FEITIAN
WE BUILD SECURITY

ambiq

White Paper

The Future of Biometric Smart Cards

A guide to biometric authentication and fingerprint card technology

Contents

Executive Summary

Fingerprint biometric technology has driven digital transformation across vital industries, such as banking, identification, and transportation. In everyday use cases like access control cards and payment cards, fingerprint authentication has enabled new possibilities. Soon, fingerprint biometrics will replace PIN codes as the dominant form of identity authentication.

This paper will assess the security risks associated with fingerprint biometrics, discuss how those risks can affect both individuals and enterprises, and recommend a modern solution by FEITIAN. Finally, this paper will examine how technology leader Ambiq's ultra-low-power system on chips (SoCs) empower the fingerprint card of the future.

From the PIN to Biometric Authentication

For the past fifty years, the personal identification number (PIN) has been the golden standard of user authentication. However, PIN codes are far less secure today. Modern cybercriminals can steal your information from thousands of miles away without physically touching your card. Thanks to the convergence of affordable sensors, increased computing power, and more advanced algorithms, biometric authentication has become a superior alternative.

Facial recognition, iris scanning, voice recognition, and fingerprint sensing are key technologies gaining traction in the user authentication market. Facial recognition was the most popular form of biometric technology, but recent high-profile mistakes and studies have led governments and enterprises alike to question its reliability and fairness. On the other hand, fingerprint authentication has become more viable thanks to its cost-effective implementation and secure user experience.

Too Many Biometric Solutions

In the age of big data and fast data, service providers and employers collect our biometric data for various purposes like never before. Some popular forms of biometric authentication include facial recognition, iris recognition, and fingerprint recognition. But with so much data and so many biometric solutions available, choosing the wrong solution can negatively impact security and user experience.

When it comes to biometric authentication, facial recognition and fingerprint biometrics are the most well-known and widely adopted technologies. However, due to facial recognition limitations, increased security risk, decreased user privacy, a high technology cost, and frustrating user experience are common pitfalls. Fingerprint authentication, on the other hand, faces none of those problems.

A Better Fingerprint Biometric Solution

Today's companies have a greater responsibility to protect their users' biometric data, especially their fingerprint data. The challenge is to find a secure solution that also optimizes the user experience. Fortunately, there is a smart card solution that meets both of those requirements. FEITIAN Technologies, a leading provider of authentication solutions, and Ambiq®, a technology leader in ultra-low power microprocessors, offer its fingerprint cards with maximum security and a long lifetime without sacrificing any accuracy, efficiency, or speed in the user experience.

Introduction

In recent years, biometric technologies like facial recognition, iris scanning, and fingerprint sensing have become popular across commercial, private, and public sectors. In particular, fingerprint biometrics has driven digital transformation across vital industries, such as banking, identification, and transportation.

Thanks to its ease of use and high-level of security, fingerprint biometrics has enabled new possibilities. Our smartphones and workstations can already use fingerprint authentication, eliminating the need for passwords. However, our credit cards and ID cards are beginning to leverage this technology as well[1].

We already use smart cards for tasks like electronic payment, identity recognition, and access controls. Adding fingerprint sensors to the card adds a next-generation layer of security.

Fingerprint Authentication is the Future of Security

Thanks to a convergence of cheap and widespread sensors, increased computing power, advanced algorithms, and efficient data collection, organizations can now implement fingerprint sensors on a tiny form factor such as payment cards and identification cards[2].

With our biometric information and data playing a larger role in our everyday lives, the stakes for cybersecurity and data privacy are high. You can change your password. Your fingerprint, not so much.

[1] https://creditcards.usnews.com/articles/what-are-biometric-credit-cards
[2] https://www.ftsafe.com/Topic/An_Introduction_to_FEITIAN_Fingerprint_Card_Series

