

**INTERNATIONAL ORGANISATION FOR STANDARDISATION
ORGANISATION INTERNATIONALE DE NORMALISATION
ISO/IEC JTC 1/SC 29/WG 11
CODING OF MOVING PICTURES AND AUDIO**

**ISO/IEC JTC 1/SC 29/WG 11
MPEG2017/m39939
January 2017, Geneva, Switzerland**

Source: DMAG-UPC, CNAG-CRG, BSC
Status: Proposal
Title: Genomic Information Compression and Storage CE4: DMAG-UPC's GENIFF v.2 implementation
Authors: Jaime Delgado, Silvia Llorente, Daniel Naro, Sara Rodríguez-Cubillas (Distributed Multimedia Applications Group – Universitat Politècnica de Catalunya), Łukasz Roguski (Centro Nacional de Análisis Genómico – Centre de Regulació Genòmica (CNAG – CRG)), Josep Lluís Gelpí, Dmitry Repchevsky, Romina Royo (Barcelona Supercomputing Center)

Contents

1	Introduction	2
2	Experiment Description.....	2
3	Core Experiment Output	3
4	Data for Evaluation	4
5	Acknowledgements	6
6	References	6
	Annex I – Examples of XACML rules.....	8

1 Introduction

This document answers to the Core Experiment CE 4 Genomic Access Abstract Layer described in [1].

The organizations presenting this work include Distributed Multimedia Applications Group from the Universitat Politècnica de Catalunya (DMAG-UPC), Barcelona Supercomputing Center (BSC) and Centro Nacional de Análisis Genómico - Centre de Regulació Genòmica (CNAG-CRG).

The documents deals with the 6 phases described in [1]:

1. The generation of a file containing encoded genomic information with the proposed abstraction layer
2. The selective access to data subsets and the assembly of meaningful subsets of data according to selected query criteria
3. The transfer of the encoded genomic information to a remote peer over a network
4. The selective access to subsets of the received data and the assembly of meaningful subsets of data according to selected query criteria
5. The controlled access to specific data subsets based on access control rules
6. The identification of specific data subsets based on metadata elements at different levels of abstraction

This response to CE 4 uses the GENIFF proposal [2], with some improvements [3]. Another document describes the software user's guide [4].

The rest of this section describes how the Core Experiment has been developed and how the information required is provided. First, we provide an explanation on how the experiment has been developed. Then, we provide information about how to access the resulting files and different measures to compare experiment results.

2 Experiment Description

In order to provide the 6 phases of the experiment, we have developed a tool to generate files in the GENIFF format described in [3]. With this tool we can include elements to provide access control to different elements inside GENIFF, to be able to access to the genomic information remotely or to protect genomic information at different levels of granularity.

Once the file in GENIFF format is generated including access control rules and protection, we have developed another tool to authorize access to the genomic information based on the permissions and / or prohibitions expressed in the access rules. These rules, as defined in [2], can define actions allowed, in which time frame, to which user role, etc.

In particular, we have generated the GENIFF file corresponding to genomic information [1], including security and access control at level of the dataset, as required in phase 1. In the instance we provide, the rules exemplify two approaches. On the one hand, we have the case where by default we deny access, and the rules indicate the exceptions to this. The reader will see this for the rules affecting the roles "physician" and "researcher" (the first role is allowed to access the whole dataset, the later only the chromosome 2). On the other hand, we have the case where the default is to grant access, while the rules provide the exceptions. For an example of this, refer to the rules applying to the role "doctor", where the access to chromosome 2 is denied.

To support phase 2, we have stored the genomic information provided in the test input BAMs, dividing each file into multiple shorter BAMs such that we have one BAM file per reference sequence. Each one of these newly created BAM files is stored as a stream within the same dataset. In the case of the input 05 this does not match the chromosomes (as there are alternative reference sequences). From the SAM header information we know to which chromosome the reference belongs to (either because the name is clear, or because we have accessed online databases during the encoding in GENIFF format), thus giving enough information to apply the rules. Regarding the encryption, certain streams are encrypted as indicated in the configuration files (for example in the case of the input 05 the stream corresponding to the reference sequence 2 is encrypted). One should note that the chosen encryption method is AES-CTR allowing easy random access to the memory. In order to decrypt the content, the user needs the passphrase, which is currently hardcoded, and the salt which is stored in the header boxes in the GENIFF file.

