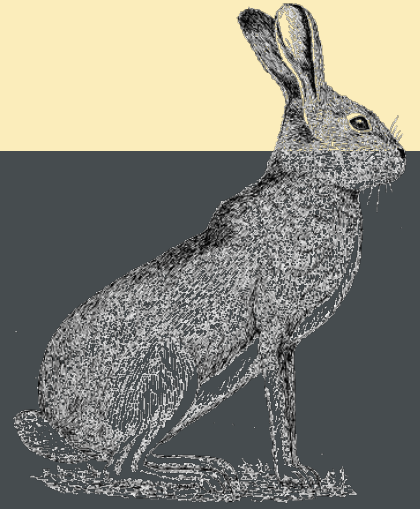
Secure Messaging Platform as a Service (SMPaaS)

Ian Stavros and Bryan Turek
Jackrabbit Consulting
December 6, 2016



Background

- Previous prototype collaboration framework:
  - Data Distribution Service (DDS) Transport
  - Operational Transformations (OT)
  - Nodejs + Electron.js
- Submitted SMPaaS proposal to DARPA
  - Distributed Hash Tables (DHT)
    - Communication routing
  - Blockchain
    - Ledger-like data storage
  - Alternative transport protocols in mind

SMPaaS Introduction

Packaged software that allows for entity collaboration with ease

- Manages and records authentic communication between systems and users.
- Developed from the ground up with proven building blocks
- Data replication
- Network auto-connect

Technologies

- Data Distribution Services (DDS)
  - Interoperable transport protocol
  - Secure
- Distributed Hash Tables (DHT)
- Blockchain
- Operational Transformation
  - Traceability

Security

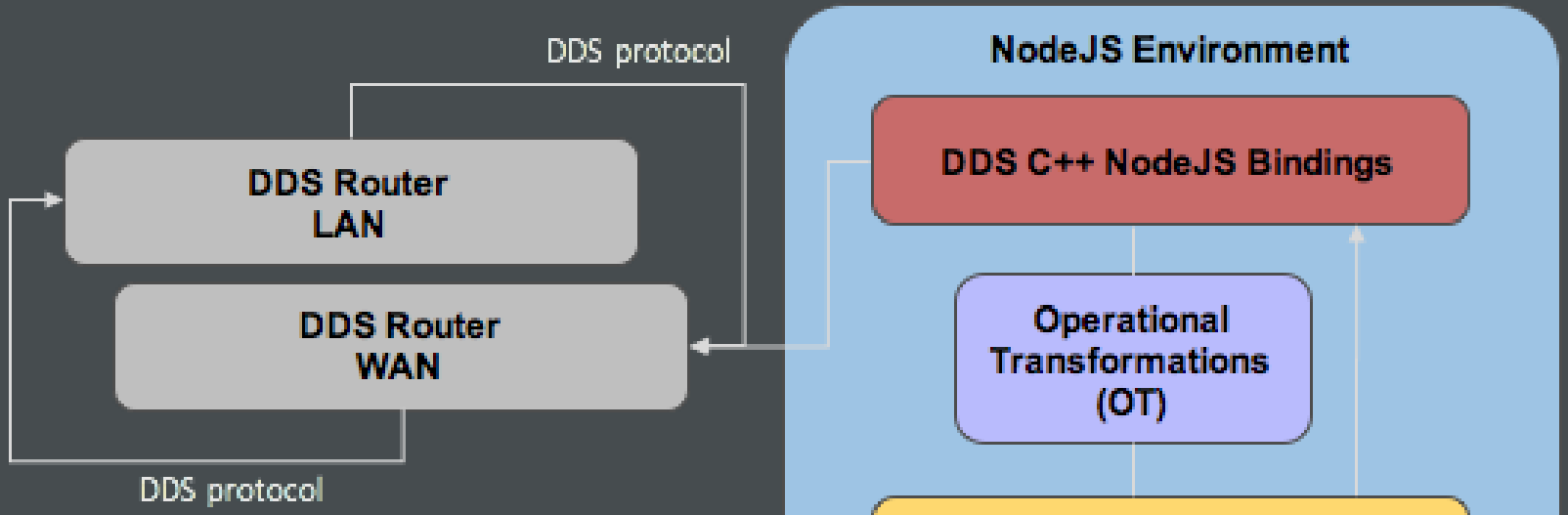
DDS Security for now

- Open to support other transport framework
- Must adhere to current security constructs such as 2 Factor Auth

Secure Messaging Platform (SMP) Node Consensus Algorithms ensures

- Authenticity of messages and operations
- Blockchain ledger-like activity over network

Current Architecture



Security Reference Architecture

Confidentiality

Authentication

X.509 Public Key Infrastructure (PKI) with a pre-configured Certificate Authority (CA).

Access Control

Specified permissions signed by CA control over domains, topics, read/write, and Quality of Service (QOS).

Cryptography

Protected key distribution, AES128 and AES256 encryption.

Integrity

Cryptography

HMAC-SHA1 and HMAC-SHA256 for message integrity.

