The IETF Geopriv and Presence Architecture Focus

Hannes Tschofenig, Henning Schulzrinne, Andrew Newton, Jon Peterson, Allison Mankin

Acknowledgements

- We would like to particularly thank the following members of the IETF Geopriv working group for their help:
  - James Polk
  - Ted Hardie
  - John Morris
  - Jorge Cuellar
  - Carl Reed
  - Jonathan Rosenberg
  - James Winterbottom
  - Martin Thomson

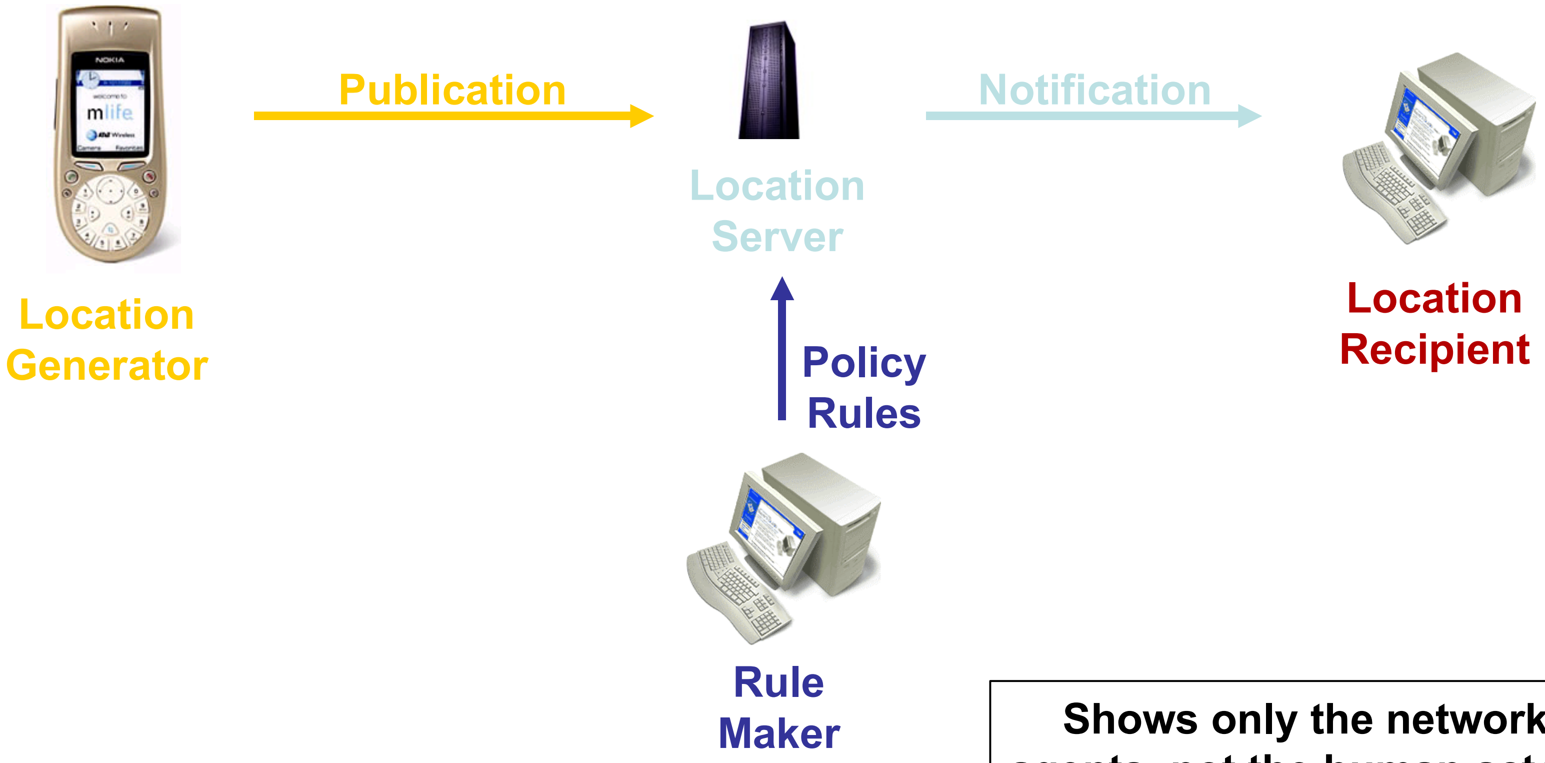
The GEOPRIV IETF Working Group

- First BoF on Spatial Location held at 48th IETF (July 2000)
  - Concerns that privacy was not sufficiently addressed
- GEOPRIV WG formed, met for the first time at 50th IETF (August 2001)
  - Strong user privacy mandate in WG charter
- Work quite mature already. A number of RFCs associated with this work are already available.
- Participation from industry vendors, standards professionals, public policy experts, and academia
- Location determination methods are out of scope
  - Scope is exclusively protecting the transmission of location information over the public Internet

GEOPRIV Objectives and Requirements

- Identify using protocols and document format for **carrying location information**
  - Allow push model and subscription model
  - Provide strong security measures to protect location information in transit
  - Insert policy directives into location information
- Develop **authorization policy language** for distribution of location information
  - Third parties enforce policies on behalf of “rule maker”
  - Motivated by a concern that many producers of geolocation information will not be controlled by end users
  - Rule Maker may be the owner of the target device, or may not

Basic GEOPRIV Architecture



Location Generator

Publication

Location Server

Notification

Location Recipient

Policy Rules

Rule Maker

Shows only the network agents, not the human actors

The Protocol: Schemas for Location Information

- The IETF does not want to define location information formats
  - Experts on these matters are largely elsewhere
- Instead, the IETF is focusing on architectures and tools for the secure distribution of location information documents
- Defining an envelope to carry any XML-based location information format
  - Popular choice is Geographic Markup Language (GML) (from OCG)
- No standardized format for civic location was available
  - Developed in Geopriv working group

Using Protocols

- Once you have a geolocation document, you need a protocol to carry it
- Traditional protocols are applicable (like HTTP, etc)
  - Anything that can carry MIME types works
- But a subscription model is ideal
  - Ability to track the location of a resource over time
  - Could use a polling model, but a subscription/notification model was deemed superior
  - Also, one-time fetch is desirable
- So far work focused on location conveyance using SIP:
- http://www.ietf.org/internet-drafts/draft-ietf-sip-location-conveyance-04.txt

(and a Diameter/RADIUS using protocol).

Tiny tutorial: http://www.ietf-ecrit.org/EmergencyWorkshop2006/
slides/SIP_Location_Conveyance.ppt

