ANDOPEN Aims Global Expansion with Serverless 1:1 Biometric Authentication ‘SnapPass’ - 'Managed and Protected by Users'

“Our On-Device AI Architecture Eliminates Hacking Vulnerabilities by Keeping Personal Biometric Information Securely in the Hands of the Individual.”

Jayden Lee, CEO of ANDOPEN

Promotional image of ANDOPEN’s SnapPass | Image provided by ANDOPEN

PANGYO, GYEONGGI-DO, SOUTH KOREA, July 16, 2026 /EINPresswire.com/ -- Amid growing concerns over recent cloud server hacking incidents and large-scale personal information leaks, a security technology startup that’s reshaping biometric authentication is drawing intense attention. The player in the spotlight is ANDOPEN Co., Ltd. (CEO Jayden Lee), headquartered in Pangyo Techno Valley, Seongnam-si, Gyeonggi-do. Departing from the conventional method of storing biometric data on centralized servers, ANDOPEN introduced ‘SnapPass,’ a privacy-centric multi-factor biometric authentication solution rooted in the philosophy that personal data must be held and controlled directly by the user rather than a server.

Because traditional biometric systems store vast amounts of personal information on central servers linked via cloud networks, they inherently pose a risk of massive data breaches in the event of a hacking attack. Furthermore, once biometric data is leaked, the consequences are critical and permanent, as it cannot be altered like a standard password.

Jayden Lee from ANDOPEN (right) answering questions at the interview

To resolve these structural vulnerabilities, ANDOPEN devised SnapPass. The comprehensive solution primarily consists of 'SNAPPIN' (also known contextually as the card-type token 'Snap'), a physical token carried directly by the user; 'SNAPCHECK MOAI' (also known on-site as SnapCheck), an on-device facial authentication terminal; and an integrated management platform, SPMS. Users face no complex registration or operational processes; they look at the terminal and tag their token on-site, encapsulated in the concept "JUST LOOK & TAG." Once the token is tagged, the terminal performs an instant 1:1 comparison and analysis between the compressed, encrypted facial data stored within the token and the live facial images captured by the terminal's camera.

The most prominent advantage of SnapPass is its absolute independence from networks during the authentication cycle, ensuring that no biometric footprints are left on the terminal. The facial imagery captured solely for authentication purposes is entirely deleted from the device immediately after the verification process concludes, fundamentally eliminating the risk of personal data leaks. Moreover, unlike conventional 1:N (one-to-many) biometric methods, where the probability of misidentification escalates as the user base expands, SnapPass performs exclusive 1:1 matching against the presented token, reducing the possibility of false recognition to near 0%. ANDOPEN has named its proprietary technology an 'On-Device AI Physical Access Control Solution.'

The company's technical expertise has already been recognized globally. It achieved the milestone of winning the CES Innovation Awards for two consecutive years, secured an Outstanding Information Security Technology designation from the Ministry of Science and ICT, and was named a finalist for the GLOMO Awards at MWC.

Pangyo Techno Valley met with ANDOPEN CEO Jayden Lee at the Startup Campus to discuss their decentralized security ecosystem, strategic enterprise pipelines, and upcoming international roadmap.

Q1. Can you introduce your company and share the vision behind it?

A. Our company, ANDOPEN, approaches biometric recognition in a fundamentally different way compared to conventional methods. When people think of biometrics, they usually think of a user's personal data being dependent on or stored within a cloud network or a device. In fact, all

security vulnerabilities in biometrics stem from that exact storage model. Because conventional systems store data in the cloud, your personal information is outside your direct control, creating inherent vulnerabilities. Users have no way of knowing whether their data is being used correctly or misused. Furthermore, if biometric data gets leaked even once, it's not information you can change like a password. Because it exists in such a high-risk format, we decided to build a physically independent system called 'SnapPass' in which the user directly controls all of the user's personal information.

Q2. So the answer here is instead of putting the information somewhere else in someone else's hands, you put it back in the user's hands. How exactly does that work?

A. Our integrated solution is called SnapPass. This ecosystem consists of a device called 'SnapCheck' and a dedicated card-type token called 'Snap' that compresses, encrypts, and stores the user's personal information via AI. To support mobile token use cases, we also offer it as a QR code. Additionally, the ecosystem includes a management platform, SPMS, to oversee the entire process. All personal information resides solely on this physical token. When a user takes this token and tags it onto the device, the system immediately runs the primary token authentication layer to filter and verify whether it is a valid token with access rights. Once it is verified as an authorized token, the device initiates the secondary authentication layer by capturing the user's face with its camera and comparing the live camera image with the compressed, encrypted data stored within the token to verify that the person holding the card is indeed its rightful owner.