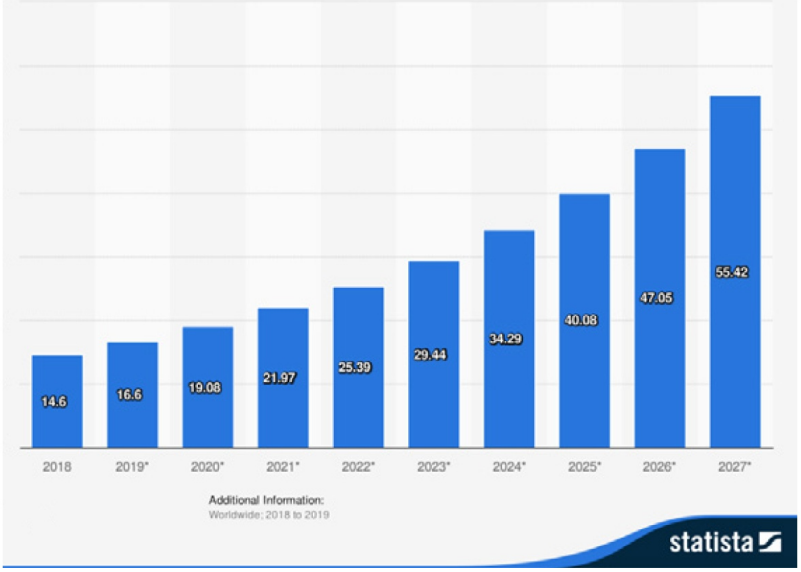
Since the introduction of the EU General Data Protection Regulation (GDPR) in 2018, any company that falls victim to a data breach will now face fines of up to €20 million or 4% of its annual turnover[1].

The strict requirements and the massive monetary threat of GDPR and its fines are a stark reminder that businesses must enforce stringent IT security policies to remain compliant with new data and IT security regulations and prevent cyberattacks. However, a study conducted by Centrify's Privileged Access Management in the Modern Threatscape survey results revealed that 74% of corporate data breaches occurred because of abuse, carelessness, or misuse of internal password credentials for secure company accounts[2].

> "Biometrics are quickly becoming the preferred method of identity authentication"

Biometrics are quickly becoming the preferred method of identity authentication. According to Statista, the global biometric technologies market is expected to reach 19.08 billion U.S. dollars in 2020 as shown in Figure 1. The contactless biometric technologies market is also expected to grow to over eight billion U.S. dollars in size[3].

Figure 1: Global Biometric Technologies Market Trends in 2020



Meanwhile, the world is becoming increasingly digital and contactless, a trend that has been accelerated by the COVID-19 pandemic. If you are seeking a cost-effective technology that offers a convenient and secure user experience, fingerprint authentication is the ideal solution.

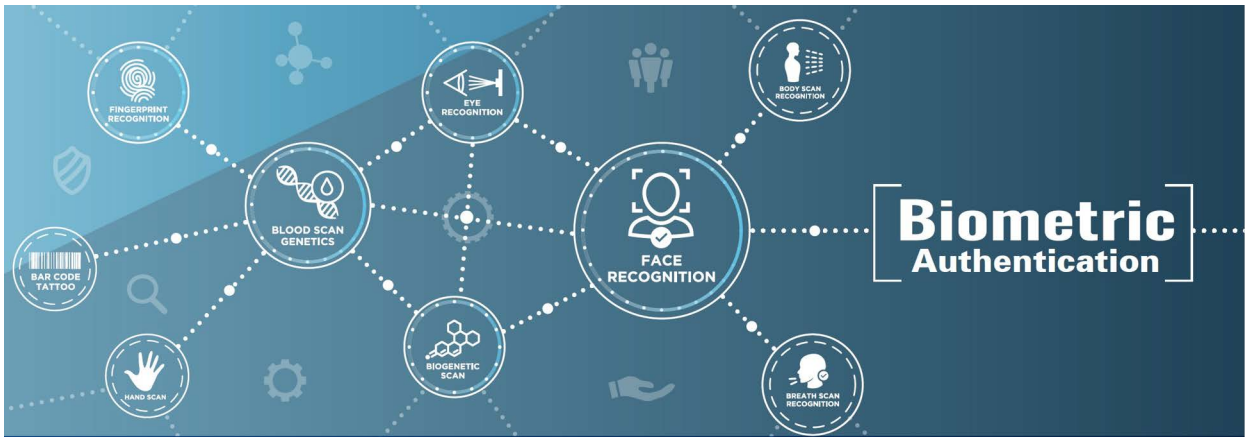
[1] https://gdpr.eu/fines/
[2] https://www.forbes.com/sites/louiscolumbus/2019/02/26/74-of-data-breaches-startwith-privileged-credential-abuse/?sh=22f954d63ce4
[3] https://www.statista.com/topics/4989/biometric-technologies/

From the PIN to Biometric Authentication

For the past fifty years, the personal identification number (PIN) has been the golden standard of user authentication. However, thanks to increased technology risks and an increasingly digital world, PIN codes are less secure and less convenient than other authentication methods available today.

