Solution Brief

THALES
CYBERSECURITY



Thales OneWelcome European Digital Identity Wallets and Verifiable Credentials

cpl.thalesgroup.com

THALES

CYBERSECURITY

European wallet and verifiable credential support within the OneWelcome Identity Platform

The OneWelcome Identity Platform extends CIAM with capabilities for European digital identity wallets and verifiable credentials. It provides a common layer for connecting EUDI Wallets, national eIDs, commercial wallets and existing identity-verification methods, while applications continue to use established identity standards. The platform supports credential presentation and verification, trust policy, consent, attribute mapping, identity matching, journey orchestration and credential issuance.

European market context

The European identity ecosystem is expanding from national eIDs and document-based verification toward portable, user-controlled credentials. Under the European Digital Identity framework, Member States must offer wallets that can link national identity with attributes such as driving licences, diplomas and bank-account information. Affected service providers that are legally required to identify customers unequivocally will need to support wallet-based verification. In practice, EUDI Wallets will coexist with national eIDs, commercial wallets, passkeys and established verification methods. Organisations therefore need an architecture that can accommodate different issuers, credential formats, assurance levels and customer adoption patterns.

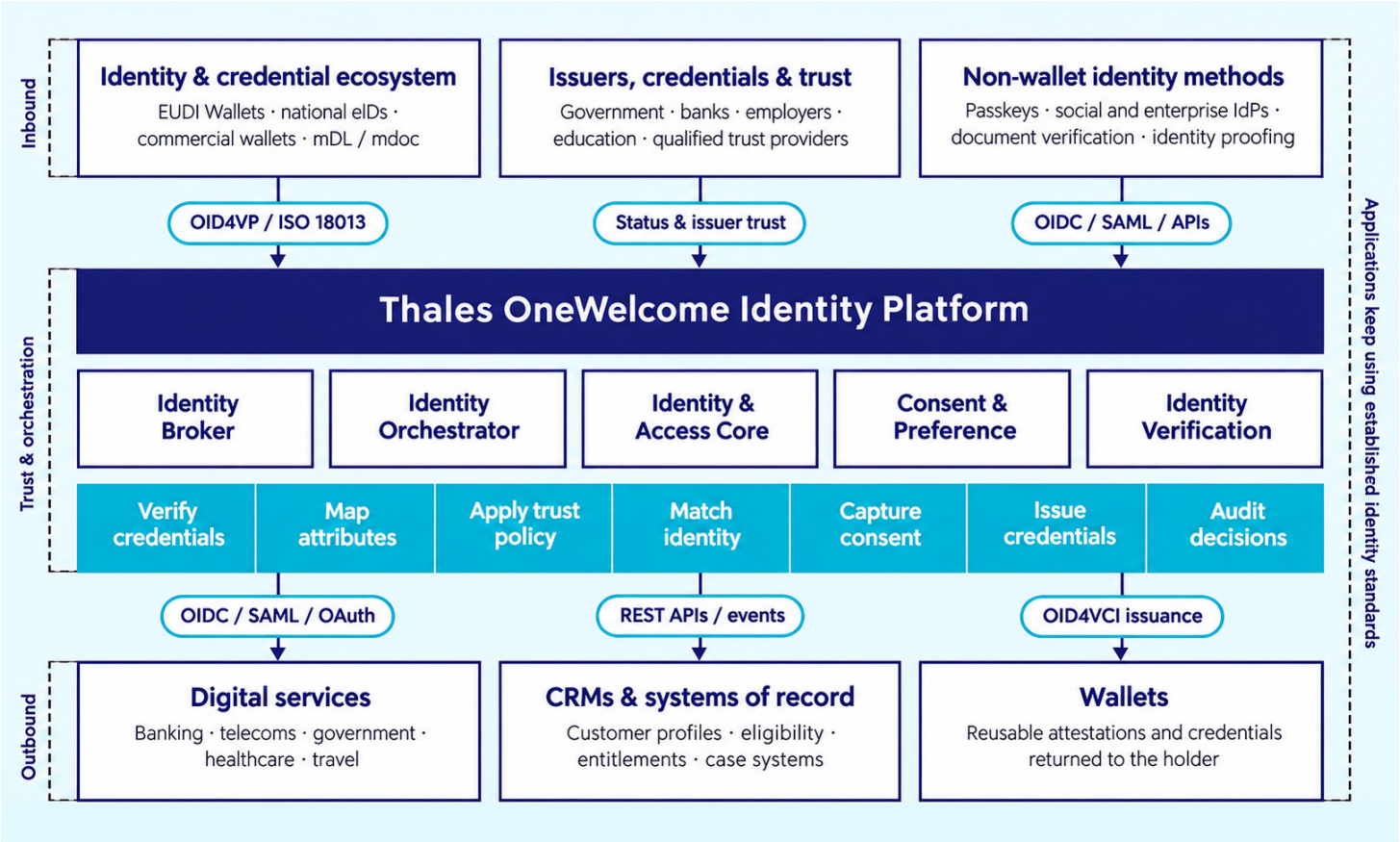
- **A diverse identity ecosystem:** EUDI Wallets, national eIDs and commercial schemes may use different credentials, issuers, trust frameworks and attribute models.
- **Coexisting customer journeys:** Wallet adoption will vary by country and use case. Services may need to support same-device, cross-device and non-wallet journeys in parallel.
- **Policy and data control:** Organisations need to define accepted issuers, credentials, assurance requirements, requested attributes and retained evidence for each journey.

