For more information visit www.indykite.com

A financial services provider boosted consent capabilities with IndyKite to share protected data

With a large number of citizens and 300,000+ businesses and public sector agencies reliant on its identity services, our customer was looking to enhance its products and services, while increasing revenue.

As such a trusted entity both by end-users, merchants and government, the company is in a unique position to enable seamless and secure user journeys that create benefits for both merchants and end-users.

Merchants currently spend significant amounts of resources managing customer contact data. Our customer saw an opportunity to ease this burden, while empowering the end-user with control over their data.

The customer wanted to enable the end-user with consent options for sharing contact data from its application to 3000+ merchants reliant on its identity services. Depending on the use case, this could be relatively straightforward, or quite complex depending on the data, who owns it and who is entitled to share it and for what purpose.

Opportunity

- ✓ New service offering for 3000+ merchants
- ✓ Improving customer retention and customer value
- ✓ Seamless experience for end-users
- ✓ Market positioning for eIDAS standards
- ✓ Basis for service expansion in the future

Challenge: current consent controls too coarse and restrictive

To enable this data sharing service, our customer required hyper-granular consent controls that could scale and provide enough flexibility to adapt to a changing regulatory environment (with the eIDAS standards currently in development).

Currently consent is most often captured at login or authentication. Our client needed flexibility to capture it at any point in the customer journey and push notifications to vendors when the end-user had approved sharing of new data.

In addition, the customer required secure, high-trust sharing protocols to protect customer contact data, sharing only approved individual data points (i.e. email address) to specific approved merchants, rather than all-or-nothing sharing solution.

Further, each merchant may collect different types of data with different categories or ways of categorizing data. To scale, the solution must be able to handle a high level of complexity.

Solution: Flexible and granular high trust data sharing framework

With IndyKite's solution, the customer was able to establish hyper-granular and flexible consent controls for seamless sharing of first-party data.

The end-user can now make updates/changes to first-party data in the customer's application. Instead of having to alter contact details for all services and accounts the user might have with various merchants, the user can action this update within the application and relevant merchants will be notified of the new data shared and ready for collection.

This enables the merchants to passively receive updated first-party data, without disrupting the end-user journey. This saves cost for the merchant, improves customer experience (one update instead of many), and offers a new revenue stream for our customer.

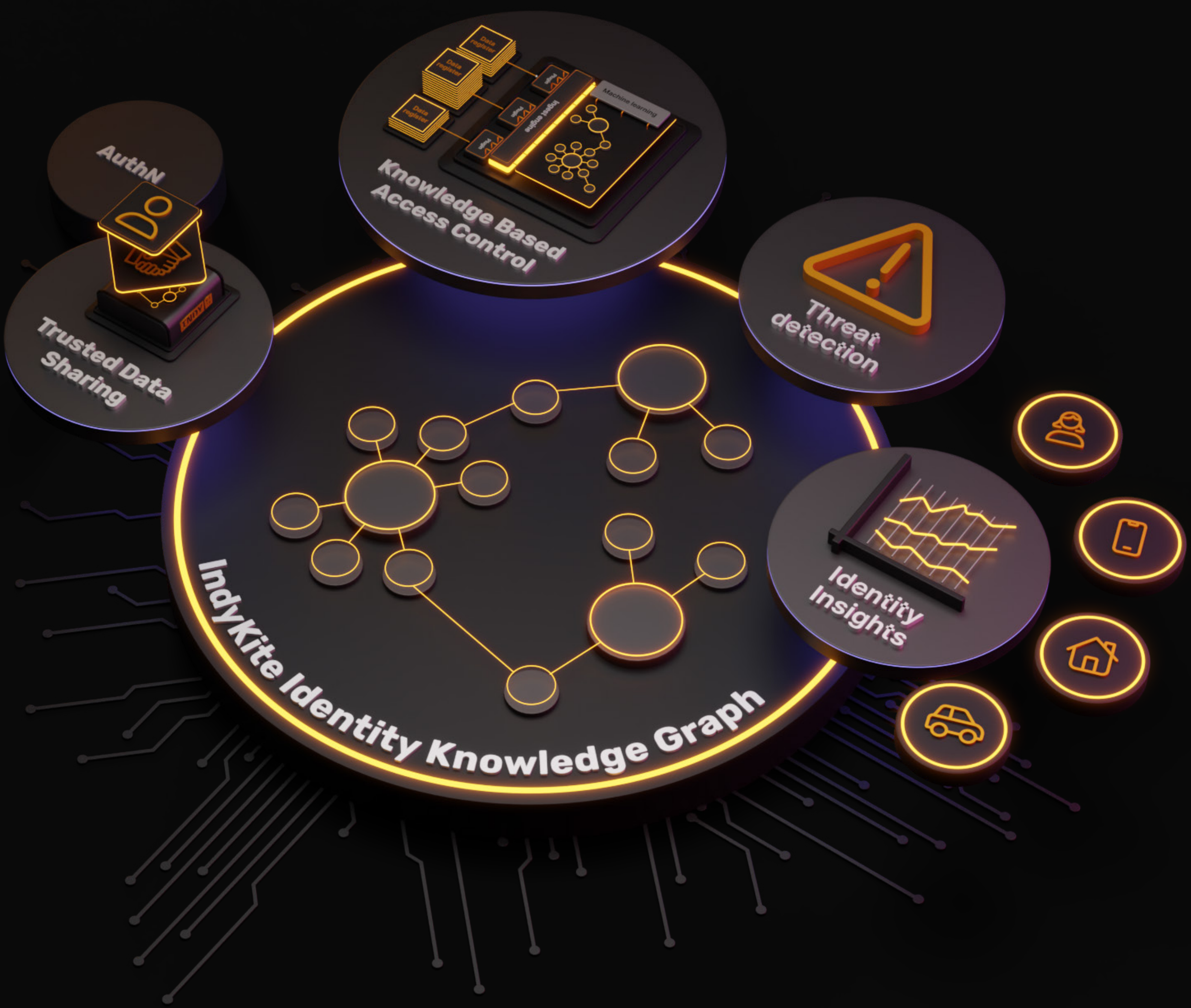
IndyKite delivers

Granular and flexible consent framework

Efficiency saving and value creation for both merchants and end-users

Secure sharing of protected data within a partner ecosystem

User empowerment to share first-party data


AuthN
Trusted Data Sharing
Knowledge Based Access Control
Threat detection
Identity Insights
IndyKite Identity Knowledge Graph

Want to learn more?

For more information on how IndyKite can help you share protected data, Book a Demo.

INDY KITE