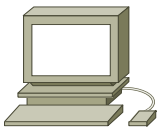
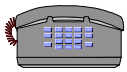
SIP for Presence and Instant Messaging

A Role for Presence in "VoIP"

Awareness of other users: availability, location, …

- To perform existing functions
  - User location, call routing, follow-me, ...
- To improve existing services
  - Call completion ratio
  - Indicate availability
- To enable new services
  - Presence per se: Simplify meeting people
  - Messaging per se: "SMS"
  - Presence and Messaging as basis for other applications
  - Location-based services
  - New inter-personal communication paradigms
- To provide another differentiator from traditional telephony

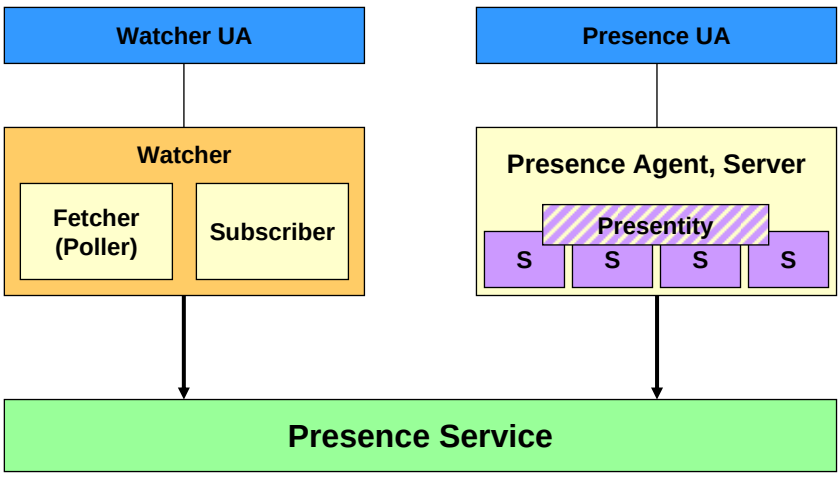




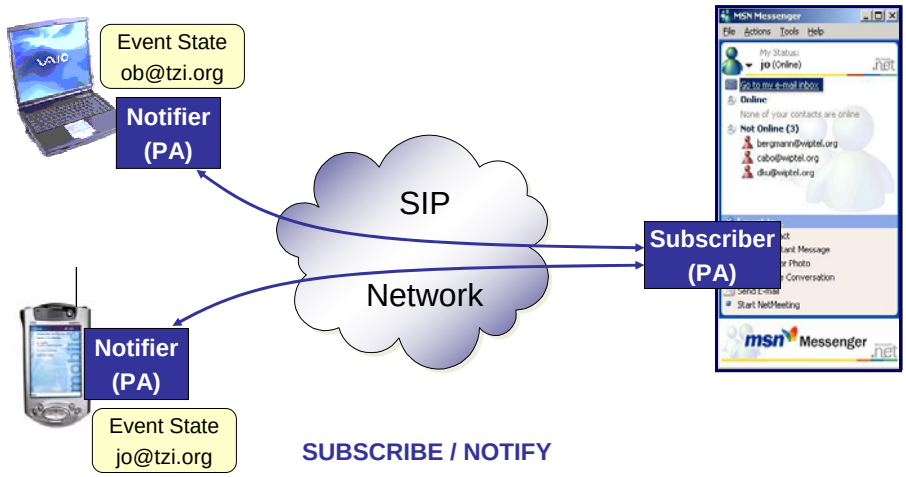
SIP: Personal Presence and Instant Messaging

- "Buddy Lists + Chat"
- Idea: re-use SIP infrastructure
  - Maintain user locations
  - Route messages
  - Contact users
- SIP Event package for "presence"
  - SUBSCRIBE / NOTIFY fit well
  - Define presence formats
- Define a new method for Instant Messaging
  - MESSAGE
  - MSRP for messaging sessions
  - Define basic message content format (text/plain)