Biometric authentication has become one of the fastest-growing technologies, thanks to rapid technological advancements. Facial recognition, iris scanning, voice recognition, and fingerprint sensing are key technologies gaining traction in the user authentication market. Unlike PIN codes, these methods of authentication can't be easily stolen from thousands of miles away.

How you choose to secure private and privileged credentials will determine your future.



Facial Recognition vs. Fingerprint Recognition

For years, facial recognition had been championed as the most compelling authentication option. However, it's proven to be unreliable and vulnerable in the digital age.

Recent high-profile mistakes[1] and studies[2] have led governments and enterprises alike to question the reliability and fairness of facial recognition technology. The rise of face masks in the wake of the COVID-19 pandemic has also made it more challenging to implement facial recognition algorithms.

> "Fingerprint authentication has become more practical than facial recognition thanks to its cost-effective implementation and secure user experience."

[1] https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html
[2] https://www.bbc.com/news/technology-50865437

On the other hand, fingerprint authentication has become more practical thanks to its cost-effective implementation and secure user experience. Over 1.09 billion fingerprint sensing units were shipped worldwide this year, a trend that will only increase as everyone adapts to a post-pandemic world.

Fresh approaches to fingerprint authentication, such as attaching fingerprint sensors onto a card, offer a more secure and more convenient user experience than other biometric technologies. These innovations are ushering in a new era of consumer biometrics.

The Problem: Too Much Data, Too Many Biometric Solutions

We live in the age of big data[1], where massive amounts of information are collected every second. With fast data[2], we can quickly analyze these datasets to generate real-time insights that improve the user experience or enhance security.

Service providers and employers are collecting our biometric data for various purposes like never before. One moment, you're tracking your vitals with your smartwatch. The next, you're accessing your work building with facial recognition.

Biometric authentication is driving digital transformation. Different organizations use different forms of biometric authentication, such as:

- Facial recognition
- Iris recognition
- Fingerprint recognition

Unfortunately, choosing the wrong option can lead to higher security risks and a catastrophic data breach. Let's compare the options.

Facial Recognition

Facial recognition is familiar to consumers and business users alike. It comes pre-packaged with most smartphones, presenting a fast and convenient security method. In theory, facial recognition is frictionless, high speed, and widely applicable.

In practice, facial recognition algorithms can be challenging to deploy. The basic level of facial recognition can lack accuracy, especially when there are low lighting and poor camera placement. Mask wearing has gone up following the pandemic, making facial recognition less reliable unless paired with other solutions, such as behavioral analytics.

[1] https://en.wikipedia.org/wiki/Big_data
[2] https://whatis.techtarget.com/definition/fast-data#:~:text=Fast%20data%20is%20the%20application,that%20action%20can%20be%20taken

Iris Recognition

Iris recognition offers another contactless form of biometric authentication. This method is flexible and has begun to be included in smartphones. Iris recognition is fast, highly accurate, and flexible. Users can even scan their separate eyes.

For glass wearers, iris recognition can be an inconvenient method of authentication. Similar to facial recognition, the amount of light can affect the accuracy depending on the scanner position. Most iris recognition authentication solutions are still limited by range, as the user must be near the scanner for it to scan correctly.

Fingerprint Recognition

Fingerprint recognition offers a universal and unique biometric authentication solution. 99.99% of the population has fingerprints, and no one has identical fingerprints to another person. Mainstream phones already offer fingerprint scanning, and other use cases involving fingerprint sensors are growing across different verticals and industries.

Fingerprint biometrics requires physical contact, which can be inconvenient if the user is wearing gloves. Also, fingerprints can't be changed like a PIN code. Once stolen, there's nothing you can do to re-secure your data.

Choosing the Right Solution

Modern organizations need to juggle cost, user experience, and data security when it comes to biometrics. Often, a single solution alone is not enough. The most advanced biometric solutions, such as implementing fingerprint sensors on a smart card, offer the best mix of speed, efficiency, and accuracy. But how do you choose the right solution?

This guide can help. It provides information to help you weed out the biometric solutions that aren't right for you. Combing through the different options will take a little time, but picking the right solution will enable you to provide a secure and seamless user experience.

Choosing Facial Recognition Over Fingerprinting is a Mistake

When it comes to biometric authentication, facial recognition and fingerprint biometrics are the most well-known and widely adopted technologies. However, if you implement the wrong biometric solution, you may be opening yourself up to these problems:

Problem 1 - Increased Security Risk

Facial recognition technology relies on sophisticated software. Most software requires updates, and less robust software may have databases that need to be maintained manually. Either way, there is downtime, increasing the opportunity for cybercriminals to attack. Less secure image databases may also be tampered with.

