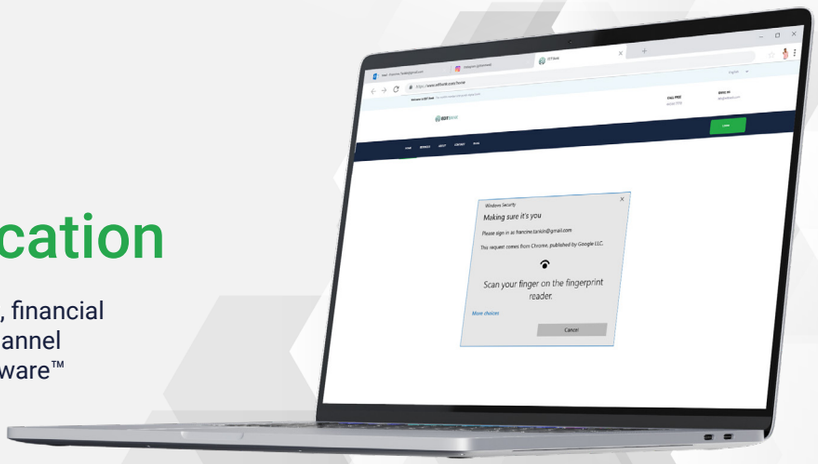
entersekt

The Financial Authentication Company.

Browser Authentication

With Browser Authentication from Entersekt, financial institutions can futureproof their browser channel as part of a more modern, secure Context Aware™ Authentication strategy.



78%
users want to be protected from browser fingerprinting.[1]

>40%
users immediately block cookie consent.[1]

86%
users prefer to use biometrics.[2]

11 weeks
device fingerprint data storage .[1]

Stop fighting modern-day fraud with outdated authentication

Browser Authentication enables FIs to both silently and actively identify and protect customers transacting via their browsers, while delivering enhanced user experiences. Thanks to FIDO-enabled passkeys, passwordless methods – with or without an app – are now a reality. With its world-class set of features, Browser Authentication from Entersekt protects your customers against the most dangerous fraud attack vectors threatening FIs today, while effectively reducing reliance on device fingerprinting and cookies.

Browser authentication is part of Entersekt's proprietary Context Aware™ Authentication solution that uses risk-based authentication data, a customer's cross-channel interactions, and personalized authentication preference to minimize friction, prevent fraud, and deliver the best customer experience.

A continuously evolving focus on privacy

Leading companies realize the fraud reduction benefit by uniquely identifying a device and browser and eliminating mistaken identity (for example, device collision when using fingerprinting).

Browser ID: Silent attestation

- Creates a cryptographically unique browser ID with no device collision.
- Employ across multiple use cases to uniquely identify most browser interactions.
- Turn a browser instance into a strong possession factor that can be leveraged in a multi-factor journey.
- Requires no customer action to enable Frictionless Login after trusting the browser.
- Supplement with fingerprinting to further minimize device drift.
- Works across most browsers and OS platforms.
- Digital transaction signing that supports non-repudiation.
- W3C is severely limiting down the ability to fingerprint, due to privacy concerns. The Entersekt Browser ID solution is built on new industry standards that are unaffected by the changes – providing consistency into the future.

Layering with Risk-based Authentication

- Get access to the world's largest behavioral network.
- Leverage real-time device reputation scores to identify high risk devices.
- Protect your users against automated attacks.
- Real-time risk scores that enable advanced risk decisioning.
- Identify account take-over attempts in real-time.
- Configurable authentication policies, frictionless for low-risk, challenge for medium-risk, and decline for high-risk interactions.

Introducing Passkeys

- Passkeys enable biometric authentication on all major browsers.
- Supports both app-less and passwordless implementations.
- Does not require a mobile app for authentication.
- Eliminates the risks of phishing, password theft and replay attacks.
- Supports roaming hardware authenticators and on-device authenticators like fingerprint scanners.
- Facilitates passkeys, the new standard in authentication driven across Google, Apple and Microsoft.

See for yourself

Want to learn more about the solution and see it in action?

Book a demo

1. https://petsymposium.org/2020/files/papers/issue2/popets-2020-0041.pdf
2. https://fidoalliance.org/fido-consumer-e-commerce/

info@entersekt.com