We have checked phase 3, and the resulting file is the same as in phase 1. As the file is the same as in phase 1, phase 4 has the same results as phase 2. Nevertheless, we have added an extra functionality, implementing an HTTP server that supports remotely requesting parts of the genomic file expressed in GENIFF format. This server works using a description of the GENIFF file which states at which location which information is provided. Depending on the nature of the content (BAM in a unique stream, BAM in multiple streams, a FASTQ file compressed with gzip), the user can access, through the familiar interface of the URLs, precisely to the desired content. For example, we can access to the header file of a dataset or a stream, its index or the data's bytestream. Currently, the server takes up the task to decrypt the content and return it (over HTTPS) to the client. Nevertheless, thanks to the HTTPS connection, the client is authenticated through his certificate (it is the information stored in the certificate which is used to process the XACML rules). We should also note that thanks to the HTTP option "range bytes", and the encryption using CTR (Counter), the access to disk, and the information send over the network is reduced as much as possible.

To support phase 5, we have defined several access control rules. They are described in phase 1 and can be found in Annex I.

To support phase 6, the user, or his tool, can access the headers at different levels of the GENIFF file in order to discover which regions he wants to access: this allows, for example, retrieving information about the alternative reference sequences. A new definition of metadata will extend these capabilities.

3 Core Experiment Output

For the CE output, we provide the following files:

Under CE4 UPC-DMAG/GeniffExamples:

- File ID02.geniff, which contains the complete GENIFF file for input 02.
- File Id05.geniff, which contains the complete GENIFF file for input 05.
- File Id07.geniff, which contains the complete GENIFF file for input 07.
- File Id20.geniff, which contains the complete GENIFF file for input 20.

Under Genome for CEs:

- Folder 02, which contains the input 05 original file alongside a divided in multiple BAM files, one for each reference sequence, version and the header as contained in the original file.
- Folder 05, which contains the input 05 original file alongside a divided in multiple BAM files, one for each reference sequence, version and the header as contained in the original file.
- Folder 07, which contains the input 07 original files.
- Folder 20, which contains the input 20 original files.

4 Data for Evaluation

This section describes the information required to perform the evaluation of the proposed format and tools.

The following results have been obtained using a virtual environment. The hosting computer is a Windows 7 machine, with an i7-3770 CPU. The guest environment is an Ubuntu 16.04, with 5GB of RAM, running within Virtual Box and using acceleration technologies (VT-x/AMD-V, PAE/NX, KVM).

Table 1 – Description of functionality provided

Functionality	Provided	Description
Granularity of access	YES	The smallest granularity provided is at the level of the data of a stream, which, in the examples we provide, corresponds to the data for one reference sequence.
Indexing	YES	The smallest indexing information is at the level of the data of a stream. In the examples we provide, this corresponds to the data for one reference sequence, and as we use BAI files for the indexing, we obtain the same granularity as in the case of a BAM file.
Protection and access control	YES	Access control: XACML rules and authorization. Security: As can be seen in the User Guide, the encryption can be set on and off at the level of the complete dataset, if it is mono-stream, or for each stream.
Metadata elements	YES	Metadata can be included in the GENIFF format at different levels and in different formats, to support existing metadata (i.e. SAM Header) or newly generated one. We have also provided an XML schema to express SAM Header inside GENIFF.
Extensibility	YES	The proposed structure can be easily extended to add new levels and to add new elements inside the existing ones.