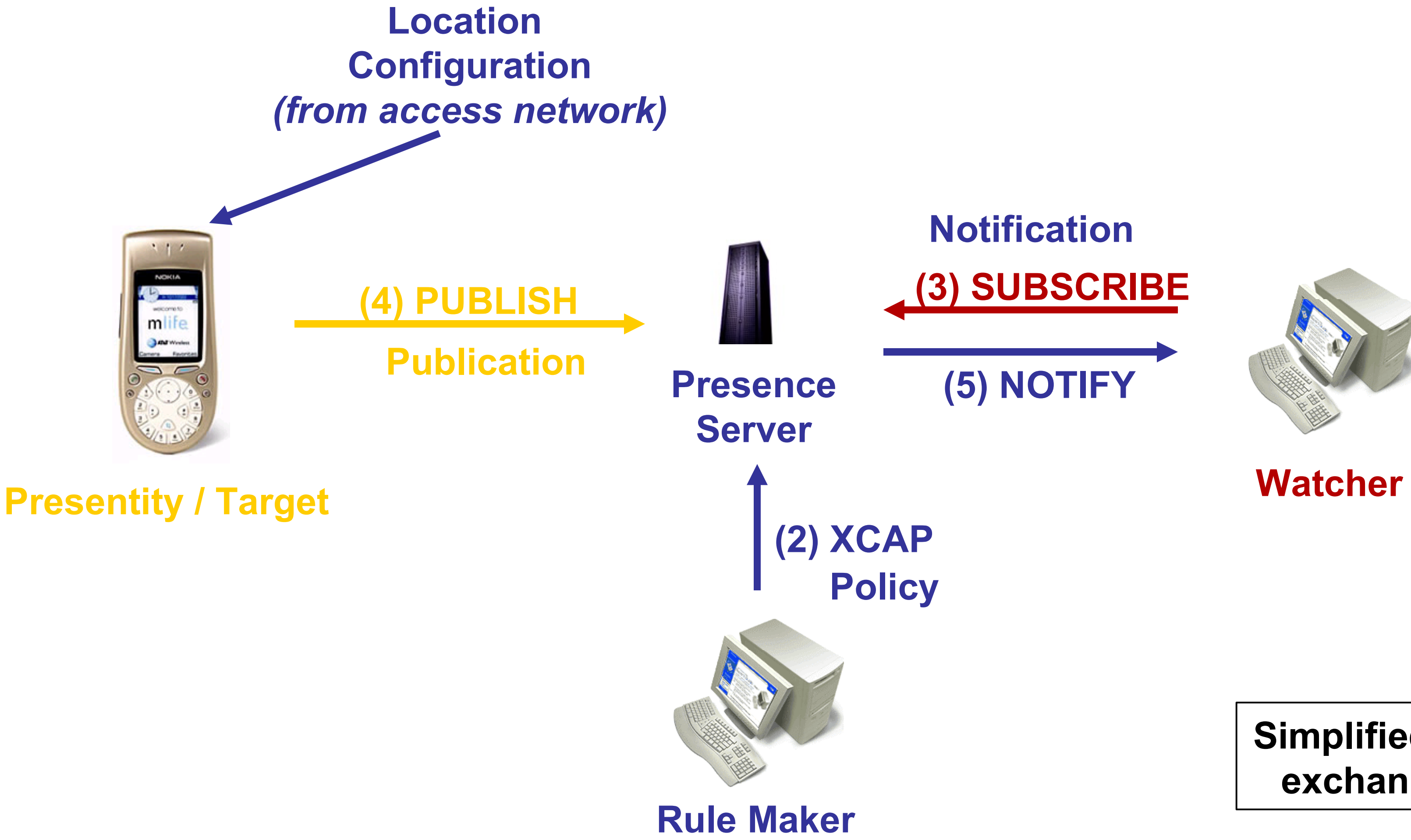
A Using Protocol: Overview of Presence

- Presence emerged as a component of instant messaging applications
- Foremost, provides binary availability data
  - Online or offline?
- Closely tied to the concept of a friends list
  - Based on subscription, a persistent relationship
- Modern presence systems also provide a disposition towards communication
  - Not just am I online, but am I busy, away, etc
- Capability information
  - What kinds of communication can I accommodate with my endpoint?
- Customized responses
  - Give different answers to different subscribers

Presence in the IETF

- Instant Messaging and Presence Protocol (IMPP) Working Group founded in 1999
- Originally, hoped to arrive at a single, standard instant messaging and presence protocol
  - Instead, became a massive religious war
  - Surviving proposals today are SIMPLE and XMPP
- Eventually, created a toolset for interoperability of instant messaging and presence protocols
  - Assumes an pluralistic environment
- Among those tools, defined the “pres:” URI scheme and an XML-based format for presence
  - Presence Information Data Format (PIDF)

Basic Presence Model Instantiating the GEOPRIV model



Simplified SIP exchanges

Geolocation and Presence

- Geopriv
  - Real-time information, changing frequently
  - Requires subscription model
  - Use servers to enforce policy
  - Need to be able to share information selectively
  - Strong authentication & confidentiality model
  - Extensibility (XML) required

- Presence
  - Ditto
  - Ditto
  - Ditto
  - Ditto
  - Ditto
  - Ditto

PIDF-LO: RFC 4119

- Presence Information Data Format (PIDF) is an XML-based format for presence (RFC 3863)
- Extends PIDF to accommodate two new elements:
  - Location-Info
    - Encapsulates location information
    - GML 3.0 <feature.xsd> schema (mandatory-to-implement)
    - Supports civic location format (optional-to-implement)
  - Usage-rules
    - Used to indicate privacy preferences

PIDF-LO: RFC 4119 Basic Ruleset

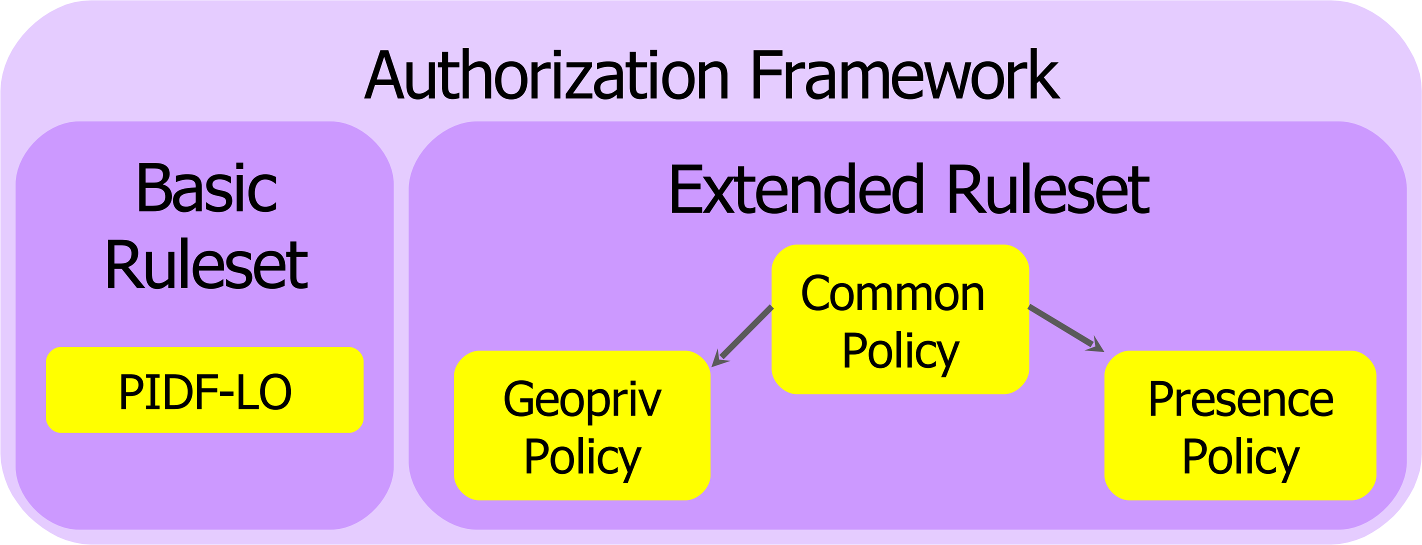
- MUST always be attached to a PIDF-LO document:
  - Retention expires (how long are you allowed to keep the object)
  - Policy for retransmission of location information (Yes/No)
  - Reference to an external ruleset (optional)
  - A “note well” of free text, human readable privacy policy
- Specified in RFC 4119
- Example:

```
<usage-rules>
  <retransmission-allowed>yes
   </retransmission-allowed>
  <retention-expires>2003-06-23T04:57:29Z
   </retention-expires>
</usage-rules>
```

Abbreviated PIDF-LO Example

```
<presence… entity=“pres:joe@example.com”>
 <tuple id=“sg89ae”>
  <status>
   <geopriv>
    <location-info>
      <gml…>
      </gml>
    </location-info>
    <usage-rules>
      <retention-expiry/>
      <retransmission-allowed/>
      <note-well>…</note-well>
    </usage-rules>
   </geopriv>
  </status>
 </tuple>
</presence>
```

Authorization for Presence and Location Information



draft-ietf-geopriv-common-policy-11.txt

draft-ietf-simple-presence-rules-07.txt

draft-ietf-geopriv-policy-08.txt

Extended Ruleset (1/2) Common Policy

- Two Usage Models:
  - Attached (per-value or per-reference) to PIDF-LO document
  - Available at the Location/Presence Server
- Design Goals:
  - Permit only
  - Additive permissions
  - Upgradeable/Extensibility
  - Capability/Versioning support
  - No false assurance
  - Efficient implementation (no regular expressions)
  - Protocol-independent
- Conflict resolution mechanism to ensure that new rules do not remove permissions; they can only add permissions.

