openIDL ND UIM POC - Security Policy

This document outlines the security policy for the system during the POC.

Scope

The scope of this policy is the ND UIM POC. It applies to all systems and activities used for the execution of the POC.

Policy

Identity and Access Management

Identity and Access Management - Application

Identities used to access the applications are managed in Cognito. The Cognito instance and it's userpools are separate for each carrier node. There is no shared Cognito across carriers in the carrier nodes. The multi-tenant node uses shared Cognito userpools. We are not utillizing the multi-tenant node for carrier activity during this POC. AAIS and the DOI will have identities on the multi-tenant node.

A userid and password are required to access the applications.

Identity and Access Management - Cloud Infrastructure

Each carrier has a node which is hosted in a separate AWS organization. AWS is the hosting cloud provider. The overall account is managed by AAIS. The specific organization is separate from all other organizations. IAM users are set up for Chainyard by AAIS. Every IAM user is distinct from others and has access only to the local AWS organization. Chainyard manages the infrastructure on behalf of the Carrier at the direction of AAIS. AAIS and Chainyard are able to administer the AWS organization and it's services. No other entity has access to the AWS organization or it's services. The carrier may request an IAM identity.

Identity and Access Management - Blockchain Network

Organizations are provided access to the blockchain network using certificates. Carrier certificates are created for the carrier node and shared with the network administrator. The certificates are managed in HashiCorp Vault.

Data Privacy

The data used during the POC is private to the carrier. It remains in its raw form only on the carrier node. When the extraction occurs, a salted hash is passed through the blockchain to the analytics node. Once on the analytics node, the results of the extraction from all carriers are compared with the ND DOT registered VINs and a report is generated.

Personally Identifiable Information

The system uses email address as the user id. The organization for the user is also identified. This is only visible inside Cognito. Each carrier node has a separate Cognito instance and userpool.

Data captured inside the openIDL Harmonized Data Store contains no PII.