Blockchain

Public and distributed ledger of all operational messages. All nodes in the network maintain a copy of the blockchain.

Data-Tagging

Classifies messages being sent across the network. Tags can provide valuable data including confidential parameters.

Availability

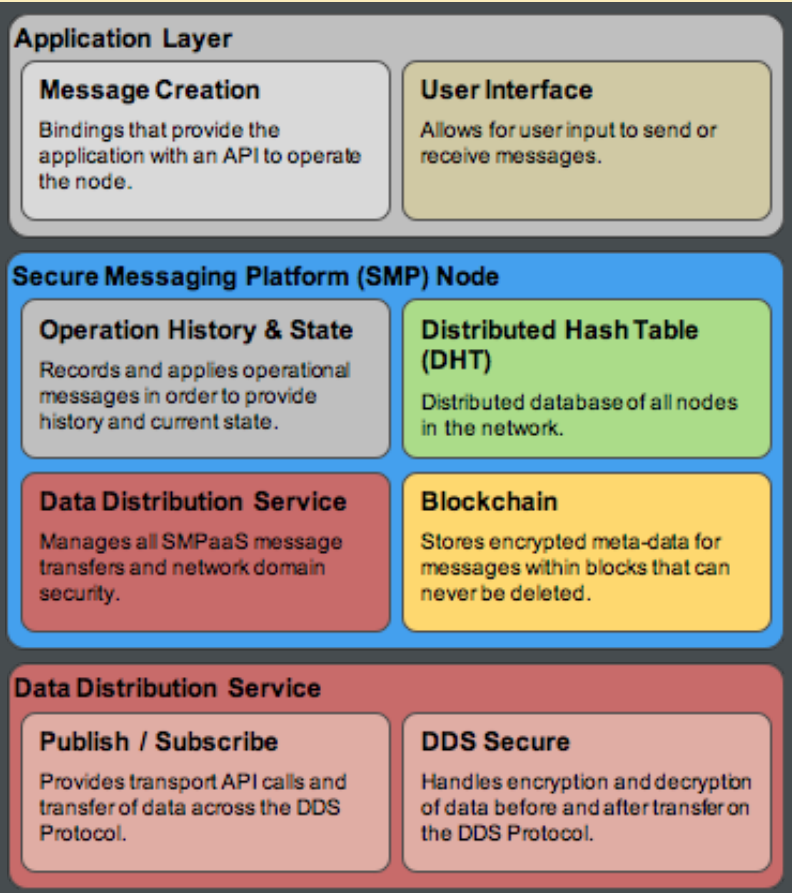
Non-Repudiation

Nodes or Recording Nodes manage the distribution of data throughout the network. Distribution of data can be customizable through full replication or segmented replication of data.

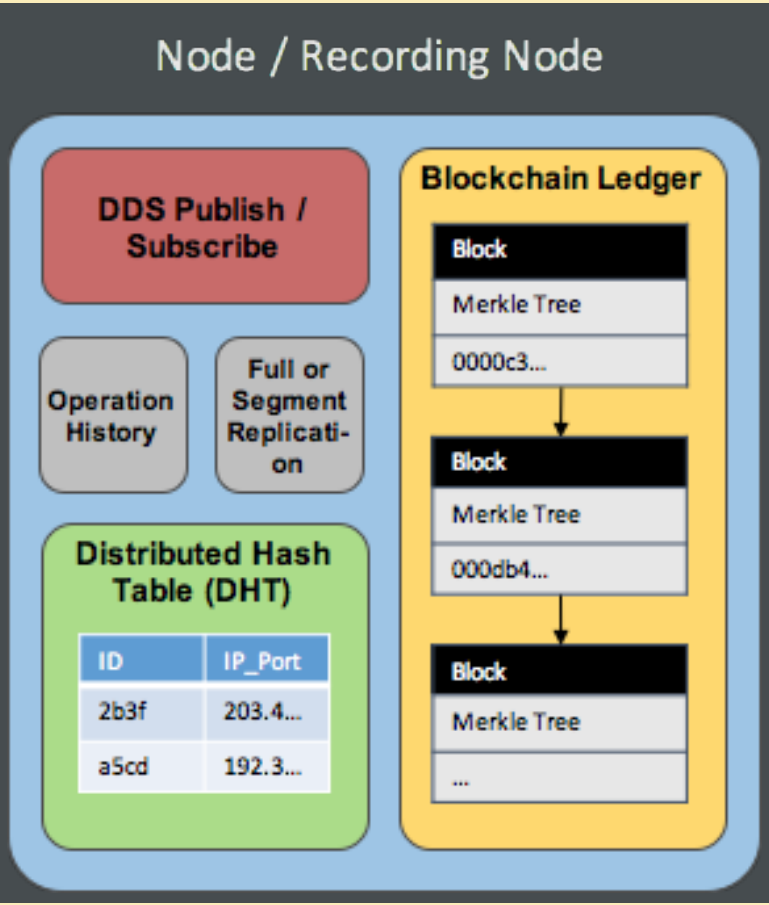
Network Address Translation (NAT) Relay

Nodes sitting behind a firewall or specific types of NATs can be setup with a NAT Relay Node to manage the network of nodes behind the NAT.

