any white space before and after the attribute and value will be ignored. Only attributes which have been defined in the selected profile will be considered by **arched**. For each profile in WS-ARC a corresponding INI configuration file exist which defines sensible values and at the time list all configurable attributes. When it comes to multiple attributes with identical names defined in the same section, it is the selected profile which determines if multiple attributes is allowed and will be interpreted or not. It is possible that attributes from one section can override attributes from another section, however this behaviour is completely determined by the profile.

Comments in the INI configuration file are specified by letting the first non white space character be the sharp character (#), and these will be ignored by **arched**.

## 2.1 Examples

### 2.1.1 Echo service

```
profile = /usr/share/arc/profiles/EchoService.xml

pidfile = /tmp/arched.pid
logfile = /tmp/arched.log
loglevel = INFO

port = 60000

cacert = /etc/grid-security/certificates
host_cert = /etc/grid-security/hostcert.pem
host_key = /etc/grid-security/hostkey.pem

[ echo ]
prefix = {{
suffix = }}
```

### 2.1.2 Other service

## 2.2 Limitations

Configuring WS-ARC services in INI format may pose some limitations, since this configuration format depend on profiles. If one wants to configure a service setup which is not covered by any of the available profiles, it is simply not possible to configure that service setup in INI format and one has to use the XML format described in section 3. It should however be noted that it is easy to switch from INI to XML format since the **arched** command provide a way to convert a INI configuration into XML. See section 5 for further details.

## 3 XML configuration

### 3.1 Overview

XML configuration in WS-ARC provides full flexibility for configuring services, and to construct an adequate configuration one need to address the following subjects. If not done already, a choice on which service(s) being setup need to be made and a short discussion of the available WS-ARC services is given in section 3.2. Upon the choice of service(s) the proper message chain need to be configured and a discussion about message chains is given in section 3.3. Most people also want some kind of security setup capable of allowing/denying certain users, which can be done with security handlers and is discussed in section 3.4. Common configuration options like specifying plugins required for instance by the message chain, and configuring logging, is discussed in section 3.5. In section 3.6 example XML configuration files are given.

### 3.2 Service configuration

The following services are part of WS-ARC and specific configuration details for these are given in the respective references below:

**A-REX** A-REX

**Chelonia**

**ISIS**

**Charon**

**hopi** hopi, a lightweight HTTP webserver, is described in details in %% REFERENCE.

### 3.3 Message Chain

To configure WS-ARC services, a basic knowledge about how these are communicating with clients or other services is needed. WS-ARC uses a chain of message components (MCCs) which serves different levels of functionality. In one end it accepts messages from an interface and in the other a service processes them and produce a response. Two types of MCCs exist, and they differ in that the first type should be able to listen on some interface for messages, while the other simply receives messages from another MCC. The MCC then process the message and pass it on to a single or multiple other MCCs or services. MCCs should be configured using the XML element **Component**, where the **name** attribute specifies the MCC to use. The following MCCs is part of WS-ARC:

**tcp.service** Listens on the TCP interface, see section 3.3.1,

**tls.service** Adds encryption layer to communication, see section 3.3.2,

**http.service** Processes HTTP messages, see section 3.3.3,

**soap.service** Processes SOAP messages, see section 3.3.4.

Additionally a special MCC, the Plexer, exist which is able to pass messages to different components simply based on the endpoint the messages was sent to, and it should be configured using the **Plexer** element, see section 3.3.5. In the end of the chain a service should be specified, using the **Service** element, where the **name** attribute indicates the given service.

A working configuration should then link a set of MCCs and services, starting with a MCC that receives messages from some interface. The MCCs and services should be uniquely identifiable, by setting the **id** attributes of these elements. A MCC links to another or several MCCs or services using the **next** element, where the **id** attribute specifies the **id** of that MCC or service. The message chain should be contained in the root element **ArcConfig**, which is shown in the conceptual configuration example below:

```

...
<Component name="mcc1.service" id="mcc1">
  <next id="mcc2"/>
</Component>
<Component name="mcc2.service" id="mcc2">
  <next id="service"/>
</Component>
<Service name="service" id="service"/>
...

```

For readability the message chain can be grouped into a **Chain** element in one or more levels.

### 3.3.1 TCP MCC

The TCP message component is named **tcp.service** and should be the first component in a chain. It is used to setup a server socket which will listen for incoming connections. The socket can be configured using the **Listen** element, which can occur multiple times and under each element the following child elements can be specified:

**Interface** This element specifies the interface which socket should listen on. If this element is not specified then the socket will listen on all available interfaces.

**Port** The port which the socket should bind to should be specified with this element. If no port is specified an error will be reported and this **Listen** element will be ignored.

**Version** The IP version can be specified by this element, and by default both version 4 and 6 will be used. It is possible to specify version 4 or 6 only.

**NoDelay** By default Nagle's algorithm is used for sending data, however if the **NoDelay** element is set to **true** data will be send when ready.

**Timeout** Specifies how much time, in seconds, there should be used on waiting for a client response. If no client response is obtained before timeout the connection is dropped. The default value is 60 seconds.

It is also possible to put a limit on incoming connections, and how these should be handled if the limit is reached. The limit can only be put on all configured interfaces, and not per interface. The **Limit** element specifies the limit on incoming connections, and the **drop** attribute specifies whether new connections, above the limit, will be put on hold (default) or if they should be dropped, which is specified by setting the attribute to **true**.