Capabilities within the OneWelcome Identity Platform

A shared trust and orchestration layer for wallet and non-wallet identity methods.

- **Wallet connectivity and verification:** Receive standards-based credential presentations, validate issuers and credential status, and map attributes from EUDI, national and commercial schemes into the identity context used by applications.
- **Wallet-based authentication:** Enable customers to authenticate or perform higher-assurance step-up using verified credentials from compatible digital identity wallets, with consent, trust-policy evaluation and identity matching managed within the OneWelcome Identity Platform.
- **Identity journey orchestration:** Configure onboarding, sign-in, step-up and recovery journeys that can include wallet selection, consent, identity matching, same-device and cross-device interactions, API calls and non-wallet alternatives.
- **Credential issuance:** Create standards-based issuance journeys that place reusable attestations or business credentials into compatible wallets, introduced independently or alongside credential verification based on the use case and ecosystem readiness.

The capability allows wallet interactions to be handled within the wider identity platform, rather than implemented independently in each application. This can simplify integration, support consistent policy and allow wallet and existing identity methods to operate together.



Within this model, wallet support complements existing CIAM, federation and identity-verification capabilities. Applications can continue to use established protocols while the platform handles wallet presentation, trust evaluation, attribute mapping, consent and issuance.

Supported journey patterns

Onboard

Verify identity and relevant KYC attributes from a wallet, with document and identity-verification fallback.

Authenticate

Use wallet credentials for sign-in or higher-assurance step-up in existing applications.

Issue

Return reusable proof of customership, employment, qualification, eligibility or entitlement to a wallet.

