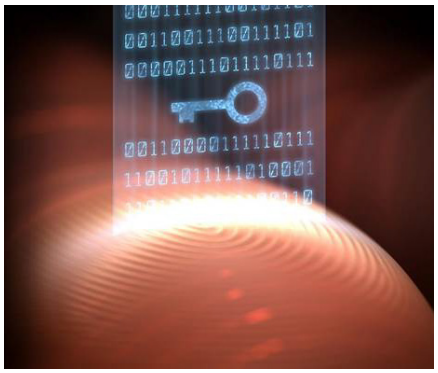

Fingerprint Sensing: The Next Generation

PN: 507-000178-01 Rev. C

Table of Contents

SentryPoint™

Overview

Biometric identification techniques for user authentication are more secure and easier to use than a typed password. Of the techniques available, fingerprint sensing strikes the sweet spot between security and convenience. Rather than having to remember a “strong” password, and possibly needing a token as well, users can simply swipe a finger to prove their identity.

Fingerprint sensors are now prevalent in mobile devices, and new applications for biometric identification include online and in-person banking, point-of-sale transactions, facilities access, and more. But the creation, processing, and storage of fingerprint data raises some privacy and security issues.

This white paper provides an overview of existing fingerprint sensing and security technologies and introduces the most recent advance — the ability to perform the “match” directly in the fingerprint sensor itself.

Match-on-Host: Current State-of-the-Art

As with all fingerprint authentication solutions, Match-on-Host fingerprint sensing positively identifies the user by matching the fingerprint read by the sensor with a known, secured "template" (record of the user's fingerprint). The fingerprint template is created and stored during an "enrollment" process. This template is used during every subsequent access attempt to identify and authenticate the user.

Fingerprint authentication solutions usually make the match during a process that runs on the host system (smartphone, tablet, PC, point-of-sale security device, and so forth). As a result, the Match-on-Host architecture splits the functional requirements amongst the sensor IC that captures the fingerprint image and the software and/or a separate controller IC that makes the actual match.

The functions performed by the software identify the fingerprint's characteristics, create a biometric asset (the fingerprint template), store the template in a secure database, and match a newly created fingerprint image with the template's secure representation. Encrypted communication between the fingerprint sensor and the host, such as that provided by Synaptics SentryPoint™ technology, ensures data integrity and security with Match-on-Host solutions. An advanced matching engine delivers quick and accurate sensing to ensure a superior user experience.

In addition to data integrity and high security, Match-on-Host solutions offer aesthetic advantages. A wide array of shapes and sizes are possible for the fingerprint sensing module. This variety of design options is made possible by Synaptics' LiveFlex™ technology which separates the sensing element from the controller IC. Sensors can be implemented as narrow as a typical finger; even designs that fit on the side of a smartphone are possible. The user can place a fingertip at virtually any angle and still get an accurate reading.

Optional design enhancements include LEDs, haptic feedback, or even LED "guides" to improve usability. Other Match-on-Host advantages achieved through Synaptics' Natural ID™ and SecurePad™ is "upon touch" activation to minimize power consumption.

Value-optimized options — in addition to a choice of sensor types, mechanical designs, and driver features — help expedite development cycles and minimize total cost.

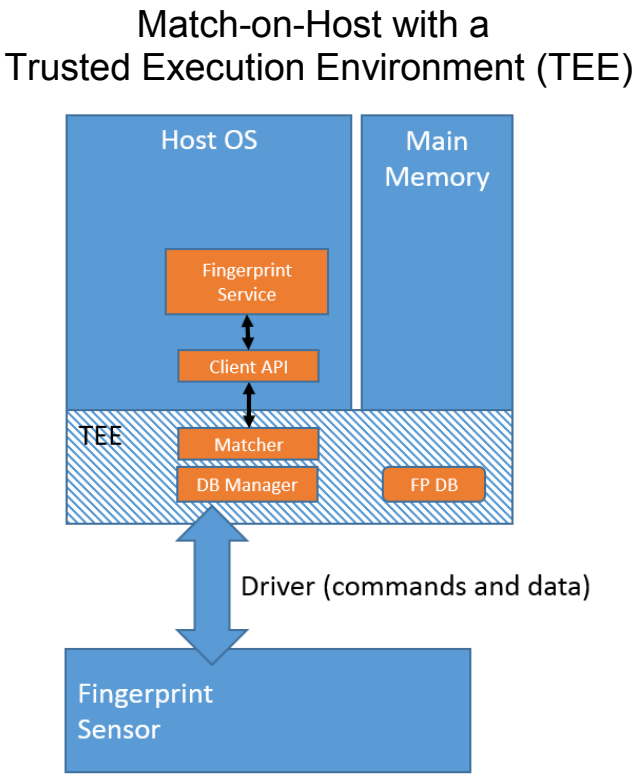

Figure 1. The Trusted Execution Environment (TEE) provides a secure area running within the host environment.

Synaptics' Match-on-Host fingerprint sensing technology has been used successfully in over 200 million devices, and its advanced functionality makes it a preferred solution in a wide variety of applications including smartphones, tablets, notebook PCs, PC peripherals, and more. With the rich feature offerings of Natural ID and SecurePad, Synaptics expects the Match-on-Host architecture to remain popular in low-cost devices well into the future.

Match-in-Sensor: The Next Generation

As the name implies, the Match-in-Sensor architecture integrates matching and other biometric management functions directly within the sensor IC. The IC contains a high-performance microprocessor, storage for instructions and data, secure communications, and high-performance cryptographic capabilities. To achieve this level of integration while creating a secure execution environment within the sensor IC, Synaptics employs a system on a chip (SoC) design.