Extended Ruleset (2/2) Common Policy

- Rule consists of:
  - conditions part
  - actions parts
  - transformations part
- Conditions:
  - Identity Conditions
    - Matching One Entity
    - Matching Multiple Entities
    - Matching Any Authenticated Identity
    - Matching Any Authenticated Identity Excepting Enumerated Domains/Identities
  - Sphere
  - Validity
- No actions & no transformations specified

Common Policy Example

```
<?xml version="1.0" encoding="UTF-8"?>
 <ruleset xmlns="urn:ietf:params:xml:ns:common-policy">
   <rule id="f3g44r1">
     <conditions>
       <identity>
         <one id="sip:alice@example.com"/>
         <one id="tel:+1-212-555-1234" />
         <one id="mailto:bob@example.net" />
         <many domain="example.com"/>
       </identity>
       <sphere value="work"/>
       <validity>
         <from>2003-12-24T17:00:00+01:00</from>
         <until>2003-12-24T19:00:00+01:00</until>
       </validity>
     </conditions>
     <actions/>
     <transformations/>
   </rule>
 </ruleset>
```

Common Policy Post-poned or Rejected

- Capability Discovery
- More sophisticated identity-based authorization techniques
  - P-Asserted ID (RFC 3325)
  - SIP Identity (RFC 4474) / Authenticated Identity Body (RFC 3893)
  - SIP SAML (draft-ietf-sip-saml-00.txt)
  - SIP CERTS (draft-ietf-sip-certs-01.txt)
  - SIP Payment (draft-jennings-sipping-pay-05.txt)
- Trait-based authorization
  (e.g., based on SAML features)
- Rejected in the past: Conditions regarding authentication types, Actions to log and encrypt

Geopriv Policy

- Adds location-based authorization policies to the Common Policy framework
- Conditions:
  - Civic Location Condition
  - Geospatial Location Condition
- Transformations:
  - Retention Transformation
  - Distribution Transformation
  - Keep Rules Transformation
  - Civic Location Transformation
    ('null', 'country', 'region', 'city', 'building', 'full')
  - Geospatial Location Transformation

Geopriv Policy Example (1/2)

```
<cp:rule id="AA56i09">
  <cp:conditions>
    <gp:civic-loc-condition>
      <country>DE</country>
      <A1>Bavaria</A1>
      <A3>Munich</A3>
      <A4>Perlach</A4>
      <A6>Otto-Hahn-Ring</A6>
      <HNO>6</HNO>
    </gp:civic-loc-condition>
  </cp:conditions>
```

```
    <cp:rule id="AA56i09">
      <cp:conditions>
       <gp:geospatial-loc-condition>
         <gp:polygon
           crsName=
                 "urn:ietf:params:xml:ns:geopriv-policy:crs:wgs84">
           <gp:point>
             <gp:lat>38.8986</gp:lat>
             <gp:lon>-77.03724</gp:lon>
           </gp:point>
           <gp:point>
             <gp:lat>38.8986</gp:lat>
             <gp:lon>-77.03722</gp:lon>
           </gp:point>
           <gp:point>
             <gp:lat>38.8987</gp:lat>
             <gp:lon>-77.03722</gp:lon>
           </gp:point>
           <gp:point>
             <gp:lat>38.8987</gp:lat>
             <gp:lon>-77.03724</gp:lon>
           </gp:point>
         </gp:polygon>
      </gp:geospatial-loc-condition>
  </cp:conditions>
```

Geopriv Policy Example (/2)

```
 <cp:actions/>
  <cp:transformations>
     <gp:distribution-transformation>true
     </gp:distribution-transformation>
     <gp:keep-rules-transformation>true
     </gp:keep-rules-transformation>
     <gp:civic-loc-transformation>full
     </gp:civic-loc-transformation>
     <civic-loc-transformation>city
     </civic-loc-transformation>
   </cp:transformations>
</cp:rule>
```

Presence Policy

- Attributes mostly taken from Rich Presence Extensions to the Presence Information Data Format (RPID)
- Conditions
  - Details identity usage for SIP
- Actions
  - Subscription Handling (block, confirm, allow, polite block)
- Transformations
  - Providing Access to Data Component Elements (device, person, service)
  - Providing Access to Presence Attributes
    - Provide Activities (e.g., appointment>, <breakfast>, <dinner>, <holiday>, <lunch>, <meal>, <meeting>, <performance>, <travel>, or <vacation>)
    - Provide Class
    - Provide DeviceID
    - Provide Mood (e.g., happy, angry, etc.)
    - Provide Place-is (e.g., noisy, quiet)
    - Provide Place-type (e.g., bus, ship, ... RFC 4589)
    - Provide Privacy (e.g., audio, text, video)
    - Provide Relationship (e.g., family, friend)
    - Provide Sphere
    - Provide Status-Icon
    - Provide Time-Offset
    - Provide User-Input (e.g., idle)
    - Provide Note
    - Provide Unknown Attribute
    - Provide All Attributes

Presence Policy Example

```
<?xml version="1.0" encoding="UTF-8"?>
  <cr:ruleset xmlns="urn:ietf:params:xml:ns:pres-rules"
   xmlns:pr="urn:ietf:parmas:xml:ns:pres-rules"
   xmlns:cr="urn:ietf:params:xml:ns:common-policy">
   <cr:rule id="a">
    <cr:conditions>
     <cr:identity>
      <cr:one id="sip:user@example.com"/>
     </cr:identity>
    </cr:conditions>
    <cr:actions>
     <pr:sub-handling>allow</pr:sub-handling>
    </cr:actions>
    <cr:transformations>
     <pr:provide-services>
       <pr:service-uri-scheme>sip</pr:service-uri-scheme>
       <pr:service-uri-scheme>mailto</pr:service-uri-scheme>
     </pr:provide-services>
     <pr:provide-persons>
       <pr:all-persons/>
     </pr:provide-persons>
     <pr:provide-activities>true</pr:provide-activities>
     <pr:provide-user-input>bare</pr:provide-user-input>
      <pr:provide-unknown-attribute
       ns="urn:vendor-specific:foo-namespace"
       name="foo">true</pr:provide-unknown-attribute>
    </cr:transformations>
   </cr:rule>
  </cr:ruleset>
```

Relevant IETF Work

- Creating, Modifying and Deleting XML Documents:
  - XCAP / WebDav
    http://www.jdrosen.net/papers/xcap-tutorial.ppt
- Presence Server Performance
  - Partial Notifications / Event Throttling / Event Filters
- Session (dependent/independent) policies
- Mechanisms to obtain location information
- Discovering features of a Presence/Location Server
- Refinement of location formats

Summary

- Keep it simple
- Reuse existing work (e.g., SIP, GML)
- (Location) privacy is an architectural problem and rarely needs cryptography as a solution

> “If you think cryptography is the solution to your problem, you don’t know what your problem is.”
>
> --- Roger Needham

References

- **Geographic Location/Privacy (GEOPRIV) WG**
  - http://www.ietf.org/html.charters/geopriv-charter.html
- **SIP for Instant Messaging and Presence Leveraging Extensions (SIMPLE) WG**
  - http://www.ietf.org/html.charters/simple-charter.html
- **Session Initiation Protocol (SIP) WG**
  - http://www.ietf.org/html.charters/sip-charter.html
- **GMLv3**
  - http://www.opengis.net & http://schemas.opengis.net/gml/3.0.0/base/
  - http://www.opengeospatial.org/

Backup Slides

Privacy Concerns

- Location
  - Many entities know your location today
  - In many cases, you do not control the systems that determine your location
  - Examples:
    - NetGeo database (see RFC 1876)
    - Skymo (see http://www.skymo.com)
- In many cases, location is only one data element in the larger presence context.
- Distribution of these other attributes also deserves privacy protection.

Conflict Resolution

Combining Permissions

- Alice provided a few policy rules for access to her location information:

Conditions					Actions/Transformations		
Id	WR-ID	sphere	from	to	X	Y	Z
1	bob	home	A1	A2	TRUE	10	o
2	alice	work	A1	A2	FALSE	5	+
3	bob	work	A1	A2	TRUE	3	-
4	tom	work	A1	A2	TRUE	5	+
5	bob	work	A1	A3	undef	12	o
6	bob	work	B1	B2	FALSE	10	-

- Bob asks for location information (between A1 and A2).