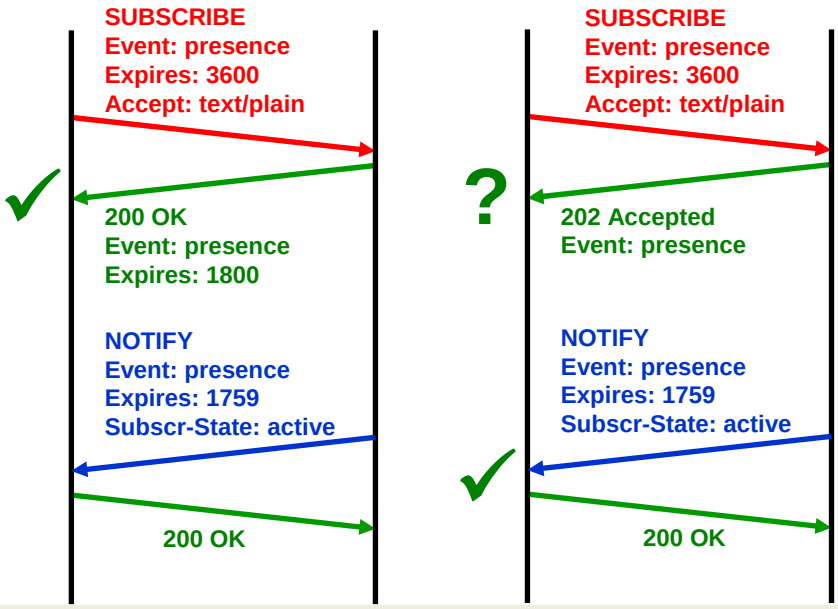
IMPP Presence Model



SIP Entities for Presence (1)



Example: SIP for Presence



SIP Presence Notification (PIDF)

```
<presence ... entity="pres:jo@tzi.org">
  <tuple id="mobile-im">
    <status>
      <basic>open</basic>
    </status>
    <contact priority="0.8">im:jo@sms-gw.tzi.org</contact>
    <note xml:lang="en">Don't Disturb Please!</note>
    <note xml:lang="fr">Ne dérangez pas, s'il vous plaît</note>
    <timestamp>2006-02-23T10:49:29Z</timestamp>
  </tuple>
  <tuple id="interactive-mm">
    <status>
      <basic>closed</basic>
    </status>
    <contact priority="1.0">sip:jo@tzi.org</contact>
  </tuple>
  <note>I am in Paris this week</note>
</presence>
```


Rich Presence Information Data Format (RPID)

- Introduces additional (more descriptive) elements
  - Ideally to be derived automatically from user activity
  - Describe a tuple, a person, or a device
  - May be grouped according to a class element
- Extension for a person
  - activities away, appointment, busy, travel, steering, vacation, ...
  - mood afraid, angry, annoyed, distracted, happy, impressed, thirsty, …
  - place-type aircraft, bus, car, home, hotel, office, outdoors, public, quiet, …
  - sphere work, home
  - status-icon convey a URI pointing to an image
  - timezone
- Extensions for tuple, device
  - user-input active, idle (idle since)
- Extensions for a tuple
  - privacy, relationship, service-type, status-icon

