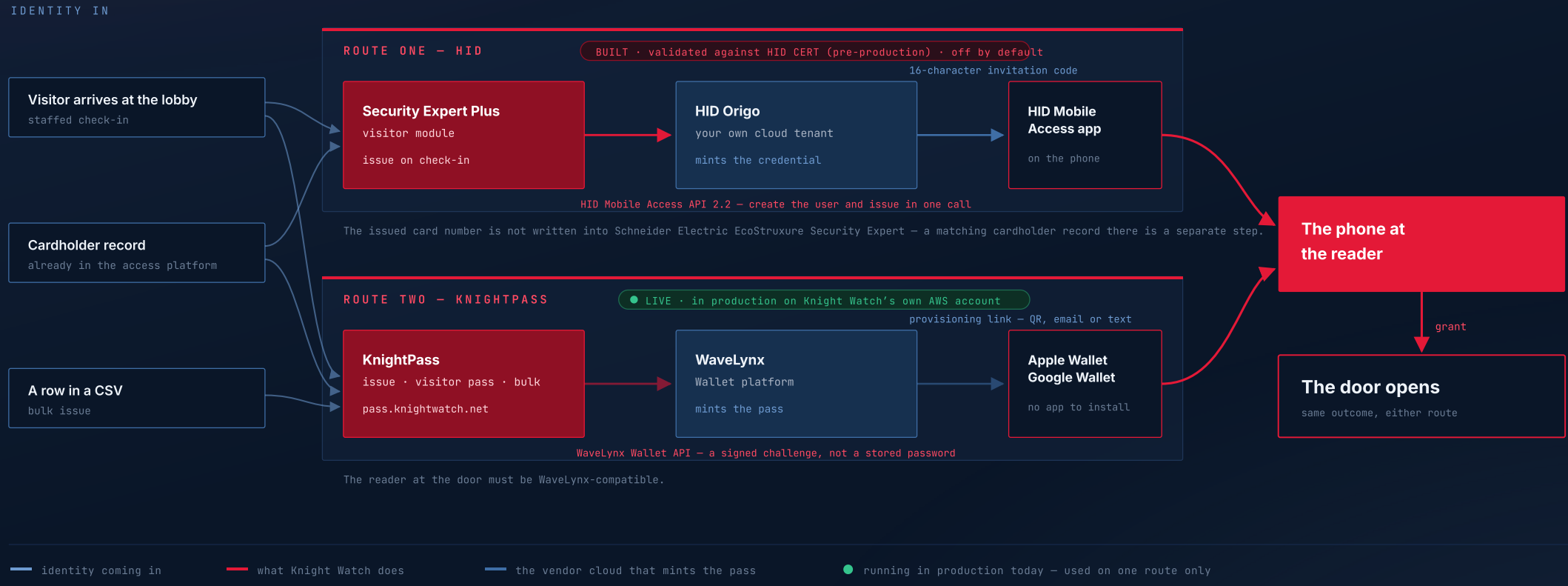
THE CATEGORY

The badge is already in their pocket

Every mobile credential does the same three things: turn an identity into a pass, put the pass in a phone, and let a reader at a door honour it. Knight Watch has built **two routes** into that. One is running in production today. One is built, hand-validated against the vendor's certification tier, and available on request. Which is which is printed on the board, not in a footnote.



Green means running in production today on Knight Watch's own AWS account — not a deployment at a named customer. It appears on one of these two routes. The HID integration is built and hand-validated against HID's CERT (pre-production) tier, ships disabled by default, and is not deployed in a production tenant, so it carries no green anywhere in this deck.

ROUTE ONE · HID

HID Origo, wired into Security Expert Plus

CARDHOLDERS, FROM THE USER PROFILE

Employee (cardholder) credentials can be issued and revoked by an operator from the user profile.

Honest status sits next to the capability, not after it. This integration is implemented, covered by tests, and hand-validated against HID's certification environment — and it is available on request. It is not running in production, and nothing on this board carries a green marker.

ROUTE TWO · KNIGHTPASS

KnightPass issues into Apple and Google Wallet

KnightPass is Knight Watch's own mobile credential platform. It provisions mobile access credentials into **Apple Wallet** and **Google Wallet** through the **WaveLynx Wallet API**, and it runs in production today on Knight Watch's own AWS account. Four ways to issue, all live — confirm the target WaveLynx environment with us before a pilot.

Direct device provisioning

One of the two underlying paths: the credential is provisioned directly to the device.

A wallet provisioning link

The console delivers the credential as a WaveLynx provisioning link — displayed as a QR code, or copied and sent by email or text. The holder opens it on their phone and adds the pass to Apple Wallet or Google Wallet. KnightPass itself has no end-user app to install.

A visitor pass with an active window

Issue a visitor pass with its lifetime set at the moment of issue — days, hours and minutes, from a five-minute minimum up to thirty days. The pass is provisioned into the visitor's phone wallet as an ephemeral guest credential, and the WaveLynx Wallet platform stops honouring it when the time is up. Nobody has to remember to switch it off.

Bulk issuance from a CSV

Upload or paste a CSV and issue a credential per row, with per-row results and a downloadable success/failure report.

Green marks what is running in production today on Knight Watch's own AWS account — not a deployment at a named customer. Which WaveLynx environment the live service points at is per-deployment configuration the repository does not record, and the code default is staging; confirm the environment with us before you plan a cutover.

AFTER ISSUE

Issuing is easy. Revoking is the product.

A credential you cannot take back is a liability. KnightPass listens to WaveLynx for the whole life of the credential and pushes each change into the customer's access control system through **one adapter contract** — with a retry ladder that gives up loudly rather than quietly.

COLUMN HEADERS — ILLUSTRATIVE SAMPLE

WAVELYNX STATUS	BACKEND ACTION	WHAT HAPPENS
ACTIVE	Provision	The adapter writes the credential into the customer's access control system
SUSPENDED	Suspend	The adapter suspends it
DELETED	Delete	The adapter deletes it
NOT_COMMISSIONED	— none —	Transitional. Deliberately no backend sync
PENDING	— none —	Transitional. Deliberately no backend sync

Green marks what is running in production today on Knight Watch's own AWS account — not a deployment at a named customer. The adapter contract carries no green: the generic webhook path is the one available today, and the three vendor-specific adapters ship in the same container but have not been validated against a live panel.

CONTROL AND AUDIT

Role-gated, audited, and scoped on purpose

A credential platform is a permission machine. It has to prove who issued what, refuse the people it should refuse, and be honest about the events it **does not** hold.

Microsoft Entra ID single sign-on

Operators sign in with Microsoft Entra ID single sign-on, single tenant. Those operators are Knight Watch staff: KnightPass ships today as an internal Knight Watch administration tool, not a customer self-service portal.

Admin is re-checked, not merely hidden

Administrative surfaces re-check the admin role against the database and return 403, rather than only hiding a menu item in the browser.

A credential-lifecycle record, not a door log

The audit trail is a credential-lifecycle record, not a door-event log. Reader taps stay in the access control platform, where they belong — one system of record per domain.

A limitation sits next to the capability it limits, on the board, not in a legal appendix. The audit ledger's coverage gap is printed above rather than discovered in your security review. Green marks what runs in production today on Knight Watch's own AWS account — not a deployment at a named customer.

HOW YOU BUY IT

What is live, what is only built

WHAT TO ASK FOR NEXT

LIVE — KNIGHTPASS

Running in production today on Knight Watch's own AWS account.

One route is live and one is built. That sentence is on every board in this deck, so this is the only place anyone has to look it up. Green marks what runs in production today on Knight Watch's own AWS account, not a deployment at a named customer.