Table 2 – Resource requirements

Resource requirements	Description																				
Computation overhead	<table border="1"> <thead> <tr> <th data-bbox="603 338 1018 376">Data used</th> <th data-bbox="1026 338 1415 376">Measured overhead</th> </tr> </thead> <tbody> <tr> <td colspan="2" data-bbox="603 383 1415 421" style="text-align: center;">Input 02</td> </tr> <tr> <td data-bbox="603 421 1018 600">Input 02 split in 25 streams (each one being a BAM file containing the information for only one of the reference sequences)</td> <td data-bbox="1026 421 1415 600" style="text-align: center;">4792s</td> </tr> <tr> <td colspan="2" data-bbox="603 607 1415 645" style="text-align: center;">Input 05</td> </tr> <tr> <td data-bbox="603 645 1018 824">Input 05, split in 86 streams (each one being a BAM file containing the information for only one of the reference sequences)</td> <td data-bbox="1026 645 1415 824" style="text-align: center;">215s</td> </tr> <tr> <td data-bbox="603 831 1018 869">Input 05, as the original final</td> <td data-bbox="1026 831 1415 869" style="text-align: center;">244s</td> </tr> <tr> <td colspan="2" data-bbox="603 875 1415 913" style="text-align: center;">Input 07</td> </tr> <tr> <td data-bbox="603 913 1018 1010">Input 07, as two datasets one for each of the FASTQ files (Encrypting both files)</td> <td data-bbox="1026 913 1415 1010" style="text-align: center;">1585s</td> </tr> <tr> <td colspan="2" data-bbox="603 1016 1415 1055" style="text-align: center;">Input 20</td> </tr> <tr> <td data-bbox="603 1055 1018 1155">Input 20, as two datasets one for each of the FASTQ files (Encrypting both files)</td> <td data-bbox="1026 1055 1415 1155" style="text-align: center;">42s</td> </tr> </tbody> </table>	Data used	Measured overhead	Input 02		Input 02 split in 25 streams (each one being a BAM file containing the information for only one of the reference sequences)	4792s	Input 05		Input 05, split in 86 streams (each one being a BAM file containing the information for only one of the reference sequences)	215s	Input 05, as the original final	244s	Input 07		Input 07, as two datasets one for each of the FASTQ files (Encrypting both files)	1585s	Input 20		Input 20, as two datasets one for each of the FASTQ files (Encrypting both files)	42s
	Data used	Measured overhead																			
	Input 02																				
	Input 02 split in 25 streams (each one being a BAM file containing the information for only one of the reference sequences)	4792s																			
	Input 05																				
	Input 05, split in 86 streams (each one being a BAM file containing the information for only one of the reference sequences)	215s																			
	Input 05, as the original final	244s																			
	Input 07																				
	Input 07, as two datasets one for each of the FASTQ files (Encrypting both files)	1585s																			
	Input 20																				
Input 20, as two datasets one for each of the FASTQ files (Encrypting both files)	42s																				
Memory usage	<p data-bbox="603 1173 1415 1205">As reported by Vagrant the memory allocated is:</p> <table border="1"> <tbody> <tr> <td data-bbox="603 1205 1018 1384">Input 05, split in 86 streams (each one being a BAM file containing the information for only one of the reference sequences)</td> <td data-bbox="1026 1205 1415 1384" style="text-align: center;">93 588 926</td> </tr> <tr> <td data-bbox="603 1391 1018 1496">Input 20, as two datasets one for each of the FASTQ files (Encrypting both files)</td> <td data-bbox="1026 1391 1415 1496" style="text-align: center;">232 492</td> </tr> </tbody> </table> <p data-bbox="603 1503 1415 1570">The difference is caused by the memory allocation for the headers in the case of Input 05.</p>	Input 05, split in 86 streams (each one being a BAM file containing the information for only one of the reference sequences)	93 588 926	Input 20, as two datasets one for each of the FASTQ files (Encrypting both files)	232 492																
Input 05, split in 86 streams (each one being a BAM file containing the information for only one of the reference sequences)	93 588 926																				
Input 20, as two datasets one for each of the FASTQ files (Encrypting both files)	232 492																				
Code footprint size	<p data-bbox="603 1588 1415 1682">The C++ code represents 233 KB (including the java code to retrieve information online), the Java code (server’s implementations) represent 92.2 KB.</p>																				
Binary footprint size	<p data-bbox="603 1700 1415 1794">The main tool requires 606 320 bytes on the hard drive. The server program requires 4 528 248 bytes in its jar packaged form with dependencies included.</p>																				