An example of a TCP MCC configuration using the described elements is shown below:

```

...
<Component name="tcp.service" id="tcp">
  <Listen>
    <Interface>w.x.y.z</Interface>
    <Port>44444</Port>
    <Version>4</Version>
    <NoDelay>true</NoDelay>
    <Timeout>120</Timeout>
  </Listen>
  <Listen>
    <Interface>a:b:c:d:e:f:g:h</Interface>
    <Port>55555</Port>
    <Version>6</Version>
    <NoDelay>false</NoDelay>
    <Timeout>20</Timeout>
  </Listen>
  <Limit drop="true">30</Limit>
</Component>
...

```

### 3.3.2 TLS MCC

A security layer can be configured with the TLS MCC, named `tls.service`, and it should be put on top of a TCP MCC. By default it is able to understand the SSLv2, SSLv3 and TLSv1 protocols, however the `Handshake` element can be used to specify another behaviour. The supported values for the `Handshake` element are TLS (default) and SSLv3, where specifying the latter will configure a MCC which only understand the SSLv3 protocol. If other values than the mentioned ones are given, then TLS will be used.

For the TLS MCC to function, it should have access to a host key-certificate pair. The key should be the private one, and it should not be password protected. The path to the key-certificate pair can be specified by using the `KeyPath` and `CertificatePath` elements. If the `KeyPath` element is not specified the default path `/etc/grid-security/hostkey.pem` will be used, and likewise if the `CertificatePath` element is not specified the default path `/etc/grid-security/hostcert.pem` will be used. The supported key and certificate formats are PEM and DER.

When establishing a connection with a client, the client certificate are per default verified against the Certificate Authority (CA) certificates, known to the TLS MCC. The CA certificates used for verification can be specified with either the `CACertificatesDir` or the `CACertificatePath` element, or both elements can be used. The `CACertificatesDir` element should point to a directory containing one or more CA certificates (in PEM format). The files should each contain exactly one certificate, and should be named by the hash value of the CA subject name. CA certificates provided by NorduGrid uses this option. The `CACertificatePath` element should point to a file containing one or more CA certificates (in PEM format) identified by:

```
-----BEGIN CERTIFICATE-----  
... (CA certificate in base64 encoding) ...  
-----END CERTIFICATE-----
```

sequences. If both elements have been specified, CA certificates will first be looked up in the file pointed to by the `CACertificatePath` element and then in the directory pointed to by the `CACertificatesDir` element. If none of the two elements have been specified, then the `CACertificatesDir` element will be initialised to the `/etc/grid-security/certificates` location. Client certificate verification can also be skipped, which is done by setting the `ClientAuthn` element to `false`.

```
...  
<Component name="tls.service" id="tls">  
  <KeyPath></KeyPath>  
  <CertificatePath></CertificatePath>  
  <CACertificatePath></CACertificatePath>  
  <CACertificatesDir></CACertificatesDir>  
  <ClientAuthn></ClientAuthn>  
  <Handshake>SSLv3</Handshake>  
</Component>  
...
```

### 3.3.3 HTTP MCC

The HTTP protocol is supported by the HTTP MCC named `http.service`, and it should either be put on top of the TCP or TLS MCC. A working configuration of this MCC is simple, since it should only use the `next` element which must have a value equal to one of the HTTP request methods. An example of a HTTP MCC configuration is shown below.

```
...  
<Component name="http.service">  
  <next id="component1">GET</next>  
  <next id="component2">POST</next>  
  <next id="component3">PUT</next>  
</Component>  
...
```



### 3.3.4 SOAP MCC

SOAP is supported by the SOAP MCC, named `soap.service`. It parses and processes incoming messages as SOAP messages. This component should be put right after the HTTP MCC in the message chain. The component is needed by most of the services in WS-ARC. The only option which should be configured for the SOAP MCC is to which component or service the valid SOAP messages should be directed to, and it is done with the `next` element as for the other components.

### 3.3.5 Plexer

The Plexer is a special MCC which filters messages based on their URL endpoints. One or more regular expressions (POSIX extended) should be defined using one or more `next` elements, and these will then be used to filter incoming messages, thus forwarding messages, where the path of the endpoint URL matched a given regular expression, to the component or service specified by the `id` attribute of the corresponding `next` element. At the first match the message will be forwarded to the respective component or service and no more expressions will be tried. If a message did not match any of the regular expressions then it is discarded and an error code is returned to the client. An example of a Plexer configuration is shown below.

```
...
<Plexer>
  <next>~/arex$</next>
  <next>~/[eE][cC][hH][oO]$</next>
</Plexer>
...
```

## 3.4 Security Handlers

### 3.4.1 Identity Mapping

### 3.4.2 ARC Authorization

### 3.4.3 Delegation Collector

### 3.4.4 Username Token

## 3.5 General Daemon Configuration

The following options configures the `arched` daemon, and thus applies to all services. Some of the options can also be set using command line arguments, and if used these will override the configuration file options. See section 5 for a description of the `arched` daemon.

Under the `Server` element the file to store the PID in, can be specified using the `PidFile` element, if not specified the PID will be stored in the file `/var/run/arched.pid`. This options can also be set using a command line argument. If the `Foreground` element is present under the `Server` element, `arched` will run in foreground and thus the `PidFile` element will be ignored. It is also possible to specify that `arched` should run in foreground on the command line, however it is not possible to specify that it should run as a daemon, if configured to run in foreground in the configuration file. Also under the `Server` the user and group owning the `arched` process can be specified, which is accomplished with the `User` and `Group` elements. These can also be set on the command line.

