End-to-End (E2E) Cash Authentication: A Revolution to ATM Security?

Jackpotting at the ATM is a global problem that has been growing more severe over the last several years. A successful attack may not only result in financial losses, but also have long-lasting effects on the ATM deployer's brand image. To combat this type of attack, the CEN/XFS committee will publish a new security standard later this year called End-to-End (E2E) Cash Authentication that will help eliminate the vulnerabilities that make jackpotting possible. We talked to security expert Andi Coleman and our own Matthias Runowski and David Powell to find out what we might expect from this new standard.

Andi Coleman
Information Security Officer,
Bank of America

Matthias Runowski
Director R&D Security,
Diebold Nixdorf

David Powell
Product Management,
Diebold Nixdorf

The weak link in protecting against jackpotting has always been the cash dispenser's inability to authenticate the dispense request. Securing and authenticating the channel between both the ATM and host as well as CPU and dispenser provides some protection, but if the attacker can either inject malware into the ATM or successfully attach a black box it can be bypassed.	**WHY SHOULD FIs CONSIDER USING E2E CASH AUTHENTICATION?**	E2E is the next step in protecting cash transactions. It's a holistic approach where the entire transaction is authorized and authenticated by the secure host environment of the customer. Thus, the protection of transactions does not rely on local countermeasures on the system only and improves the protection from certain attack types considerably.
Depending on the implementation, E2E authentication would enable additional authentication factors (channel within ATM and Host) to better ensure dispense request is authorized. Logical attacks would require an increase in sophistication with both insider access and a coordinated onsite assistant.	**HOW WILL E2E CASH AUTHENTICATION CHANGE THE GAME?**	E2E is a new approach to protect cash transactions at a self-service system. Using state-of-the-art security protocols—that are already well known to the financial services industry—it moves dispense authorization from the local ATM to the more secure network host. Enhancing what has been the standard method of running ATMs for 30+ years, will protect against black box, jackpotting and network-based attacks. E2E offers a new level of ATM security.
Cyber-attacks will always require layers of defense, both logical and physical and from ATM to it host application. E2E cash authentication will not solve all ATM jackpotting. From experience, as soon as one weakness is discovered they will find or create others to harvest data or access cash. Inserting E2E in the process may now put a level of risk to ATM host and its networks. Network and data security controls need to expand to protect the entire transaction and its process, not just card and PIN. Sophisticated attacks may now concentrate on issuer hosts, payment networks and ATM acquirers, leaving ATMs only as a means to access the cash and no longer the point of attack. Attackers will always go for the easiest targets both from a logical and physical perspective. Older ATMs with known weaknesses that can't support current security controls (e.g., weak safe doors, old operating systems, insecure communications channels to host/cash dispenser, unencrypted hard drives, etc.) or ATMs with limited site security will always be vulnerable.	**SHOULD FIs STILL CONSIDER OTHER LAYERS OF SECURITY TO PROTECT THEMSELVES FROM CYBERATTACKS?**	Effective security is always a combination of countermeasures and should be designed in a layered approach. There is no one single countermeasure that protects against everything. The intelligent combination of different countermeasures should be the standard. While E2E significantly reduces the risk of black box and jackpotting attacks, effective protection against physical, data and other cyber-attacks secures customer data and maintains operational integrity.
It is a new standard. Much depends on ATM vendors' ability to support, updates by software vendors to host applications and with primary push from FIs and processers to those vendors to support them. If existing standards and processes, such as X9.24-2 and TR-34/X9.139 can be leveraged, implementations may be faster and more streamlined. If I were to guess, early implementors (those who are already suffering losses) may have something in place within the next two years, again, depending on those vendors who are needed to support it.	**WHEN DO YOU THINK WE WILL SEE THIS SOLUTION IMPLEMENTED?**	The CEN standard for E2E is expected to be released in late 2022, and DN is already working on product offerings to provide upgraded protection for our customers shortly after. But implementation will take time as it requires a change to standard methods and software that have been used for 30+ years. As with any new standard, we expect FI's will migrate to E2E based on their own schedule and perception of risk as well as other planned upgrades and support activities.
At this point, I don't see a significant difference in the way networks are managed. But, it would require changes to the ATM application, the cash-dispenser, and the ATM host application. The level of impact depends on how both message integrity and non-repudiation is achieved. PKI signatures can authenticate the host, but there needs to be a counter or date timestamp or something shared and known between dispenser, ATM application and ATM host to prevent replay attacks. The biggest issue here is ensuring consistent implementation so neither the software vendors nor the FIs need to worry about supporting different methodologies and implementations. Differences result in extra time and effort needed by FIs to keep up with changes as the standard and implementations mature. ATM acquirers will assess the cost benefit of this as usual for any security counter measure. Organizations with the highest risk due ATM numbers, locations, etc., along with organizations already being hit by black box attacks, will likely the first implementers.	**IMPLEMENTING E2E WILL BE A CHANGE FROM THE WAY ATM NETWORKS HAVE ALWAYS WORKED. WILL E2E BE A SIGNIFICANT ENOUGH BENEFIT TO ENCOURAGE FIs TO UNDERTAKE THESE CHANGES?**	Successful FIs are always looking at opportunities for efficiency and improvement. Innovation in self-service banking has traditionally been focused on providing additional customer convenience at the ATM (single throat deposit, cash recycling, etc.). The new CEN standard for E2E offers security benefits—against an attack type that has grown in frequency recently no less—that were not practical before, especially without an industry standard.

THE TAKEAWAY

End-to-End cash authentication takes a new and promising approach to protecting the ATM from attacks like jackpotting. How reliable this protection will be and how long it will take attackers to find a way around it will need to be seen. However, a multi-layered approach to security will remain necessary to ensure that cash and users are kept safe. Nevertheless, considering the growing frequency of jackpotting attacks, financial institutions need to evaluate if E2E cash authentication could provide them with the needed security.