Combining Permissions

Conditions					Actions/Transformations		
Id	WR-ID	sphere	from	to	X	Y	Z
1	bob	home	A1	A2	TRUE	10	o
2	alice	work	A1	A2	FALSE	5	+
3	**bob**	**work**	**A1**	**A2**	**TRUE**	**3**	**-**
4	tom	work	A1	A2	TRUE	5	+
5	**bob**	**work**	**A1**	**A3**	**undef**	**12**	**o**
6	bob	work	B1	B2	FALSE	10	-

Firing rules

Actions/Transformations

X	Y	Z
TRUE	3	-
undef	12	o

Combining Permissions Algorithm →

Actions/Transformations

X	Y	Z
TRUE	12	-

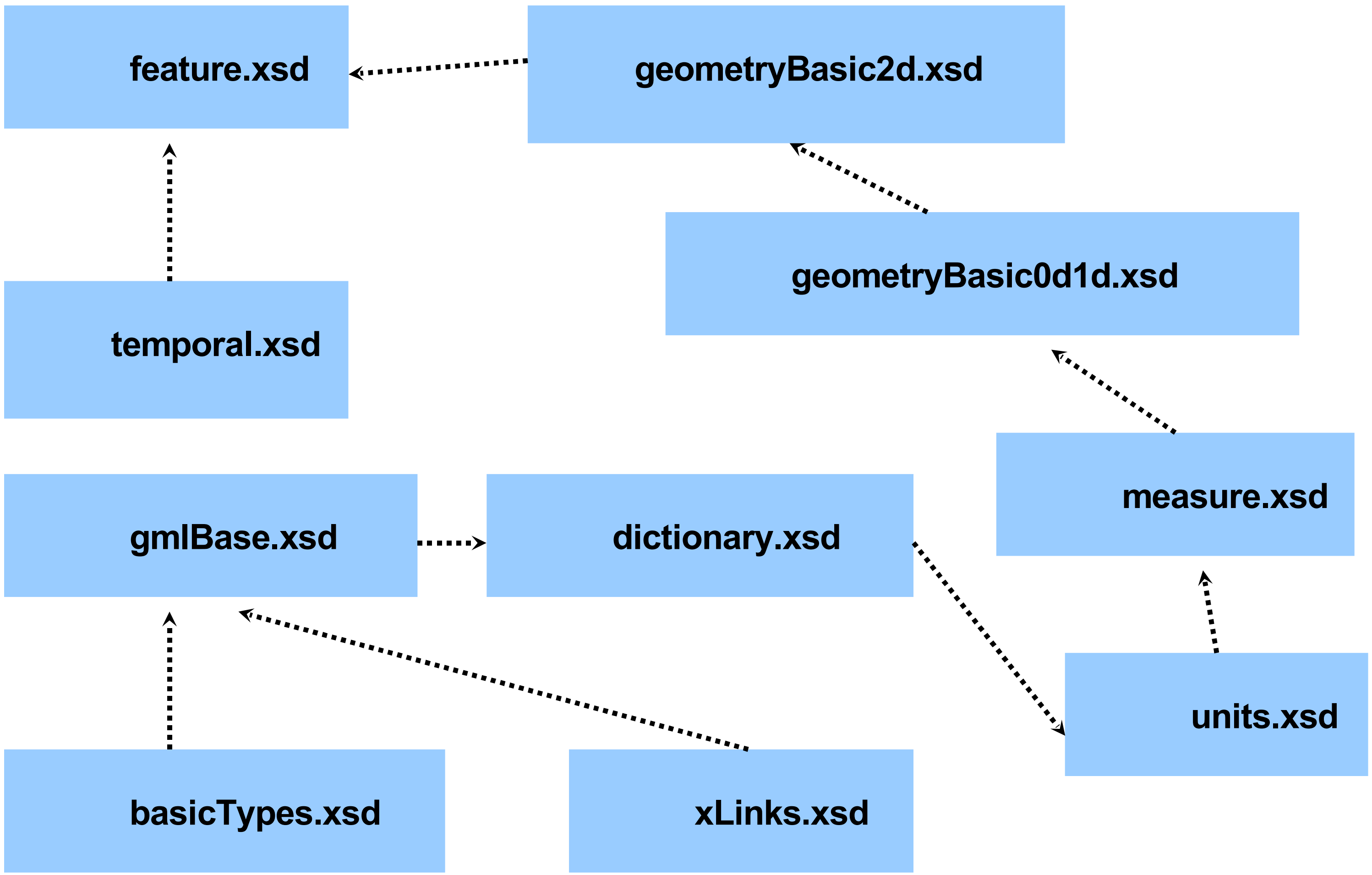
Combining Rules (CR)

- data types of permissions to be combined = Boolean or Undef:
  - if there is one value = true: CV = true
  - otherwise: CV = false
- data types of permissions to be combined = Integer or Undef:
  - if all permission values = undef: CV not specified (bad!)
  - otherwise: CV = max {single values}
- data types of permissions to be combined = Set or Undef:
  - CV = intersection of all single values not equal undef

(CR = Combining Rule, CV = Combined Value)

GML

Feature.xsd Dependency



Geometry

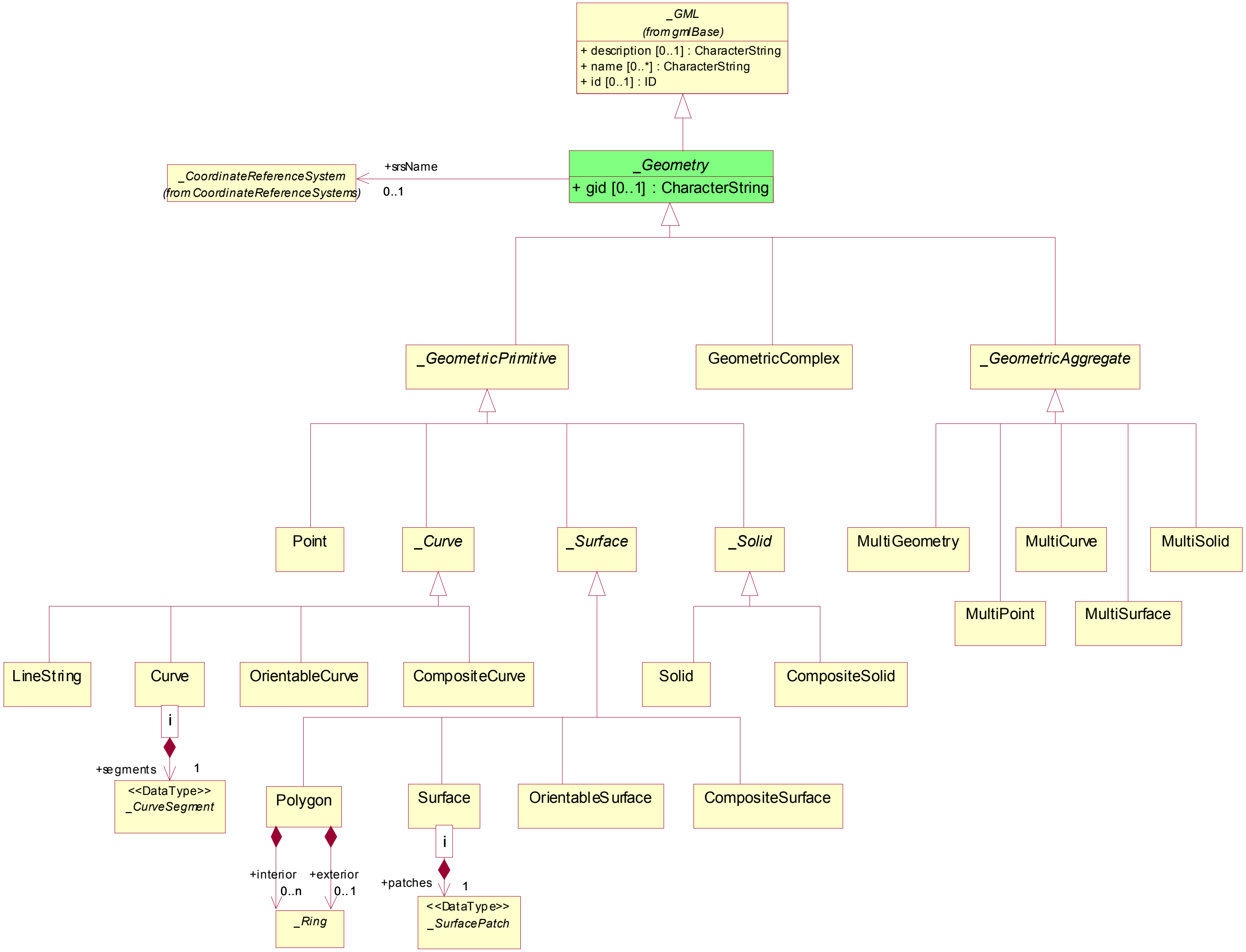
The geometry model of GML is identical to ISO DIS 19107, which is described in following schemas:

- geometryBasic0d1d.xsd
- geometryBasic2d.xsd
- geometryPrimitives.xsd
- geometryAggregates.xsd
- geometryComplexes.xsd

Geometry

General concepts Coordinate Geometry Simple Geometric Primitives (0- and 1-dimensional)	geometryBasic0d1d.xsd
Simple Geometric Primitives (2-dimensional)	geometryBasic2d.xsd
More Geometric Primitives (1-, 2- and 3-dimensional)	geometryPrimitives.xsd
Geometric Complex and geometric composites	geometryComplexes.xsd
Geometric Aggregates	geometryAggregates.xsd
Geometric Properties	n/a
User-defined Geometry Types and Geometry Property Types	n/a