Logging options should be specified under the `Logger` element under the `Server` element. The `File` element specifies which file to write log messages to and if not present log messages will be written to the `/var/log/arched.log` file. Each log message is associated with a log level which indicates the severity of the message. The following log levels exist in WS-ARC, ordered by severity: `FATAL`, `ERROR`, `WARNING`, `INFO`, `VERBOSE` and `DEBUG`. With the `Level` element the level of messages being reported can be specified. Log messages with a higher or same level as specified by the `Level` element will be written to the log file. The default log level is `WARNING`.

By default the log file is not limited in size, neither will any log rotation be done. The `Maxsize` and `Backups`

elements can be used to change this behaviour. The **Maxsize** element sets the maximum file size of the log file in bytes, while the **Backups** element specifies the number of files used for log rotation. When the size of the log file exceeds the limit specified by the **Maxsize** element the log file is renamed to `<log-file>.1`. If this file exist it is renamed to `<log-file>.2` and so forth up to the number specified by **Backups**, which means that the last file will be deleted. The log file size is only allowed to exceed the specified limit by the size of one log message. If the **Maxsize** element have been specified and no **Backups** element is specified then log rotation will not be carried out, thus the log file is truncated when the limit is exceeded.

Plugins which should be used later in the configuration should be specified under the **Plugins** element where the **Name** element specifies the name of the plugin. The **Path** element under the **ModuleManager** element specifies where to locate the plugins.

The following example show the use of the above configuration options:

```
<?xml version="1.0"?>
<ArcConfig>
  <Server>
    <PidFile>/tmp/arched.pid</PidFile>
    <User></User>
    <Group></Group>
    <Logger>
      <File>/tmp/arched.log</File>
      <Level>WARNING</Level>
      <MaxSize>1000000</MaxSize>
      <Backups>5</Backups>
    </Logger>
  </Server>
  <ModuleManager>
    <Path>/usr/lib/arc</Path>
  </ModuleManager>
  <Plugins>
    <Name>plugin1</Name>
    <Name>plugin2</Name>
    ...
  </Plugins>
  ...
</ArcConfig>
```

## 3.6 Examples

### 3.6.1 Echo Service

```
<?xml version="1.0"?>
<cfg:ArcConfig xmlns="http://www.nordugrid.org/schemas/loader/2009/08"
  xmlns:cfg="http://www.nordugrid.org/schemas/arcconfig/2009/08"
  xmlns:tcp="http://www.nordugrid.org/schemas/tcp/2009/08"
  xmlns:tls="http://www.nordugrid.org/schemas/tls/2009/08"
  xmlns:echo="http://www.nordugrid.org/schemas/echo/2009/08"
  xmlns:infosys="http://www.nordugrid.org/schemas/infosys/2009/08"
  >
  <cfg:Server>
    <cfg:PidFile>/tmp/arched.pid</cfg:PidFile>
    <cfg:Logger>
      <cfg:File>/var/log/arched.log</cfg:File>
      <cfg:Level>WARNING</cfg:Level>
    </cfg:Logger>
  </cfg:Server>
  <ModuleManager>
    <Path>/usr/lib/arc</Path>
  </ModuleManager>
  <Plugins>
```

```

    <Name>mcctls</Name>
    <Name>mcchttp</Name>
    <Name>mccsoap</Name>
    <Name>mcctcp</Name>
</Plugins>
<Chain>
  <Component name="tcp.service" id="tcp">
    <next id="http"/>
    <tcp:Listen>
      <tcp:Interface>0.0.0.0</tcp:Interface>
      <tcp:Version>4</tcp:Version>
    </tcp:Listen>
  </Component>
  <Component name="http.service" id="http">
    <next id="soap">POST</next>
    <next id="plexer">GET</next>
  </Component>
  <Component name="soap.service" id="soap">
    <next id="plexer"/>
  </Component>
  <Plexer id="plexer">
    <next id="echo">/Echo</next>
  </Plexer>
  <Service name="echo" id="echo">
    <echo:prefix>[</echo:prefix>
    <echo:suffix>]</echo:suffix>
  </Service>
</Chain>
</cfg:ArcConfig>

```

## 4 Profiles

In WS-ARC the concept of profiles have been introduced. A profile is a complete XML configuration template, for a specific service setup and it is used when configuring services in INI format. The core of WS-ARC uses an XML struture for service initialization, which makes the XML format the apparent choice for configuration. However the XML language is not simple and easy to use, which is why WS-ARC utilizes profiles, namely to provide a configuration format (the INI format) easy to use.

To write a profile, some knowledge on the INI (see section 2) and XML configuration formats (see section 3) is needed. Not necessarary to say, knowledge on the desired service setup is also needed. A XML configuration file is only a profile if it defines a option mapping from INI format to XML, thus making it possible to utilise the XML configuration through the INI format.

Two XML attributes have been introduced to be able to create a mapping, and these are **inisections** and **initag**. XML elements which should be configurable in INI format must specify these attributes. The **initag** attribute defines the name of the tag which represent the respective XML element in the INI configuration file, and the **inisections** attribute is used to specify, as a space separated list, which sections the tag can occur in. The list is ordered, in the sense that the listed sections is searched, in the specified order, for the tag specified by the **initag** attribute, and if found in a section no further sections will be searched. Only leaf XML elements (elements with no child elements) should be mapped, mapping non leaf element result in a undefined behaviour. A profile example of a XML element mapping is shown in the listing below:

ElementMapping.xml

```

...
<Server>
  ...
  <Logger>
    <File inisections="special common"
      initag="logfile">/var/log/arched.log</File>

```

```

...
</Logger>
</Server>
...

