
🔹 1. Overview of State Farm's Digital Portals

State Farm operates a suite of digital platforms tailored to serve various stakeholders

- **Public Website**: statefarm.com (https://www.statefarm.com
    - **Audience**: General public and policyholder
    - **Purpose**: Provide information on insurance products, allow policy management, claims filing, and access to customer support
- **B2B Portal**: b2b.statefarm.com (https://b2b.statefarm.com
    - **Audience**: Business partners such as auto repair facilities, medical providers, suppliers, and lender
    - **Purpose**: Offer self-service applications and information for managing claims, payments, policies, and supplier interactions
- **Agent Portal**: agents.statefarm.com (https://agents.statefarm.com
    - **Audience**: State Farm agent
    - **Purpose**: Facilitate policy sales, customer relationship management, and access to internal resources
- **Claims Portal**: claims.statefarm.com (https://www.statefarm.com/claims
    - **Audience**: Policyholder
    - **Purpose**: Enable users to file and track insurance claims online
- **SFNet Portal**: sfnet.statefarm.com (https://sfnet.statefarm.com
    - **Audience**: Internal employee
    - **Purpose**: Serve as an internal network for employee resources, communications, and tools

---

🔹 2. In-Depth Look at the B2B Portal

The **State Farm B2B Portal** is a centralized platform designed to streamline interactions between State Farm and its business partner.

A. Functionalities

- **Claims Management**:
    - **Select Service®** Auto repair facilities can manage claims, create assignments, and access performance report.
    - **Medical Billing** Healthcare providers can submit medical claims related to auto accidents and access payment information.
- **Payments**:
    - **Electronic Payments** Partners can set up and manage Electronic Funds Transfer (EFT) payments, view remittances, and access related form.
- **Supplier Management**:
    - **Suppliers Portal** Vendors can engage with State Farm's procurement processes through the Coupa platform, managing orders, invoices, and supplier information.
- **Lender Services**:
    - **Home & Auto Lenders** Financial institutions can verify insurance policies, manage escrow billing, and access mortgage payment system.

B. Relation to Other Categories

The B2B Portal interfaces with multiple State Farm systems to ensure seamless operation:

- **Integration with Claims Systems** Facilitates real-time updates between repair facilities and State Farm's internal claims processing system.
- **Financial Systems Connectivity** Ensures that payment information flows accurately between suppliers, medical providers, and State Farm's accounting department.
- **Data Security and Compliance** Implements robust security measures, including Multi-Factor Authentication (MFA), to protect sensitive partner information.

More about the B2B Portal

The B2B portal is designed to support all business partners of State Farm. Instead of handling everything over phone or mail, partners use this website to do things faster and online.

Examples of how it helps:

- A **car repair shop** can accept a vehicle claim and update repair progress.

- A **hospital or clinic** can send bills directly to State Farm for accident treatment.
- A **supplier** can send an invoice and get paid quickly.
- A **bank** can check if a house has the right insurance.

Tools inside the portal:

- **Select Service:** Helps repair shops connect with claims.
- **Medical Billing:** Helps doctors and clinics get paid for treating accident victims.
- **EFT Setup:** Makes it easy to receive payments electronically.
- **Supplier Center:** Manages orders and payments through Coupa.
- **Mortgage Tools:** Lenders can manage insurance data for escrow and home loans.

How it connects to other portals:

- It pulls claims data from State Farm's internal systems (used by claims.statefarm.com).
- It works with finance tools that connect to agent systems and the employee portal (sfnet).
- It keeps everything secure and up-to-date across all platforms.

Why the B2B Portal is Important

- It saves time for both State Farm and its partners.
- It improves accuracy by avoiding manual errors.
- It makes the process faster – claims get processed, payments made, services delivered.
- It allows scaling – thousands of partners can be handled efficiently.

Thanks for the update, Nani! Since your State Farm B2B portal doesn't use a direct database but instead relies on **LDAP**, **TPAR**, **Vault**, and possibly other internal systems for authentication, user data, and configuration/secrets management — here's the **updated version** explaining how it works, how it is developed, and what your **responsibilities might have been**.

✅ **Updated Overview: How State Farm B2B Portal Works Without Direct DB**

🔒 1. Authentication & Identity (LDAP)

- **What is LDAP?**
    - LDAP (Lightweight Directory Access Protocol) is used for user authentication and user data.
- **Usage in B2B Portal:**
    - User login is validated against corporate LDAP.
    - User roles (Supplier, Agent, Medical Provider, etc.) are fetched from LDAP groups.
- **Your Work Might Include:**
    - Integrating LDAP with Spring Security.
    - Setting up role-based authorization based on LDAP groups.
    - Fetching user info (name, role, access level) after successful login.

🔐 2. TPAR (Trusted Partner Access Request)

- **What is TPAR?**
    - TPAR is an internal State Farm system for managing third-party partner access.
- **Usage in B2B Portal:**
    - External vendors (repair shops, hospitals, etc.) get access only after TPAR approval.
    - Validates if the partner is allowed to access specific modules (like EFT, medical billing).
- **Your Work Might Include:**
    - Calling TPAR APIs to validate third-party users.
    - Checking access levels and restricting UI/API based on TPAR roles.
    - Showing different screens/modules depending on partner type.

🔐 3. Vault (Secrets Management)

- **What is Vault?**

    - Vault is used to securely store credentials, API keys, and secrets (e.g., encryption keys).

