

Analog Dialogue

How Secure Electronic Authentication Mitigates Risk at the Point-of-Care

Aileen Cleary, Marketing Manager, Kris Panaro, Field Applications Engineer, and Chang Liu, Business Manager

Abstract

The growing adoption of rapid point-of-care (PoC) testing has significantly increased the number of in vitro diagnostic (IVD) tests being performed outside of the automated laboratory environment. This article explores the security challenges associated with PoC diagnostics tests, the impact of reuse and misuse of patient samples, and how testing manufacturers can mitigate risk through secure electronic authentication.

Introduction

For many years, diagnostics testing performed on human samples was exclusively processed in clinical laboratories. The trend toward PoC testing is changing this by moving sample processing to the physician's office, clinic, hospital, or even the home. PoC testing brings a clear benefit of achieving a faster time to diagnosis by removing the need to transport the patient sample to the centralized lab. It also has the potential to significantly improve workflows and provide more convenience to the patient. The need for robust PoC testing became significantly more evident during the COVID-19 pandemic when testing delays had a major impact on society and the spread of the virus during the early months of the pandemic.

The trends toward PoC testing are here to stay, and diagnostic manufacturers are broadening their assay portfolio to include multiple targets, such as respiratory panels, sexually transmitted infections (STIs), bloodstream infections, and more. As this market expands, the number of patient samples processed outside of the laboratory setting is steadily increasing. Patient samples are now not only handled by professionals in closely controlled workflows but also by physicians in clinics and patients themselves in their homes, increasing the risk of misuse and reuse.

Challenges in PoC Testing: The Risk of Reuse, Misuse, and Counterfeit Samples

To fully achieve the benefits of PoC testing, the systems must produce a result that can be trusted by both patients and physicians alike. Measurement accuracy is a critical component of this, as without an accurate result, it is clear to see

how misdiagnosis can occur. Even the highest accuracy test could result in the wrong diagnosis if the incorrect patient sample is processed. Providing a means to ensure that the correct patient samples are processed is therefore essential in creating a trusted result and reducing the risk of misdiagnosis.

One major risk factor for patient samples is the potential for reuse. This can happen when a swab or cartridge is accidentally processed multiple times through the testing device. Imagine the scene of a busy kitchen with a large family, all taking home tests prior to the morning school run. It is easy to see how a parent could accidentally reuse one child's swab in place of another. This risk also exists in the clinic or in the growing number of CLIA-waived labs that don't require trained laboratory technicians to perform the diagnostic tests.

A second key risk is the potential for intentional misuse of patient samples. For certain tests, such as the identification of the presence of illegal drugs, patients may be motivated to falsify results. Switching the sample cartridge prior to processing is one way of achieving this. Another challenge to obtaining accurate results is the availability of counterfeit cartridges in the market. In the traditional lab environment, purchasing is done through qualified channels. For home-based PoC testing, patients are often purchasing tests directly from major online retailers. This opens the door to counterfeit suppliers who may have lower quality products leading to less accurate results.

Lab environments are not immune to misuse. After use, sample kits used in the lab are discarded as medical waste. When this medical waste is collected by a third party, there is a risk for sample kits to be refurbished and resold to the test lab. Unknown to the lab, the refurbished kits may appear to be new but will either have no reagents or simply be refilled with water. This can contribute to false test results that can lead to the improper treatment of the patient.

The impact of both reuse and intentional misuse of patient samples can be felt by patients and device manufacturers alike. Patients can experience a misdiagnosis—for example, a false positive test resulting in unnecessary disruption and unnecessary treatment. A false negative would conversely result in delayed diagnosis and ultimately a delay or absence of correct treatment. Device manufacturers can also pay a heavy price in the form of damage to their brand reputation, the unfair labeling of their device as inaccurate, or in a worst-case scenario, triggering a product recall. The prevalence of counterfeit cartridges poses a significant business risk to device manufacturers with the potential to disrupt the lucrative disposable revenue stream obtained from the sample cartridge.

Why Traditional Solutions Fall Short of Mitigating Risk in PoC Testing

There are two traditional methods for ensuring the authenticity of patient samples. One method is labeling, such as 1D or 2D barcoding. The second method utilizes mechanical features that prevent the reinstallation of a cartridge. The use of 1D and 2D barcodes is the favored method of sample tracking in the laboratory environment. Batch information, serial numbers, and unique device identification can be used to ensure the authenticity of the cartridge. In addition, barcodes can be reviewed prior to sample processing to ensure that reuse has not occurred. Although barcodes provide a robust means of ensuring the authenticity of the patient sample, they have limitations. Firstly, barcode labels require a barcode scanner, which places a burden on the design of the instrument due to size and focal length requirements. Barcodes also require significant memory to store sufficient serial numbers to prevent reuse. While this may not be an issue in large laboratory equipment, it is a cost and size challenge for compact PoC equipment. Critically, barcodes are visible to the user, making them less secure and prone to be copied or forged.



