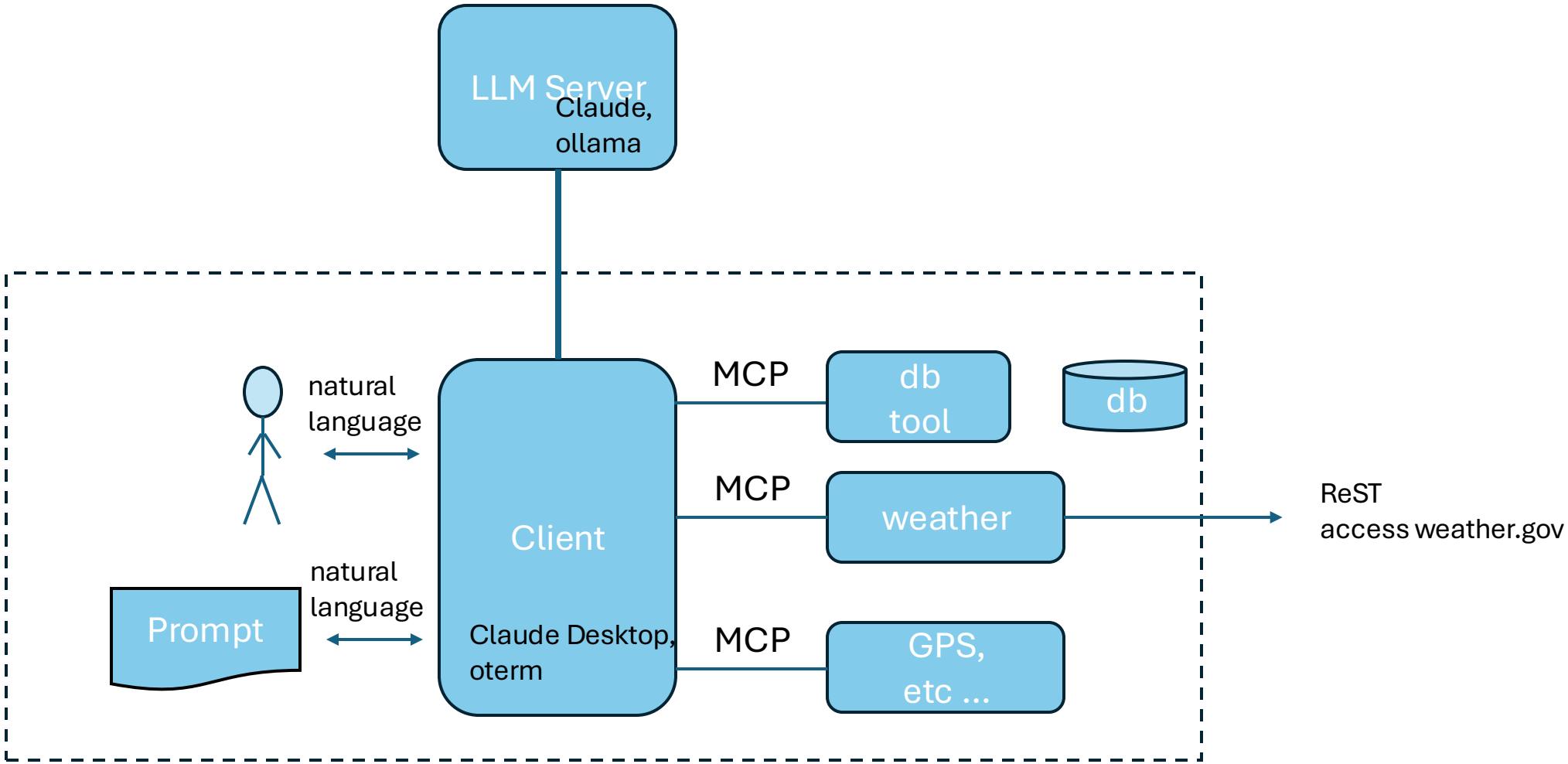
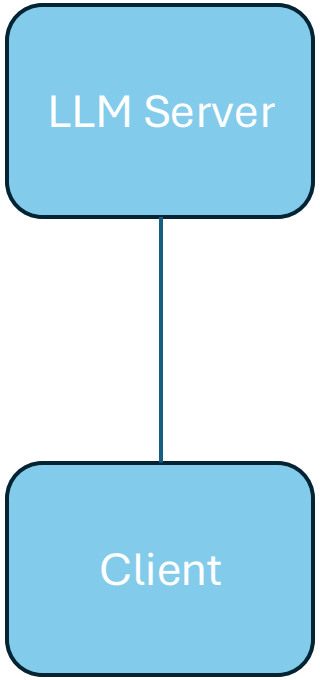
Tools and LLMs