Table 3 – Overall bitrate overhead

Bitrate overhead	Description																				
Bitstream new tools	Server's statistics (localhost, redirecting downloaded information to null): Bitrate: 120Mbps; Header's size: 168; Time before transfer: 4ms (if server initialized, i.e. there was at least one previous request) 584ms (otherwise)																				
Bitstream overhead on encoded content	<table border="1"> <thead> <tr> <th>Data used</th> <th>Measured overhead</th> </tr> </thead> <tbody> <tr> <td colspan="2" style="text-align: center;">Input 02</td> </tr> <tr> <td>Input 02, split in one stream per reference sequence</td> <td>4.2KB</td> </tr> <tr> <td colspan="2" style="text-align: center;">Input 05</td> </tr> <tr> <td>Input 05, split in 86 streams (each one being a BAM file containing the information for only one of the reference sequences)</td> <td>14.7 KB</td> </tr> <tr> <td>Input 05, as the original final</td> <td>299B</td> </tr> <tr> <td colspan="2" style="text-align: center;">Input 07</td> </tr> <tr> <td>Input 07, as two datasets one for each of the FASTQ files</td> <td>402B</td> </tr> <tr> <td colspan="2" style="text-align: center;">Id20</td> </tr> <tr> <td>Input 20, as two datasets one for each of the FASTQ files</td> <td>416B</td> </tr> </tbody> </table>	Data used	Measured overhead	Input 02		Input 02, split in one stream per reference sequence	4.2KB	Input 05		Input 05, split in 86 streams (each one being a BAM file containing the information for only one of the reference sequences)	14.7 KB	Input 05, as the original final	299B	Input 07		Input 07, as two datasets one for each of the FASTQ files	402B	Id20		Input 20, as two datasets one for each of the FASTQ files	416B
	Data used	Measured overhead																			
	Input 02																				
	Input 02, split in one stream per reference sequence	4.2KB																			
	Input 05																				
	Input 05, split in 86 streams (each one being a BAM file containing the information for only one of the reference sequences)	14.7 KB																			
	Input 05, as the original final	299B																			
	Input 07																				
	Input 07, as two datasets one for each of the FASTQ files	402B																			
	Id20																				
Input 20, as two datasets one for each of the FASTQ files	416B																				

5 Acknowledgements

The work done in this proposal has been partially supported by the Spanish Government under the project: Secure Genomic Information Compression (GenCom, TEC2015-67774-C2-1-R and TEC2015-67774-C2-2-R) and the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement No. 305444 (RD-Connect).

6 References

- [1] ISO/IEC JTC 1/SC 29/WG 11 / N16526 - ISO/TC 276/WG 5 / N120 – Core Experiments on Genomic Information Representation, Chengdu, October 2016.
- [2] Jaime Delgado, Silvia Llorente et al., ISO/IEC JTC 1/SC 29/WG 11 M39175, GENIFF (GENomic Information File Format), a proposal for a Secure Genomic Information Transport Layer (GITL) based on the ISO Base Media File Format, Chengdu, China, October 2016.
- [3] Jaime Delgado, Silvia Llorente et al., ISO/IEC JTC 1/SC 29/WG 11 M39940, GENIFF v2, December 2016.

[4] Daniel Naro, Jaime Delgado and Silvia Llorente, ISO/IEC JTC 1/SC 29/WG 11 M39941, User's Guide for DMAG-UPC's GENIFF v.2 software used for Genome information CEs, December 2016.

