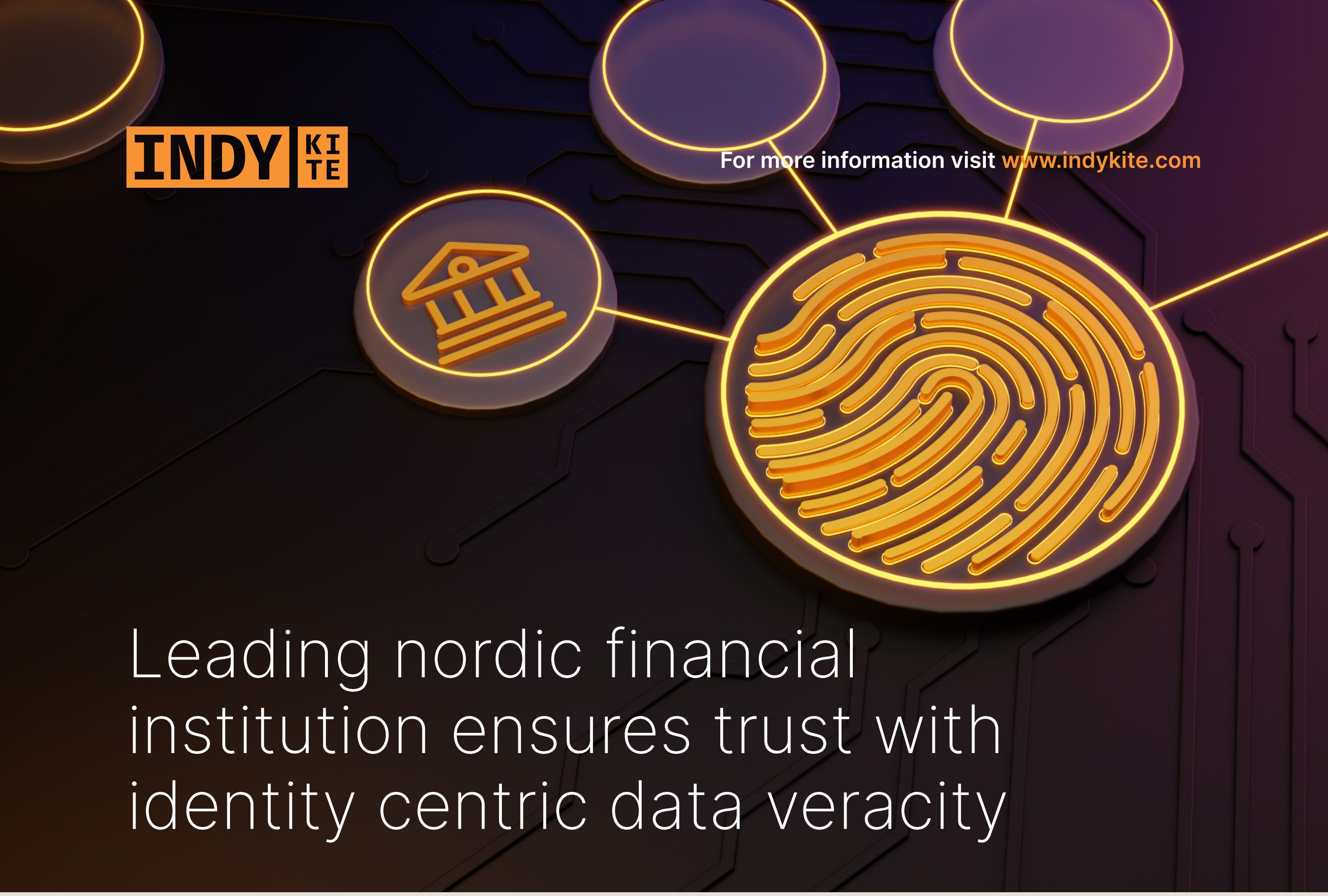


For more information visit www.indykite.com

Leading nordic financial institution ensures trust with identity centric data veracity

With a large number of citizens and a robust network of 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 provide trusted first-party data on to its partners by empowering its end-users with granular consent controls in its application. 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
- ✓ End-user empowerment over own data
- ✓ Seamless experience for end-users
- ✓ Market positioning for eIDAS standards
- ✓ Basis for service expansion in the future

Challenge: sharing protected data in a trustworthy, secure and useable way

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: deploying safe and secure tooling to collect and manage user data

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.

