

# Digital authentication

New opportunities to enhance the customer journey



Customer expectations for seamless experiences are being raised every day, and businesses must focus on delivering superior user experiences—or risk losing business. At the same time, experiences are moving online and to mobile as fraud attacks become more sophisticated.

How can businesses create elegant user experiences with effective fraud prevention?

By intelligently deploying targeted authentication tools that cut through the confusion of the authentication landscape.

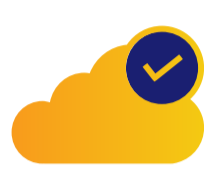
## Navigating the complex authentication landscape and establishing a common lexicon

### Detection



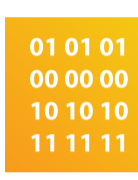
The ability to identify suspicious patterns indicative of fraudulent activity.

### Authentication



Assesses the likelihood that a person is who they say they are. This is validated using something they have, something they are or something they know.

### Verification



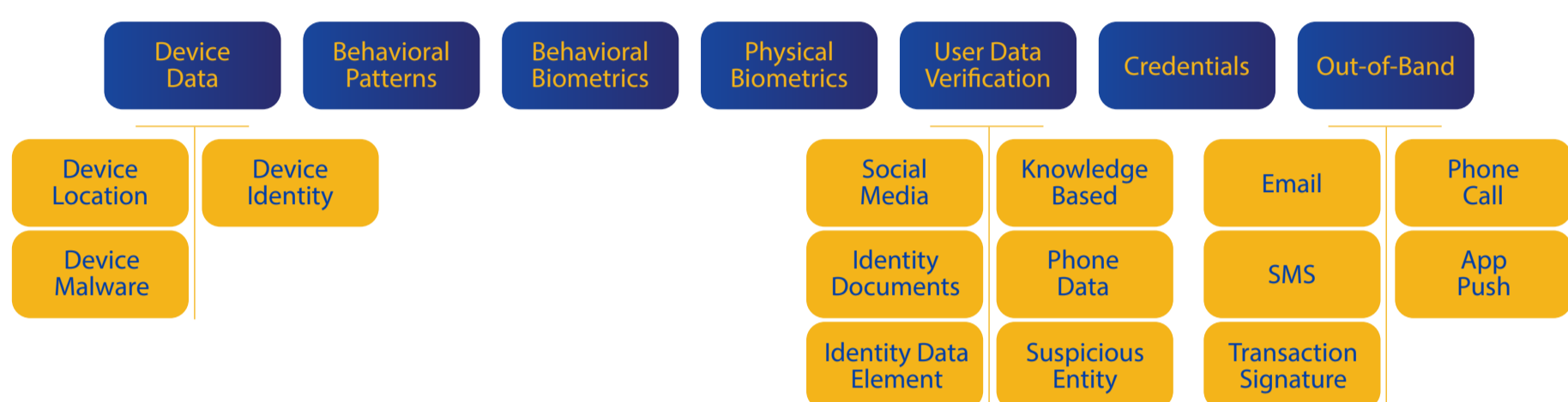
A subset of authentication. Compares the data input by the user with external data sources to determine the likelihood that the person presenting the data is legitimate.

