Automated Hearings Solution (AHS)

System Architecture Document (SAD)

Functional Overview

Functional Processes

There will be a few changes to the NC DMV business processes for the AHS project. All changes required for AHS will centralize and streamline the administrative hearing process and reduce/eliminate manual data entry and manual management for all L&T Hearings.

There are six primary solution processes expected of the AHS solution:

1. Triggering the Violations Process: Instead of creating handwritten violation notices (audit reports, AOF, NOC, etc.), DMV will be able to record the violations for all hearings in AHS and generate the corresponding documentation to be sent to the customer.

2. Collecting/Requesting Hearing Fees: AHS will allow customers to make payments for hearing requests and civil penalties via multiple methods - online card payments (PayIt) and offline payments (personal checks, certified checks, cash, or money orders). Once the payment is successfully recorded in AHS, the customer will receive an email notification with the confirmation receipt. Upon approval, AHS will allow hearing fee refunds.

3. Scheduling the Hearing: AHS will integrate with NCID for ADFS, allowing HSU staff to access all Hearing Officers' calendars, MS Teams, Hearing Locations to easily schedule, reschedule, and cancel a hearing. Additionally, AHS will automatically send appointment notification messages via text, email, and letter to the customer, hearing officers, and all other parties for initial appointments, rescheduled appointments, and cancelled appointments.

4. Generating all Hearing related Correspondence: AHS will send appointment notification messages via text and email to all parties. AHS will create and maintain all correspondence templates. AHS will allow NC DMV to generate hearing correspondence (letters, forms, orders) in PDF form and send to the customer by mail (via integration with Xerox), electronically or print for in-person delivery.

5. Conducting the hearing: AHS will allow NC DMV hearing officers to enter and categorize hearing notes, witness comments and details. The hearing officer will be able to enter the hearing decision along with any details, probations, agreements, motions, and/or civil penalty fines. AHS will transfer the hearing data and hearing decisions to the legacy system.

6. Capturing Hearing Decisions and Outcomes: Once a hearing is concluded, all supporting documentation (additional evidence, hearing recording, etc.) will be stored in AHS, hearing decision orders and forms will be generated and shared with the relevant parties. AHS will also send the hearing decision codes/actions to the corresponding DMV systems allowing NC DMV users to complete any further actions (suspensions, revocations, civil penalties, etc.). The solution will also provide reporting and workflow functionality.

