Solution Brief

Thales OneWelcome
Identity Platform

Identity Broker

cpl.thalesgroup.com

THALES
Building a future we can all trust

THALES
Building a future we can all trust

In today's complex digital landscape, the success of your business depends on secure, compliant, and flexible tools for managing the identities of employees, customers, partners, gig workers and more. The Thales OneWelcome Identity Platform is an adaptable, modular solution offering your users a frictionless and trusted experience throughout their journey, no matter which channel they use to engage with your brand.

The Thales Identity Broker capability allows you to seamlessly enable external Identity Providers (IDPs), identity wallets and login through social providers.

Quickly enable Federated Authentication & Registration

Access to Social Login providers (Google, Facebook, LinkedIn, Apple, X.), known IDPs (ID.me, DigiD, eHerkenning..), eIDs, SAML or OpenID Connect

Multiple Flows for Federation Requests

Start with Authentication, requiring minimum user information. Support Identification for a more enhanced onboarding user journey

Future Proof

Integrations for Self Sovereign Identity wallets & Zero Knowledge Proof available in user journeys

Meeting the evolving demands of Bring-Your-Own-ID or BYOI

One of the developing elements in today's security landscape is the need for external identity providers (IDPs) for both authentication and identification. This trend is driven by regulatory requirements, business needs, and evolving user expectations. Some analysts predict that Bring Your Own ID (BYOI) will surpass organization-provided IDs, while digital wallets are emerging as a new component in this spectrum.

For prospect logins, social identities provide a quick way to create accounts without requiring strong identification initially. However, many organizations struggle with implementing and maintaining these integrations, especially when compliance evidence is required annually.

Identity federation challenges and how Identity Broker Helps

Organizations typically face several challenges when implementing federated identity solutions:

Most federated identity schemes use open standards but implement advanced features or proprietary extensions that complicate integration. Each identity schema uses different attribute names, making integration with multiple schemas simultaneously complex. Setting up and maintaining trust relationships with external IDPs requires significant effort, and the rapidly evolving global market demands constant updates to support new technologies and schemas.

By acting as an intermediary service, the Identity Broker connects your applications with different identity providers, eliminating the need to individually integrate every IDP into your apps, significantly reducing complexity and maintenance overhead.

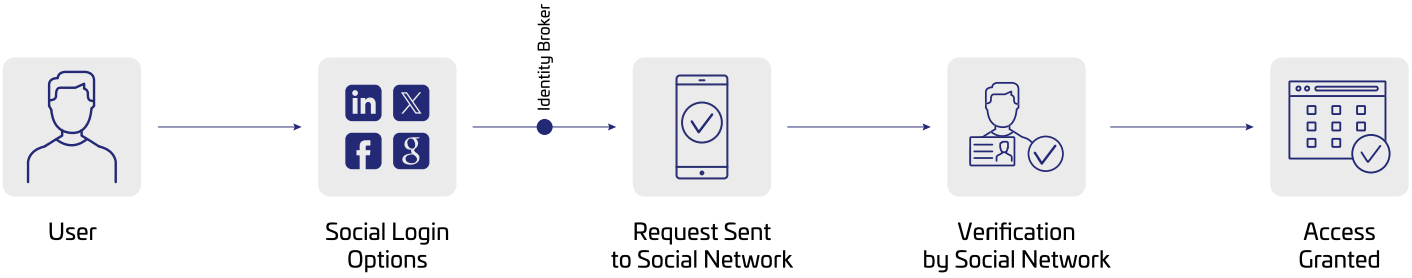
The Thales OneWelcome Identity Platform's Identity Broker solution

The Thales OneWelcome Identity Broker was built from the ground up following three core principles:

- ### Privacy by design
  The Identity Broker does not persist Personal Identifiable Information (PII). Its transactional approach ensures that PII is removed immediately after first use, providing maximum privacy protection for your users. This approach helps your organization maintain compliance with privacy regulations while still enabling seamless authentication experiences.
- ### Universal compatibility
  The Identity Broker works with any type of identity provider through open protocols. It supports standard authentication protocols and many proprietary extensions, ensuring compatibility with a wide range of identity providers. Its flexible architecture allows for adding new protocols and extensions based on customer demand.
- ### Simplified management
  The user-friendly admin panel makes it easy to set up new connections and manage existing ones. The attribute mapping feature normalizes attributes from different schemas according to your requirements, significantly reducing the complexity of Identity Broker

Identity Broker

User Journey - Social Login



01

The **user** arrives at the **login page** and is presented with **Social Login** options

02

The **user** is given the opportunity to choose one of the presented **Social Networks**

