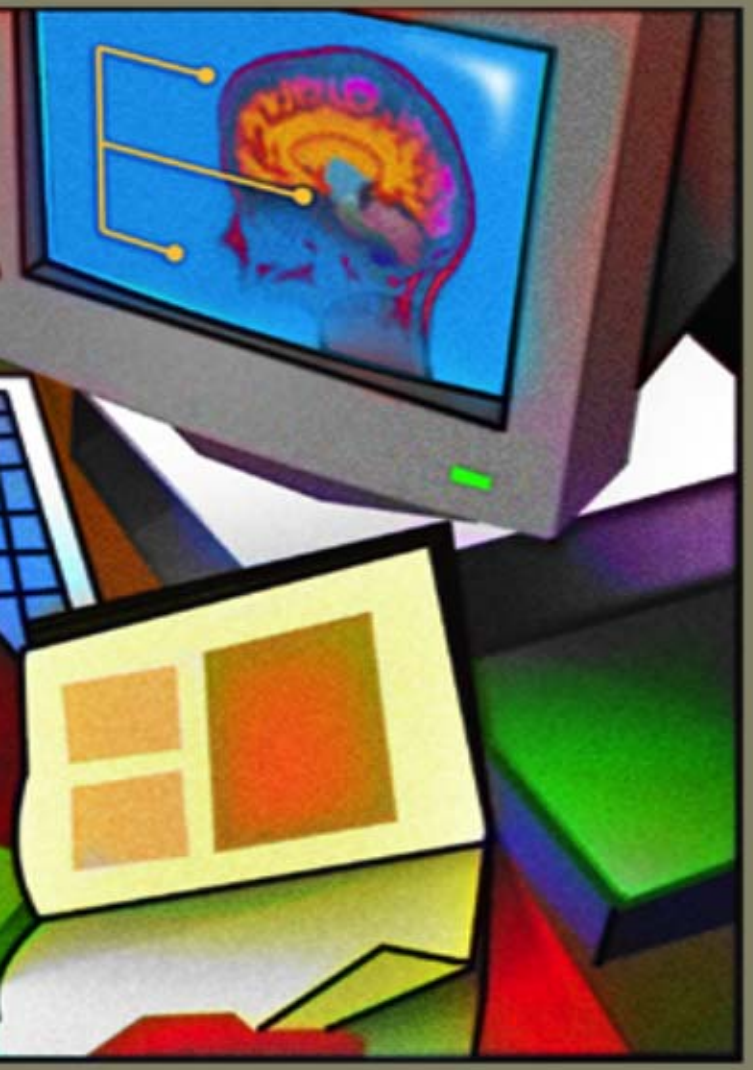
cations



EHI Connecting Comm
Forum
April 11, 2006

Don Grodecki
Browsersoft, Inc

CONNECTING FOR H
MARKLE FOUNDATION A Public-

HRE

n Source Health Records Exchang

p://openhre.org

n Source software toolkit for buildi

th Records Exchange within a RHI

een RHIOs

loped by Browsersoft Inc.

p://browsersoft.com

to build SHARE for the Alliance fo
l Community Health (ARCH) in
docino California

p://ruralcommunityhealth.org

by the Mendocino HRE for the Ma
necting for Health (CfH) Record Lo
ce (RLS) project.

p://mendocinohre.org

p://www.connectingforhealth.org

HRE

d by the Mendocino HRE for the
N Prototype project, as part of t
/CfH team.

p://www.hhs.gov/healthit

HRE

sists of three main services

ecord Locator Service (RLS)

ecord Exchange Service (RES)

thentication and Access Control Se
ACS)

We will concentrate here on the AACS

ent Practice

-Based Authorization

s are assigned one or more Roles

ess to information and operations i

rolled by Role

’s about it!

ss to information and operations
rolled by:

Address

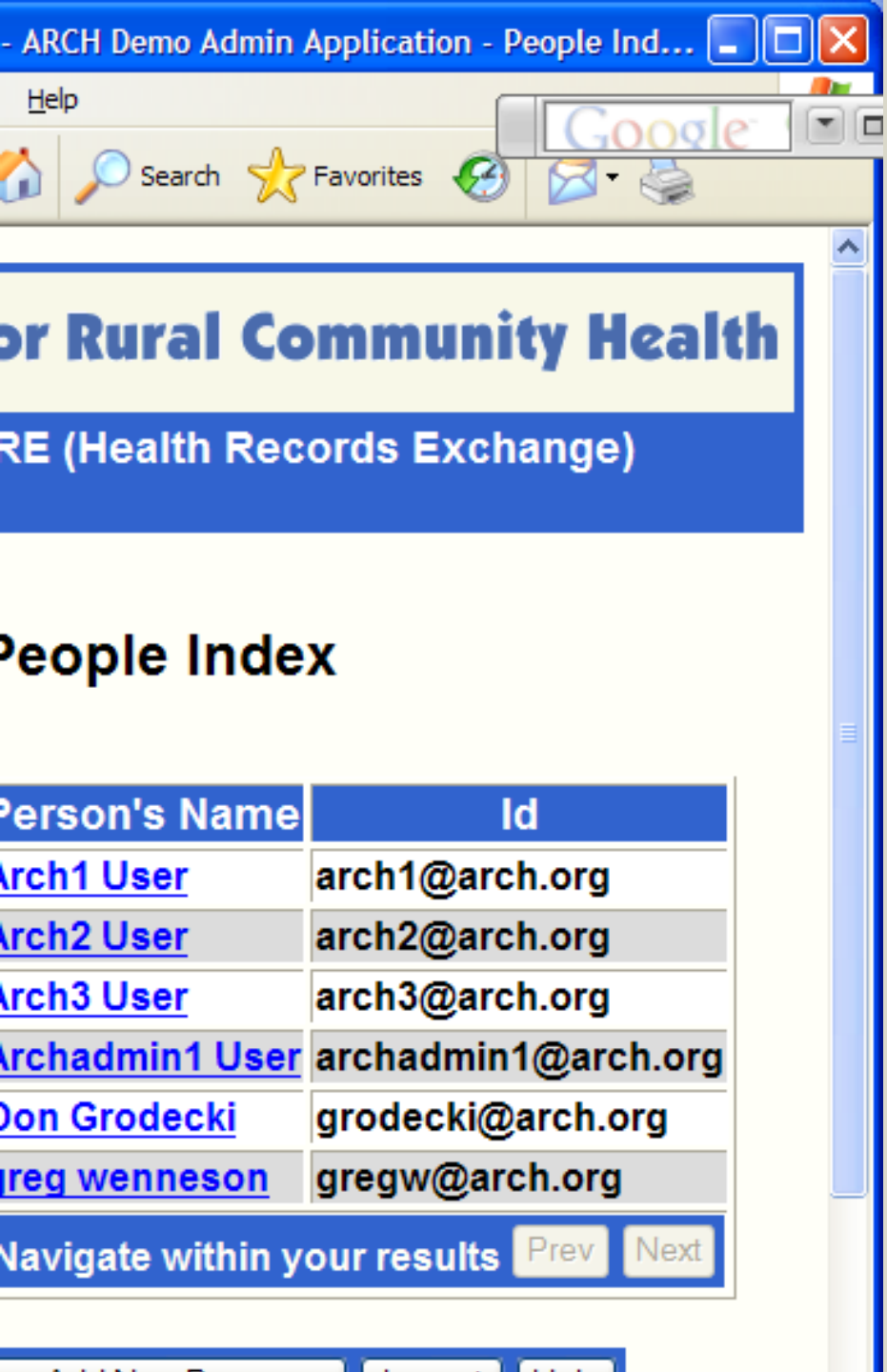
le

oup

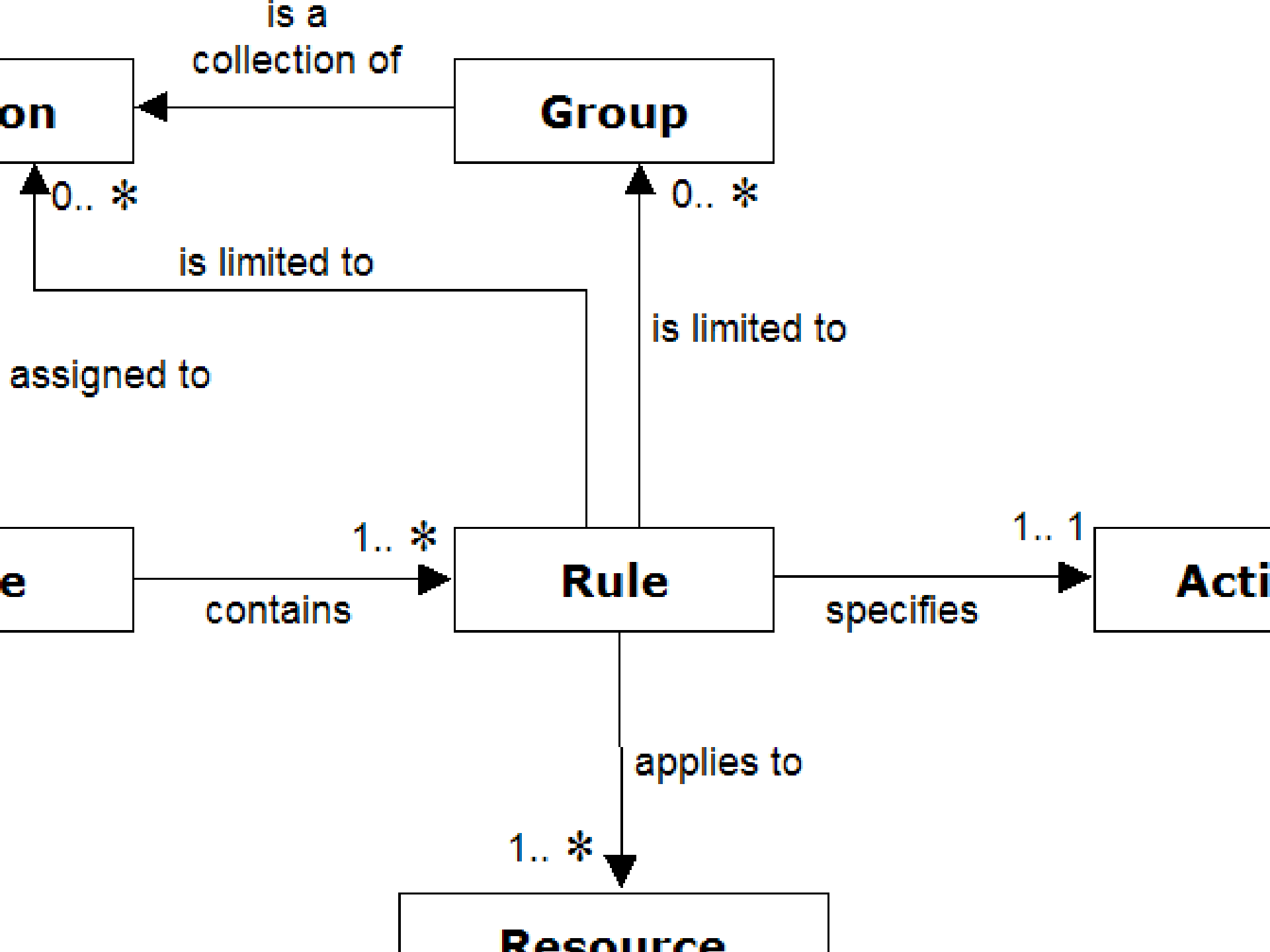
ormation Content

rity Policies expressed in XACML

SIS eXtensible Access Control Markup Lan



- Access Co
  Administra
  available vi
  Web Applic


is a
collection of
on
Group
0.. *
0.. *
is limited to
is limited to
assigned to
1.. *
1.. 1
e
Rule
Acti
contains
specifies
applies to
1.. *

l stuff ...

it Person

quired Information

t Name: Arch1

t Name: User

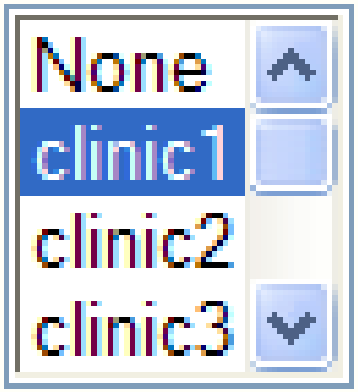
arch1

ail: gregw@ruralcommunityhealt

e(s): admin
physician
staff

te so usual ...

ormation



lid from (MM/DD/YYYY): 08/16/2005

newal required after: -1 days

must access via an IP Address that i
one of the specified ranges.

? Addresses are specified, then the u
cess from anywhere, but, as we shal
limit their access permissions.

onal to Roles

can have allowed IP Addresses

in via a different IP temporarily removes
om a Group

roup

me:

clinic1

ed IP address(es)/range(s):

69.152.171.128/16
69.243.105.35/16
63.196.238.122/8

seem to be as expected ...

Role Index

Role Name
admin
physician
staff

re is
them

pply
o a
ce

Role Name: physic

Applicable Resource: DNS:A

Parent Role(s):