Recover

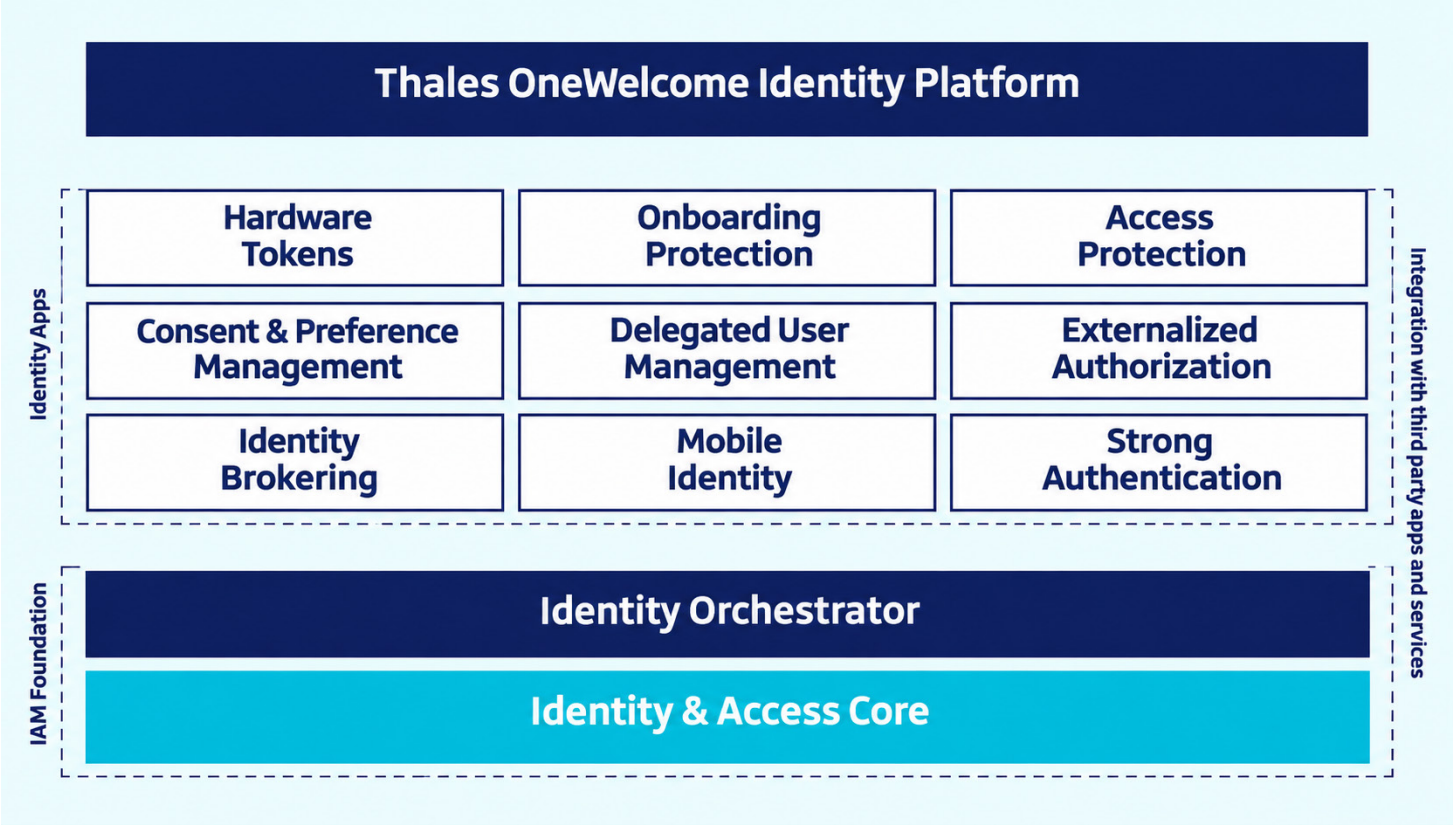
Re-establish trust using verified wallet attributes, existing factors and risk-aware orchestration.

Platform characteristics

- Common integration layer for standards-based wallet and non-wallet identity schemes.
- Central configuration of accepted issuers, credentials, attributes and assurance policies.
- Support for same-device, cross-device and alternative identity journeys.
- Consent, data-minimisation policy and evidence associated with verification decisions.
- Integration with existing CIAM capabilities, from credential verification to credential issuance.

Key Benefits

- **Wallet-Ready Without Rewriting Applications:** Wallet presentation and trust evaluation run in the platform, so existing applications keep their current OIDC or SAML integrations.
- **One Trust Policy Across Schemes:** Accepted issuers and assurance levels are configured centrally and applied to every journey, whatever wallet or eID the customer brings.
- **Faster Onboarding Where Wallets Exist:** Verified KYC attributes come straight from the wallet. Document verification stays in place as the fallback for customers who don't have one yet.
- **Data Minimisation With an Audit Trail:** Each journey defines exactly which attributes it requests and keeps the consent and verification evidence behind every decision.
- **Credentials Issued Back to the Customer:** Return reusable proof of customership or eligibility to the customer's wallet, turning a verified relationship into something they can present elsewhere.



About Thales

Thales is a global leader in cybersecurity, helping businesses, governments, and the most trusted organizations in the world protect critical applications, sensitive data, identities, and software anywhere, at scale — with the highest ROI. With more than 30,000 customers, including 58% of the Fortune Global 500, our solutions are deployed in 148 countries around the world. Through our innovative services and integrated platforms, Thales helps customers achieve better visibility of risks, defend against cyber threats, close compliance gaps, and deliver trusted digital experiences for billions of consumers every day.

© Thales - November 2026 • HP • V3

cpl.thalesgroup.com

Contact us – For contact information, please visit cpl.thalesgroup.com/contact-us