Geometry

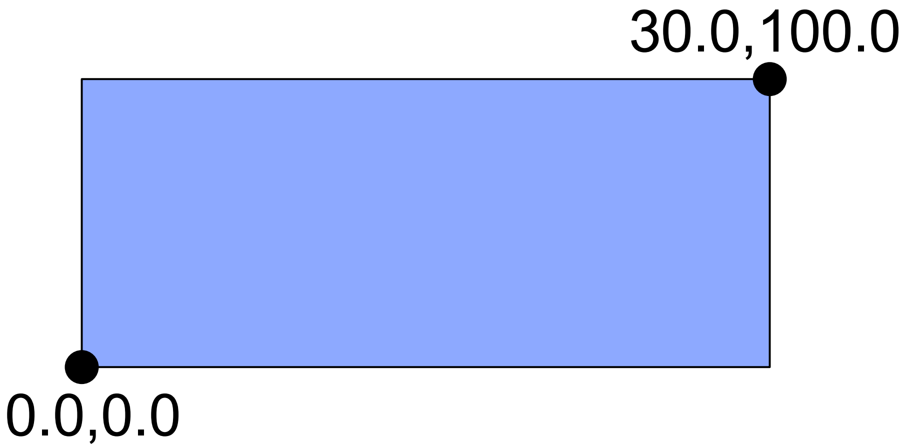

_GML
(from gmlBase)
+ description [0..1] : CharacterString
+ name [0..*] : CharacterString
+ id [0..1] : ID
_Geometry
+ gid [0..1] : CharacterString
_CoordinateReferenceSystem
(from CoordinateReferenceSystems)
+srsName
0..1
_GeometricPrimitive
GeometricComplex
_GeometricAggregate
Point
_Curve
_Surface
_Solid
MultiGeometry
MultiCurve
MultiSolid
MultiPoint
MultiSurface
LineString
Curve
OrientableCurve
CompositeCurve
Solid
CompositeSolid
i
+segments
1
<<DataType>>
_CurveSegment
Polygon
Surface
OrientableSurface
CompositeSurface
+interior
0..n
+exterior
0..1
_Ring
i
+patches
1
<<DataType>>
_SurfacePatch

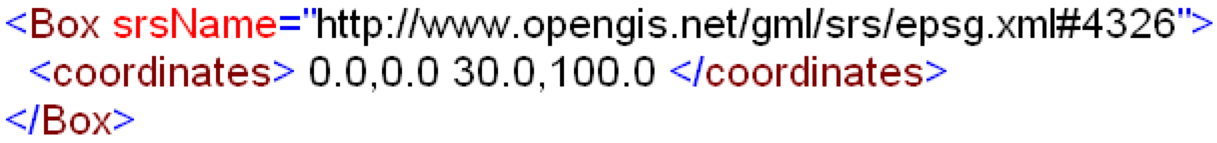
Geometry

Geometry Classes in Geometry

- Box
- Point
- LineString
- LinearRing
- Polygon
- Multigeometry (combination of primitive geometry elements)

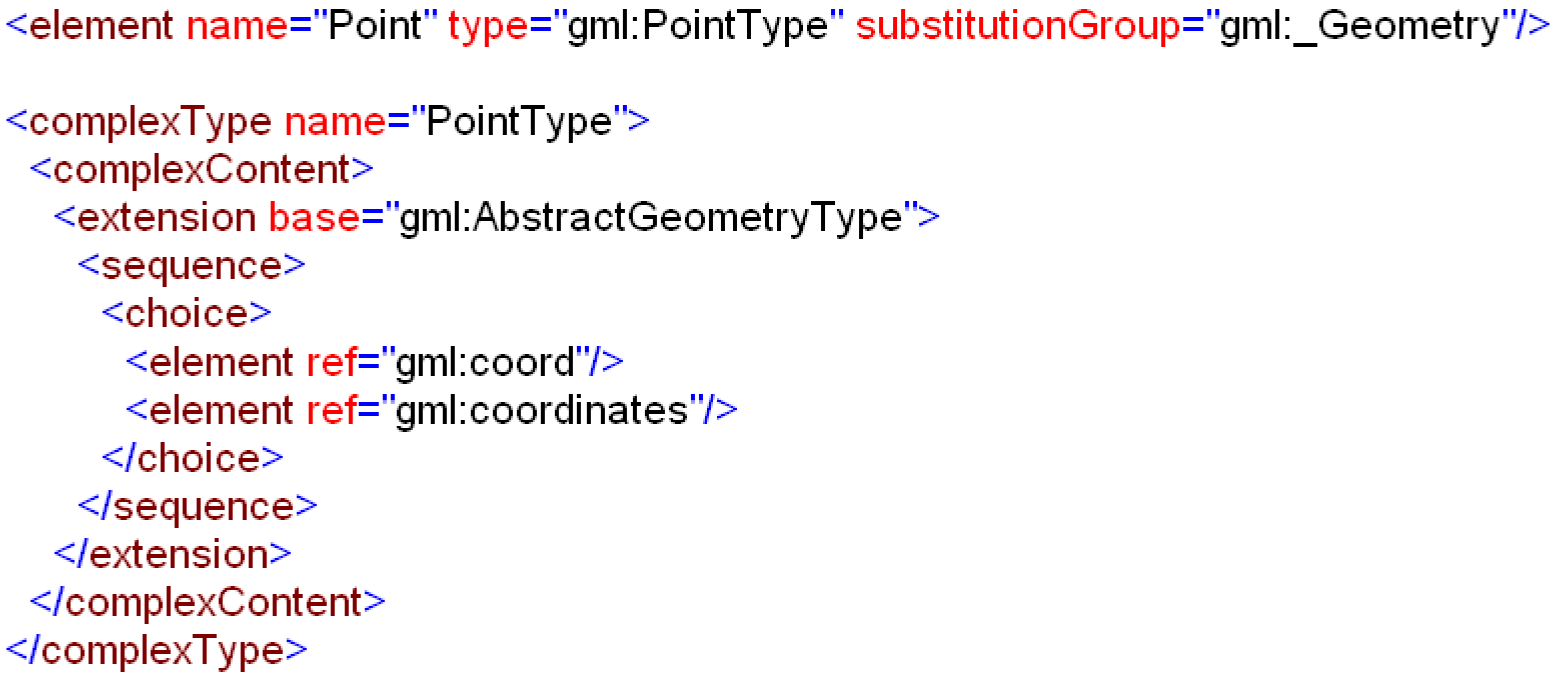
Box in Geometry




```
<Box srsName="http://www.opengis.net/gml/srs/epsg.xml#4326">
  <coordinates> 0.0,0.0 30.0,100.0 </coordinates>
</Box>
```

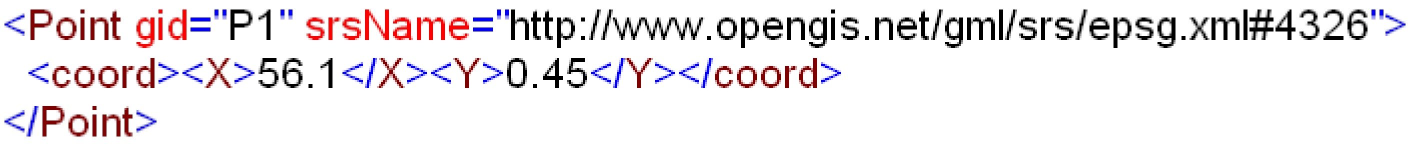
Point in Geometry

Point consists of a coordinate tuple:



```
<element name="Point" type="gml:PointType" substitutionGroup="gml:_Geometry"/>

<complexType name="PointType">
 <complexContent>
  <extension base="gml:AbstractGeometryType">
   <sequence>
    <choice>
     <element ref="gml:coord"/>
     <element ref="gml:coordinates"/>
    </choice>
   </sequence>
  </extension>
 </complexContent>
</complexType>
```