Compare with fingerprint cards, a form of fingerprint authentication is becoming adopted across various industries. The user's fingerprint image is enrolled, scanned, and stored on a system on a chip (SoC). The fingerprint image is converted into a specific format of data and stored on the card. Even if someone steals the card, they won't have your reference fingerprint to use it.

Problem 2 - Decreased User Privacy

With facial recognition software, companies can track anyone they choose anywhere and anytime. Facial recognition systems can analyze millions of images and videos from many sources, such as CCTV cameras and social media photos. This technology automatically tags pictures when a person is recognized and analyzed, whether they consented or not. There are already multiple lawsuits filed against biometric companies and tech giants8 in Illinois, alleging their violations of the Biometric Information Privacy Act (BIPA) by analyzing people's images with biometrics without their permission.

> "Facial recognition systems automatically tag pictures when a person is recognized and analyzed, whether they consented or not."

Under Europe's General Data Protection Rule (GDPR), all companies doing business in Europe must adhere to the strict requirements of its privacy rules, data collection, and the usage and distribution of all personal information. The most controversial of all is facial recognition, including its accuracy, fairness, legitimacy, and inherent biases.

On the other hand, fingerprint authentication requires users to enroll their fingerprints only if they want to be scanned. Their fingerprint data is also encrypted and stored on a secure device (smartphone) or a secure token (smart card). The fingerprint data is never backed up or stored on any servers, and it can't be used to match against other fingerprint databases.

Problem 3 - High Technology Costs

Facial recognition systems require powerful imaging recognition technology, massive data collection, and intensive machine learning. This software must pick out a face from a crowd and compare it to a database of stored images. Highly accurate and easy to use facial authentication solutions exist, but many companies lack the budget.

Fingerprint authentication can be highly cost-effective. For example, smart cards with fingerprint sensors are cheap to manufacture and deploy. Although this solution integrates high technology components such as a system on a chip, they are cheap to produce in bulk. The cards themselves are made from the same material as a regular credit or debit card.

Problem 4 - Frustrating User Experience

Facial recognition can make for a frustrating user experience when the user has to frequently confirm their identity, such as entering a building or accessing a workstation. The more a user needs to authenticate, the more friction there is in the user experience.

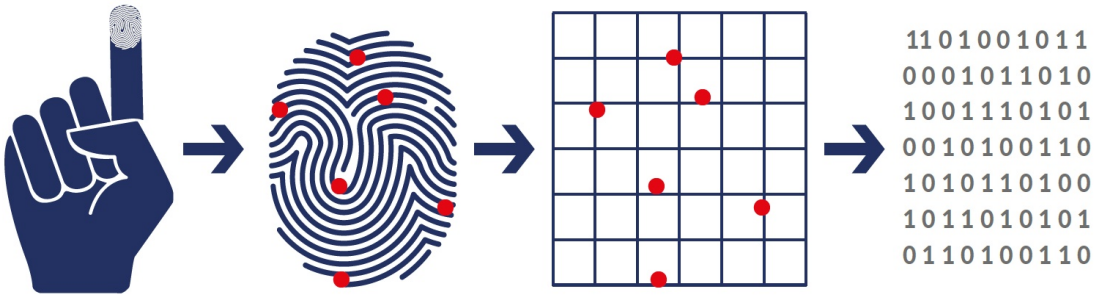
Fingerprint biometrics offers a more frictionless user experience. In most solutions, the user can place their finger at any angle to authenticate their fingerprint data. The sensor recognizes the user no matter what angle their finger touches the card, making for a smooth and seamless user experience.

How Biometric Fingerprint Recognition Works

Fingerprint recognition is one of the oldest and most recognized forms of biometric recognition. It traces its use as a form of identity authentication back to ancient China[1].Fingerprints can be easily captured with fresh ink and paper, and we can verify them by comparing each pattern's unique arches, loops, and whorls.

> "Fingerprint sensors convert fingerprint images into electrical signals that are processed and converted into digital form."

Today, fingerprint captures are done using fingerprint sensors, a vital component that converts the captured fingerprint image into an electrical signal. This signal is in analog form and needs to be converted into digital form. The signal may also need to be amplified, calibrated, and processed further before it is usable.