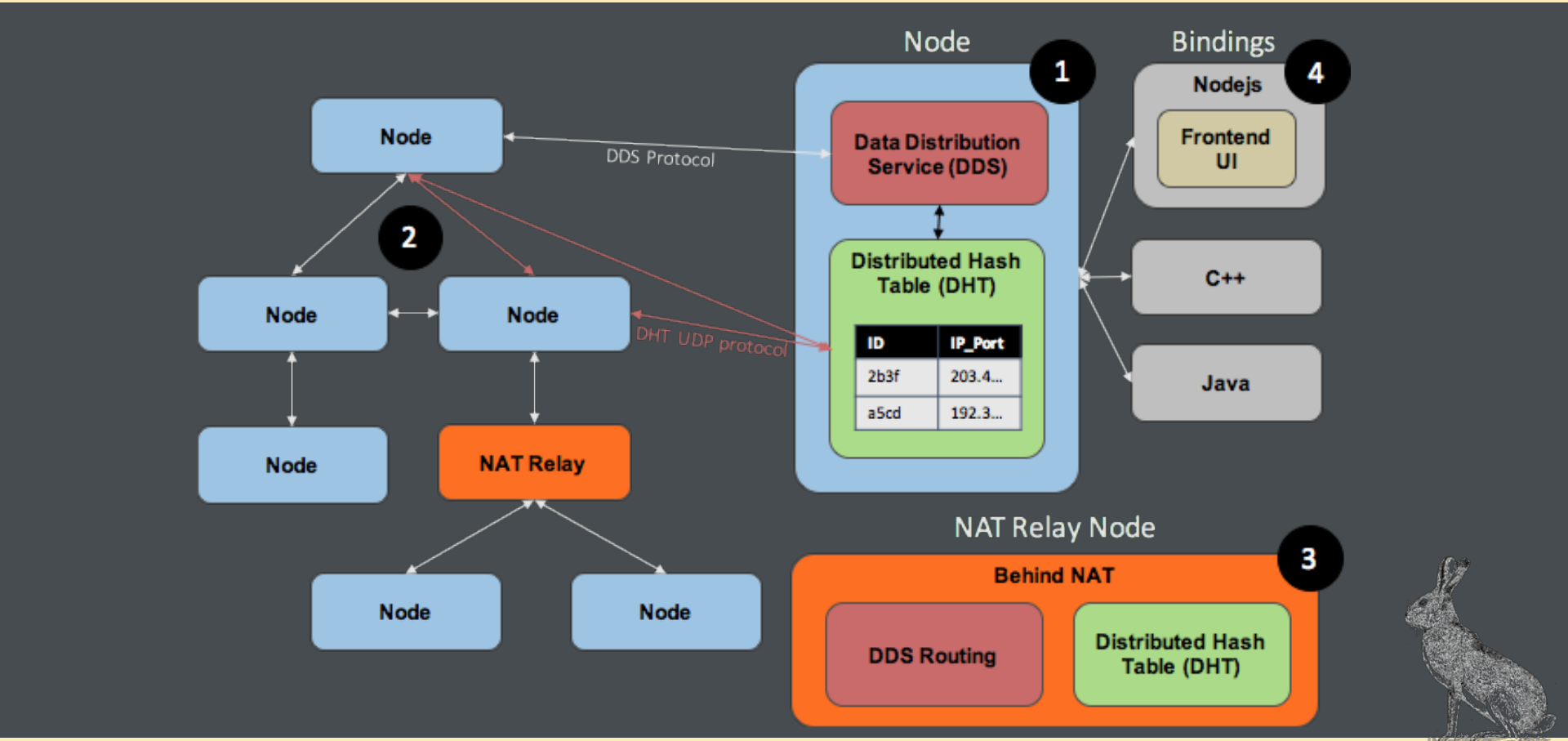
Architecture Layers



SMP Node Architecture



Network Architecture



Demo

Visit us at the vendor's table Wednesday night!

What is Secure Messaging Platform as a

SMPaaS will be designed to work equally well for both military applications in the Department of Defense (DoD) and for Federal/commercial business applications, with virtually any type of payload. SMPaaS messaging could be used *for* almost anything: collaborative document editing, financial transactions, vehicle communication in automated transportation systems, telemetry data for the health of any space or IT system, email systems, even flight crew/command center communication between nations in coalition military actions. SMPaaS messaging could be used *between* almost anything: human-human communication, or machine-machine communication in the Internet of Things (IoT). One appeal of SMPaaS will be its ability to perfectly record an audit trail of messages sent in a distributed ledger, so that an after-action review can reconstruct who said what when. Auditing is a vital need in our world of accountability for compliance with rules and regulations (e.g., Rules of Engagement, Federal Acquisition Regulations (FARs), Health Insurance Portability and Accountability Act (HIPPA)), and for detection of fraud and tracing the origins of phishing.