By deploying Trusted Data Sharing, our customer can be certain that they are managing the risk of dealing with data in two ways. Data validated and received directly from the customer is the most trusted data source of truth. Secondly, Trusted Data Sharing provides a mechanism to track, monitor and audit data collection for compliance and security at the organization.

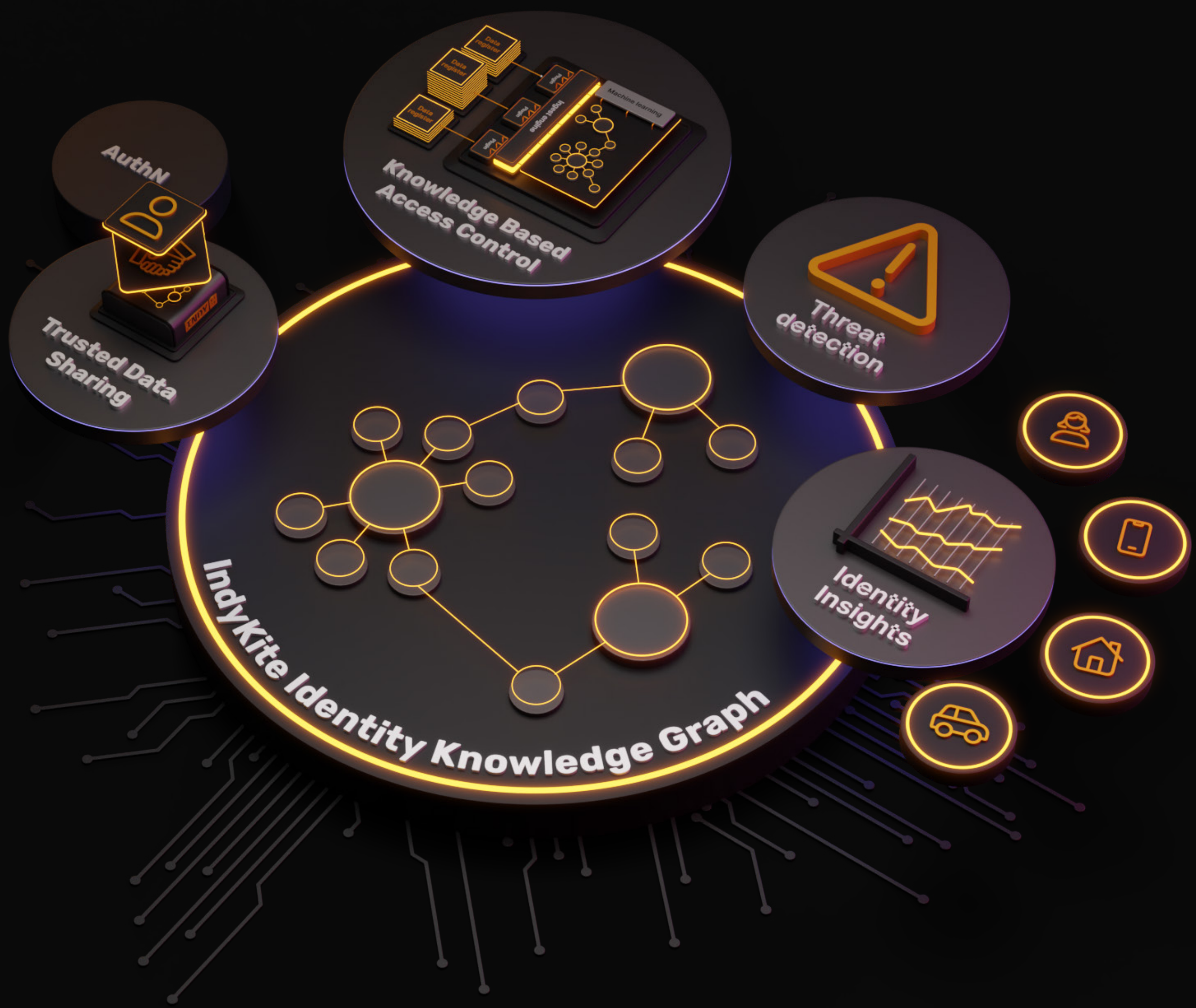
IndyKite delivers

Granular and flexible consent framework

Increased compliance and security tracking to deliver peace of mind and maintain customer trust

Secure sharing of protected data within a partner ecosystem

Data veracity delivered from first party data collection


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

Want to learn more?

For more information on how IndyKite can help you build trust into your data, Book a Demo.

INDY KI TE