Physical Location Overview

Insert brief high-level physical description of the application or service infrastructure physical locations. This should include both the location of the systems/servers and also define who provides support and maintenance of the systems or service.
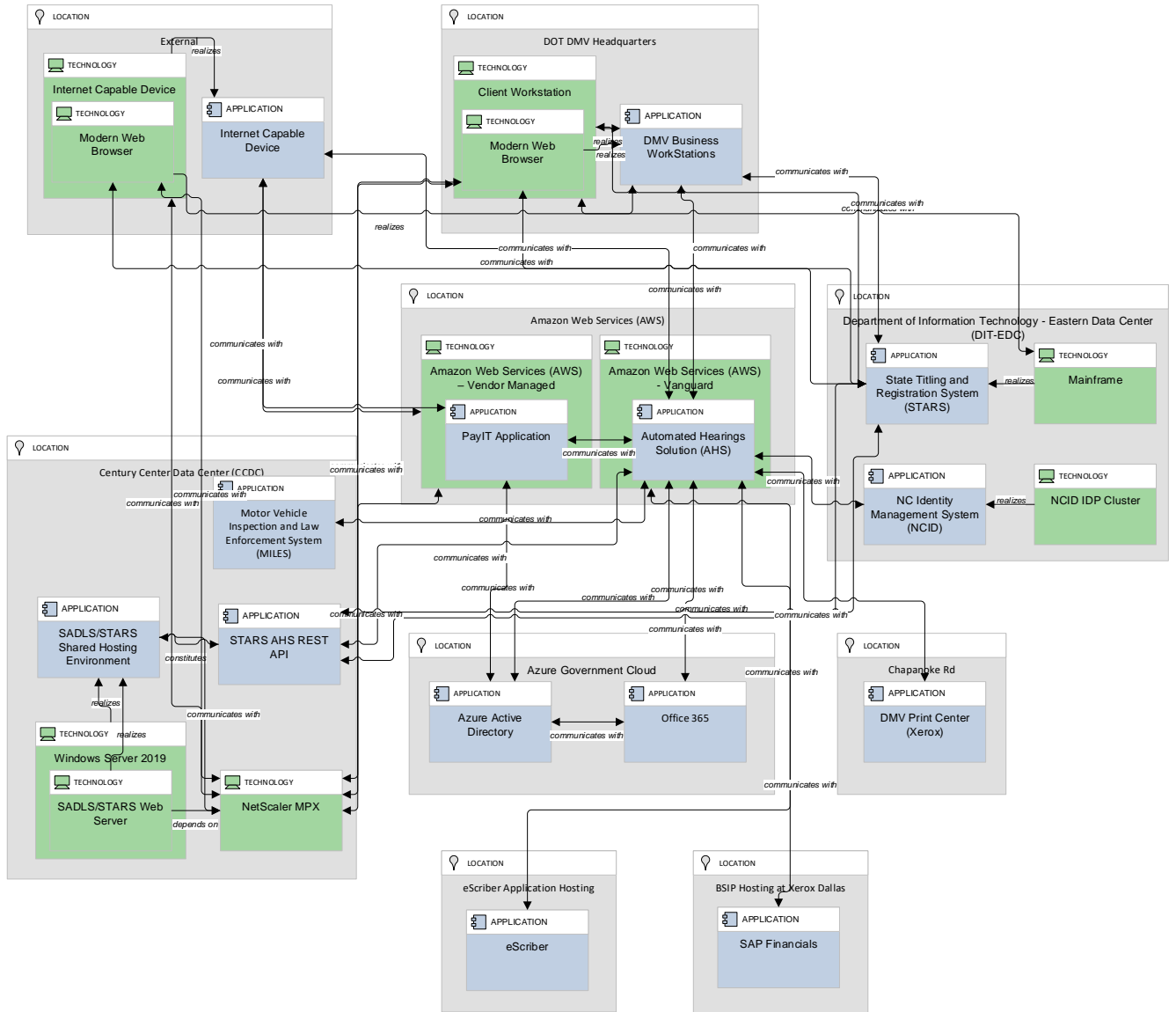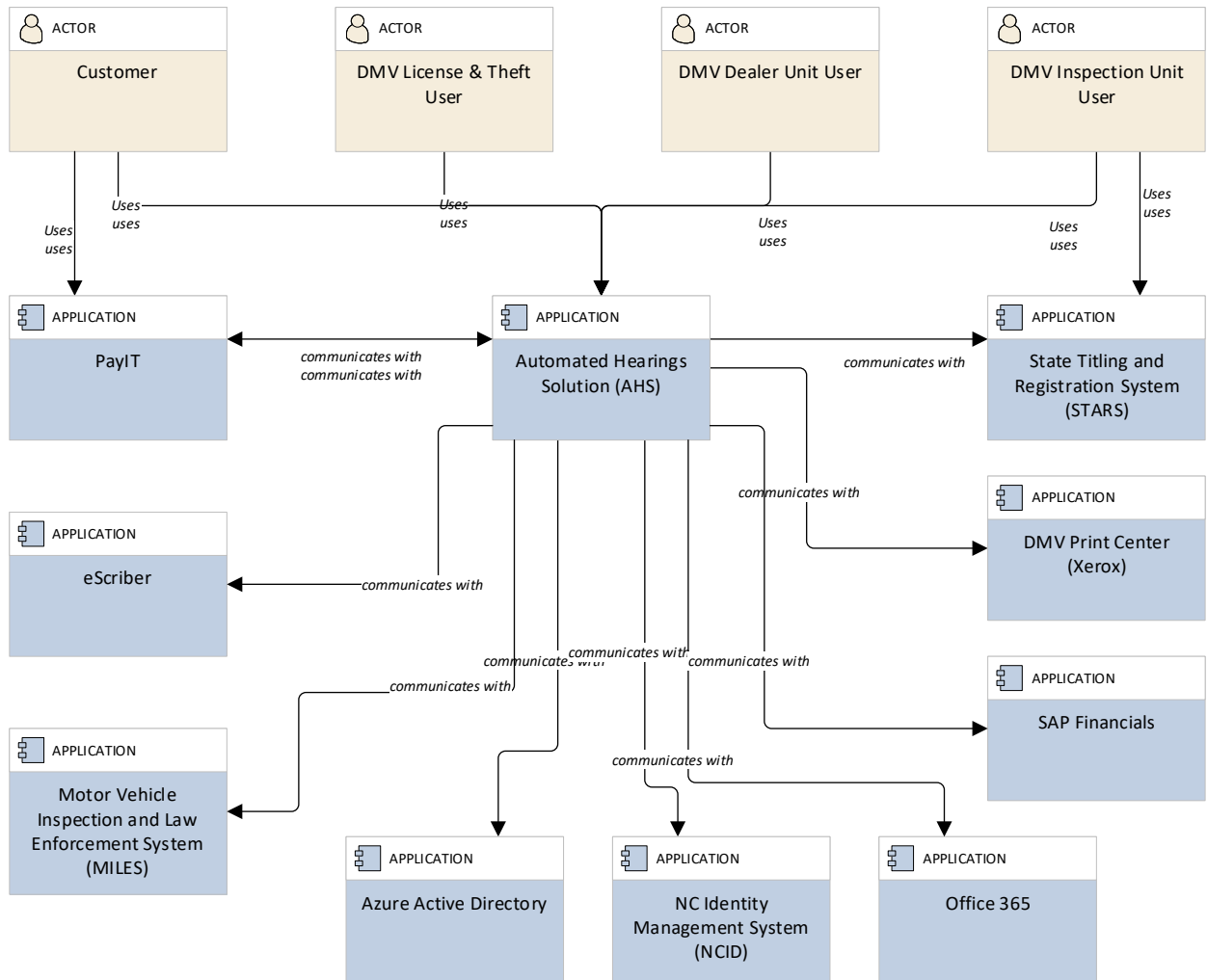