None
admin
physic
staff

Update Role | Delete Role

Add New Rule | Cancel | Logout | Help

Rules

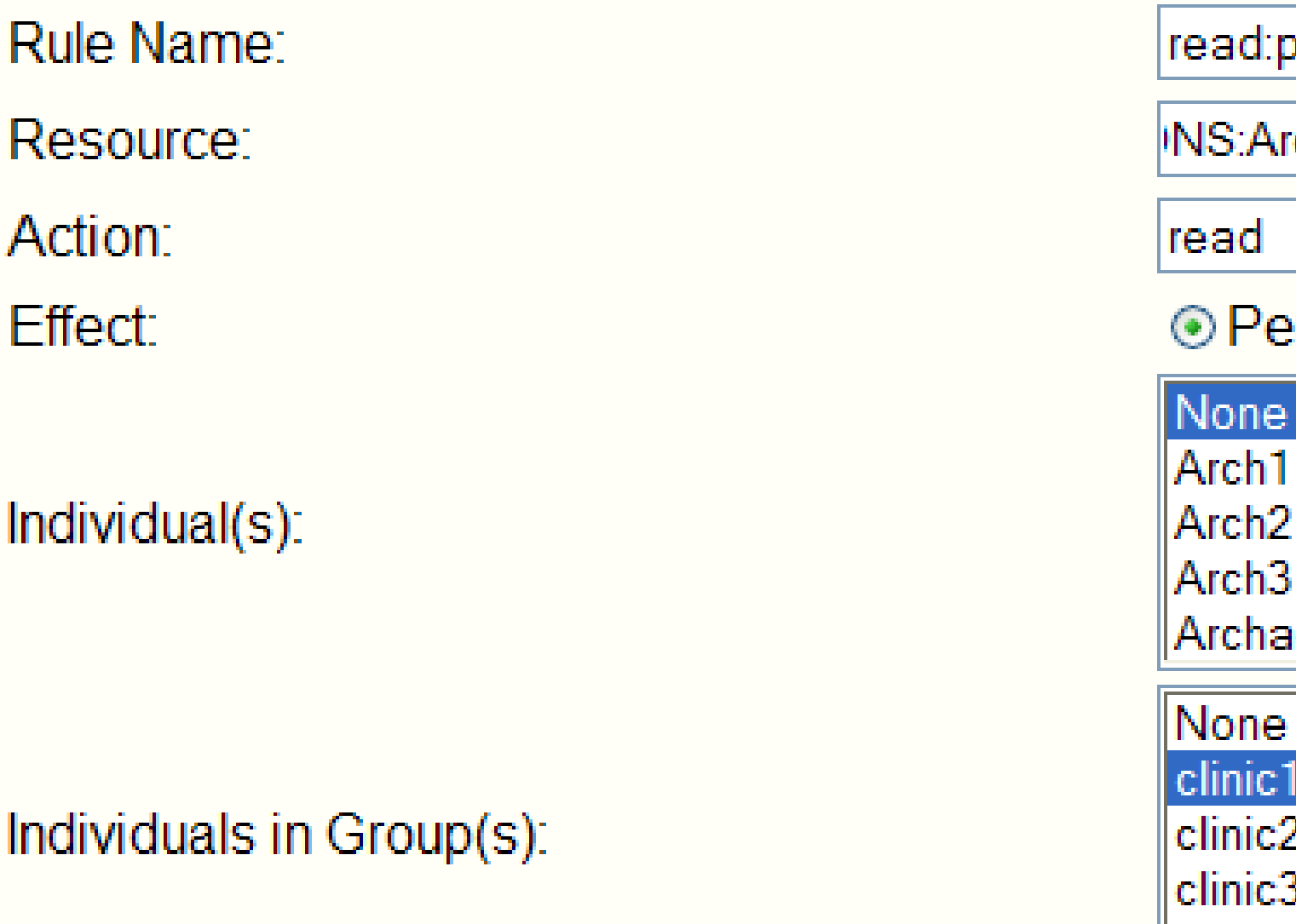
Rule Name
read:patient_record:clinic1

rmit or
Action
ource
uals or

s are a
its

s

Edit Rule



dmin web application creates XACML file
be the policies it supports, including the
by the user.

ed by the generated XACML, Sun's XACM
eter examines the supplied data and gra
permission.

//sunxacml.sourceforge.net

es outside of what is possible using the A
specified by editing the XACML directly

agment specifies that permission will be
er has the “read” Action.

```
RuleId="CommitRule" Effect="Permit">

n>
ionMatch
hId="urn:oasis:names:tc:xacml:1.0:function:
l">
ttributeValue
Type=“.../XMLSchema#string">read</Attribute
ctionAttributeDesignator
Type=“.../XMLSchema#string"
ibuteId="urn:oasis:names:tc:xacml:1.0:actio
>
```

gment specifies that “read” will be granted if
ce-id matches “clinic2” and the User is in the

```
leId="read:...:clinic2” Effect="Permit">

rceMatch MatchId=”...:function:regexp-string-mat
ributeValue>DNS:Arch.org://OTHER:/clinic2/</Attr
ourceAttributeDesignator AttributeId=”...:resour

Match MatchId=”...:function:string-equal">
ributeValue>read</AttributeValue>

tion FunctionId=”...:string-is-in">
ibuteValue DataType=”...#string">MC2</AttributeV
ectAttributeDesignator AttributeId=”...:group"/>
```