### Authorization



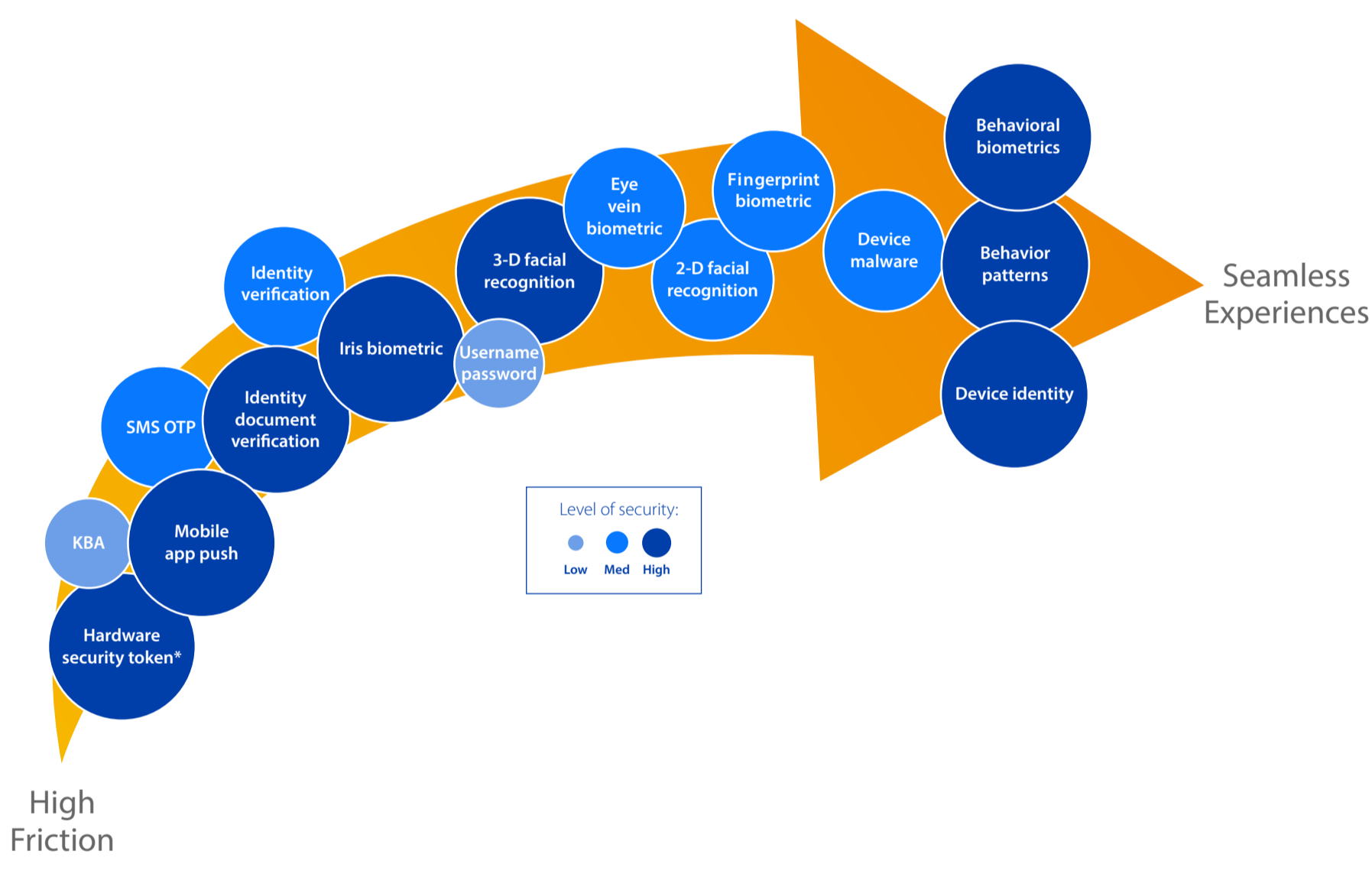
Asserts that the person is permitted to perform an action. The issuing bank then determines whether to approve or decline a given transaction.

## Authentication methods—breadth and depth



## Balancing ease of use and security

Businesses want to mitigate fraud, but that's often at the expense of a good user experience. It doesn't have to be. Here is how different authentication solutions balance fraud prevention with user experience—and which ones can offer the best of both.



\*A hardware security token may be a physical device that an authorized user is given to help prove their identity.

## The challenge

Every business wants to offer great user experiences while keeping fraud rates low—traditionally, that has been difficult to accomplish.

### Disjointed solutions



Authentication solutions need to work together in order to ensure there is no disconnect in user experience or fraud detection.

### Constrained resources



Strapped internal development resources can result in long lead times that make it difficult to get projects done.

### Long approval times



Vetting outside vendors that offer the newest authentication technology can be a long process.

## The solution

A fraud and authentication platform can help address these challenges.