Logical Overview

Insert an overview of the physical and logical system architecture of the application or service. This should fully describe all the components of the application or system.

ACTOR
Customer

ACTOR
DMV License & Theft User

ACTOR
DMV Dealer Unit User

ACTOR
DMV Inspection Unit User

Uses
uses

Uses
uses

Uses
uses

Uses
uses

Uses
uses

Uses
uses

APPLICATION
PayIT

communicates with
communicates with

APPLICATION
Automated Hearings Solution (AHS)

communicates with

APPLICATION
State Titling and Registration System (STARS)

APPLICATION
eScriber

communicates with

communicates with

APPLICATION
DMV Print Center (Xerox)

APPLICATION
Motor Vehicle Inspection and Law Enforcement System (MILES)

communicates with

communicates with
communicates with

communicates with

APPLICATION
SAP Financials

communicates with

APPLICATION
Azure Active Directory

APPLICATION
NC Identity Management System (NCID)

APPLICATION
Office 365

Data Flow and Classification

Insert data flow diagrams and description for all use cases. Please classify the data and sensitivity of data in the system. Please see the [Data and System Classification Policy](#) for a complete description of the data classification ratings.
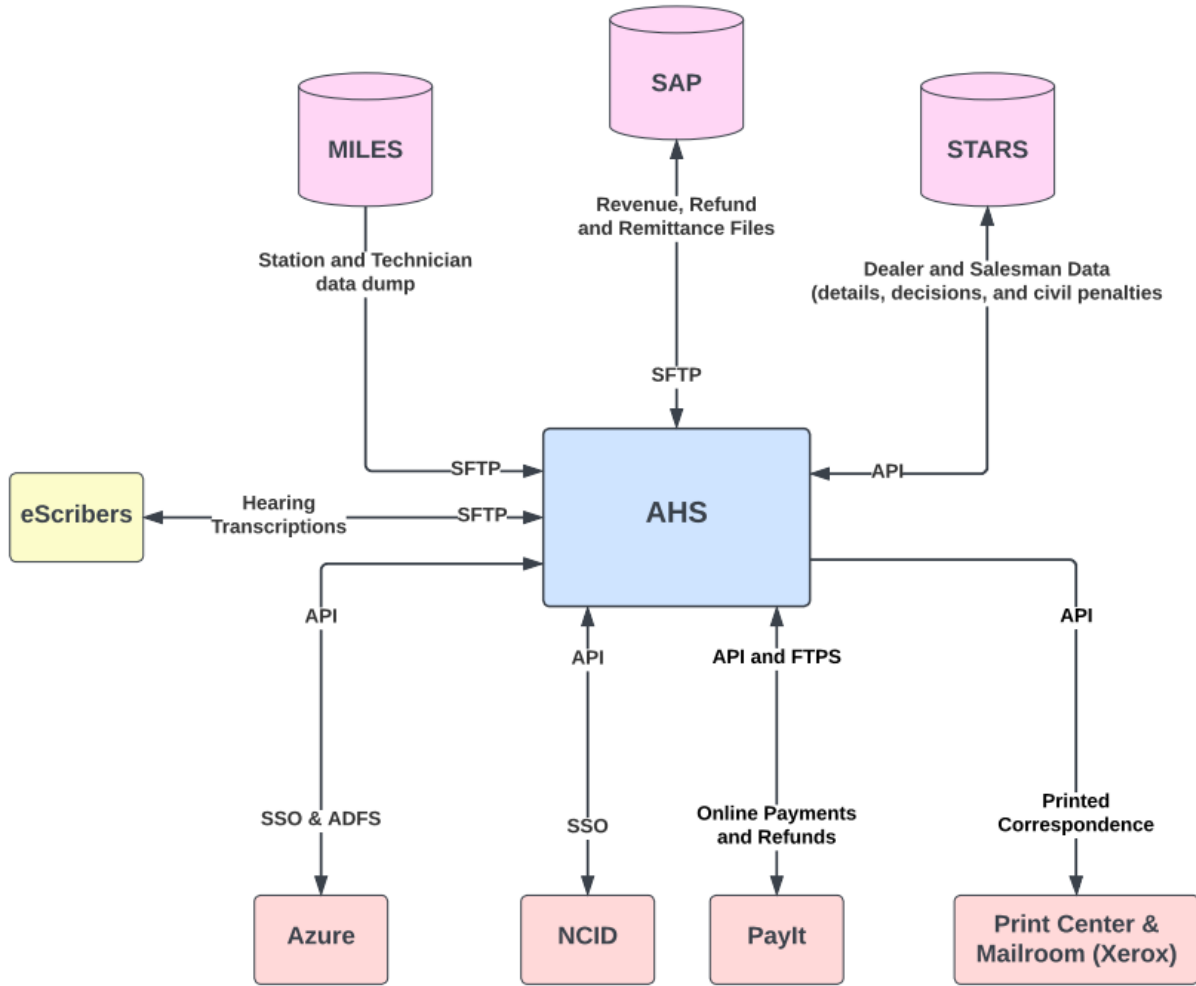
Data Element Name	Description	Classification
Dealer, Salesman, and Civil penalties	**STARS** sends/receives name, address, and civil penalties.	☐Highly Restricted ☒Restricted ☐Unrestricted
Station and Technician information	**MILES** sends station name, technician name, along with address (interim solution).	☐Highly Restricted ☒Restricted ☐Unrestricted
Revenue, Refund, and Remittance Files	**SAP** sends/receives revenue, refund, and remittance files, which includes name and address.	☐Highly Restricted ☒Restricted ☐Unrestricted
Payments and refunds	**PayIt** sends/receives payment and refund information, which includes name and address.	☐Highly Restricted ☒Restricted ☐Unrestricted

For each Highly Restricted data element, describe the data flow for the systems that process, store, or transmit the information.

**North Carolina
Department of Transportation**

Business Continuity and Disaster Recovery

Application Criticality

Application Criticality – Application criticality has the following 4 categories. One must be identified per each application.	• *Statewide Critical* – From an information technology perspective, in the agency's opinion, the loss of this application will have a direct impact to statewide core functions, processes and/or activities. The applications loss may also impact a large portion of the State's population. • *Agency Critical* – From an information technology perspective, in the agency's opinion, the loss of this application will have a direct impact to this department's core functions, processes and/or activities. • *Program Critical* – From an information technology perspective, in the agency's opinion, the loss of this application will have a direct impact to the core functions, processes and/or activities associated with a program within an agency. • *Non Critical* – From an information technology perspective, in the agency's opinion, the loss of this application will have little or no impact to statewide and/or this department's core functions, processes and activities or the core functions, processes and activities associated with a program within an agency.	*Statewide critical*