```

And this example profile can then be utilised in a INI configuration file as:

#### ElementMapping.ini

```

profile=ElementMapping.xml
logfile=/etc/arc/arched.log
...
[ special ]
logfile=/var/arc/arched.log
...

```

And the resulting XML configuration will look like:

```

...
<Server>
...
  <Logger>
    <File>/var/arc/arched.log</File>
    ...
  </Logger>
</Server>
...

```

To be able to map XML attributes the use of a new XML element `AttributeRepresentation` have been introduced. The element should have three attributes set, the two attributes `inisections` and `initag` used as described above, and a new attribute `id` which specifies which attribute of the parent element is being mapped. A profile example of a XML attribute is shown in the listing below:

#### AttributeMapping.xml

```

...
<Component name="tcp.service">
...
  <Limit drop="false">
    <AttributeRepresentation id="drop" inisections="common" initag="drop"/>
    100
  </Limit>
</Component>
...

```

And this example profile can then be utilised in a INI configuration file as:

#### AttributeMapping.ini

```

profile=AttributeMappingExample.xml
drop=true
...

```

And the resulting XML configuration will look like:

```

...
<Component name="tcp.service">
...
  <Limit drop="true">100</Limit>
</Component>
...

```

## 5 The arched daemon

The **arched** daemon is the daemon which is used to start every service in WS-ARC. It will load a configuration file, and start the services specified herein.

### arched [OPTION...]

(ARC 0.9)

<b>-f, --foreground</b>		run daemon in foreground
<b>-c, --xml-config</b>	<i>path</i>	full path of XML configuration file
<b>-i, --ini-config</b>	<i>path</i>	full path of INI configuration file
<b>-d, --config-dump</b>		dump generated XML configuration
<b>-p, --pid-file</b>	<i>path</i>	full path of PID file
<b>-u, --user</b>	<i>user</i>	user name
<b>-g, --group</b>	<i>group</i>	group name
<b>-s, --schema</b>	<i>path</i>	full path of XML schema file
<b>-h, --help</b>		Show help options

If no configuration file is specified, **arched** first looks for the `/etc/arc/server.ini` INI configuration file if it does not exist then the `/etc/arc/server.xml` XML configuration file is tried. If none of these is found **arched** will abort with an error and exit code 1.

A INI configuration file can be specified with the **-i** option, while the **-c** option makes it possible to specify a XML configuration file. If both options are given, the INI configuration will be chosen.

**arched** also has the capability of printing the XML configuration which will be generated from a given INI configuration. By specifying the **-d** option along with the **-i** option and the path to the INI configuration **arched** will transform the INI configuration to XML and dump the output to standard out and exit.

## A List of standard profiles in WS-ARC

### A.1 A-REX

**ComputingElementWithFork** MINIMAL configuration template for a secure standalone Computing Element (CE) with a fork queue.

**InsecureComputingElement**

**ComputingElementWithMapfile**

**ComputingElementWithMapfileAndPBSBackend**

**ComputingElement\_DNlist**

**ComputingElement\_VOMS**

### A.2 Chelonia

**CheloniaAllCentralizedAHash**

**CheloniaAllCentralizedAHashWithISIS**

**CheloniaAllReplicatedAHash**

CheloniaAllReplicatedAHashGatewayVOMSWithISIS

CheloniaAllReplicatedAHashWithISIS

CheloniaReplicatedAHash

CheloniaShepherdWithHopi

InsecureNonDistributedStorageElement

NonDistributedStorageElement\_DNlist

NonDistributedStorageElement\_VOMS

### A.3 ISIS

InsecureP2PIIS

InsecureStandaloneIIS

P2PIIS

StandaloneIIS

### A.4 Charon

Charon

### A.5 Hopi

Hopi

HopiInsecure

HopiWithPlexer

HopiWithPlexerInsecure

### A.6 Combined services

InsecureComputingAndStorageElement

ComputingAndStorageElement\_DNlist

ComputingAndStorageElement\_VOMS

### A.7 Testing

Echo

EchoInsecure

EchoPython

EchoPythonInsecure

EchoSAMLToken

EchoUsernameToken

EchoX509Token

InsecureHopiService

## B Profile attributes naming convention

Since profiles defines a mapping of XML elements or attributes to INI tags, they control the naming of the tags. So for consistency tags in different profiles representing the same XML element or attribute should not be named differently. A naming convention list for the XML elements and attributes described in section 3 is presented below. Note that there are only conventions for leaf XML elements (element with no children).

XML element/attribute	INI tag
/Server/PidFile	pidfile
/Server/User	user
/Server/Group	group
/Server/Logger/File	logfile
/Server/Logger/Level	loglevel
/Server/Logger/Maxsize	logmaxsize
/Server/Logger/Backups	logbackups
TCP MCC	
/Component/Listen/Interface	interface
/Component/Listen/Port	port
/Component/Listen/Version	ipversion
/Component/Listen/NoDelay	nodelay
/Component/Listen/Timeout	timeout
/Component/Limit	limit
/Component/Limit.drop	drop
TLS MCC	
/Component/KeyPath	x509_user_key
/Component/CertificatePath	x509_user_cert
/Component/CACertificatePath	x509_cacert_path
/Component/CACertificatesDir	x509_cacert_dir
/Component/CACertificatesDir.PolicyGlobus	policyglobus
/Component/ClientAuthn	clientauthn
/Component/VOMSCertTrustDNChain/VOMSCertTrustDN	
/Component/VOMSCertTrustDNChain/VOMSCertTrustRegex	
/Component/VOMSCertTrustDNChainsLocation	
/Component/Handshake	handshake