Q3. A key point is that anyone can take a traditional physical key and use it, but this token ensures that only the rightful owner can use it. And then what is the benefit of that?

A. Since users always carry their biometric information in a physically independent format, the SnapCheck hardware device stores no personal information. Although it captures a facial image via the camera for face recognition, the process immediately deletes all acquired personal information after verification. Conventional biometric systems inevitably experience an increase in false recognition rates as the user pool scales up. With our model, the possibility of false recognition is eliminated because it always performs a strict 1:1 local matching process. Consequently, it remains free from false acceptance errors, imposes no limit on the number of registered users, and requires no network connection. Never sending personal data over a network creates a powerful differentiator. This is why we refer to our SnapPass solution as an "On-Device AI Access Control Solution."

Q4. What are your initial target industries or commercial spaces where you see this solution being deployed first?

A. Our primary target market is physical access control—the physical security market. We're focusing our initial efforts on this sector. Once we establish solid trust and a proven track record there, our goal is to expand into other verticals. A prime example is membership management at

Costco, which cleanly resolves the issue of membership card sharing and unauthorized use with minimal overhead. With support from the Seattle Economic Development Office, we're continuing to engage with Costco about potential deployment. In addition, we are already moving forward on several fronts. Through our sales pipeline in the United States, we are currently progressing projects for casino memberships and patient registration cards for large-scale US hospitals. Concurrently, we finalized a supply agreement to deliver our workforce management solution to a food manufacturing facility in the US, with deployment confirmed for this September.

Q5. That sounds like a major step. Are there any notable deployments or validation projects happening locally in South Korea?

A. Yes, we are currently moving forward with a significant agreement. We were selected for a demonstration project managed by the National IT Industry Promotion Agency (NIPA) in Korea to apply sustainable development solutions to data centers. Data center security is obviously incredibly critical. We are conducting a pilot project to upgrade their security infrastructure with our multi-factor authentication system, which will run until the end of this year. We are also planning a validation project with an international organization to verify the employment credentials of vocational trainees across South America, accelerating our global expansion.

Q6. You mentioned earlier that personal data is not managed in the cloud or on a server. How does the system handle overall management and administrative monitoring if the data is entirely decentralized?

A. Since we do not store personal data on a cloud or server, people often wonder how the administration works. We manage the ecosystem strictly through the token's hardware serial numbers. A separate layer is built entirely within our SPMS management platform to handle these audit trails and management configurations without touching personal identities.

Q7. Can you share more about your upcoming international roadmap and where your solutions are launching next?

A. Currently, we are receiving partnership requests from a wide range of companies in the United States and in European countries such as Spain, Italy, Switzerland, and Portugal. Most security tech firms in Korea tend to start locally, enter the Japanese market, and then gradually pursue global expansion. We took a slightly different path. By participating multiple times in major international platforms such as CES and MWC, we proactively identified global partners. For instance, a partner company that anchors its operations in Spain and runs parallel branches in Switzerland signed an MOU with us directly on-site at the MWC exhibition floor last March. They are actively promoting our solution across Europe, and we have been invited to present at their upcoming Partners' Day in Switzerland this September.

Q8. What are your thoughts on Pangyo Techno Valley as an innovation hub for tech companies

like ANDOPEN?

A. A few years ago, a Japanese buyer mentioned to me that Pangyo feels like a place where only geniuses gather. He was amazed at how many companies here are successfully commercializing advanced concepts. I strongly agree with that sentiment. The infrastructure, support agencies, and tech enterprises are tightly clustered here to foster rapid technology development. It offers a significant competitive edge over other regions. Furthermore, since the headquarters of South Korea's leading IT giants are concentrated in the Pangyo and Bundang areas, it is geographically advantageous for recruiting top-tier technical talent.

Q9. What is the ultimate goal for ANDOPEN moving forward?

A. Our ultimate goal is to establish SnapPass as the global standard for secure identity and biometric access control. We are working to reach the global stage, and soon you will see our serverless authentication solutions deployed worldwide, returning data sovereignty to individual users.

Kim Seung Yeon
Gyeonggi Business & Science Accelerator
+82 31-776-4834
email us here
Visit us on social media:
LinkedIn
Instagram
Facebook
YouTube
Other