Fingerprint Sensor Technology for Safe and Convenient Card Payments

whitepaper

V1.0 ·· June 2019

NEXT BIOMETRICS

Fingerprint Sensor Technology for Safe and Convenient Card Payments

Banking and payment cards have been issued to consumers for more than 50 years. Technical evolution into today's smart cards was in most cases driven by two key aspects: safety and convenience. The technological development of smart cards is currently on the cusp of seeing yet another major evolutionary step: integration of fingerprint sensor technology.

Contactless smart card technology has significantly increased user convenience and speed of transactions in various use cases – from faster access to public transport to instant settlement of low-value payments at the point of sale.

The constant struggle between payment networks and fraudsters has resulted in the introduction of the EMV®[1] chip as a safer alternative to the magnetic stripe and major payment networks are driving this change on a global level to reduce fraud-related costs. According to The Nilson Report[2] fraud costs rose from 4.5 cents per USD 100 transaction volume in 2010 to 7.2 cents per 100 USD transaction volume in 2016. Fraud losses typically occur from lost and stolen cards, counterfeit cards[3], card-not-present[4] (CNP) transactions as well as fraudulent applications. According to a 2017 report by the U.S. Payments Forum[5], the increased security of EMV smart cards has led to a shift in fraud losses from card-present fraud to CNP fraud with a projected increase in CNP fraud in the U.S. from USD 3.1 billion in 2015 to USD 6.4 billion in 2018.

Whereas EMV smart cards offer much higher security against counterfeit fraud for card-present transactions compared to magnetic stripe cards, they do not address CNP fraud and fraud from lost and stolen cards. According to statistics, consumers carry 2.35 to 3.5 credit cards on average, depending on region. Each requires memorizing the correct PIN. In light of an ever-increasing number of passwords and PIN codes consumers need to enter for a multitude of log-in and access control situations in daily life, the number of PIN codes and passwords that are forgotten, lost and stolen (because they have been noted down) increases. This is where fingerprint sensor technology comes in: payment transactions performed with contact-based and contactless EMV smart cards can conveniently and securely be authorized by the unique fingerprint of the card holder from the first dollar spent.

[1] For further information on the EMV® Integrated Circuit Card Specifications, visit www.emvco.com. EMV is a trademark owned by EMVCo LLC.

[2] The Nilson Report: Card Fraud Worldwide, Issue 1096, October 2016, p. 6f.

[3] Card-present fraud involves unauthorized copying of payment card information when e.g. handing over the card for payment, from skimming devices at ATMs to capture card account number and PIN codes as well as from card information gathered from hacked enterprise servers such as hotels, hospitality services and social media accounts.

[4] Card-not-present (CNP) transactions include payments made via telephone, mail, mobile and online in which the cardholder does not physically present the card to the merchant.

[5] U.S. Payments Forum: Card-Not-Present Fraud around the World, Version 1.0, March 2017, p. 28f.

Larger Sensor Size for Higher User Convenience and Security

It is a matter of fact that smaller sensors are only capturing a smaller number of fingerprint features and thus producing higher failure rates. This has been demonstrated and verified by ➜ independent research.