## C XML Schemas

### C.1 General Daemon Schema

```
<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  targetNamespace="http://www.nordugrid.org/schemas/arcconfig/2009/08"
  xmlns="http://www.nordugrid.org/schemas/arcconfig/2009/08"
  xmlns:loader="http://www.nordugrid.org/schemas/loader/2009/08"
  elementFormDefault="qualified"
  attributeFormDefault="unqualified">
```

```

<xsd:import namespace="http://www.nordugrid.org/schemas/loader/2009/08"
  schemaLocation="loader.xsd"/>
<!-- Root element -->
<xsd:element name="ArcConfig">
  <xsd:complexType>
    <xsd:annotation>
      <xsd:documentation>
        This is the top level element of ARC configuration document.
      </xsd:documentation>
    </xsd:annotation>
    <xsd:sequence>
      <xsd:element ref="Server" minOccurs="0" maxOccurs="1"/>
      <xsd:element ref="loader:ModuleManager" minOccurs="0" maxOccurs="1"/>
      <xsd:element ref="loader:Plugins" minOccurs="0" maxOccurs="1"/>
      <xsd:element ref="loader:Component" minOccurs="0" maxOccurs="unbounded"/>
      <xsd:element ref="loader:Chain" minOccurs="0" maxOccurs="unbounded"/>
      <xsd:element ref="loader:Plexer" minOccurs="0" maxOccurs="unbounded"/>
      <xsd:element ref="loader:Service" minOccurs="0" maxOccurs="unbounded"/>
      <xsd:element ref="loader:SecHandler" minOccurs="0" maxOccurs="unbounded"/>
    </xsd:sequence>
  </xsd:complexType>
</xsd:element>

<!-- Server -->
<xsd:element name="Server">
  <xsd:complexType>
    <xsd:annotation>
      <xsd:documentation xml:lang="en">
        Server specific configuration options.
      </xsd:documentation>
    </xsd:annotation>
    <xsd:all>
      <xsd:element name="PidFile" type="xsd:string" minOccurs="0" maxOccurs="1"
        default="/var/run/arched.pid">
        <xsd:annotation>
          <xsd:documentation xml:lang="en">
            Path to process ID file.
          </xsd:documentation>
        </xsd:annotation>
      </xsd:element>
      <xsd:element name="Foreground" type="xsd:boolean" minOccurs="0" maxOccurs="1"
        default="false">
        <xsd:annotation>
          <xsd:documentation xml:lang="en">
            Indicates whether the server runs in foreground or daemon mode. If
            it runs in foreground the log goes to standard error as well.
          </xsd:documentation>
        </xsd:annotation>
      </xsd:element>
      <xsd:element name="User" type="xsd:string" minOccurs="0" maxOccurs="1">
        <xsd:annotation>
          <xsd:documentation xml:lang="en">
            arched will run under the specified user. If not specified the
            effective user will not be changed.
          </xsd:documentation>
        </xsd:annotation>
      </xsd:element>
      <xsd:element name="Group" type="xsd:string" minOccurs="0" maxOccurs="1">
        <xsd:annotation>
          <xsd:documentation xml:lang="en">
            arched will run under the specified group. If not specified the

```



```

        effective group will not be changed.
    </xsd:documentation>
</xsd:annotation>
</xsd:element>
<xsd:element ref="Logger" minOccurs="0" maxOccurs="1"/>
</xsd:all>
</xsd:complexType>
</xsd:element>

<!-- Logger -->
<xsd:simpleType name="LoggerLevel_Type">
    <xsd:annotation>
        <xsd:documentation xml:lang="en">
            The enumeration lists the supported log levels.
        </xsd:documentation>
    </xsd:annotation>
    <xsd:restriction base="xsd:string">
        <xsd:enumeration value="FATAL"/>
        <xsd:enumeration value="ERROR"/>
        <xsd:enumeration value="WARNING"/>
        <xsd:enumeration value="INFO"/>
        <xsd:enumeration value="VERBOSE"/>
        <xsd:enumeration value="DEBUG"/>
    </xsd:restriction>
</xsd:simpleType>

<xsd:element name="Logger">
    <xsd:complexType>
        <xsd:annotation>
            <xsd:documentation xml:lang="en">
                Logger configuration element.
            </xsd:documentation>
        </xsd:annotation>
        <xsd:all>
            <xsd:element name="File" type="xsd:string" minOccurs="0" maxOccurs="1"
                default="/var/log/arched.log">
                <xsd:annotation>
                    <xsd:documentation xml:lang="en">
                        This element configures the file which should be used for storing
                        log messages.
                    </xsd:documentation>
                </xsd:annotation>
            </xsd:element>
            <xsd:element name="Level" type="LoggerLevel_Type" minOccurs="0" maxOccurs
                ="1" default="WARNING">
                <xsd:annotation>
                    <xsd:documentation xml:lang="en">
                        Specifies the log level of the messages which should be logged.
                    </xsd:documentation>
                </xsd:annotation>
            </xsd:element>
            <xsd:element name="Maxsize" type="xsd:nonNegativeInteger" minOccurs="0"
                maxOccurs="1">
                <xsd:annotation>
                    <xsd:documentation xml:lang="en">
                        Defines the maximal size of the log file in bytes.
                    </xsd:documentation>
                </xsd:annotation>
            </xsd:element>
            <xsd:element name="Backups" type="xsd:nonNegativeInteger" minOccurs="0"
                maxOccurs="1">
                <xsd:annotation>
                    <xsd:documentation xml:lang="en">

```

```

        Defines the maximal number of log files used in log rotation.
    </xsd:documentation>
</xsd:annotation>
</xsd:element>
</xsd:all>
</xsd:complexType>
</xsd:element>

</xsd:schema>