03

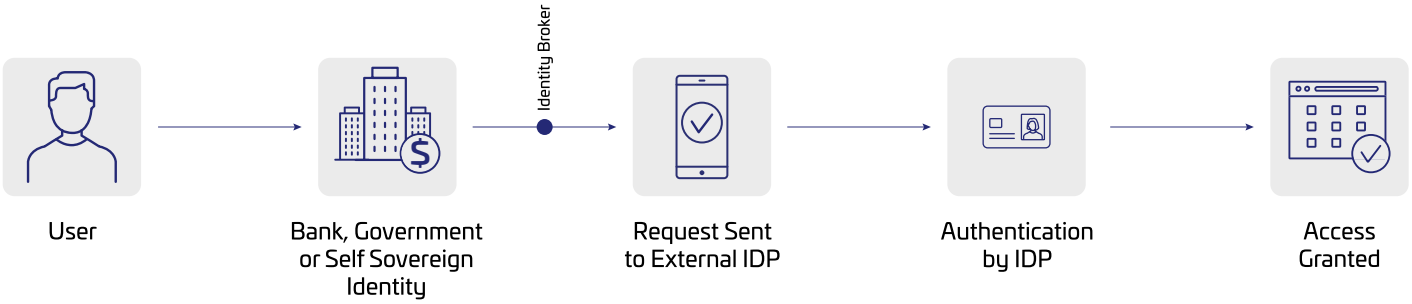
The **login request** is sent via **Identity Broker,** to the **Social login provider**

04

Once validated by the **Social login provider,** the user is granted access to the application

Identity Broker

User Journey - Extrenal IDPs (Bank, Government or Self-Sovereign Identity Providers)



01

The **user** arrives at the **login page** with **Bank, Government** or **Self Sovereign Identity** options

02

The **user** is given the opportunity to choose one of the presented external **Identity Providers**

03

The **login request** is sent via **Identity Broker,** to the external **Identity Provider**

04

Once validated by the **External IDP,** the user is granted access to the application

Key features and capabilities

Comprehensive protocol support

The Identity Broker supports a wide range of authentication protocols and standards:

Generic SAML with redirect, POST, and artifact binding, plus signing, encryption, and mTLS support. Generic OIDC with client secret basic, post and JWT authentication, signing and encryption support, and both ID token-only and userinfo modes. Generic OAuth 2.0 with opaque tokens. Integration with social IDPs like Google, Facebook, and Apple. Support for government identities like DigiD and eIDAS (via eHerkenning), and Pro Sante Connect.

Advanced capabilities

The Identity Broker provides several advanced capabilities that enhance your identity management system:

Attribute mapping normalizes attributes from different schemas according to your requirements. External IDP selection based on domain name (company SSO through Home Realm Discovery), ACR, or scopes provides flexible authentication options. Direct integration with the OneWelcome Identity Platform ensures seamless operation within the Thales ecosystem. Just-in-time user creation automatically creates and updates user accounts in the identity store with data received from external IDPs.

Identity Broker

User Journey - Social Login

Support Social Login and BYOI

Identity Broker acts as a trusted intermediary for federated registration and authentication to known social networks, such as Facebook, Google, Linkedin, X and more

Out of the Box integrations with Public IDPs

Select from pre-integrated and certified integrations with known IDPs such as ID.me, IDN, eHerkenning, DigiD, Itsme, FranceConnect, EU-ID, Finnish Trust Network and more

IDP's using Open Protocols

Configure and connect to any IDP using open protocols such as SAML, OAuth or OpenID Connect

Just-in-time User Creation

Create user accounts in the Identity Store with data received from external IDPs - user account details updated automatically each time user logs in

Point and click interface

Use our web-based console to select pre-integrated IDPs, or use it to configure SAML, OAuth or OpenID Connect ready external IDP's

The Identity Broker is a key component of the OneWelcome Identity Platform, which provides a complete solution for managing all types of digital identities. As part of this comprehensive platform, the Identity Broker works seamlessly with other components like User Journey Orchestration, Identity Verification & Affirmation, Consent & Preference management and Delegated User Management to provide a complete identity management solution.

By choosing the Thales OneWelcome Identity Broker, you gain reduced integration complexity, enhanced security and privacy compliance, improved user experience through simplified authentication, and a future-proof architecture ready for emerging identity technologies—all backed by a global leader in digital security solutions.

Thales. Building a future we can all trust.

About Thales

Thales helps organizations protect sensitive data and software and deliver seamless digital experiences, with advanced encryption, identity and access management and software licensing solutions.

cpl.thalesgroup.com

Contact us – For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us

Thales - May 2025 • HP • V2