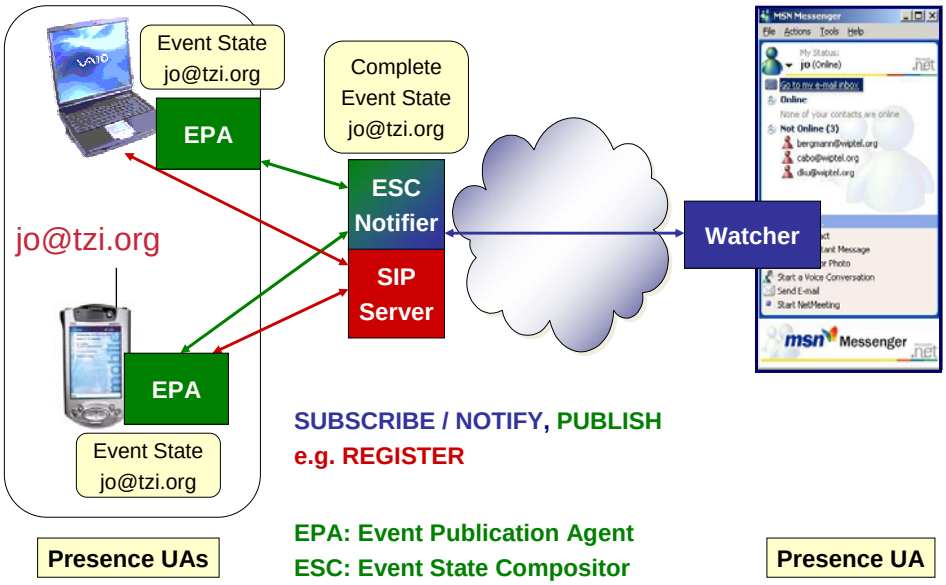
Further Presence Format Extensions

- User Agent capabilities
  - Add further hints to a contact beyond contact means (protocol) and address
  - Set of attributes also available from the caller preferences and callee capabilities framework
- Contact information
  - Display name and business card
  - Pointer to home page
  - Sound + icon
- Timed presence information
  - Specify information about time periods (past, future)
  - E.g., as derived from a calendar entry

Learning Presence State

- Co-location
  - Presence agent (PA) co-located with the presence user agent (PUA)
- REGISTER
  - SIP UAs (de)registering for a certain AoR contribute presence state
  - Presence server may derive information from co-location w/ registrar
  - Alternative: registration event package
    - A presence server may subscribe to an AoR at a registrar
    - Registrar provides change notifications: application/reginfo+xml
    - Per AoR per contact: identification, registration state, last event, params\
- Uploading presence documents
  - Explicit provisioning from a PUA

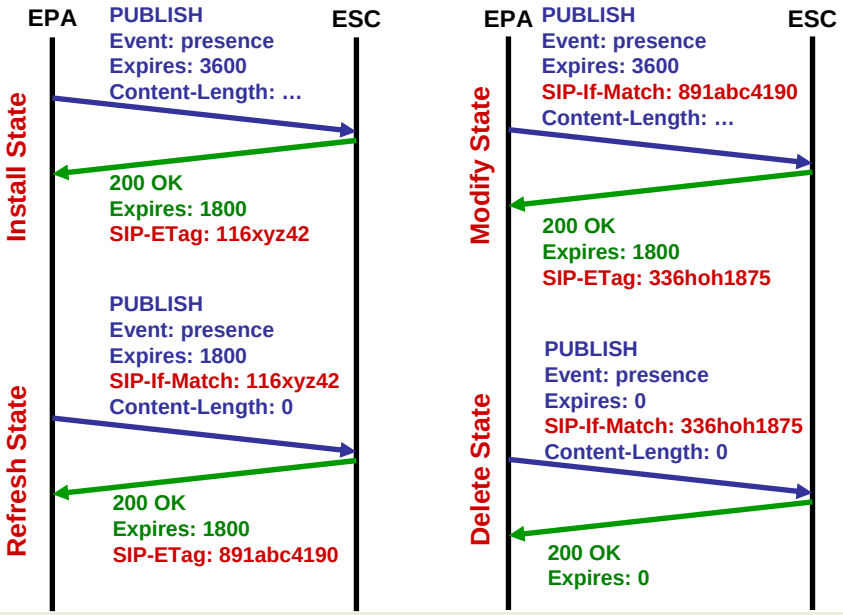
SIP Entities for Presence (2)