```

## C.2 Loader Schema

```

<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  targetNamespace="http://www.nordugrid.org/schemas/loader/2009/08"
  xmlns="http://www.nordugrid.org/schemas/loader/2009/08"
  xmlns:ini="http://www.nordugrid.org/schemas/ini/2009/08"
  elementFormDefault="qualified"
  attributeFormDefault="unqualified">

  <!-- ModuleManager -->
  <xsd:element name="ModuleManager">
    <xsd:complexType>
      <xsd:annotation>
        <xsd:documentation xml:lang="en">
          The child element Path specifies the location in the filesystem where
          plugin libraries should be located. Multiple locations can be specified
          using multiple Path elements.
        </xsd:documentation>
      </xsd:annotation>
      <xsd:sequence>
        <xsd:element name="Path" minOccurs="0" maxOccurs="unbounded"/>
      </xsd:sequence>
    </xsd:complexType>
  </xsd:element>

  <!-- Plugins -->
  <xsd:element name="Plugins">
    <xsd:complexType>
      <xsd:annotation>
        <xsd:documentation xml:lang="en">
          This element holds a list of library names, specified by one or more
          Name child elements, which should be used at runtime.
        </xsd:documentation>
      </xsd:annotation>
      <xsd:sequence>
        <xsd:element name="Name" minOccurs="0" maxOccurs="unbounded"/>
      </xsd:sequence>
    </xsd:complexType>
  </xsd:element>

  <!-- Chain -->
  <xsd:element name="Chain">
    <xsd:complexType>
      <xsd:annotation>
        <xsd:documentation xml:lang="en">
          The usage of this element is for grouping Component, Service and/or
          Chain elements in a logical structure to ease readability.
        </xsd:documentation>
      </xsd:annotation>
    </xsd:complexType>
  </xsd:element>

```

```

    <xsd:sequence>
      <xsd:element ref="Chain" minOccurs="0" maxOccurs="unbounded"/>
      <xsd:element ref="Component" minOccurs="0" maxOccurs="unbounded"/>
      <xsd:element ref="Plexer" minOccurs="0" maxOccurs="unbounded"/>
      <xsd:element ref="Service" minOccurs="0" maxOccurs="unbounded"/>
      <xsd:element ref="SecHandler" minOccurs="0" maxOccurs="unbounded"/>
    </xsd:sequence>
  </xsd:complexType>
</xsd:element>

<xsd:element name="next">
  <xsd:complexType>
    <xsd:simpleContent>
      <xsd:extension base="xsd:string">
        <xsd:attribute name="id" type="xsd:string" use="optional"/>
      </xsd:extension>
    </xsd:simpleContent>
  </xsd:complexType>
</xsd:element>

<!-- Component -->
<xsd:element name="Component">
  <xsd:complexType>
    <xsd:annotation>
      <xsd:documentation xml:lang="en">
        This element defines MCC plugin. Required attribute 'name' specifies
        name of plugin as defined in MCC description. Required attribute 'id'
        assigns identifier which is used to refer to this element from others.
        Sub-elements 'next' refer to next components in a chain through their
        attribute 'id' and their content represent assigned component-specific
        label. If attribute 'id' is missing all 'next' refer to next component
        in document. If 'next' is missing one label-less 'next' is assigned
        automatically. Presence of attribute 'entry' exposes this MCC through
        Loader class interface to external code. That is meant to be used in
        code which creates chains dynamically like client utilities. Rest
        elements define component-specific configuration.
      </xsd:documentation>
    </xsd:annotation>
    <xsd:sequence>
      <xsd:element ref="next" minOccurs="0" maxOccurs="unbounded"/>
      <xsd:element ref="SecHandler" minOccurs="0" maxOccurs="unbounded"/>
      <xsd:any namespace="##other" processContents="strict" minOccurs="0"
        maxOccurs="unbounded"/>
    </xsd:sequence>
    <xsd:attribute name="name" type="xsd:string" use="required"/>
    <xsd:attribute name="id" type="xsd:string" use="required"/>
    <xsd:attribute name="entry" type="xsd:string" use="optional"/>
    <xsd:anyAttribute namespace="##other" processContents="strict"/>
  </xsd:complexType>
</xsd:element>

<!-- Plexer -->
<xsd:element name="Plexer">
  <xsd:complexType>
    <xsd:annotation>
      <xsd:documentation xml:lang="en">
        This element is a Plexer. Optional attribute 'id' assigns identifier
        which is used to refer to this element from others. If not specified it
        will be assigned to "plexer" automatically. Sub-elements 'next' refer
        to
        next components in a chain and their content represent requested
        endpoints. In Plexer content of element 'next' represents Regular
        Expression pattern. For every incoming message path part of messages