Annex I – Examples of XACML rules

XACML policy containing several rules, exemplifying two different approaches. On the one hand, we have the case where by default we deny access, and the rules indicate the exceptions to this. These rules are the ones defined for roles “physician” and “researcher” (the first role is allowed to access the whole dataset, the later only the chromosome 2). On the other hand, we have the case where the default is to grant access, while the rules provide the exceptions. For an example of this, refer to the rules applying to the role “doctor”, where the access to chromosome 2 is denied.

```
<Policy
  xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17
    http://docs.oasis-open.org/xacml/3.0/xacml-core-v3-schema-wd-17.xsd"
  PolicyId="urn:genomeaccesscontrol:policyid:2"
  RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:first-applicable"
  Version="1.0">
  <Description> Policy rules sample</Description>
  <PolicyDefaults>
    <XPathVersion>http://www.w3.org/TR/1999/REC-xpath-19991116</XPathVersion>
  </PolicyDefaults>
  <Target/>
  <Rule RuleId="urn:oasis:names:tc:xacml:3.0:ejemplo:RuleSAM" Effect="Permit">
    <Description> A physician may view the genomic information file
      for which he or she is the designated primary care
      physician, provided an email is sent to the patient</Description>
    <Target>
      <AnyOf>
        <AllOf>
          <!-- Which kind of user: physician -->
          <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
              physician
            </AttributeValue>
            <AttributeDesignator MustBePresent="false"
              Category="urn:oasis:names:tc:xacml:3.0:role" AttributeId="role"
              DataType="http://www.w3.org/2001/XMLSchema#string"/>
          </Match>
          <!-- Which resource -->
          <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:regexp-string-match">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
              toy.sam
            </AttributeValue>
            <AttributeDesignator MustBePresent="false"
              Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
              AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
              DataType="http://www.w3.org/2001/XMLSchema#string"/>
          </Match>
          <!-- Which action -->
          <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
              VIEW
            </AttributeValue>
            <AttributeDesignator MustBePresent="false"
              Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
              AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
              DataType="http://www.w3.org/2001/XMLSchema#string"/>
          </Match>
        </AllOf>
      </AnyOf>
    </Target>
    <Condition>
      <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:and">
        <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:integer-less-than">
          <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:integer-one-and-only">
            <AttributeDesignator MustBePresent="false"
              Category="urn:oasis:names:tc:xacml:3.0:count" AttributeId="countView">

```



```

        DataType="http://www.w3.org/2001/XMLSchema#integer"/>
    </Apply>
    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#integer">
        4
    </AttributeValue>
</Apply>
</Condition>
</Rule>
<Rule RuleId="urn:oasis:names:tc:xacml:3.0:ejemplo:RuleSAMChromosome" Effect="Permit">
    <Description>A researcher may view chromosome 20 of a genomic information
        file if he is the responsible of the study,
        provided an email is sent to the data sharer </Description>
    <Target>
        <AnyOf>
            <AllOf>
                <!-- Which kind of user: researcher -->
                <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                        researcher
                    </AttributeValue>
                    <AttributeDesignator MustBePresent="false"
                        Category="urn:oasis:names:tc:xacml:3.0:role" AttributeId="role"
                        DataType="http://www.w3.org/2001/XMLSchema#string"/>
                </Match>

                <!-- Which resource -->
                <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:regexp-string-match">
                    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                        toy.sam#ref2
                    </AttributeValue>
                    <AttributeDesignator MustBePresent="false"
                        Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
                        AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
                        DataType="http://www.w3.org/2001/XMLSchema#string"/>
                </Match>

                <!-- Which action -->
                <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                        VIEWCHROMOSOME
                    </AttributeValue>
                    <AttributeDesignator MustBePresent="false"
                        Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
                        AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
                        DataType="http://www.w3.org/2001/XMLSchema#string"/>
                </Match>
            </AllOf>
        </AnyOf>
    </Target>

    <Condition>
        <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:and">
            <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:integer-less-than">
                <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:integer-one-and-only">
                    <AttributeDesignator MustBePresent="false"
                        Category="urn:oasis:names:tc:xacml:3.0:count" AttributeId="countView"
                        DataType="http://www.w3.org/2001/XMLSchema#integer"/>
                </Apply>
                <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#integer">
                    4
                </AttributeValue>
            </Apply>
        </Apply>
    </Condition>
</Rule>
<Rule RuleId="urn:oasis:names:tc:xacml:3.0:ejemplo:RuleSAMChromosomeDeny" Effect="Deny">
    <Description>A doctor cannot view chromosome 2 </Description>
    <Target>
        <AnyOf>
            <AllOf>
                <!-- Which kind of user: researcher -->
                <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                        doctor
                    </AttributeValue>
                    <AttributeDesignator MustBePresent="false"