The sensor is a part of the larger scanner, or the entire device that transmits the electrical signal to another device in a digitally encoded form. There are currently four types of fingerprint scanners: the optical scanner, the capacitance scanner, the ultrasonic scanner, and the thermal scanner. These scanners all use different methods to capture the fingerprint:

1. **Optical scanners** use a digital camera to take a visual image of the fingerprint.
2. **Capacitive scanners** use capacitors and electrical current to form an image of the fingerprint.
3. **Ultrasonic fingerprint** scanners transmit an ultrasonic pulse against the finger to create a 3D image of the fingerprint.
4. **Thermal scanners** sense the temperature difference on the contact surface between ridges and valleys of the fingerprint.

[1] https://en.wikipedia.org/wiki/Fingerprint#History

After a biometric sensor captures an image of a fingerprint, it is sent to another crucial component—the system on chip. The system on chip processes the image to produce a unique digital biometric template.

The system on chip uses this template to run inference, calculating posterior probabilities based on multiple data observations. Essentially, the system on chip considers all of the data of a fingerprint image to determine the likelihood that the fingerprint matches an existing fingerprint in the database.

> "The system on chip considers all of the data of a fingerprint image to determine the likelihood that the fingerprint matches an existing fingerprint in the database."

Low-Power Fingerprint Biometrics

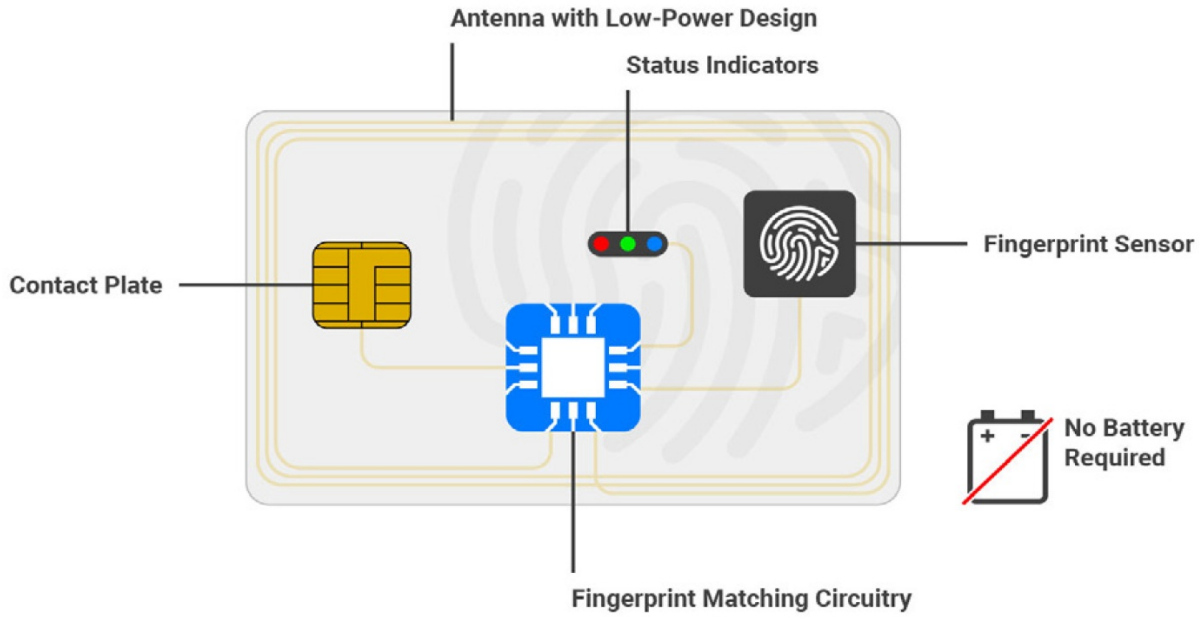
Sensors and the system on chip both need electricity to function. In the past, this was a hurdle for engineers. However, the rise of low-power technologies has led to ultra-low-power components, which enable efficient solutions such as biometric fingerprint cards.

Fingerprint cards need low-power sensors because they cannot be plugged into a wall outlet like a smartphone. That also means fingerprint cards cannot run power-intensive processes or use power while inactive. There must be a terminal like a card reader or POS machine to overcome these limitations. The energy that a fingerprint card or a smart card needs is harvested from the terminal.

> "New ultra-low-power sensor and system on chip components have enabled energy-efficient biometric fingerprint cards."

The fingerprint card works similarly to other fingerprint biometric scanners. A sensor, as shown in Figure 2 on page 14, captures the fingerprint image, which is extracted by fingerprint algorithms running on the system on chip. The fingerprint image is then converted into a specific data format and stored on the system on chip or another secure element. The newly captured fingerprint image is compared with the reference fingerprint template to confirm or deny a match.

