



Pacific Northwest
NATIONAL LABORATORY

*Proudly Operated by **Battelle** Since 1965*

VOLTRON™ Security

CRAIG ALLWARDT

Pacific Northwest National Laboratory

VOLTRON™ 2016

Overview



Pacific Northwest
NATIONAL LABORATORY

*Proudly Operated by **Battelle** Since 1965*

- ▶ Background
- ▶ Creating keys and authorization.
- ▶ Demo



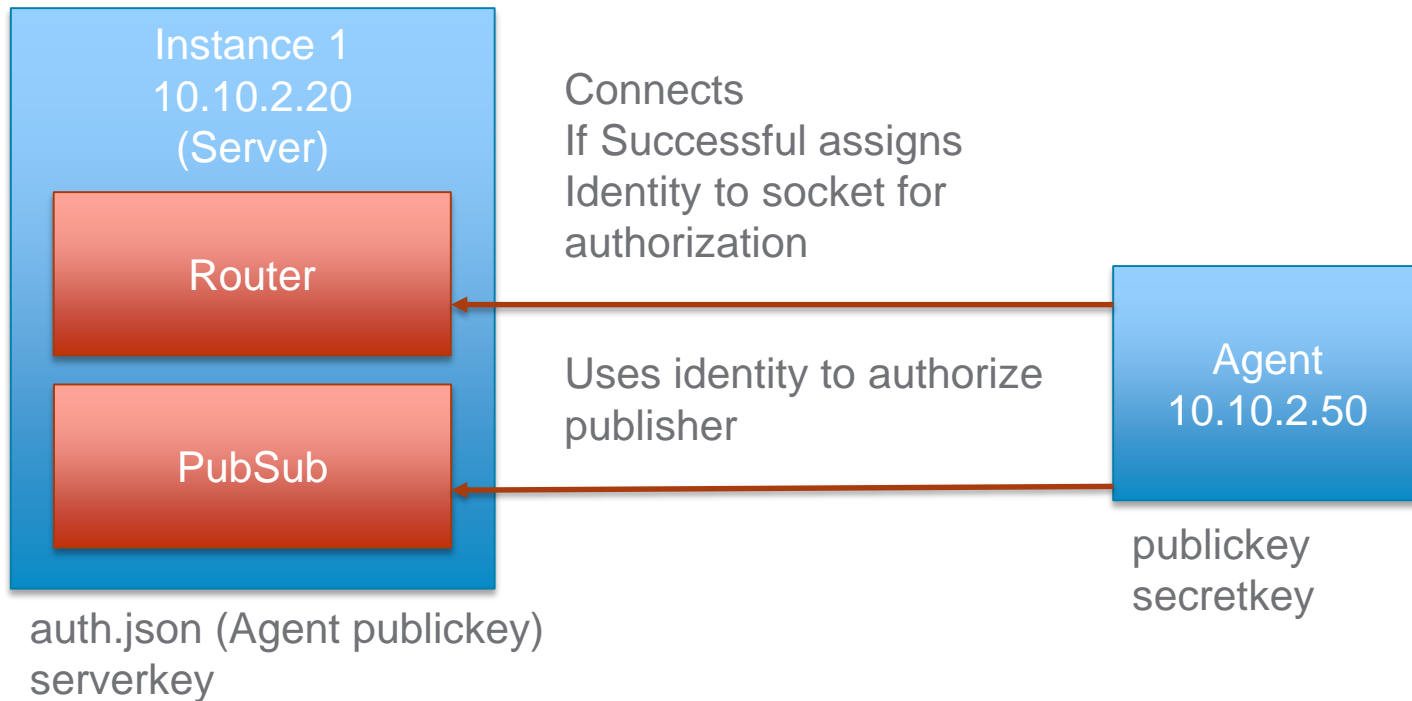
Background

- ▶ ZeroMQ's ZeroMQ Authentication Protocol (ZAP)
 - <http://rfc.zeromq.org/spec:27/ZAP/>
 - Elliptic Curve
 - Long term public and secret key
 - Short term communication keys based upon the public and secret key.
- ▶ VOLTTRON™ Interconnect Protocol (VIP)
 - http://voltron.readthedocs.io/en/develop/core_services/messagebus/VIP/VIP-Overview.html
 - Uses ZMQ frames to route to specific peers.
 - [SENDER, RECIPIENT, PROTOCOL, USER_ID, MSG_ID, SUBSYSTEM, ...]

- ▶ All VOLTTRON™ instances have a serverkey
 - Available from `volttron-ctl serverkey` command (publickey of server)
 - If web enabled available from `/discovery/` endpoint.
- ▶ Agent Keys
 - Public and secret key are created automatically and stored under `VOLTTRON_HOME/keystore` directory.
 - Each identity has it's own public/secret key pair.
- ▶ Allowing Agent Connections
 - Modify `auth.json` file in `VOLTTRON_HOME`
 - `volttron-ctl 'serverkey', 'auth-list', 'auth-add', 'auth-remove', 'auth-update'`



How Does This Relate?





Operational Awareness

- ▶ VOLTTRON™ Central
 - Green – Grey – Red
 - System Metric Plots
 - Remote Platform Monitoring
- ▶ Status and Alert Infrastructure
 - Threshold Detection Agent
 - System Monitoring Agent
 - SysLog Agent
 - Emailer Agent

Demo



Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by **Battelle** *Since 1965*

- ▶ Create a new instance
- ▶ Start a listener that will show messages on the bus
- ▶ Show an agent using an rpc method to publish
- ▶ Secure the rpc method.
- ▶ Show the rpc method is not permitted
- ▶ Show the publish method is secured