### Universal API



Universal APIs simplify initial integration and allow for connectivity to multiple service providers.

### Streamlined contracting



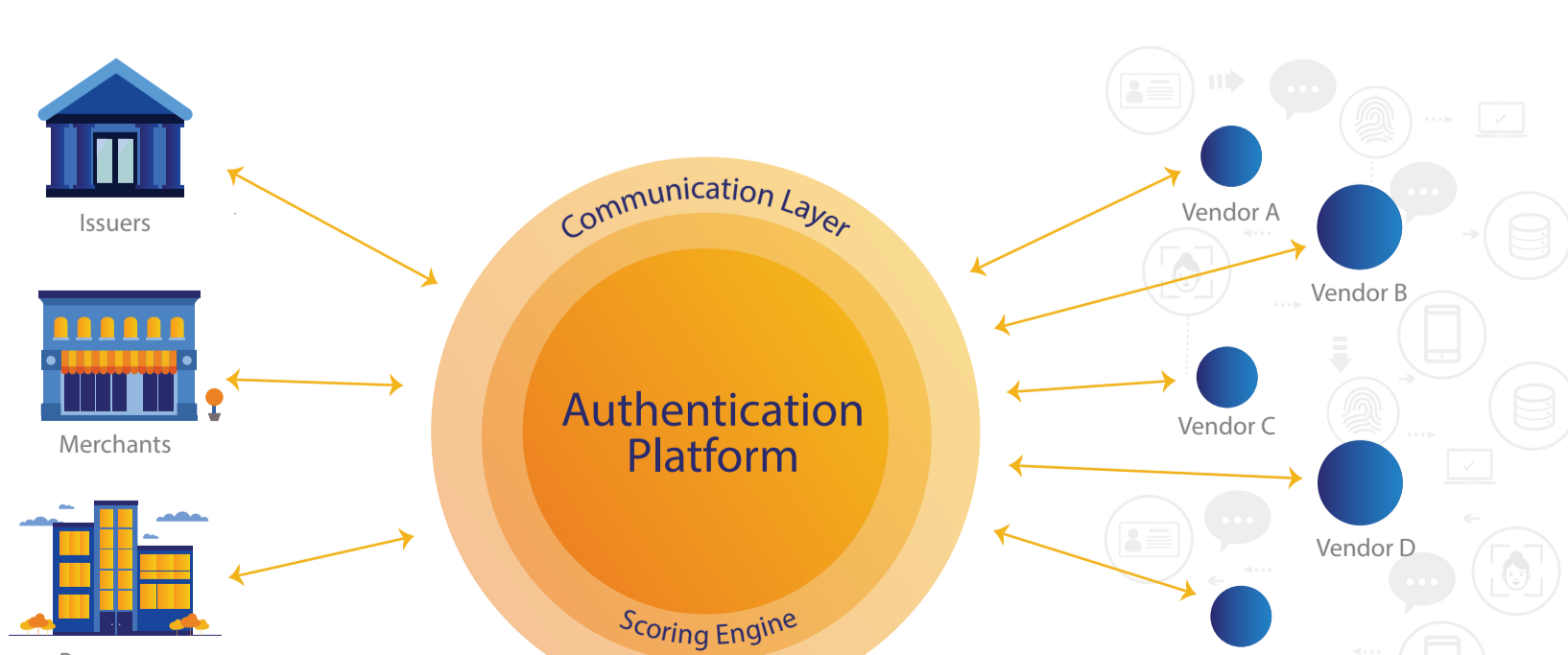
Streamlined contracting simplifies access to all services available through the platform.

### Policy and scoring engine



A policy and scoring engine allows authentication services to work together to determine transaction risk.

## An authentication platform enables simple access to multiple service providers



Businesses can interact directly through the authentication hub with a single communication layer.

Multiple vendors are collectively managed by the authentication hub.

Visit

[GlobalClient.Visa.com/AiteDigitalAuthenticationWhitePaper](https://GlobalClient.Visa.com/AiteDigitalAuthenticationWhitePaper)

to request Aite's full digital authentication white paper