SUBSCRIBE / NOTIFY, PUBLISH
e.g. REGISTER

EPA: Event Publication Agent
ESC: Event State Compositor

Example: PUBLISHing State



Excursion

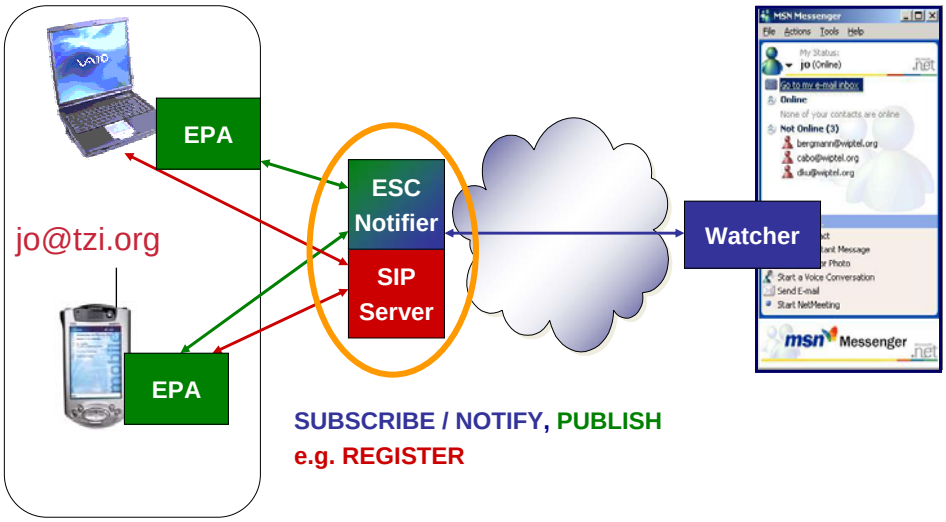
Important Issue:
Privacy of Presence Information

GEOPRIV: Focus on geographic location data

Specific Threats to a Location Based System

- Who is in control?
  - Smart devices: authorized access only
  - Substrates: external control
  - Third-party services: users cannot control access!
    (e.g. cell phone company)
- Tracking applications
  - The good: friend-finder, emergency services
  - The ugly: your employer's time tracking system
  - The bad: profiling for commercial reasons (health insurance, …),
    and criminal intent (e.g. surveillance)
- SPLOC (Spam over LBS)
  - Unsolicited business advertisements
- Attacks
  - Eavesdropping, forging identity, replay, DoS, …

Aggregation of Presence & Location Information



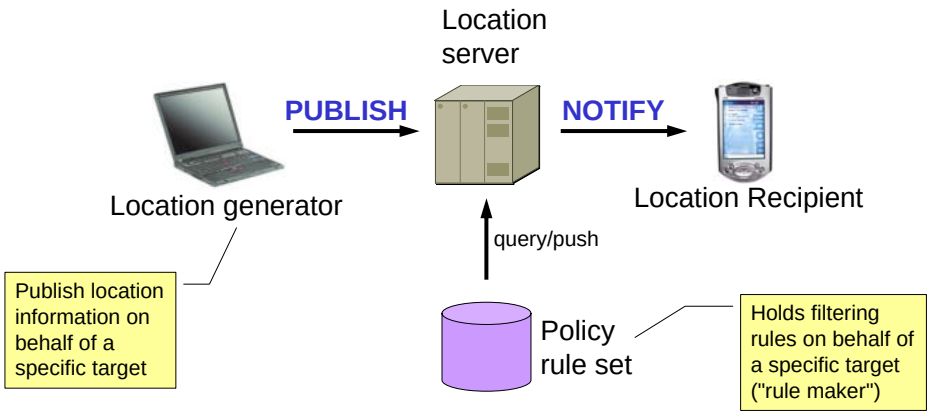
SUBSCRIBE / NOTIFY, PUBLISH
e.g. REGISTER

EPA: Event Publication Agent
ESC: Event State Compositor

Presence UAs

Presence UA

Retrieving Location Info in GEOPRIV



Publish location information on behalf of a specific target

Holds filtering rules on behalf of a specific target ("rule maker")

GEOPRIV: No Geo-Information without Privacy

- Location information is sensitive data in almost any application
  - Tracking movements, profile creation, relate with other persons' locations …
  - Equipment in use (apparently)
  - Emergency situations
- Problem: many applications rely on sensitive information (e.g., emergency handling, follow-me services)
- GEOPRIV
  - Location model (protocol-agnostic)
    - PIDF extension (PIDF-LO)
    - Re-use OpenGIS GML syntax
  - Rules, Policies
  - Leverage usage in existing presence protocols (esp. SIP)

