Nordic Concur Connector — Architecture

Multi-tenant SaaS that connects SAP Concur expense and employee data to target systems (Nordic tax authorities available or in development), with optional enrichment from the customer's HR and accounts payable systems.

SOURCE SYSTEM

SAP Concur

Source of paid expense reports, benefit data, and employee data. Connected once via Concur App Center OAuth; ongoing administration is done in the Nordic Concur Connector UI.

- Expense & employee APIs
- Optional SFTP

→ Fetch expense & employee data

INTEGRATION PLATFORM

Nordic Concur Connector

Processes, enriches, and delivers data to target systems. Web application, background workers, and data stores.

- Map reports to companies
- Qualify & enrich data
- Generate & submit to targets

→ Deliver to target systems

TARGET SYSTEMS

Downstream destinations

Extensible connector model for destination systems. Nordic tax authority connectors are available or in development; other target types can be added.

- Vero / Tulorekisteri (KATRE, FI) — available
- Skatteverket (SE) — in development
- Skatteetaten / a-melding (NO) — in development

Enrich with identity & payment data ↑

CUSTOMER SYSTEMS

HR & Accounts payable

Used to enrich Concur data before delivery — for example employee identity (SSN) from HR, and payment confirmation from accounts payable where required.

- HR: Workday, SuccessFactors, Oracle, Hailey, Concur fields
- Accounts payable: e.g. SAP S/4 supplier invoice API

Data flows from SAP Concur into Nordic Concur Connector, is enriched from customer systems when needed, then delivered to the relevant target system.

1 Connect
Company registers and connects via Concur App Center OAuth. Tokens are stored per corporation.

2 Fetch
Scheduled jobs pull paid expense reports and employee data from SAP Concur into the platform.

3 Enrich
Missing identity or payment data is filled from HR / accounts payable systems or import.

4 Deliver
Processed data is submitted to the configured target system connector, then status-polled.

Security & data protection

As data processor under GDPR (customer is the controller), Nordic Concur Connector protects employee and expense data with the following measures. A Data Processing Agreement is included in the Terms of Service.

Encryption
Personal data encrypted at rest and in transit. In transit, TLS 1.3 is preferred; TLS 1.2 is also available. Sensitive fields (including SSNs) are encrypted in the database.

SSN masking
Social security numbers are masked on the server before they reach the browser, so the full SSN is never sent to the UI for client-side masking.

Access control & SSO
Role-based access with corporation/company isolation. Single Sign-On (SAML / OIDC) supported for customer identity providers. Strong passwords, account lockout, and session timeout where password login applies.

EU data residency
Production servers are located in secure datacenters in the EU. Production customer data does not leave production servers.

No subprocessors
All processing happens inside the Nordic Concur Connector application. Customer data is not sent to third parties for processing.

Backups & monitoring
Daily backups to a secure remote location (retained 30 days). Servers are hardened and kept up to date. Breach notification commitments apply under GDPR.

Vulnerability scanning
Periodic vulnerability scans are performed to identify and remediate security issues in the application and infrastructure.

IN PROGRESS

Web application firewall
A WAF is being added in front of the web application to filter malicious traffic and strengthen edge protection.

Secure tax submission
KATRE filings are submitted over HTTPS with our client certificate (mTLS) and digitally signed XML, using Nordic Concur Connector's Vero PKI certificate.

Secrets hygiene
Integration credentials and secrets are protected in application configuration. Sensitive parameters (passwords, tokens, SSNs, certificates) are filtered from application logs.

Key management
Secrets and encryption keys are managed in a dedicated secrets management solution, centralizing and hardening handling of integration credentials and application secrets.

Tenant isolation
Multi-tenant design isolates each corporation's configuration, employees, expenses, and filings so customers only access their own data.