

TRANSMIT PLATFORM

Datasheet Version 4.0 2019 ©

Transmit is a cross-channel identity platform designed to simplify, accelerate, and reduce the cost of identity-related projects, such as authentication, authorization, fraud detection, and account opening.

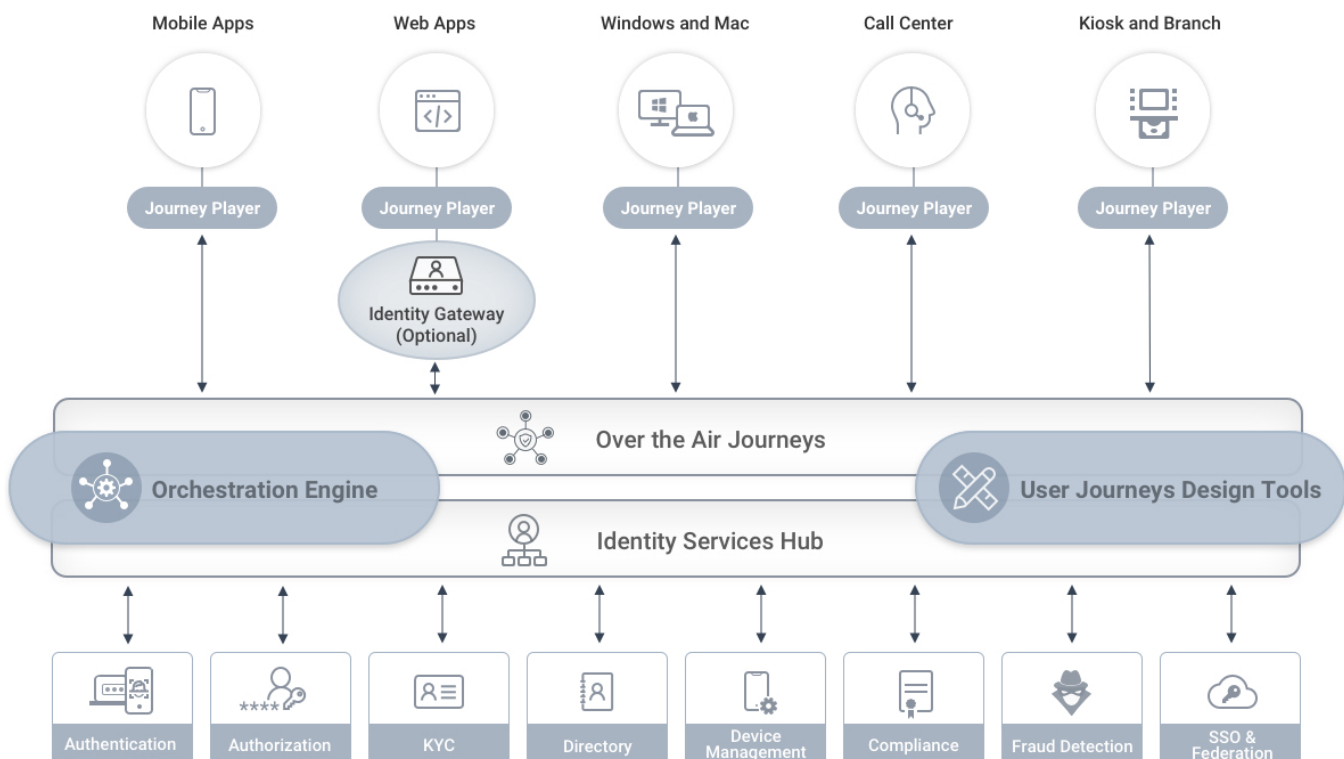
The platform allows enterprises to consolidate and accelerate multiple initiatives in the identity space while still supporting their existing IAM technologies, if needed. The platform's built-in services save massive development, maintenance, and license costs, allowing faster adoption of innovation while avoiding building more "legacy."

The Transmit platform supports both customer-facing use cases (CIAM) and workforce use cases (IAM). The platform's modular **Identity Services Hub** allows connecting existing third-party services such as authenticators, identity-proofing tools, directories, and risk engines, or simply using out-of-the-box services provided by Transmit, in any of these categories.

Over-the-Air Journeys is the technology that sets Transmit apart from all other vendors. With Over-the-Air Journeys, application owners can use graphical tools and an orchestration language to design simple and complex user journeys that involve authorization, authentication, KYC, fraud prevention, regulatory requirements, and more. Once done, these journeys can be pushed "over the air" and played in any application that is connected to Transmit, without making any code changes to the application and without the need to re-publish the application.

Top Use Cases:

- Biometrics, Behavioral, Social Login, and FIDO
- Account Opening and KYC
- Strong Customer Authentication
- Transaction Signing
- Multi-Factor Authentication
- Risk Engine Orchestration
- Machine Learning Fraud Prevention Techniques
- Using the Mobile Device Across Channels
- Call Center Authentication and Transaction Approval
- Self-Service
- Enterprise Passwordless Login
- Soft Token and TOTP
- Directory Services and Directory Aggregation
- Federation Services and SSO
- IoT and API Access Management
- Device ID, Device Risk and Device Management
- PSD2 and Regulatory Compliance
- Web Access Management
- Zero Trust Networks



Platform Services	Description
Authentication	Full set of authentication services to manage primary login, multi-factor, and step-up authentication across various applications and channels. The platform includes a large set of built-in authenticators such as OTPs, soft tokens, biometric authenticators, and knowledge-based authenticators, and full FIDO support.
Authorization	Role-based access control (RBAC) and attribute-based access control (ABAC) services across all applications. Use a built-in entitlement store or read and orchestrate entitlements and risk indicators from multiple sources.
Risk and Fraud Detection	Built-in behavioral profiling capabilities. Automatically profile devices, locations, access times, activities, transactions, payments, and many other factors. Machine learning for device identification to add trust in known user devices. Orchestration of third-party fraud detection engines using simple graphical design tools.
Directory	Bring your own directory from any vendor and connect it to the Transmit Identity Services Hub or just enable the built-in LDAP-based directory that is already included in the Transmit platform. Transmit also includes modern APIs which can be used to access directory information as an alternative to LDAP.
Identity Gateway	A Zero-Trust reverse proxy that sits in front of applications or APIs and enforces authorization and authentication policies without the need to make any changes to applications. Typical use cases include controlling access to hundreds of web applications and the replacement of outdated Web Access Management solutions.
Device Management	Transmit automatically tracks all devices for each user (laptops, computers, mobile devices, and tablets) and provides the tools to bind these devices and build trust in them. This process uses cryptography to secure the channel between the device and your systems and to mutually authenticate the device.
Regulatory Compliance	Manage identity-related regulatory requirements for privacy and authentication. PSD2 RTS capabilities for strong customer authentication are provided out of the box with full control over the user experience. Managing consents and managing identity-related information are integral parts of the platform.
Single Sign On	The platform can serve as a federation IdP or SP and includes support for SAML, OpenID Connect, and OAuth. The platform includes built-in device identification technologies that can automatically identify a user who is using the same device to access more than one application.
Account Opening	Build account opening journeys by orchestrating Know Your Customer (KYC) and identity-proofing tools, such as scanning a government identity card and comparing the photo on the card to a live video stream of the user's face. Access third-party databases such as Mobile Network Operators for identity validation.



An average of 80% in cost saving for new identity use cases



Used by 6 of the top 8 banks in the US



Supporting tens of millions of users and events



Deploy on-premise, in the cloud or in hybrid mode



Graphical tools for designing user journeys



No software code required when changing user journeys