GEOPRIV: Components

- Location information
  - Raw (pre-configuration databases, generated by sensors, …)
  - Computed (from multiple sensors, personal presence status, …)
- Data model (Location Objects)
  - Location information
    - Civil addresses, geo-coordinates, place type (e.g., at SIP tutorial)
  - Owner (identity)
  - Privacy rules
- Policies
  - Declaring presence processing rules formally
  - Identity of users
  - Concept of filtering and transformation
  - Designed for simplicity to ease conflict resolution

PIDF-LO Example Document

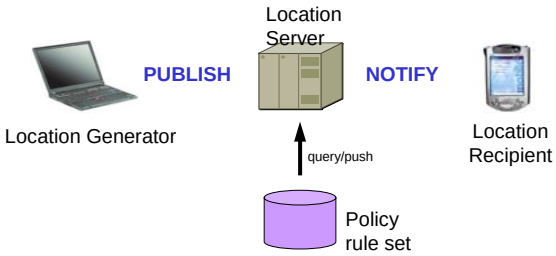
```
<presence entity="pres:dku@tzi.org" xmlns="urn:ietf:params:xml:ns:pidf"
  xmlns:gp="urn:ietf:params:xml:ns:pidf:geopriv10"
  xmlns:gml="urn:opengis:specification:gml:schema-xsd:feature:v3.0">
  <tuple id="xyz">
    <status>
      <gp:geopriv>
        <gp:location-info>
          <gml:Point …>
            <gml:coordinates> … </gml:coordinates>
          </gml:Point>
        </gp:location-info>
        <gp:usage-rules>
          <gp:retransmission-allowed>no</gp:retransmission-allowed>
          <gp:retention-expiry>2006-01-20T10:00:00Z</gp:retention-expiry>
          <gp:ruleset-reference
               >https://example.org/rset.xml</gp:ruleset-reference>
        </gp:usage-rules>
      </gp:geopriv>
    </status>
```


Civic Locations in PIDF-LO

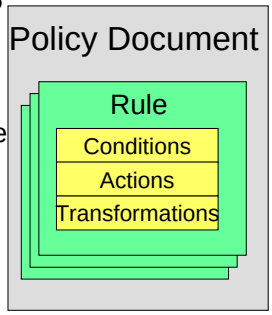
```
<presence …
          xmlns:cl=" urn:ietf:params:xml:ns:pidf:geopriv10:civicLoc">

            .
            .
            .

        <gp:location-info>
          <cl:civicAddress>
            <cl:country>FI</cl:country>
            <cl:A1>Espoo</cl:A1>
            <cl:A3>Espoo</cl:A3>
            <cl:A6>Otakaari</cl:A6>
            <cl:HNO>5A</cl:HNO>
            <cl:LOC>SE 324</cl:LOC>
            <cl:FLR>3</cl:FLR>
            <cl:NAM>Laboratory</cl:NAM>
          </cl:civicAddress>
        </gp:location-info>
```

GEOPRIV Policies

- Framework for authorization policies
  - General framework
  - Adaptation to LBS applications
- General idea
  - Control distribution of and access to personal information by explicit rules
  - Leverage GEOPRIV framework

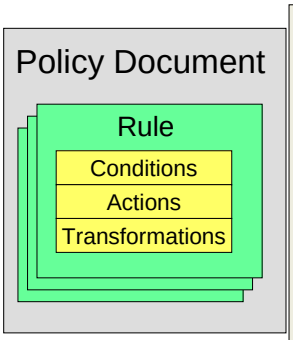


GEOPRIV Policy Rules



- Conditions
  - Expressions that evaluate to TRUE or FALSE
  - All conditions must evaluate to TRUE for a rule to become active
  - Some sample conditions:
    - Matching identities (URI-based)
    - Matching spheres
      (matching abstract presence state: “at home”, “at work” etc.)
    - Validity: specify timeframe, when this rule is valid
- Actions and transformations (“permissions”)
  - Specify how to handle a request
  - Formulate positive permissions
    (what the system is allowed to do)

Sample Condition (1)




```
<ruleset xmlns="urn:ietf:params:xml:ns:common-policy">

      <rule id="f3g44r1">
          <conditions>
              <identity>
                  <one id="alice@example.com"/>
                  <one id="+1-212-555-1234" scheme="tel"/>
                  <one id="bob@example.net" scheme="sip mailto xmpp"/>
              </identity>
          </conditions>
          <actions/>
          <transformations/>
      </rule>
</ruleset>
```