Outage and Recovery

		Business Requirement	**Current Capability**
RTO - Recovery Time Objective Clarification	The duration of time and a service level within which systems, applications, or functions must be restored after an outage to the predetermined Recovery Point Objective (RPO), for example, one business day. The duration of time (and a service level) within which systems, applications, & or services in support of a specific agency business function, must be restored after an outage within the stated (RTO) time, and to the predetermined state as specified as per the most current "production" version	*Not a business response, thereby this field is not populated.* *Use hours. As one day may mean 8 hours & or 24 hours, etc.*	*.25 hours (15 mins)* *Use hours. As one day may mean 8 hours & or 24 hours, etc.*
RPO - Recovery Point Objective Clarification	The point in time to which systems and data must be recovered following an adverse event, e.g. the last completed transaction or the point immediately before the last backup commences. Also known as the Critical Data Point Age of the data to be restored to, once the application / system is recovered in the DR environment & made available to the business. For example, 8 hours, means the data is "8 hours older than the time the incident occurred.	*4 hours* *Use hours. As one day may mean 8 hours & or 24 hours, etc.*	*Aurora storage provides a near realtime replication, w/ lag time as typically < 1 second* *Use hours. As one day may mean 8 hours*

			& or 24 hours, etc.
MTD - Maximum Tolerable Downtime	The maximum number of hours for which it is acceptable that a function can be interrupted following a continuity event. (FEMA) *See*, Recovery Time Objective, Maximum Acceptable Outage	*4 hours* *Use hours. As one day may mean 8 hours & or 24 hours, etc.*	*The prior column provides MTD, established by the business as a formal business requirement, stated in disaster recovery terminology*
Clarification	The MTD represents the total amount of time leaders/managers are willing to accept for a mission/business process outage or disruption and includes all impact considerations. RTO is required to recover the IT Application / system. MTD includes RTO plus existing business work arounds, which would be applied in the early stages of an outage prior to a disaster declaration. *Ref picture below*		*IT (applications, data & services), supports the given application's MTD in RTO terms, in the next row below. RTO is one of two parts making up the MTD.* *Use hours. As one day may mean 8 hours & or 24 hours, etc.*

Parent Dependencies

Parent dependencies are defined as network or application services that provide direct support to the application being reviewed by this Application Architecture Document.

NCDOT NCID
- **AHS** uses NCDOT NCID to authenticate all external users.

Azure EntraID
- **AHS** uses Azure AD to authenticate all DMV users.

STARS web service
- **AHS** calls a STARS web service to get STARS and SADLS information via a VPN.

Xerox Printer
- **AHS** sends print jobs to the production Xerox printer on Chapanoke Rd via a VPN.

Payit
- **AHS** calls a PayIt web services to send financial information.

eScriber
- **AHS** interfaces with eScraber to automatically scribe the call.

SAP
- **AHS** calls a SAP web services to send financial information.

Office365
- **AHS** calls Office365 web services to setup calendar events.

Application Security

The **AHS** application is built and classified as a **Highly Restricted** environment application.

Authentication

The AHS application uses SAML AD and SAML NCID authentication to login.
.

Authorization

This section should describe how, once authenticated, users are authorized to access your service's data and resources. This could be via AD security groups, database roles, etc.

AD authorization for Staff Portal:
  - User must have a valid AD account
  - ADs are provisioned through the AHS Staff portal by an AHS Staff ADMIN by entering their NC State government email (.gov) and Role (Admin, Manager, Staff).
NCID authorization for Public Portal:
  - Individual must have a valid NCID account
  - When registering on AHS Public Portal, include your NCID email address.
  - AHS will send a welcome email to the new user with a link to complete the onboarding
  - New user will click on the link and will be redirected to AHS Staff Portal login screen
  - New user will click on login with SSO to be taken to the NCID login page
  - After successful authentication, as long as the email ID returned in NCID success authentication and the profile email ID match, the user will be allowed to login

Encryption

A VPN tunnel is used by the AHS cloud solution to call the STARS web service and submit print jobs to the production Xerox printer.