Tom Sheffler
tom.sheffler@gmail.com

Tools Architecture



Tools Messaging



Three Things:

- Tool Definitions
- Tool Calls
- Tool Results

What is in a ToolDef?

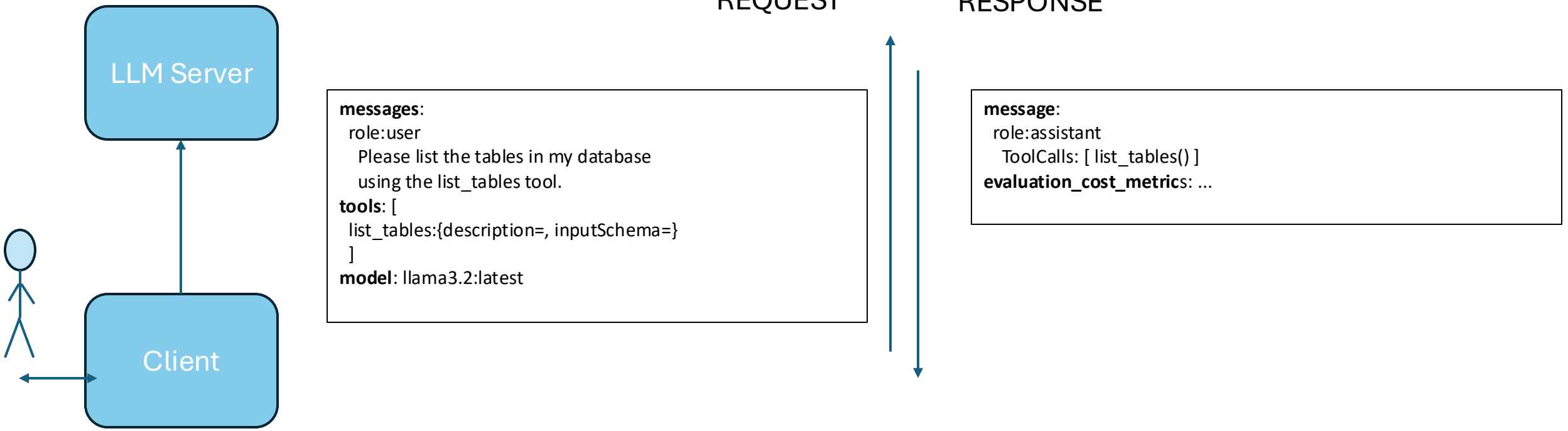
```
name='describe_table'
description='Get the schema information for a specific table'
inputSchema={
  'type': 'object’,
  'properties': {
    'table_name': {
      'type': 'string',
      'description': 'Name of the table to describe'
    }
   },
   'required': ['table_name']
}
```