- **Usage in B2B Portal:**
    - Stores sensitive credentials for calling internal services (like Coupa, Claim Systems).
    - Stores encryption keys for handling sensitive data (EFT info, PII).
- **Your Work Might Include:**
    - Integrating Vault with backend microservices using Spring Cloud Vault.
    - Fetching secrets at runtime securely (not hardcoded).
    - Rotating secrets or access tokens via Vault configuration.

🧩 4. How the System Works Without a Traditional DB

Even without a direct relational database, data flows like this:

- **User login →** Verified via LDAP
- **Partner access →** Verified via TPAR
- **Secrets (tokens, API keys) →** Retrieved from Vault
- **Data storage** is handled by internal services (e.g., Claims API stores data in their system)

Example:

- You submit a medical bill via B2B UI → Backend validates your role via TPAR → Validates claim via external Claim API → Uses Vault to authenticate to Claim API → Bill is saved in Claim System (not in your B2B service)

🛠️ What You Might Have Built or Worked On

Area	Your Role
Login Module	Integrated LDAP login, mapped roles from directory
Authorization	Used TPAR to show/hide modules based on partner access

Area	Your Role
File Upload	Uploaded docs to internal storage/S3, encrypted using keys from Vault
Form Modules (EFT, Claims)	Developed React forms, used Spring Boot backend, called external APIs
Secrets Management	Integrated Vault with Spring Boot apps for runtime secrets
Partner Validation	Called TPAR APIs before allowing claim or billing actions
Modular Access	Controlled visibility of features (Medical Billing, Repair Shop, Supplier)
Deployment	Used Docker, Kubernetes, and internal CI/CD tools for deployment

---

🔗 **How It Connects with Other State Farm Systems**

System	Integration Role
sfnet.statefarm.com	Internal employee or agent login
claims.statefarm.com	Used to fetch claim data, submit bills
Coupa	For supplier management and invoicing
Email/SMS Services	Send notifications to partners
Vault	For API keys, DB tokens, encryption keys
TPAR	For validating third-party access rights

Thank you, Nani! Based on your clarification, here's the **refined version** of your project summary in **simple, professional language**, considering the integrations were already in place and your focus was on **using** them rather than developing those integrations.

✅ **Final Project Summary for Resume / Documentation**

==========

I worked on the **State Farm B2B Portal**, a secure platform that provides external partners—such as repair shops, medical providers, and suppliers—access to business services like **Select Service, EFT Setup, Medical Billing**, and **Supplier Management**.

The system used **TIMS credentials** (username and password) for login, allowing users with different roles to access specific modules. Authentication and authorization were handled through **LDAP**, **TPAR**, and **Vault**, which were already integrated. My role involved **utilizing** these systems to securely fetch user roles, manage access, and retrieve secrets for backend services.

I developed and maintained **Spring Boot microservices** and built **React-based responsive UI components** for various partner-facing modules.

We consumed internal APIs for functionalities such as claim lookups, document uploads, and EFT updates—without using a traditional database.

The platform was containerized and deployed using **Docker**, **Kubernetes**, **AWS ROSA (Red Hat OpenShift on AWS)**, and managed via **GitLab CI/CD** pipelines.

My responsibilities included bug fixes, new module enhancements, form validations, API integrations, and secure communication across services using credentials stored in **Vault**.

Here's a polished final version of your project summary for documentation, resumes, or LinkedIn — written professionally, concisely, and clearly capturing your work on the State Farm B2B Portal:

Project Summary: State Farm B2B Portal

I contributed to the development of the **State Farm B2B Portal**, a secure, web-based platform enabling external partners—such as auto repair facilities, medical providers, suppliers, and lenders—to interact with State Farm's internal systems for services like **Claims Management**, **Medical Billing**, **EFT Payments**, and **Supplier Integration via Coupa**.

🔐 **Authentication & Authorization**

- Implemented secure login using **LDAP**, leveraging corporate directory services for user identity and role mapping.
- Integrated with **TPAR (Trusted Partner Access Request)** to validate third-party access and control module-level permissions.
- Utilized **Vault** to securely access credentials, API tokens, and encryption keys, avoiding hardcoded secrets.

🧩 **Responsibilities**

- Developed and maintained **Spring Boot microservices** for backend operations, interacting with internal APIs (Claims, Payments, TPAR, etc.).
- Built responsive frontend modules using **React.js** for EFT setup, claim submission, and supplier onboarding.
- Enabled **modular access control** by dynamically rendering UI based on user roles and partner types.
- Managed **file uploads** to internal storage (e.g., S3-like services), with encryption keys securely retrieved from Vault.
- Ensured **seamless integration** with enterprise systems such as Claims Processing, Coupa (Supplier Center), and internal finance tools.

🚀 **Deployment & DevOps**

- Deployed services using **Docker** and **Kubernetes** within a secured internal cloud environment.
- Used internal **CI/CD pipelines** (e.g., GitLab) to manage builds, testing, and deployment workflows.

🔗 **Key Integrations**

- **LDAP**: User authentication and group-based authorization.
- **TPAR**: Verified third-party partner access before API/UI operations.
- **Vault**: Fetched runtime secrets securely using Spring Cloud Vault.
- **Coupa**: Managed procurement workflows, invoices, and supplier data.
- **Claims APIs**: Submitted and tracked claim status in real time.

- **Internal Communication Systems**: Email/SMS notification services for status updates.

🎯 Impact

- Enabled self-service access for thousands of partners, reducing manual support.
- Improved claim and billing efficiency through real-time integrations.
- Increased platform security with robust identity and secret management.