```

```

    endpoint is matched pattern. In case of ordinary service element 'next'
    may look like
    <next>~/service$</next>
    If service is also responsible for whole subtree then simple solution
    is
    <next>~/service</next>
    But more safer solution would be to use 2 elements
    <next>~/service$</next>
    <next>~/service/</next>
    Unmatched part of message endpoint is propagated with incoming message
    in attribute PLEXER:EXTENSION and may be used by service to determine
    response.
    </xsd:documentation>
  </xsd:annotation>
  <xsd:sequence>
    <xsd:element ref="next" minOccurs="0" maxOccurs="unbounded"/>
    <xsd:any namespace="##other" processContents="strict" minOccurs="0"
      maxOccurs="unbounded"/>
  </xsd:sequence>
  <xsd:attribute name="id" type="xsd:string" use="optional"/>
  <xsd:anyAttribute namespace="##other" processContents="strict"/>
</xsd:complexType>
</xsd:element>

<!-- Service -->
<xsd:element name="Service">
  <xsd:complexType>
    <xsd:annotation>
      <xsd:documentation xml:lang="en">
        This element represents a service - last compnent in a chain. Required
        attribute 'name' specifies name of plugin as defined in Service
        description. Required attribute 'id' assigns identifier which is used
        to refer to this element from others. Rest elements define
        service-specific configuration.
      </xsd:documentation>
    </xsd:annotation>
    <xsd:sequence>
      <xsd:element ref="SecHandler" minOccurs="0" maxOccurs="unbounded"/>
      <xsd:any namespace="##other" processContents="strict" minOccurs="0"
        maxOccurs="unbounded"/>
    </xsd:sequence>
    <xsd:attribute name="name" type="xsd:string" use="required"/>
    <xsd:attribute name="id" type="xsd:string" use="required"/>
    <xsd:anyAttribute namespace="##other" processContents="strict"/>
  </xsd:complexType>
</xsd:element>

<!-- SecHandler -->
<xsd:element name="SecHandler">
  <xsd:complexType>
    <xsd:annotation>
      <xsd:documentation xml:lang="en">
        This element specifies security handler plugin to be called at various
        stages of message processing. Depending on produced result message may
        be either sent farther through chain or processing would be cancelled.
        Required attribute 'name' specifies name of plugin. Attribute 'id'
        creates identifier of SecHandler which may be used to refer to it. If
        attribute 'refid' is defined then configuration of SecHandler is
        provided by another element within ArcConfig with corresponding 'id'.
        Attribute 'event' defines to which queue inside MCC SecHandler to be
        attached. If it is missing SecHandler is attached to default queue if
        MCC has such. Names of queues are MCC specific. If not otherwise
        specified they are 'incoming' and 'outgoing' and are processed for

```

```

        incoming and outgoing messages. There is no default queue by default.
    </xsd:documentation>
</xsd:annotation>
<xsd:sequence>
    <xsd:any namespace="##other" processContents="strict" minOccurs="0"
        maxOccurs="unbounded"/>
</xsd:sequence>
<xsd:attribute name="name" type="xsd:string" use="required"/>
<xsd:attribute name="id" type="xsd:string" use="optional"/>
<xsd:attribute name="refid" type="xsd:string" use="optional"/>
<xsd:attribute name="event" type="xsd:string" use="optional"/>
<xsd:anyAttribute namespace="##other" processContents="strict"/>
</xsd:complexType>
</xsd:element>

</xsd:schema>

```

### C.3 TCP Schema

```

<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema
    xmlns:xsd="http://www.w3.org/2001/XMLSchema"
    targetNamespace="http://www.nordugrid.org/schemas/tcp/2009/08"
    xmlns="http://www.nordugrid.org/schemas/tcp/2009/08"
    elementFormDefault="qualified"
    attributeFormDefault="unqualified">

    <!-- Listen -->
    <xsd:element name="Listen">
        <xsd:complexType>
            <xsd:annotation>
                <xsd:documentation xml:lang="en">
                    This element defines a TCP socket.
                </xsd:documentation>
            </xsd:annotation>
            <xsd:sequence>
                <xsd:element name="Interface" type="xsd:string" minOccurs="0" maxOccurs="1"
                    default="0.0.0.0">
                    <xsd:annotation>
                        <xsd:documentation xml:lang="en">
                            Element Interface specifies which interface to listen on.
                        </xsd:documentation>
                    </xsd:annotation>
                </xsd:element>
                <xsd:element name="Port" type="xsd:nonNegativeInteger">
                    <xsd:annotation>
                        <xsd:documentation xml:lang="en">
                            Specifies the port to listen on.
                        </xsd:documentation>
                    </xsd:annotation>
                </xsd:element>
                <xsd:element name="Version" minOccurs="0" maxOccurs="1">
                    <xsd:simpleType>
                        <xsd:annotation>
                            <xsd:documentation xml:lang="en">
                                This element defines TCP/IP protocol version. If not specified
                                both versions will be used whenever possible.
                            </xsd:documentation>
                        </xsd:annotation>
                        <xsd:restriction base="xsd:string">
                            <xsd:enumeration value="4"/>

```

```

        <xsd:enumeration value="6"/>
    </xsd:restriction>
</xsd:simpleType>
</xsd:element>
<xsd:element name="NoDelay" type="xsd:boolean" minOccurs="0" maxOccurs="1"
    " default="false">
    <xsd:annotation>
        <xsd:documentation xml:lang="en">
            Apply no delay socket option. If set to true TCP packets will
            be proceesd as soon as possible without waiting for more data
            to become available.
        </xsd:documentation>
    </xsd:annotation>
</xsd:element>
<xsd:element name="Timeout" type="xsd:nonNegativeInteger" minOccurs="0"
    maxOccurs="1" default="60">
    <xsd:annotation>
        <xsd:documentation xml:lang="en">
            Specifies the amount of time, in seconds, to wait for a response
            before cancelling communication.
        </xsd:documentation>
    </xsd:annotation>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>

<!-- Connect -->
<xsd:element name="Connect">
    <xsd:complexType>
        <xsd:annotation>
            <xsd:documentation xml:lang="en">
                This element defines that a TCP connection should be established to the
                specified host and port.
            </xsd:documentation>
        </xsd:annotation>
        <xsd:sequence>
            <xsd:element name="Host" type="xsd:string"/>
            <xsd:element name="Port" type="xsd:nonNegativeInteger"/>
            <xsd:element name="Timeout" type="xsd:nonNegativeInteger" minOccurs="0"/>
            <xsd:element name="NoDelay" type="xsd:boolean" minOccurs="0"/>
        </xsd:sequence>
    </xsd:complexType>
</xsd:element>

<xsd:element name="Limit" type="xsd:nonNegativeInteger" minOccurs="0">
    <xsd:complexType>
        <xsd:annotation>
            <xsd:documentation xml:lang="en">
                This element defines an upper limit on the number of simultaneous
                active
                TCP connections. If the drop attribute is specified and set to true,
                then when the limit is reached, new incoming connections will be
                dropped. If the drop attribute has not been specified or set to false,
                they will be put on hold, until an active connection has finished.
            </xsd:documentation>
        </xsd:annotation>
        <xsd:attribute name="drop" type="xsd:boolean" use="optional"/>
    </xsd:complexType>
</xsd:element>

</xsd:schema>

