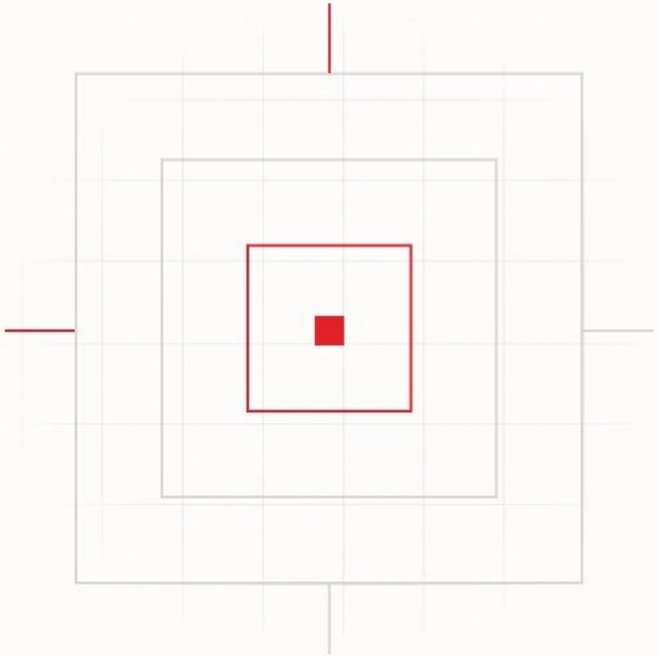
AmbiSecure

AMBIMAT
GROUP

EMBEDDED SECURITY · IDENTITY · HARDWARE-ROOTED TRUST

AmbiSecure

FIDO authenticators, JavaCard applets, secure elements, PKI and IoT trust — engineered by the Ambimat Electronics team, shipping since 1982.



EAL6+ SECURE ELEMENT

EST. 1982 · 40+ YEARS EMBEDDED ENGINEERING

ambisecure.ambimat.com
↗

AmbiSecure within the Ambimat Group

The security and trusted-identity business unit of Ambimat Electronics — an embedded engineering team that has shipped hardware since 1982 and identity systems since 2017.

EST.	EMBEDDED	IDENTITY
1982	**40+ yrs**	**since 2017**

> AmbiSecure is the embedded security and identity layer across the Group's connected products.

AMBIMAT GROUP

AmbiSecure SECURITY	**AmbiPay** PAYMENT	**AmbiSpace** AEROSPACE	**AmbiSense** MEDICAL
AmbiPower UTILITY	**AmbiLogistics** LOGISTICS	**AmbiCon** RETAIL	**AmbiAutomation** INDUSTRIAL

The AmbiSecure security stack

Enterprise · telecom · IoT systems	CONSUME
Device identity & authenticators	OnePass
Applets — FIDO · PIV · OpenPGP · IoT	JavaCard
AmbiSEC module — nano-card / MFF2	PACKAGE
Secure silicon — EAL6+ Secure Element	ROOT

— ONE TRUST CHAIN

Identity begins in silicon and travels intact to the application layer.

— ONE TEAM

Silicon selection, applet engineering, personalisation and validation — in-house.

— MANY SURFACES

Cards, USB keys, solderable modules and IoT applets share the same chip and certifications.

A chain that begins below the OS

Trust is anchored in an EAL6+ secure element and carried up through every boundary with verifiable transitions — not inherited from software that can be cloned or spoofed.

— Custom applets define how keys, credentials, identity and policy are enforced inside the trust boundary.

ROOT OF TRUST
Secure Element
EAL6+ certified silicon

VERIFY
Boot ROM & signed bootloader

MEASURE
Firmware — signed, anti-rollback

ATTEST
OS / runtime — isolated

CONSUME
App — FIDO · PKI · identity

Product & service portfolio

AUTHENTICATORS

OnePass ecosystem

OnePass Card
Multi-application FIDO2 smart card

OnePass Bio Card
On-card fingerprint biometrics

OnePass USB Key
FIDO2 / U2F security key

BioKey & Tappable
Biometric USB key & NFC tap

PLATFORMS & APPLETS

Engineering surface

AmbiSEC module
Nano-card / MFF2 · EAL6+ SE

Java Card applet services
Custom applets — auth, identity, PKI, IoT

IoT Security Co-Processor
Identity below the firmware

FIDO Validation Server
Multi-tenant WebAuthn SaaS

TRUST & IDENTITY

PKI · documents · telecom

Embedded PKI & signature
Tokens, PKCS#11, eIDAS flows

ePassport platform
ICAO 9303 · CSCA / DSC / PKD

DESFire / transit
SAM-backed offline fare trust

eSIM / SIM-Auth
eUICC & telecom identity

→ 13

One identity card. Phishing-resistant.

Replace badges and separate security keys with a single FIDO2 smart card — multiple identity roles, selectable on one EAL6+ secure element.

- ✓ FIDO2 / U2F passwordless
- ✓ PIV & OpenPGP roles
- ✓ Door access & NDEF
- ✓ Issuer keys & brand artwork

FOR · ENTERPRISE · GOVERNMENT · SECURE ACCESS

Backed by AmbiSecure's Java Card & secure-element engineering — adaptable to customer-specific workflows.

USB Key & BioKey

OnePass USB Key

A FIDO2 / U2F hardware key — plug in and tap to confirm presence. No codes to type, no software to run.

- ✓ FIDO2 & U2F, EAL6+ secure element
- ✓ No battery, no network required
- ✓ Compact, metallic, waterproof options

BioKey

The biometric USB security key — adds an on-device fingerprint to hardware-bound credentials for higher-assurance access.