Condition Processing Semantics

AND

OR

OR

```
<ruleset xmlns="urn:ietf:params:xml:ns:common-policy">

      <rule id="f3g44r1">
          <conditions>
              <sphere value="home"/>
              <identity>
                  <one id="alice@example.com"/>
                  <one id="+1-212-555-1234" scheme="tel"/>
                  <one id="bob@example.net" scheme="sip mailto xmpp"/>
              </identity>
              <validity>
                  <from>2006-01-16T17:00:00+01:00</from>
                  <until>2006-01-17T17:00:00+01:00</until>
              </validity>
          </conditions>
          <actions/>
          <transformations/>
      </rule>
</ruleset>
```

Transformation Rules

- Distribution transformation
  - Specify whether a LO may be distributed

```
<gp:distribution-transformation> true
</gp:distribution-transformation>
```

- Retention transformation
  - Specify for how long the LS may keep the LO

```
<gp:retention-transformation> 3600
</gp:retention-transformation>
```

- Keep rules transformation
  - Specify whether the LS may keep all authorization policy rules in the LO when delivering the LO to recipients

```
<gp:keep-rules-transformation> false
</gp:keep-rules-transformation>
```

- Civic location transformation
  - Restrict the level of civic location information

```
<gp:civic-loc-transformation> city
</gp:civic-loc-transformation>
```

- Geospatial location transformation
  - Restrict resolution of geospatioal information

```
<gp:geospatial-loc-transformation>
  <gp:lat-resolution>0.2
  </gp:lat-resolution>
  <gp:lon-resolution>0.1
  </gp:lon-resolution>
</gp:geospatial-loc-transformation>
```


Sample Policy

```
<cp:ruleset
      xmlns:cp="urn:ietf:params:xml:ns:common-policy"
      xmlns:gp="urn:ietf:params:xml:ns:geopriv-policy"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

      <cp:rule id="AA56i09">
          <cp:conditions>

              <cp:validity>
                  <cp:from>2004-11-01T00:00:00+01:00</cp:from>
                  <cp:until>2005-11-01T00:00:00+01:00</cp:until>
              </cp:validity>

              <gp:civic-loc-condition>
                  <gp:country>DE</gp:country>
                  <gp:A1>Bavaria</gp:A1>
                  <gp:A3>Munich</gp:A3>
                  <gp:A4>Perlach</gp:A4>
                  <gp:A6>Otto-Hahn-Ring</gp:A6>
                  <gp:HNO>6</gp:HNO>
              </gp:civic-loc-condition>
          </cp:conditions>
          <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>
              <gp:geospatial-loc-transformation>
                  <gp:lat-resolution>
                   0.00001
                </gp:lat-resolution>
                  <gp:lon-resolution>
                   0.00001
                </gp:lon-resolution>
              </gp:geospatial-loc-transformation>
          </cp:transformations>
      </cp:rule>
</cp:ruleset>
```

Matching Location Filter

Sample Policy

```
<cp:ruleset
       xmlns:cp="urn:ietf:params:xml:ns:common-policy"
       xmlns:gp="urn:ietf:params:xml:ns:geopriv-policy"
       xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

       <cp:rule id="AA56i09">
           <cp:conditions>

               <cp:validity>
                   <cp:from>2004-11-01T00:00:00+01:00</cp:from>
                   <cp:until>2005-11-01T00:00:00+01:00</cp:until>
               </cp:validity>

               <gp:civic-loc-condition>
                   <gp:country>DE</gp:country>
                   <gp:A1>Bavaria</gp:A1>
                   <gp:A3>Munich</gp:A3>
                   <gp:A4>Perlach</gp:A4>
                   <gp:A6>Otto-Hahn-Ring</gp:A6>
                   <gp:HNO>6</gp:HNO>
               </gp:civic-loc-condition>
           </cp:conditions>
           <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>
               <gp:geospatial-loc-transformation>
                  <gp:lat-resolution>
                   0.00001
                 </gp:lat-resolution>
                   <gp:lon-resolution>
                   0.00001
                 </gp:lon-resolution>
               </gp:geospatial-loc-transformation>
           </cp:transformations>
       </cp:rule>
   </cp:ruleset>
```