Figure 2: An example of a smart card with a fingerprint sensor



A Better Fingerprint Biometric Solution

More than ever, today's companies have a greater responsibility to protect their users' biometric data. Any biometric information used for identity authentication or access control, such as fingerprint data, needs to be exceptionally secure. The challenge is to find a fingerprint authentication solution that optimizes the user experience while providing maximum security.

Fortunately, there is a fingerprint biometric solution that meets both of those requirements from FEITIAN Technologies, a leading provider of authentication solutions.

> "FEITIAN's new smart card makes transactions and authentication more secure in critical industries, such as banking, identity, and transportation."

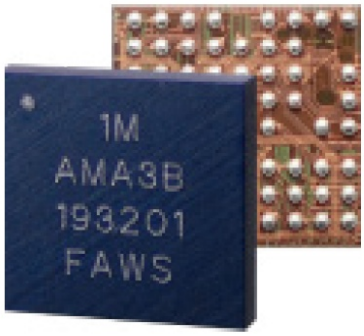
The FEITIAN fingerprint card, as shown in Figure 3 on page 15, integrates high-technology components, including a capacitive sensor that eliminates the need for a battery. Consumers can enjoy a biometric card without sacrificing the form factor of a regular smart card. FEITIAN's card design architecture reduces security risk without sacrificing any accuracy, efficiency, or speed in the consumer experience.

Figure 3: FEITIAN FT-JCOS Fingerprint Card Series

> "The FEITIAN Fingerprint Card Series integrates Ambiq's ultra-low-power system on chip, the Apollo3 Blue Thin SoC."

The card integrates ultra-low-power system on chips from Ambiq, an industry leader in SoC, SoC, and wireless communications technology. Ambiq's powerful processors, such as the Apollo3 Blue Thin SoC (as shown in Figure 4), are equipped with powerful biometric algorithms that determine if the current user's fingerprint matches the reference fingerprint template stored on the card. The system on chip runs on ultra-low power, making FEITIAN's card a cost-effective solution for power consumption.

Figure 4: Ambiq Apollo3 Blue Thin SoC



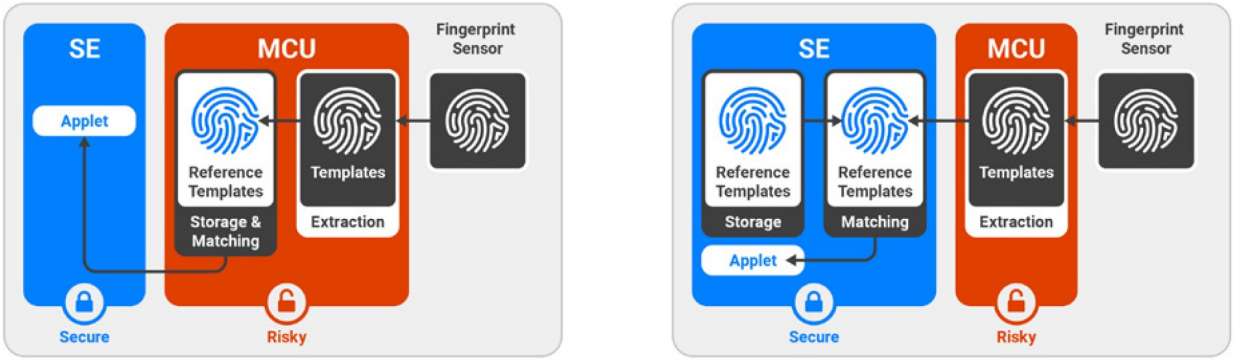
Key Use Cases for Fingerprint Cards

Today, the convergence of existing technology trends allows us to deploy biometric cards across many industries quickly. These technologies include the Internet of Things (IoT), edge computing, faster networks, systems on a chip (SoC), and miniaturized higher-definition biometric sensors.

FEITIAN's fingerprint card uses decentralized authentication, where each person's biometric data is stored on their card only. Their biometric data is stored directly on the card rather than being uploaded to a cloud database.

> "The FEITIAN fingerprint card stores users' biometric data directly on the card rather than upload it to a cloud database."

Figure 5: Different design architecture of the FEITIAN FT-JCOS fingerprint card series



Because there is no centralized database with an entire dataset of sensitive biometric information on it, criminals cannot break into a single data center and have immediate access to your data. By storing the fingerprint image directly on the card, FEITIAN's biometric card offers a secure option across banking, identity, enterprise, and transportation:

Banking

Banks and other financial institutions are under pressure to protect customer financial data while providing safe and easy transactions for their customers. The COVID-19 pandemic has accelerated the trend towards contactless payment cards, with many offering fingerprint biometrics.