A more complicated ToolDef

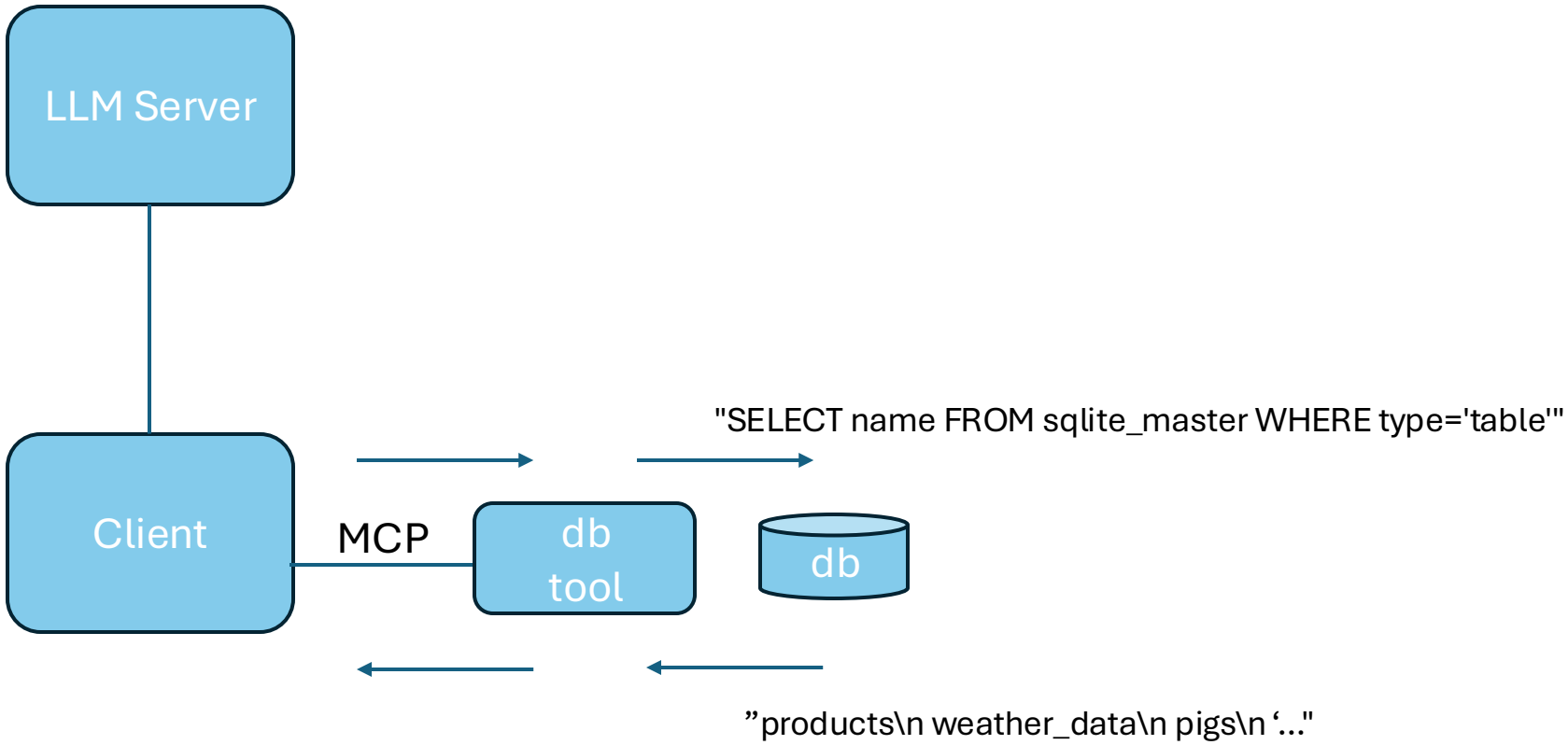
```
name='preparation_tool'
description="Prepare the samples for analyze.  Mark samples as 'passed' or 'failed'. "
inputSchema={
 '$defs': {
  'InputSample': {
   'properties': {
    'sample_name': {
     'description': 'sample name identifier',
     'title': 'Sample Name',
     'type': 'string'
    },
    'mass': {
     'description': 'sample mass in ng',
     'title': 'Mass',
     'type': 'integer'
    }
   },
   'required': ['sample_name', 'mass'],
   'title': 'InputSample',
   'type': 'object'
  }
 },
 'properties': {
  'sample_list': {
   'items': {
    '$ref': '#/$defs/InputSample'
   },
   'title': 'Sample List',
   'type': 'array'
  }
 },
 'required': ['sample_list'],
 'title': 'preparation_toolArguments',
 'type': 'object'
}
```