These advances are truly "next generation" due to the additional security afforded by *fully* integrating the sensing and matching functions. The advanced security available with the Match-in-Sensor architecture applies to both the system *and* the protection of the user's biometric information. Match-in-Sensor technology is destined to have a profound impact on the industry.

System-level security is enhanced by physically isolating the host's operating system from the environment the fingerprint image and the fingerprint matcher's execution reside in — ensuring protection from hacking or malware that might be running on the host. The sensor performs biometric identification autonomously, without relying on any input from the host that could be compromised.

The matcher uses the live fingerprint image, which is captured, encrypted, processed, and protected on the sensor chip, as the enrollment template. The receiving party is able to verify authenticity because the identification result is signed using a sensor-specific private key that is derived from the hardware. Synaptics' Fast IDentity Online (FIDO) Certified™ Authenticator software module can also be executed in-sensor for enhanced security.

Even if the host is compromised by a successful attack of any type or origin, it is not possible to: force the matcher to generate a false positive result, replay an old result, or in any way alter or manipulate the match result. This ensures that the fingerprint identification subsystem remains secure even during a worst-case scenario.

The protection of sensitive user information is also enhanced with these improvements:

- The fingerprint image, all the features and characteristics extracted from it, and all templates are processed only within the sensor's on-chip storage and are not exposed to the host.
- The enrollment database is located on private SPI flash memory, physically accessible only by the sensor.
- The enrollment templates are encrypted and signed by the sensor using algorithms and strong cryptographic keys before being stored in private flash memory.

Even if the host is compromised by a successful attack, the attacker could not extract any biometric information — one of the most invasive forms of identity theft possible to a consumer.

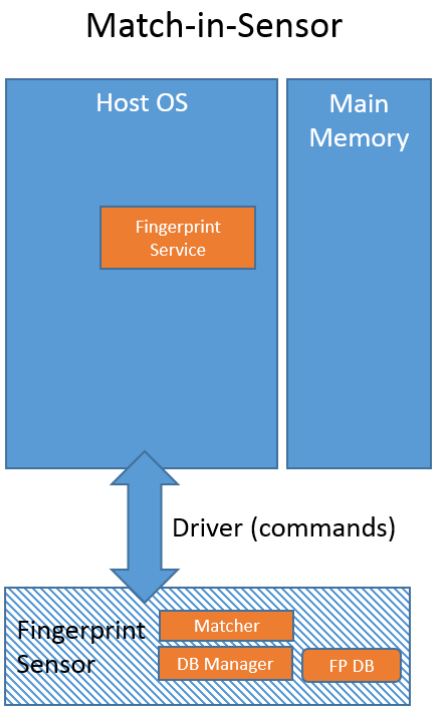

Figure 2. Match-in-Sensor solutions isolate fingerprint operations from the host OS in the sensor itself.

SentryPoint Match-in-Sensor technology builds on the many advances Synaptics made in its Match-on-Host solutions, including the ability to read fingers at various angles, options for visual or haptic feedback, and device- or application-specific optimizations.

Isolating the sensing functions entirely from the host's operating system gives Synaptics' Match-in-Sensor architecture industry-leading security for devices and applications that use fingerprints for user authentication. This higher level of security is expected to be needed initially in finance, healthcare, and some government agencies.

Over time, as volume production leads to implementation efficiencies, Synaptics expects Match-in-Sensor to become the dominant architecture in all systems with fingerprint sensors.

Conclusion

Using fingerprints for user authentication is both more secure and simpler than requiring users to create, remember, and protect passwords. Merchants prefer it. Banks prefer it. Third party clearinghouses prefer it. Most importantly, users prefer it.

The many advantages of fingerprint sensing make it an increasingly popular and competitive feature in smartphones, tablets, notebook PCs, point-of-sale systems, and more. With this latest advance, Synaptics gives equipment vendors an even greater range of design choices — from proven Match-on-Host to next-generation Match-in-Sensor solutions.

For more information about Synaptics' fingerprint sensing technology options, please visit www.synaptics.com.

About Synaptics

Synaptics is the pioneer and leader of the human interface revolution, bringing innovative and intuitive user experiences to intelligent devices. Synaptics' broad portfolio of touch, display, and biometrics products is built on the company's rich R&D and supply chain capabilities. With solutions designed for mobile, PC and automotive industries, Synaptics combines ease of use, functionality and aesthetics to enable products that help make our digital lives more productive, secure and enjoyable. (NASDAQ: SYNA) www.synaptics.com.

Copyright

Trademarks

Notice

Use of the materials may require a license of intellectual property from a third party or from Synaptics. This document conveys no express or implied licenses to any intellectual property rights belonging to Synaptics or any other party. Synaptics may, from time to time and at its sole option, update the information contained in this document without notice.

INFORMATION CONTAINED IN THIS DOCUMENT IS PROVIDED "AS-IS," WITH NO EXPRESS OR IMPLIED WARRANTIES, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND ANY WARRANTIES OF NON-INFRINGEMENT OF ANY INTELLECTUAL PROPERTY RIGHTS. IN NO EVENT SHALL SYNAPTICS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES ARISING OUT OF OR IN CONNECTION WITH THE USE OF THE INFORMATION CONTAINED IN THIS DOCUMENT, HOWEVER CAUSED AND BASED ON ANY THEORY OF LIABILITY, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, AND EVEN IF SYNAPTICS WAS ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. IF A TRIBUNAL OF COMPETENT JURISDICTION DOES NOT PERMIT THE DISCLAIMER OF DIRECT DAMAGES OR ANY OTHER DAMAGES, SYNAPTICS' TOTAL CUMULATIVE LIABILITY TO ANY PARTY SHALL NOT EXCEED ONE HUNDRED U.S. DOLLARS.