Fingerprint

Device Fingerprinting as a possession factor

Here are some of the key regulator viewpoints on the use of device fingerprinting as a part of multi-factor or strong authentication methods.

EU European Banking Authority (EBA)

Under the EU's Payment Services Directive 2 (PSD2), device fingerprinting is acknowledged as a medium to strong possession factor. For example, the device can serve as a possession factor in two-factor authentication if it has been uniquely linked to the customer, such as via a unique device identifier or fingerprint.

United States National Institute of Standards and Technology (NIST)

In its Digital Identity Guidelines (NIST SP 800-63B), the NIST outlines acceptable methods for multi-factor authentication. The NIST states "Secure device identification MAY be used to enact a session between a subscriber and a service. The record created by the [credential service provider] (CSP) SHALL contain the date and time the authenticator was bound to the account. The record SHOULD include information about the source of the binding (e.g., IP address, device identifier) of any device associated with the enrollment."

Australia The Australian Prudential Regulation Authority (APRA)

Although APRA does not specifically call out device fingerprinting, their Prudential Practice Guide does mention that "Common controls include: authentication controls commensurate with the vulnerability and threats associated with the products and services offered. This could include usage of a second channel notification/confirmation of events (e.g. account transfers, new payees, change of address, access from an unrecognised device)." Device fingerprinting is commonly used to "recognize" a device.

World Bank

Requirements around Risk-Based Authentication (RBA) include "the use of

- Transaction value
- Number of transactions within a specific time frame
- Buyer's transaction history
- Cardholder's browser fingerprint
- Whether the buyer is a new or returning customer
- Information about the buyer's location"

"Device binding is commonly used as the possession factor together with either a knowledge or inherence factor. In India, when a Unified Payment Interface (UPI) transaction is initiated using a smartphone, the device fingerprint, such as the International Mobile Equipment Identity number or other unique technical detail, is considered as the first factor of authentication."

Commercial Acceptability

Various commercial entities have also adopted browser and device fingerprinting as proof of possession. Visa's Compelling Evidence 3.0 and Mastercard's First-Party Trust Program both require device fingerprinting and/or IP address collection as proof of possession for challenging chargebacks. 3DS supports this as well. In India, device fingerprinting is utilized as the first authentication factor by the UPI (Unified Payments Interface), which currently provides connectivity to 200 banks.

About Fingerprint

Fingerprint, the world's most accurate device intelligence platform, enables companies to prevent fraud and improve user experiences. Fingerprint processes 100+ signals from the browser, device, and network to generate a stable and persistent unique visitor identifier that can be used to understand visitor behavior. Fingerprint is ISO 27001 certified, and SOC 2 Type II, GDPR, and CCPA compliant. Fingerprint is trusted by over 6,000 companies worldwide, including 16% of the top 500 websites, to help catch sophisticated fraudsters and personalize experiences for trusted users.

Learn more and get started at **fingerprint.com**