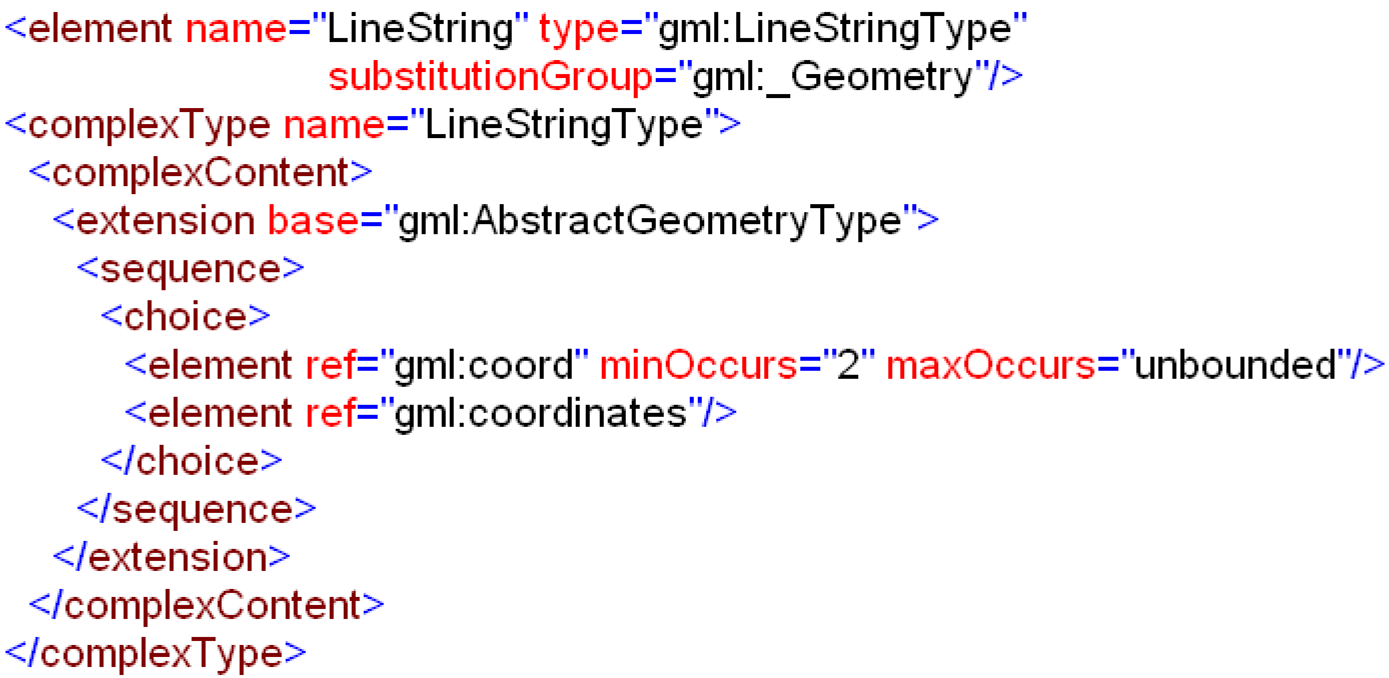
Example:



```
<Point gid="P1" srsName="http://www.opengis.net/gml/srs/epsg.xml#4326">
 <coord><X>56.1</X><Y>0.45</Y></coord>
</Point>
```

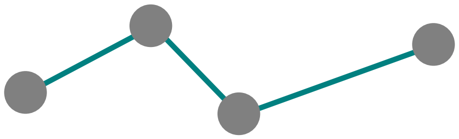
LineString in Geometry

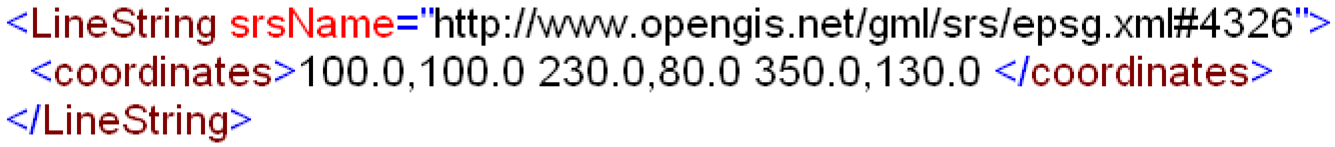
Definition:



```
<element name="LineString" type="gml:LineStringType"
                              substitutionGroup="gml:_Geometry"/>
<complexType name="LineStringType">
  <complexContent>
    <extension base="gml:AbstractGeometryType">
      <sequence>
        <choice>
          <element ref="gml:coord" minOccurs="2" maxOccurs="unbounded"/>
          <element ref="gml:coordinates"/>
        </choice>
      </sequence>
    </extension>
  </complexContent>
</complexType>
```

Example:

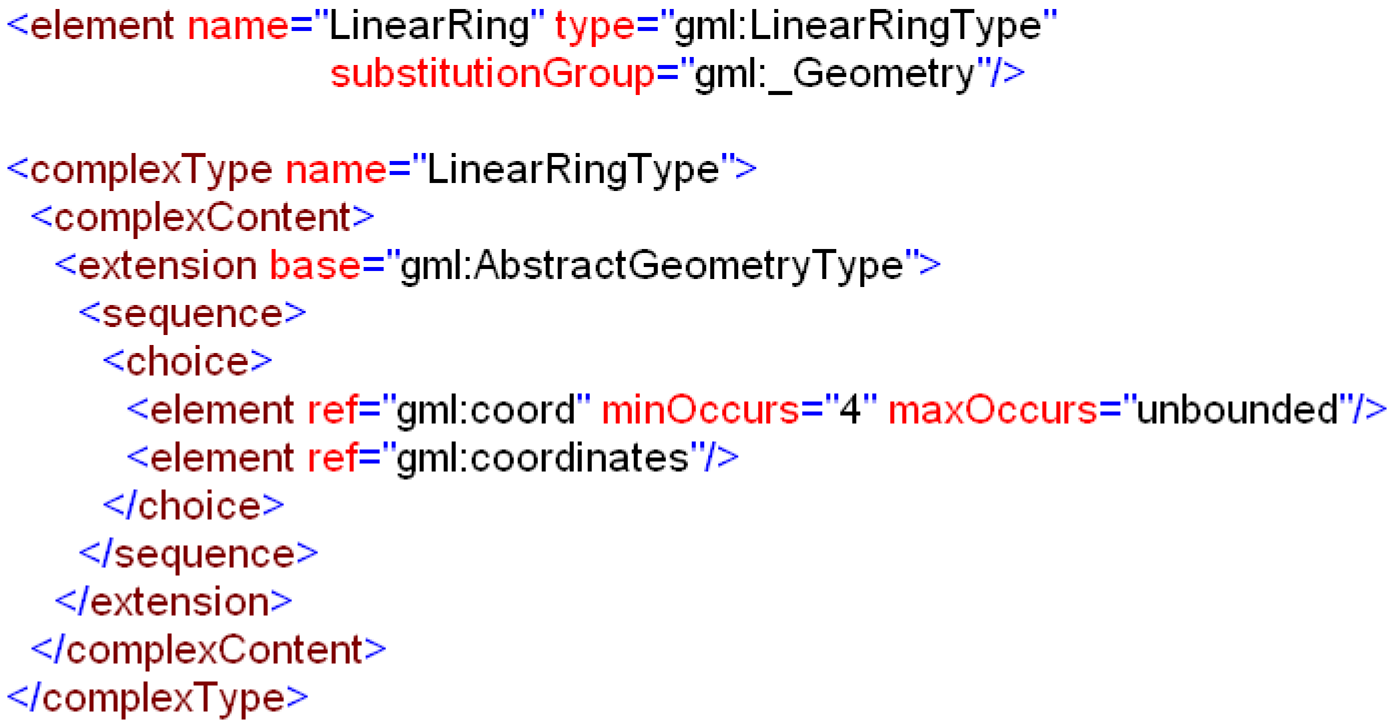




```
<LineString srsName="http://www.opengis.net/gml/srs/epsg.xml#4326">
  <coordinates>100.0,100.0 230.0,80.0 350.0,130.0 </coordinates>
</LineString>
```

LinearRing in Geometry

Definition:



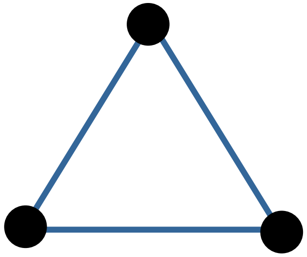
```
<element name="LinearRing" type="gml:LinearRingType"
                            substitutionGroup="gml:_Geometry"/>

<complexType name="LinearRingType">
  <complexContent>
    <extension base="gml:AbstractGeometryType">
      <sequence>
        <choice>
          <element ref="gml:coord" minOccurs="4" maxOccurs="unbounded"/>
          <element ref="gml:coordinates"/>
        </choice>
      </sequence>
    </extension>
  </complexContent>
</complexType>
```

LinearRing in Geometry

Beispiel:

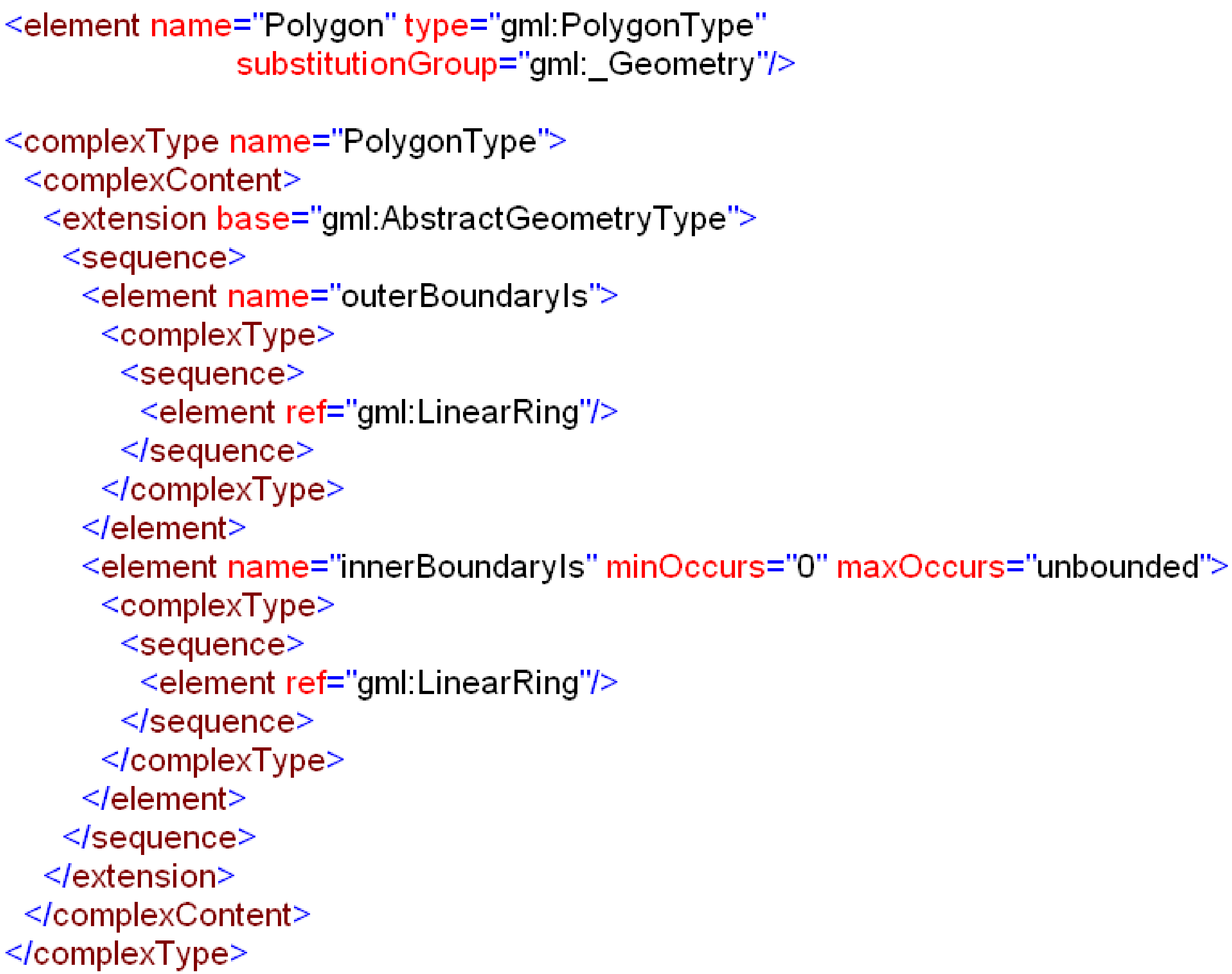
```
<LinearRing srsName="http://www.opengis.net/gml/srs/epsg.xml#4326">
 <coordinates>
   100.0,100.0
   230.0,80.0
   350.0,130.0
   100.0,100.0
 </coordinates>
</LinearRing>
```

Both point should be equal



Polygon in Geometry

Definition:

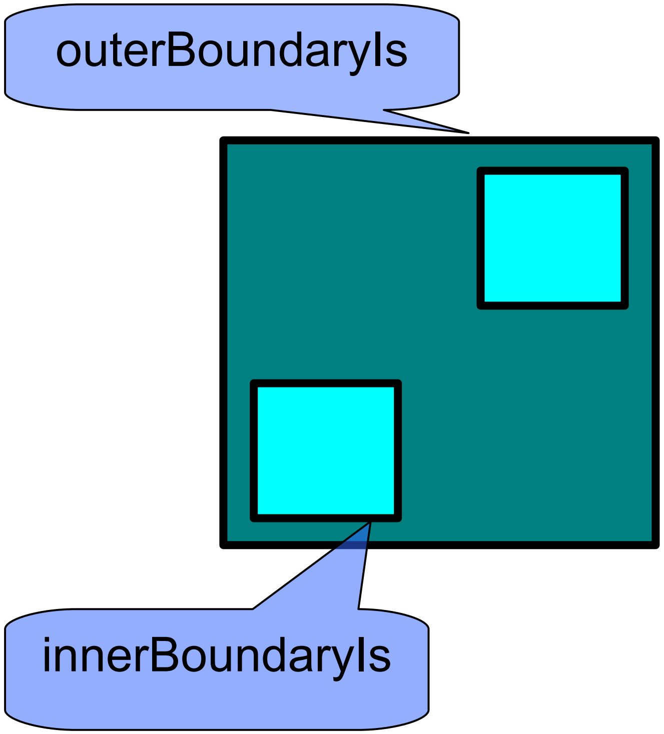


```
<element name="Polygon" type="gml:PolygonType"
            substitutionGroup="gml:_Geometry"/>

<complexType name="PolygonType">
 <complexContent>
  <extension base="gml:AbstractGeometryType">
   <sequence>
    <element name="outerBoundaryIs">
     <complexType>
      <sequence>
       <element ref="gml:LinearRing"/>
      </sequence>
     </complexType>
    </element>
    <element name="innerBoundaryIs" minOccurs="0" maxOccurs="unbounded">
     <complexType>
      <sequence>
       <element ref="gml:LinearRing"/>
      </sequence>
     </complexType>
    </element>
   </sequence>
  </extension>
 </complexContent>
</complexType>
```

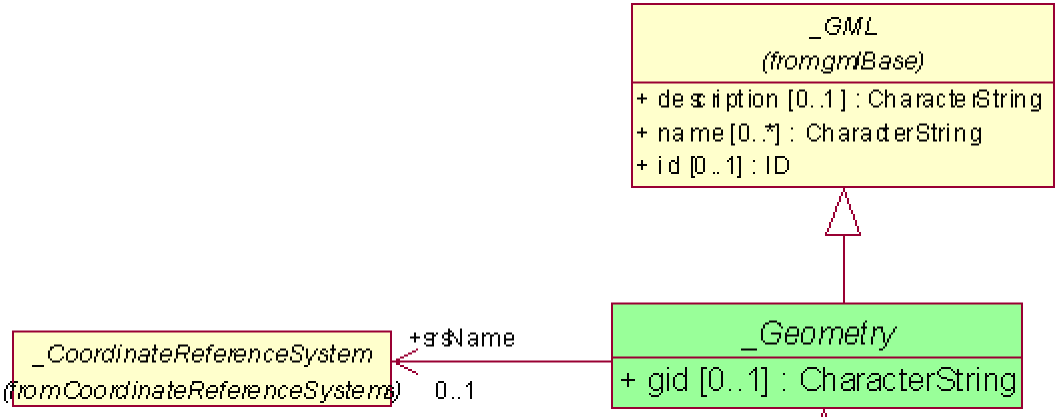
Polygon in Geometry

Example:

```
<Polygon gid="_98217" srsName="http://www.opengis.net/gml/srs/epsg.xml#4326">
 <outerBoundaryIs>
  <LinearRing>
   <coordinates>
    0.0,0.0 100.0,0.0 100.0,100.0 0.0,100.0 0.0,0.0
   </coordinates>
  </LinearRing>
 </outerBoundaryIs>
 <innerBoundaryIs>
  <LinearRing>
   <coordinates>
    10.0,10.0 10.0,40.0 40.0,40.0 40.0,10.0 10.0,10.0
   </coordinates>
  </LinearRing>
 </innerBoundaryIs>
 <innerBoundaryIs>
  <LinearRing>
   <coordinates>
    60.0,60.0 60.0,90.0 90.0,90.0 90.0,60.0 60.0,60.0
   </coordinates>
  </LinearRing>
 </innerBoundaryIs>
</Polygon>
```