An example exchange using a Tool

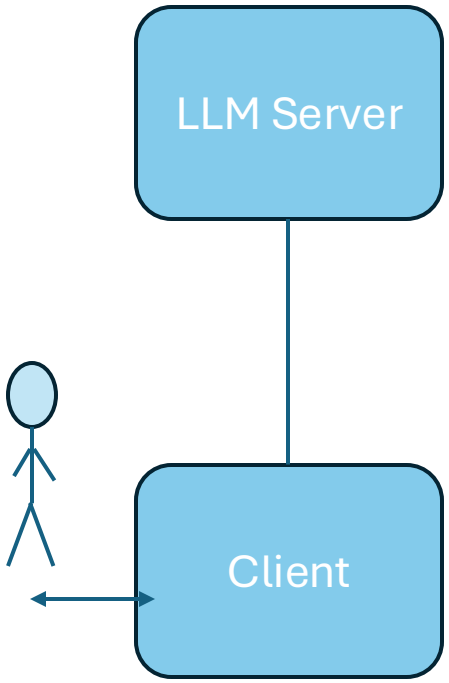
User says: “Please list the tables in my database using the list_tables tool”



Client runs the tool



Assistant returns the result and Client presents it



REQUEST

messages:
role:user
Please list the tables in my database
using the list_tables tool.
role:assistant
ToolCalls: [list_tables()]
role:tool
"[{'name': 'products'},
{'name':'weather_data'},
{'name':'pigs'} ...]"
tools:[
list_tables:{description=, inputSchema=}
]
model: llama3.2:latest

RESPONSE

message:
role:assistant
The list of tables in
your database is:
1. products
2. weather_data
3. sqlite_sequence
4. pigs
5. feed_consumption
6. health_checks
7. input_samples"
evaluation_cost_metrics: ...

Open Ends

- Definitions of Tools with structured types (arrays of structs)

- Tool return types

- Tool Execution error/exception handling:
  Consider ”n” ToolCalls and ToolCall[i] (i<n) fails
  - How does ToolCall[i] indicate failure?
  - Are ToolCall[i+1..n], etc not executed?
  - Are ToolCall[i+1..n] stripped from the messages[] array?

How this could tie into Authorization

- Oauth Scopes/Claims

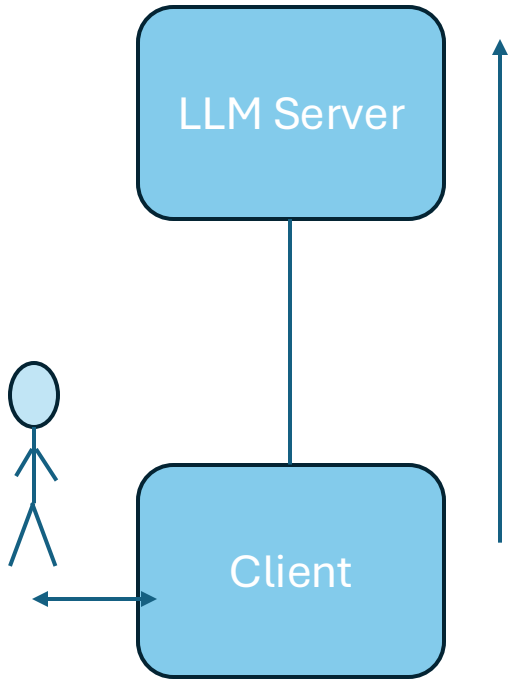
  - Scope: “nlip”
    - Claim: “nlip:messages” – user is granted basic messaging conversations
    - Claim: “nlip:tools” – user is granted permission to incorporate Tools
    - Claim: “nlip:control” – is allowed to send control messages

Extra

Tool Definition

```
name='describe_table' description='Get the schema information for a specific table' inputSchema={'type': 'object', 'properties': {'table_name': {'type': 'string', 'description': 'Name of the table to describe'}}, 'required': ['table_name']}
```

List the tables in my database using the list_tables tool




```
messages:
  role:user
    Please list the tables in my database
    using the list_tables tool.
tools:
  list_tables, description, inputSchema
model: llama3.2:latest
```

```
message:
  role:assistant
    ToolCalls: [ list_tables() ]
evaluation_cost_metrics: ...
```

```
messages:
  role:user
    Please list the tables in my database using the list_tables
tool.
  role:assistant
    ToolCalls: [ list_tables() ]
  role:tool
    "[{'name': 'products'}, {'name':'weather_data'},
{'name':'pigs'} ...]"
```

```
message:
  role:assistant
    "The list of tables in
your database is:\n\n1. products\n2. weather_data\n3.
sqlite_sequence\n4. pigs\n5. feed_consumption\n6.
health_checks\n7. input_samples"
tools:
  list_tables, description, inputSchema
evaluation_cost_metrics: ...
```