What is Keystroke Biometrics?
The Newest Addition to Crossmatch DigitalPersona®

Behavioral biometrics enhances authentication security along with delivering a superior user experience in use cases that include frequent user interaction. Crossmatch DigitalPersona® has always supported the broadest range of authentication factors on the market to help organizations secure every endpoint, user and system. The integration of behavioral biometrics adds a key component to a multilayered security strategy and poses no further privacy risk.

Thanks to our addition of BehavioSense technology into DigitalPersona, users' actual typing behavior is a verifiable factor within your composite authentication scheme.

Incorporating keystroke biometrics brings a host of advantages to an already robust authentication product. This technology uses continuous machine learning to authenticate users based not on what they type, but on how they type. The algorithm can verify who someone is based on how they naturally interact with their device and deliver instant identity verification, along with continuous authentication. No special sensors. No extra hardware. Keystroke input characteristics are analyzed to build a profile of the user which is refined over time and highly accurate — further preventing fraudulent login risk.

A mixture of legacy factors with behavioral biometrics means masterpiece security for your organization.
The user score factors in three metrics that are captured by the system: Press, Flight, and Sequence. The combination of these measurements creates a user profile that is continuously compiled and analyzed.

KEystroke BIOMETRICS AT WORK

Enhanced by machine learning, the authentication function of keystroke biometrics gets more sensitive over time. The more sessions a user participates in, the more complete a picture the system has of their behavior.

Keystroke biometrics is naturally resistant to presentation attacks, as well:
- On the digital layer, stolen session data can’t be reused, since repeated sessions are flagged as suspicious.
- On the physical layer, the measured differences between user behaviors are so minute that humans are unable to perceive and duplicate them.

Leveraging a mix of authentication modalities — including keystroke biometrics — allows organizations to defend against cybersecurity threats while preserving user experience and making compliance easier.

Visit Crossmatch.com/DigitalPersona to find out more about how the addition of keystroke biometrics can be a win-win for your organization today.

ABOUT CROSSMATCH
Crossmatch® solutions solve security and identity management challenges for hundreds of millions of users around the world. Our proven DigitalPersona® composite authentication solution is designed to provide the optimal set of authentication factors to meet today’s unique risk requirements and afford complete enterprise authentication coverage. Crossmatch identity management solutions include trusted biometric identity management hardware and software that deliver the highest quality and performance required for critical applications. Our solutions support the financial, retail, commercial, government, law enforcement and military markets. With 300 employees and customers in more than 80 countries, Crossmatch sets the standard for innovation and reliability. Learn more: Crossmatch.com

Copyright © 2017 Crossmatch. All rights reserved. Specifications are subject to change without prior notice. Crossmatch® and the Crossmatch logo are registered trademarks of Cross Match Technologies, Inc. in the United States and other countries. DigitalPersona® and the DigitalPersona logo are registered trademarks of DigitalPersona, Inc. in the United States and other countries. DigitalPersona, Inc. is owned by the parent company of Cross Match Technologies, Inc. All other brand and product names are trademarks or registered trademarks of their respective owners.