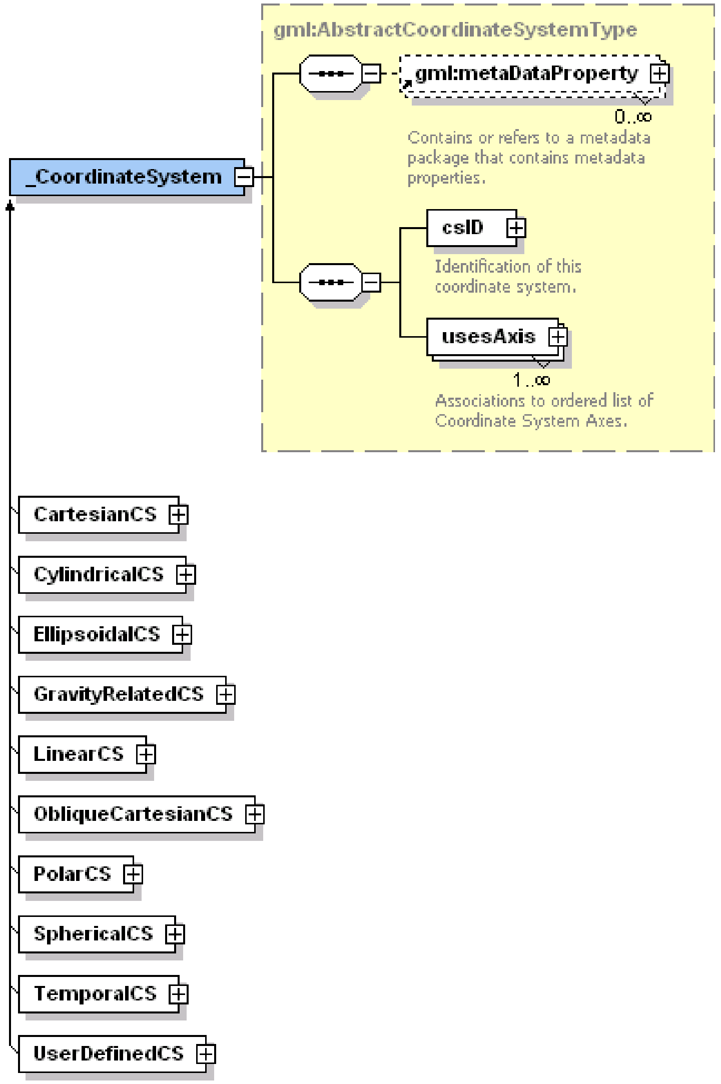


Coordinate Reference Systems (CRS)


_GML
(fromgmlBase)
+ description [0..1] : CharacterString
+ name [0..*] : CharacterString
+ id [0..1] : ID
_CoordinateReferenceSystem
(fromCoordinateReferenceSystems)
+srsName
0..1
_Geometry
+ gid [0..1] : CharacterString

GML requires a coordinate reference system (CRS) to be referenced whenever location coordinate information is given. This CRS provides the meaning for location coordinates. The referencing is generally given using the srsName attribute

Coordinate Reference Systems (CRS)

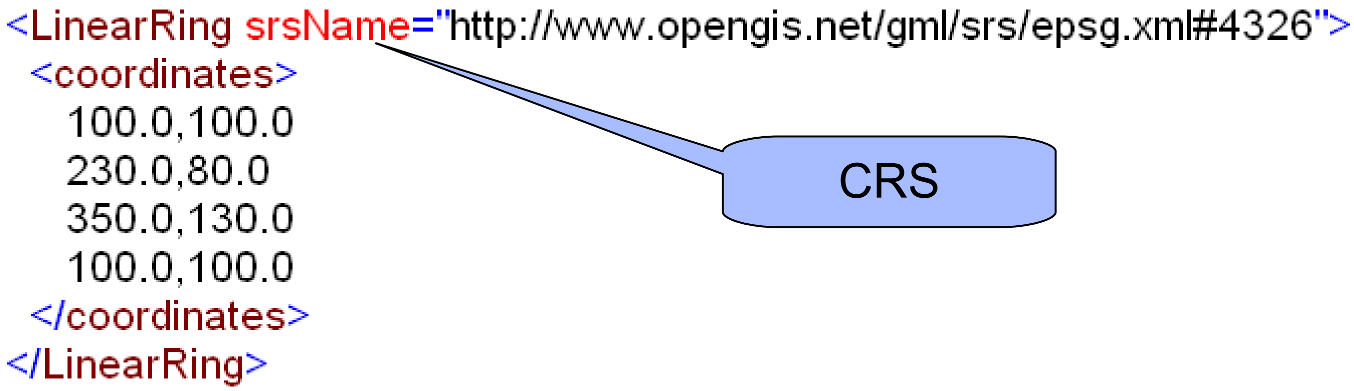

gml:AbstractCoordinateSystemType
gml:metaDataProperty
0..∞
Contains or refers to a metadata package that contains metadata properties.
_CoordinateSystem
csID
Identification of this coordinate system.
usesAxis
1..∞
Associations to ordered list of Coordinate System Axes.
CartesianCS
CylindricalCS
EllipsoidalCS
GravityRelatedCS
LinearCS
ObliqueCartesianCS
PolarCS
SphericalCS
TemporalCS
UserDefinedCS

There is a set of six XML schema documents for encoding CRS definitions.

- coordinateReferenceSystems.xsd
- datums.xsd
- coordinateSystems.xsd
- coordinateOperations.xsd
- dataQuality.xsd
- referenceSystems.xsd

Coordinate Reference Systems (CRS)

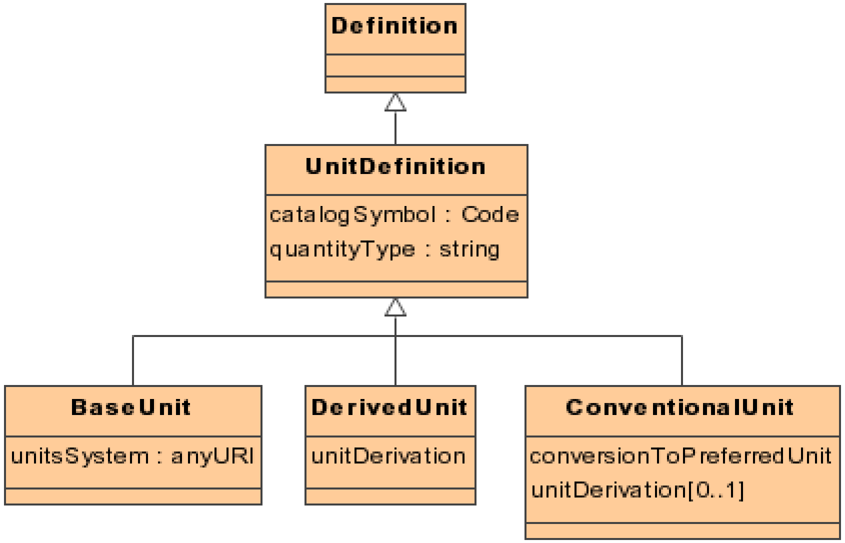
Beispiel:



```
<LinearRing srsName="http://www.opengis.net/gml/srs/epsg.xml#4326">
  <coordinates>
    100.0,100.0
    230.0,80.0
    350.0,130.0
    100.0,100.0
  </coordinates>
</LinearRing>
```

CRS

Units, Measures



- The schema units.xsd defines components to support the definition of units of measure.
- Base Units are the preferred units for a set of orthogonal fundamental quantities which define the particular system of units, which may not be derived by combination of other base units.
- Derived Units are the preferred units for other quantities in the system, which may be defined by algebraic combination of the base units.
- specific measure types are defined in measures.xsd

Example of GML 3.0

```
<gml:location>
  <gml:Point
       gml:id="point96“
       srsName="epsg:4326">
       <gml:coordinates>31:56:00S 115:50:00E
       </gml:coordinates>
  </gml:Point>
</gml:location>
```

Civic Location Example (non-GML based)

```
<gp:location-info>
  <cl:civilAddress>
    <cl:country>US</cl:country>
    <cl:A1>New York</cl:A1>
    <cl:A3>New York</cl:A3>
    <cl:A6>Broadway</cl:A6>
    <cl:HNO>123</cl:HNO>
    <cl:LOC>Suite 75</cl:LOC>
    <cl:PC>10027-0401</cl:PC>
  </cl:civilAddress>
</gp:location-info>
```