Transforming resolution of location info

GEOPRIV Summary

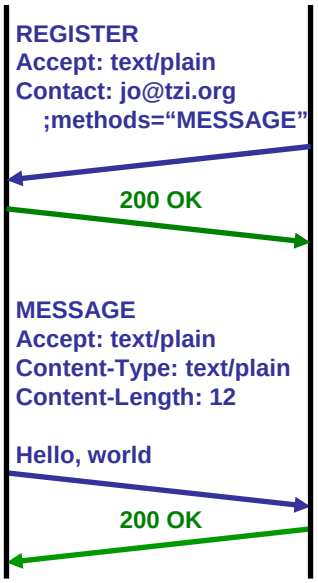
- Objective: interoperability and assurance of LBS security and privacy goals
- Conceptual model for dealing with security issues in LBS
  - Location Generator, Rule Maker, Location Server, Rule Set, Subscriber
  - Conceptually compatible with personal presence architecture (IMPP)
- Data model for Location Objects
  - Representing location information
  - Usage rules
  - Recommendations for secure transport (S/MIME)
- Policies
  - Control distribution of and access to personal information by explicit rules
  - Allows tailoring “revealed” presence / location information to the recipient
- NOT GEOPRIV:
  - Transport protocols for location objects, rules
  - For SIP-based presence, S/MIME can be applied

End of Excursion:

Back to SIP for Presence & IM

SIP for Instant Messaging (IM)

- UAs may send and receive messages
  - Similar model to Presence
- Receivers indicate support when registering
  Contact: sip:jo@tzi.org;methods="MESSAGE"
- Senders just send
  - Use sip: or im: URLs
  - Congestion control is important!
- For longer "chat sessions"
  - Create a persistent IM session
    - Just another media type
  - May not be able use TCP or TLS
  - Use MSRP-based session instead



Presence & IM Security

- Authentication of (Subscription) Requests
  - Standard SIP mechanisms: 401/407 responses
- Authorization: Users must stay in control of subscriptions
  - May subscribe to their own subscription state (“watcher info”)
  - Receive notifications for every subscription attempt
  - May authorize each subscription
  - May retrieve lists of and cancel existing subscriptions
  - Control distribution of state (e.g. GEOPRIV)
- Authentication of Instant Messages
  - May include contents to be automatically acted upon
  - User / system needs to validate originator
- Meta-issue: end-to-end authentication

Issue: Congestion Control

- PUBLISH, NOTIFY: Throttling of events
  - Keep event rate under control: one PUBLISH / NOTIFY per RTT
  - To be defined on a per-package basis
- MESSAGE: Message frequency
  - Only one outstanding message: one MESSAGE per RTT
    - But: messages are stand-alone; no dialog context to check against
- MESSAGE: Large messages
  - UDP is an acceptable transport for SIP: no congestion control
  - Even if TCP is used: impacts SIP infrastructure components
- Approach: Message Session Relay Protocol (MSRP)
  - Move message sessions off the SIP infrastructure

Message Session Relay Protocol (MSRP)

- Protocol for Messaging Sessions
  - Uses TCP or another reliable and congestion controlled transport
  - Message encoding similar to SIP and HTTP
- Just another media protocol
  - Messaging sessions require explicit setup and teardown
    - E.g., SIP dialogs (INVITE, BYE)
  - SDP to describe sessions (m=message)
  - Uses SDP Offer/Answer to convey parameters
    - Exchange dynamic transport addresses for communications (MSRP URLs)
    - Negotiate supported message formats
  - SEND method to convey messages
    - May request confirmation from the remote side (on success and/or failure)
    - Support for chunking of large messages (2 KB chunks)
  - REPORT method to provide confirmations
- Two modes of operation
  - Direct communication between peers (simple case)
  - Communication via relays (NATs, firewalls, policy)

Direction Communication between Peers