> "Biometric contactless cards enable a convenient and secure experience for users as they do not have to remember passcodes."

Biometric contactless cards enable a convenient experience for users as they do not have to remember or input their passcode. It also allows a more secure experience since the user's biometric data is stored safely on the card. Consumers have noticed these benefits. In a study by Mastercard Inc., 46 percent of consumers worldwide had made a contactless card their primary choice for purchases in the first three months of this year[1].

Contactless cards already keep the customer's data on the card, but biometric cards add another layer of security. Criminals would have to create a synthetic plant of your fingerprint to match the reference fingerprint template. This makes fraud incredibly more difficult.

Identity

Banks and other financial institutions are under pressure to protect customer financial data while providing safe and easy transactions for their customers. The COVID-19 pandemic has accelerated the trend towards contactless payment cards, with many offering fingerprint biometrics.

Because of how secure fingerprint cards are, they can be used for mission-critical tasks like identity authentication. Governments are using fingerprint biometrics for border control and immigration[2], and some countries are leveraging fingerprints in their national identification cards. Another significant use case for fingerprint recognition is ePassports, which have an embedded electronic microprocessor with biometrics stored inside. Along with other biometrics, fingerprint data ensures that a citizen's identity can't be counterfeited or duplicated, which cannot be said about a physical ID.

> "Fingerprint data ensures that your identity cannot be counterfeited or duplicated, which cannot be said about a physical ID."

[1] https://newsroom.mastercard.com/asia-pacific/press-releases/mastercard-studyshows-consumers-moving-to-contactless-payments-for-everyday-purchases-asthey-seek-cleaner-touch-free-options/
[2] https://www.federalregister.gov/documents/2020/09/11/2020-19145/collectionand-use-of-biometrics-by-us-citizenship-and-immigration-services

Currently, 75 ePassport-issuing countries belong to ICAO PKID, the central body for authenticating ePassports[1]. However, fingerprint recognition can also be used for less security-intensive identity verification. For example, a membership card to a store or a country club can also leverage fingerprint biometrics.

Enterprise

Biometric fingerprint cards are also making employee and workforce management more accurate and efficient for enterprises. Fingerprint cards offer a more secure solution than traditional username and passcode security systems and physical tokens like magnetic strip cards or key fobs.

"Fingerprint cards offer a more secure solution than traditional username and passcode security systems and physical tokens like magnetic strips cards or key fobs."

Fingerprint cards can also be used to secure enterprise-wide areas such as an office building or a warehouse. They are more reliable than traditional security systems. Enterprise-wide areas requiring physical access solutions can use biometric cards, which can also control physical access to restricted areas like vaults and data backup centers.

Fingerprint cards offer a more secure option than passwords, badges, and physical security tokens, which can easily be stolen and used. With a biometric card, even if it is stolen, the thief can't use it to get access control. Their fingerprint will not match the reference fingerprint template on the card, rendering the card useless.

Transportation

In the transportation industry, secure and accurate identification is crucial for running a safe and efficient operation. Whether it is creating secure ID cards for employees or easy use customer passes, fingerprint cards make for a smooth experience.

Employees do not have to worry about losing their ID cards and jeopardizing the security of the entire operation, while riders do not need to carry around multiple transit cards. The result is decreased wait times, more convenient payment, and quicker access.

[1] https://www.icao.int/Security/FAL/PKD/Pages/ICAO-PKDParticipants.aspx

> "With fingerprint authentication, employees do not have to worry about losing their ID card and jeopardizing the security of the entire business."

Fingerprint cards can be used along with self-service kiosks to make the process even more efficient. Whether it's the bus, subway, or train, passengers can count on a reliable and secure transportation pass rather than prepaid passes.

Choosing the Right OEM Partner for Your Biometric Fingerprint Solution

Fingerprint recognition in the form of fingerprint cards can be a cost-effective and user-friendly solution for companies. However, you need the right Original Equipment Manufacturer (OEM) partner to deploy your security solution widely. Here are the most critical factors you need to consider when shopping for the right manufacturing partner for a biometric fingerprint solution:

Capabilities

Ideally, your manufacturing partner can provide complex and custom products and solutions. Your product needs depend on the type of functionality you want to achieve. A capable OEM will have multiple resources on hand to meet your unique needs.

Specialty equipment is needed to build security and authentication products. You want to ensure that your OEM partner has suitable manufacturing facilities, utilize cutting-edge technology and materials, and incorporate quality assurance throughout the process.