- ✓ On-device biometric verification
- ✓ Anchored in an EAL6+ secure element
- ✓ Phishing-resistant by construction

FIDO2 & modern authentication

Public-key cryptography replaces shared-secret passwords. The private key never leaves the authenticator — phishing-resistant by construction.

Authenticator
Card · USB · BioKey

⇄

Relying party
App · service

⇄

Validation Server
Attestation · MDS

PUBLIC-KEY CEREMONY · THE PRIVATE KEY NEVER LEAVES THE DEVICE

- ✓ Passwordless & phishing-resistant MFA
- ✓ FIDO2 / WebAuthn / CTAP2 & passkeys
- ✓ Secure-element-backed credentials
- ✓ Multi-tenant validation server, REST + JS
- ✓ Secure-element applet development for credential policy & lifecycle

AmbiSEC module & Java Card engineering

We architect, build, personalise and validate applets in-house — shipped on the same EAL6+ secure element as a nano-card or solderable MFF2 module.

01
Silicon
EAL6+ secure element

›

02
Applet
FIDO · PIV · OpenPGP · IoT

›

03
Personalise
SCP03 load · key derivation

›

04
Form factor
Card · USB · MFF2 module

›

05
Validate
FIDO Validation Server

JavaCard 3.x | GlobalPlatform | SCP03 | JCOP 3.1 | CAP files

Read more → JavaCard ↗

Java Card applet development services

Custom secure-element applets — for authentication, identity, PKI, secure messaging and IoT trust — engineered on EAL6+ silicon.

01 Discover
Use case, threat model, APDU surface

›

02 Architect
Data model & security design

›

03 Develop
Java Card applet & policy logic

›

04 Personalize
Keys, GlobalPlatform, host interface

›

05 Validate
APDU, edge-case & lifecycle tests

›

06 Deploy
Nano-card, MFF2, AmbiSEC, product

DELIVERED WITH

- APDU & data-model design
- GlobalPlatform / SCP03
- Key storage & lifecycle
- Testing under real SE constraints

Read more → Java Card applets ↗

IoT device identity & lifecycle

PHASE 01 Factory

01 · MANUFACTURE
EAL6+ secure element / AmbiSEC module integrated

02 · PROVISION
Keys, certificates, applets & identity material

→

PHASE 02 Field

03 · DEPLOY
Device enters field or customer environment

04 · AUTHENTICATE
Device proves identity cryptographically

05 · OPERATE
Encrypted, attested operation

06 · UPDATE
Signed firmware & secure lifecycle policy

→

PHASE 03 End of life

07 · RETIRE
Key revocation & secure decommissioning

Embedded PKI, attestation & key custody

Root CA / trust anchor ANCHOR

Issuing CA

Device / credential certificate

Key generated in the EAL6+ secure element

Attestation → relying party validates

— KEY CUSTODY

Keys are generated inside the secure element and never exported.

— ATTESTATION

AAGUID and attestation certificates injected at personalisation.

— PKCS#11 · eIDAS

Audit-grade issuance, renewal and revocation under policy.

eSIM / SIM-Auth — the same trust, in telecom

The eUICC is itself a secure element — so the same EAL6+ secure-element and key-custody expertise extends into telecom-grade embedded identity.

- ✓ SGP.22 / SGP.32 eUICC remote provisioning
- ✓ OpenID Connect applet, automotive & M2M variants
- ✓ Hardens SMS OTP with SIM-rooted authentication

DEDICATED PLATFORM

SIMAuth

The eSIM / eUICC story lives on its own site.

esim.ambimat.com ↗

Services & engagement model

WHAT WE DELIVER

- ✓ Architecture & product security design review
- ✓ Secure-element feasibility & silicon selection
- ✓ Java Card applet development — define to deploy
- ✓ Personalisation, certification & deployment support

HOW ENGAGEMENTS ARE SCOPED

Architecture review | **Pilot** | **Prototype / sandbox**

Integration | **Secure manufacturing** | **Rollout**

> Most engagements start as “we need something like X, but with Y.” One accountable team takes it from there.

Target sectors & use cases

01

Government & defence

PIV, eID & ePassport identity programmes

02

Enterprise IT & CISOs

Passwordless workforce & device trust

03

Banking & fintech

Strong auth & transaction integrity

04

Connected mobility & IoT OEMs

V2X PKI & device identity in silicon

05

Transit & smart cities

SAM-backed offline fare & access trust

06

Telecom operators

eUICC & SIM-rooted authentication

An embedded team, not a security boutique

> AmbiSecure combines embedded engineering, secure elements, applet development, hardware-rooted identity and authentication products — not just software security.

GENERIC IoT / SOFTWARE SECURITY VENDOR

- Ships apps, dashboards & software agents
- Trust stops at the software layer
- Integrates someone else's secure element
- Three vendor handoffs, three RFPs

AMBISECURE

- ✓ Owns trust from silicon to validation server
- ✓ In-house JavaCard, FIDO & personalisation
- ✓ Ships hardware products, not just software
- ✓ One accountable team, 40+ years embedded

A security problem that lives in hardware?

Talk to engineers, not BDRs. Tell us what you are building and we'll tell you what is realistic, standards-aware, and shipped before.

SECURITY PLATFORM

AmbiSecure

ambisecure.ambimat.com ↗

eSIM PLATFORM

SIMAuth

esim.ambimat.com ↗

THE GROUP

Ambimat

ambimat.com ↗

AmbiSecure · Ambimat Electronics · Ahmedabad, India

 ↗