```

```

        Category="urn:oasis:names:tc:xacml:3.0:role" AttributeId="role"
        DataType="http://www.w3.org/2001/XMLSchema#string"/>
    </Match>

    <!-- Which resource -->
    <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
        <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
            file.sam#ref2
        </AttributeValue>
        <AttributeDesignator MustBePresent="false"
            Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
            AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
            DataType="http://www.w3.org/2001/XMLSchema#string"/>
    </Match>

    <!-- Which action -->
    <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
        <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
            VIEWCHROMOSOME
        </AttributeValue>
        <AttributeDesignator MustBePresent="false"
            Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
            AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
            DataType="http://www.w3.org/2001/XMLSchema#string"/>
    </Match>

    </AllOf>
</AnyOf>
</Target>

<Condition>
    <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:and">

        <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:integer-less-than">
            <ApplyFunctionId="urn:oasis:names:tc:xacml:1.0:function:integer-one-and-only">
                <AttributeDesignator MustBePresent="false"
                    Category="urn:oasis:names:tc:xacml:3.0:count" AttributeId="countView"
                    DataType="http://www.w3.org/2001/XMLSchema#integer"/>
            </Apply>
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#integer">
                4
            </AttributeValue>
        </Apply>
    </Apply>
</Condition>
</Rule>
<Rule RuleId="urn:oasis:names:tc:xacml:3.0:ejemplo:RuleSAMChromosomeALL" Effect="Permit">
    <Description>A doctor may view all genomic information,
        provided an email is sent to the data sharer </Description>
    <Target>
        <AnyOf>
            <AllOf>
                <!-- Which kind of user: doctor -->
                <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                        doctor
                    </AttributeValue>
                    <AttributeDesignator MustBePresent="false"
                        Category="urn:oasis:names:tc:xacml:3.0:role" AttributeId="role"
                        DataType="http://www.w3.org/2001/XMLSchema#string"/>
                </Match>

                <!-- Which resource -->
                <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:regexp-string-match">
                    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                        file.sam*
                    </AttributeValue>
                    <AttributeDesignator MustBePresent="false"
                        Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
                        AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
                        DataType="http://www.w3.org/2001/XMLSchema#string"/>
                </Match>

                <!-- Which action -->
                <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                        VIEWCHROMOSOME
                    </AttributeValue>
                    <AttributeDesignator MustBePresent="false"
                        Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
                        AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
                        DataType="http://www.w3.org/2001/XMLSchema#string"/>
                </Match>
            </AllOf>
        </AnyOf>
    </Target>

```

```

        </AttributeValue>
        <AttributeDesignator MustBePresent="false"
            Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
            AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
            DataType="http://www.w3.org/2001/XMLSchema#string"/>
    </Match>
</AllOf>
</AnyOf>
</Target>

<Condition>
    <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:and">
        <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:integer-less-than">
            <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:integer-one-and-only">
                <AttributeDesignator MustBePresent="false"
                    Category="urn:oasis:names:tc:xacml:3.0:count" AttributeId="countView"
                    DataType="http://www.w3.org/2001/XMLSchema#integer"/>
                </Apply>
                <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#integer">
                    4
                </AttributeValue>
            </Apply>
        </Apply>
    </Condition>
</Rule>
<Rule RuleId="urn:oasis:names:tc:xacml:3.0:genomeaccesscontrol:FinalRule" Effect="Deny"/>
<ObligationExpressions>
    <ObligationExpression ObligationId="urn:oasis:names:tc:xacml:example:obligation:email"
        FulfillOn="Permit">
        <AttributeAssignmentExpression
            AttributeId="urn:oasis:names:tc:xacml:3.0:example:attribute:mailto">
            <AttributeSelector
                MustBePresent="true"
                Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
                Path="patient-email"
                DataType="http://www.w3.org/2001/XMLSchema#string"/>
            </AttributeAssignmentExpression>
            <AttributeAssignmentExpression
                AttributeId="urn:oasis:names:tc:xacml:3.0:example:attribute:text">
                <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string"
                    >Your genomic information has been accessed by:</AttributeValue>
            </AttributeAssignmentExpression>
            <AttributeAssignmentExpression
                AttributeId="urn:oasis:names:tc:xacml:3.0:example:attribute:text">
                <AttributeDesignator
                    MustBePresent="false"
                    Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                    AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
                    DataType="http://www.w3.org/2001/XMLSchema#string"/>
                </AttributeAssignmentExpression>
            </ObligationExpression>
        </ObligationExpressions>
</Policy>

```