```

## C.4 TLS Schema

```
<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  targetNamespace="http://www.nordugrid.org/schemas/tls/2009/08"
  xmlns="http://www.nordugrid.org/schemas/tls/2009/08"
  elementFormDefault="qualified"
  attributeFormDefault="unqualified">

  <xsd:element name="KeyPath" type="xsd:string" default="/etc/grid-security/
    hostkey.pem">
    <xsd:annotation>
      <xsd:documentation xml:lang="en">
        Location of private key. Default is /etc/grid-security/hostkey.pem for
        server and $HOME/.globus/userkey.pem for client.
      </xsd:documentation>
    </xsd:annotation>
  </xsd:element>

  <xsd:element name="CertificatePath" type="xsd:string" default="/etc/grid-
    security/hostcert.pem">
    <xsd:annotation>
      <xsd:documentation xml:lang="en">
        Location of public certificate. Default is /etc/grid-security/hostcert.
        pem
        for service and $HOME/.globus/usercert.pem for client.
      </xsd:documentation>
    </xsd:annotation>
  </xsd:element>

  <xsd:element name="ProxyPath" type="xsd:string">
    <xsd:annotation>
      <xsd:documentation xml:lang="en">
        Location of proxy credentials - includes certificates, key and chain of
        involved certificates. Overwrites elements KeyPath and CertificatePath.
        Default is /tmp/x509up_u{userid} for client, and none for service.
      </xsd:documentation>
    </xsd:annotation>
  </xsd:element>

  <xsd:element name="CACertificatePath" type="xsd:string">
    <xsd:annotation>
      <xsd:documentation xml:lang="en">
        Location of certificate of CA. Default is none.
      </xsd:documentation>
    </xsd:annotation>
  </xsd:element>

  <xsd:element name="CACertificatesDir" default="/etc/grid-security/certificates"
    >
    <xsd:complexType>
      <xsd:annotation>
        <xsd:documentation xml:lang="en">
          Directory containing certificates of accepted CAs. Default is
          /etc/grid-security/certificates
        </xsd:documentation>
      </xsd:annotation>
      <xsd:simpleContent>
        <xsd:extension base="xsd:string">
          <xsd:attribute name="PolicyGlobus" type="xsd:boolean" use="optional"
            default="false"/>
        </xsd:extension>
      </xsd:simpleContent>
    </xsd:complexType>
  </xsd:element>
```

```

        </xsd:simpleContent>
    </xsd:complexType>
</xsd:element>

<xsd:element name="ClientAuthn" type="xsd:boolean" default="true">
    <xsd:annotation>
        <xsd:documentation xml:lang="en">
            Whether checking client certificate. Only needed for service side.
            Default
            is "true".
        </xsd:documentation>
    </xsd:annotation>
</xsd:element>

<xsd:element name="VOMSCertTrustDNChain">
    <xsd:complexType>
        <xsd:annotation>
            <xsd:documentation xml:lang="en">
                The DN list of the trusted voms server credential; in the AC part of
                voms proxy certificate, voms proxy certificate comes with the server
                certificate which is used to sign the AC. So when verifying the AC on
                the AC-consuming side (in ARC1, it is the MCCTLS which will consumes
                the AC), the server certificate will be checked against a trusted DN
                list. Only if the DN and issuers DN of server certificate exactly
                matches the DN list in the configuration under TLS component, the AC
                can
                be trusted
            </xsd:documentation>
        </xsd:annotation>
        <xsd:sequence>
            <xsd:element name="VOMSCertTrustDN" type="xsd:string" minOccurs="0"
                maxOccurs="unbounded"/>
            <xsd:element name="VOMSCertTrustRegex" type="xsd:string" minOccurs="0"/>
        </xsd:sequence>
    </xsd:complexType>
</xsd:element>

<xsd:element name="VOMSCertTrustDNChainsLocation" type="xsd:string">
    <xsd:annotation>
        <xsd:documentation xml:lang="en">
            DN list in an external file, which is in the same format as
            VOMSCertTrustDNChain.
        </xsd:documentation>
    </xsd:annotation>
</xsd:element>

<xsd:element name="Handshake" default="TLS">
    <xsd:simpleType>
        <xsd:annotation>
            <xsd:documentation xml:lang="en">
                Type of handshake applied. Default is TLS.
            </xsd:documentation>
        </xsd:annotation>
        <xsd:restriction base="xsd:string">
            <xsd:enumeration value="TLS"/>
            <xsd:enumeration value="SSLv3"/>
        </xsd:restriction>
    </xsd:simpleType>
</xsd:element>

</xsd:schema>

```