Experience

OEMs with a good track record and years of experience make for more reliable partners. Your OEM partner should be well versed in integrating and implementing biometric security solutions. They need to understand technology trends and customer expectations, insights that come with experience.

Your manufacturing partner should have experience providing cybersecurity products and digital security system solutions worldwide. They will know how to meet international compliance and regulations, saving you potential headaches.

Engineering Expertise

You want an OEM partner that hires many R&D engineers and continuously invests in R&D. That collective expertise enables the continuous development of diversified types of innovative products with international patent rights and certifications.

Your manufacturing partner should know how to effectively protect sensitive information, data, and software from potential breaches. Without the necessary expertise behind the products, their solutions will struggle to meet your demands and applications.

Cost

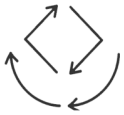
A solution's cost is a crucial factor to consider for any organization, and some OEMs offer more affordable solutions than others. If a solution is not financially practical to deploy in bulk, you have to look elsewhere.

Your ideal OEM partner should offer advanced and reliable products with a high cost-to-performance ratio. Your customers will be expecting products to be cost-effective and dependable, and you need an OEM partner who can help meet those demands.

Quality

Many factors, including engineering design, experience, and procurement, can impact the product's quality. The manufacturer's supply lines and equipment can also affect the quality of their cybersecurity and biometric solutions.

Your OEM partner should conduct quality control checks throughout the manufacturing process. What standards do they have in place to guarantee product consistency and quality? Are QC checks conducted by hand or by machine?



Flexibility

When it comes to product design and manufacturing, requirements and demands can change in a short time frame. It helps to have the flexibility to add parts, customize machines, and adjust models on a quick turnaround. Your OEM parts need to be error-free and on schedule.

The right OEM partner will provide you with the right solutions at the right time to help you meet your goals. They will have the infrastructure to manufacture parts and products of varying size and complexity.

Conclusion

Using biometric authentication for payment and access control tasks has made our personal and work lives more convenient. However, authentication solution providers must securely handle their users' sensitive biometric information, such as their fingerprint data.

Biometrics is a quickly growing field, with facial recognition, iris recognition, and fingerprint recognition gaining the most attention. With so many solutions out there, companies must choose a solution that maximizes security and user experience.

Facial recognition was one of the first biometric technologies available, but fingerprint authentication solutions have become the most sought after. This paper examines four significant reasons why organizations prefer fingerprint authentication:

1. Decreased security risk
2. Increased user privacy
3. Low technology cost
4. Seamless user experience

This paper concludes that FEITIAN's new fingerprint card offers a smoother and more secure user experience for fingerprint biometrics. Powered by Ambiq's ultra low-power system on chips, the fingerprint card of the future can help today's companies now.

To find out how FEITIAN's solution can provide a scalable and seamless consumer experience, please visit or email us at world.sales@ftsafe.com. To learn more about Ambiq's ultra-low-power processors for your biometric solutions, visit www.ambiq.com or email us at marketing@ambiq.com.

About the Company

FEITIAN

Established in 1998, FEITIAN Technologies is a leading global provider of cyber security products and solutions.

Our customers are located in more than 100 countries and regions. Five oversea branches in Asia, Europe, North America, and a professional international team enable us to serve our customers all over the world.

FEITIAN has over 1,000 employees, more than half are R&D engineers. The continuous high investment in R&D and the deep understanding of customer needs over the past 20 years have enabled FEITIAN to continuously develop diversified types of innovative products with international patent rights and certifications.

As a public company, FEITIAN has always been committed to provide customers with reliable and cost-effective products. We sincerely looking forward to being your long-term and reliable partner.

More information is available at: www.ftsafe.com

Ambiq

Ambiq was founded in 2010 with the mission to foster a cleaner, greener, and safer environment where mobile and portable devices could either reduce or eliminate their total power consumption from the batteries. We laser-focused on inventing and delivering the most revolutionary system on chip solutions in the market for the last ten years.

Through the advanced Subthreshold Power Optimized Technology (SPOT®) platform, Ambiq has helped many leading manufacturers worldwide create products that can operate for days, months, and sometimes years with a lithium battery or a single charge. For more information, visit www.ambiq.com.

6500 River Place Boulevard, Building 7, Suite 200, Austin, TX 78730
www.ambiq.com
sales@ambiq.com
+1 (512) 879-2850

A-SOCA3T-WPGA01EN v1.1
October 2022