Figure 1. The use of barcodes in PoC systems.

The second traditional method is the use of a simple mechanical feature, such as a notch in the cartridge that changes shape or position once inserted into the instrument. Such mechanical features provide a simple means of preventing reuse that can be implemented at a low cost into the system. They are however identical cartridge to cartridge, hence providing no means of distinguishing one patient sample from another. They are visible to the user and are typically easy to copy, making the design prone to counterfeiting. Mechanical features can also be reset when used kits are refurbished by an unauthorized party. As PoC devices shrink, adding a mechanical feature to the cartridge poses an additional design burden.



Visible solution that can be forged
Places design burden on equipment

Figure 2. The use of mechanical features in PoC systems.

What Is Electronic Authentication and How Is It Improving PoC Testing Results?

Finding an ideal solution for the PoC market involves looking beyond these traditional methods to electronic authentication in the form of an IC that can be integrated into the cartridge. An electronic authentication IC provides a robust means of preventing both cartridge reuse and misuse. Firstly, to address reuse, electronic authenticator ICs contain secure decrement counters that ensure single-use cartridges are only processed once. An integrated numeric unique ID identifies one patient sample from another. The potential for misuse is also addressed with the integration of cryptographic-based challenge-response algorithms that prevent third-party manufacturers from creating counterfeit cartridges. Secure authenticator ICs provide additional features, such as the ability to securely record usage history in the form of a timestamp. This can be valuable when tests need to be run frequently or at specific times each day.



Figure 3. Electronic authenticator ICs in PoC systems.



Figure 4. Secure electronic authentication from ADI.

Unlike barcodes and mechanical features, electronic authenticator solutions are integrated inside the cartridge, making the security solution invisible to users and potential counterfeiters. A compact IC also reduces design challenges associated with the size constraints of a compact PoC instrument.

By adopting an electronic authenticator IC, the risk of reuse and misuse of sample cartridges is greatly reduced, providing patients and device manufacturers a level of assurance that the testing results are authentic and can be trusted.

Electronic Authentication Solutions from Analog Devices

Analog Devices' portfolio of electronic authenticator ICs provides a turnkey solution that can be easily integrated into a PoC cartridge without extensive knowledge of cryptographic technology.

Each secure authenticator IC has a unique 64-bit serial number for secure identification and traceability of the cartridge or device. The secure memory safeguards sensitive data including manufacturing information or calibration parameters and prevents tampering. The authentication features industry-standard symmetric key SHA-2/SHA-3, or asymmetric key ECDSA crypto

algorithms to ensure the cartridges are genuine and prevent the use of thirdparty counterfeits. An integrated, secure, decrement-only counter simplifies use management and prevents the reuse of the disposable cartridge. Key products for the PoC application include the DS28E16, which uses a simple 1-Wire^{*} communication interface, and the MAX66250 with an NFC contactless interface. ADI's electronic authenticator ICs can be integrated into a design without the need for a dedicated PCB, providing a solution that eases compact PoC design.

Conclusion

The rise of PoC testing is driving the need for greater security and traceability of patient samples. Device miniaturization along with the heightened risk factors associated with PoC testing is challenging traditional means of patient sample tracking, such as the use of tracking barcodes popular in lab settings. An electronic authentication IC, such as the DS28E16 from ADI, will ease the design of PoC instruments and help device manufacturers mitigate security risks, reducing the potential of misdiagnosis, delayed diagnosis, or product recall.



About the Author

Aileen Cleary is the marketing manager of the Medical Instrumentation and Life Sciences Business Group at Analog Devices. She focuses on driving business and innovation through customer-centric engagements. Aileen has over 17 years of experience in the semiconductor industry, holding various technical and business roles in both the energy and healthcare markets. Aileen holds a master's degree in electronic and electrical engineering from the University of Edinburgh, Scotland.



About the Author

Kris Panaro joined ADI in 2021 and is currently a field applications engineer for Northeast America. Kris has a strong background in medical device design, particularly in the field of molecular diagnostics. Kris holds a bachelor's degree in electrical engineering from the State University of New York at Buffalo.



About the Author

Chang Liu is a business manager for secure authenticator products at Analog Devices with a special focus on developing broad market business in North America. Chang joined Maxim Integrated (now part of Analog Devices) in 2001 and has been supporting various product line development. She holds a master's degree in electrical engineering from Texas A&M University, College Station, Texas.



For regional headquarters, sales, and distributors or to contact customer service and technical support, visit analog.com/contact.

Ask our ADI technology experts tough questions, browse FAQs, or join a conversation at the EngineerZone Online Support Community. Visit ez.analog.com.

©2023 Analog Devices, Inc. All rights reserved. Trademarks and registered trademarks are the property of their respective owners.