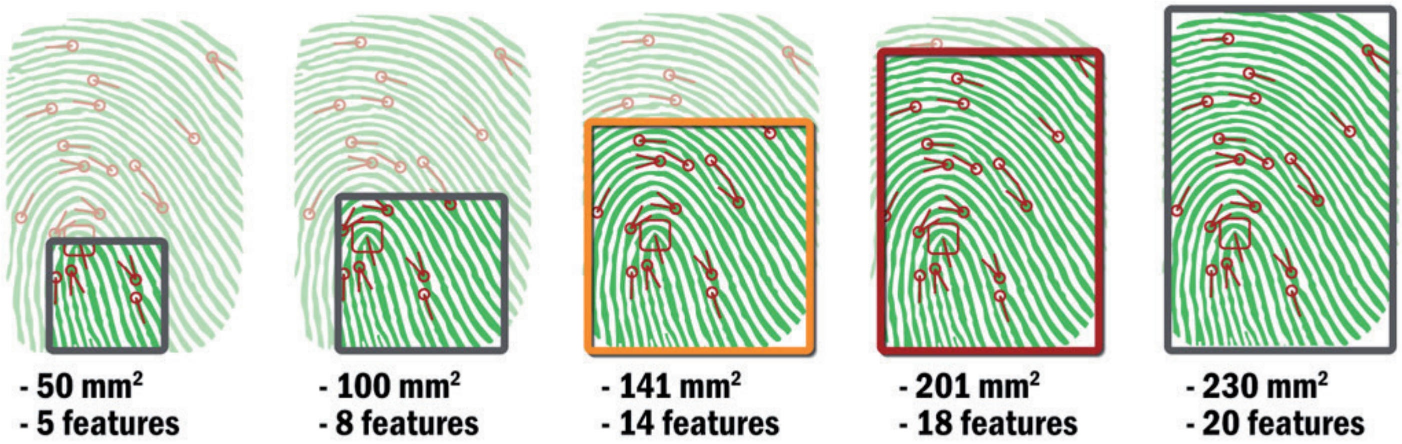
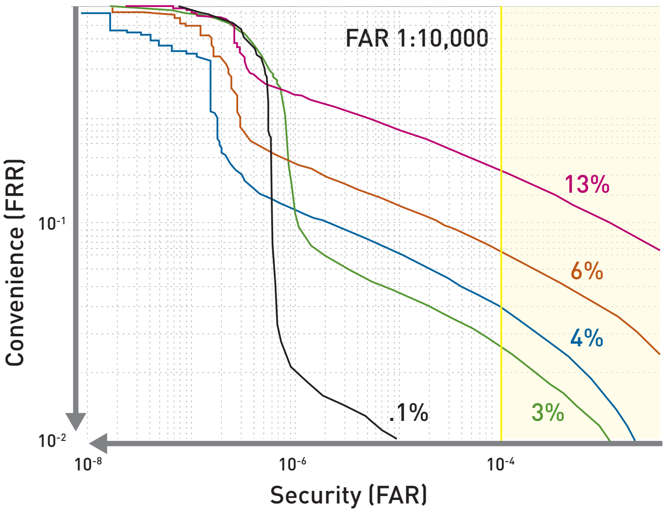


Illustration by: NEXT Biometrics

The Madrid study has clearly shown that NEXT Biometrics' fingerprint sensor technology works 20 times more often than the best competitor sensor and 100 times more often than the worst competitor sensor, resulting in a better user experience and higher user convenience.



Imagine yourself waiting in line for payment. It's Christmas time and the queues are long. Once it is your tun to pay, you put your finger on your biometric payment smart card, but the finger is not recognized, and the transaction rejected. You give it another try while at the same time fiddling around to find your PIN. Another fail and you get embarrassed while people waiting behind you in the queue are getting angry...

A larger sensor size thus significantly improves the user experience and convenience of the payment transaction for both, consumers and merchants. Besides, government regulations demand large-area sensors for high-security applications and in order to meet ISO standards, a sensor must have a minimum size of 169 mm2 and beyond.

Physics Matters!

Fingerprint sensors made out of silicon can only reach a certain size due to the characteristics of the material. Thin large silicon sensors will simply break as glass does. Sensors manufactured from Low-temperature polycrystalline silicon (LTPS), the technology that NEXT Biometrics' sensors are made of, offer numerous benefits over silicon sensors. First of all, the sensors can be scaled to large sizes cost-effectively. Secondly, the sensors can be manufactured in a flexible structure which means that the sensors will bend and not break. This is particularly important if the sensor is due to be integrated into a form factor like a smart card. Many people still carry their wallet in their trouser pockets. "Sitting" on the smart card or dropping it will not result in a broken sensor if the sensor is manufactured from LTPS.

Fast and Smooth Fingerprint Enrollment

Last but not least, a large-size sensor also offers a better enrollment experience for card users. It does make a big difference if you have to touch the sensor only up to 3 times to store your fingerprint data on the payment card or if you have to repeat it over and over and over and over again. Enrollment is the first interaction that consumers will have with their new biometric smart card. As such, this first experience should be as smooth, convenient and seamless as the whole user payment experience when using biometric smart cards.

State of Play & Conclusion

Smart cards have come a long way since they first have been introduced. From magnetic stripe cards to EMV chip cards, constant technological advancements have been driven by two key aspects: safety and user convenience. While the financial industry has started trialing fingerprint sensor technology in payment smart card pilot projects, large-scale adoption of this technology will take some time and to a large degree also depend on user acceptance.

A smaller sensor size will lead to a bad user experience from cumbersome enrollment to failure during transaction. Flexible sensors in contrary are a cost-efficient means to ensure a convenient, secure and carefree payment experience and thus suited to help spur adoption of fingerprint sensor technology in payment.

References

For further information on the EMV® Integrated Circuit Card Specifications, visit www.emvco.com
The Nilson Report: Card Fraud Worldwide, Issue 1096, October 2016, www.nilsonreport.com
U.S. Payments Forum: Card-Not-Present Fraud around the World. Version 1.0, March 2017 www.uspaymentsforum.org/cnp-fraud-around-the-world/