authID Announces Out of the Box, Biometric Security Solution Aligned with PIV Security Framework for Energy and Other Critical Infrastructure

February 12, 2026

Power grid and other critical utilities to benefit from authID's biometric platform

Denver,CO, Feb. 12, 2026 (GLOBE NEWSWIRE) -- authID (Nasdaq: AUID), authID, a leader in biometric identity, today announced the availability of its biometric security solution aligned with the Personal Identity Verification (PIV) security framework for energy infrastructure companies and other utilities. authID's industry-leading suite of biometric identity assurance solutions allows utility companies to secure US electrical, water, gas, and other critical infrastructures beyond standard homegrown defenses, with the highest grade safeguards.

Energy companies and other utilities are constantly targeted by state-sponsored infiltrators and cyber-criminals. Securing electrical, water, gas and other critical utility infrastructure is not just in the public interest, but also a matter of national security.

Utility threats are in the news every day. Iranian, Chinese, and Russian actors have compromised electric, water, and communications systems globally for many years. According to cyberthreat reporting from Check Point Research, there were 1162 documented cyberattacks on US utilities alone from January to August 2024, a 70% increase over the same period from the previous year.

In 2025, the FBI alerted a major water utility in Massachusetts that Chinese hackers had infiltrated water utility systems, gaining the ability to control chemical inputs and potentially poison the water. According to the 2025 US Homeland Threat Assessment, Chinese state hacking groups like Volt Typhoon are pre-positioning hacks for high-impact future disruptions.

Despite mandates to modernize aging infrastructure and security technology from the Nuclear Regulatory Commission (NRC) and North American Electric Reliability Council Critical Infrastructure Protection (NERC-CIP), experts worry that many defenses remain outdated, and inadequate for dealing with sophisticated foreign and AI-powered attacks.

The growing use of AI expands the threat surface. Gartner predicts that by 2027 40% of utilities will deploy AI-driven operators in control rooms, with that number expected to more than double by 2028.

Clearly these utilities require the top level of digital and facility security in the U.S. For public trust and social stability, public utilities must safeguard their services by preventing cyber-driven outages. The way to prevent these threats and lower the risk of bad actors accessing critical resources, is to tie access to a live person's face with biometrics.

The highest level of identity security that infrastructure organizations can deploy is based on a federal standard called PIV (Personal Identity Verification). It relies on establishing definitive identity before issuing access, then enforcing that access for employees, contractors, and other authorized parties. In addition, credentials must be utilized in issuing physical access.

Energy companies also utilize SCADA (Supervisory and Control Data Acquisition) systems for real-time monitoring and control of physical processes. They require identity verification as well as Multi-Factor Authentication but this still often relies on vulnerable passwords. PIV mandates strict background-check-based identification for government facilities, in accordance with NIST standards for highest assurance credentials. Therefore applying a solution aligned with a PIV-grade security framework to utilities administration represents a massive upgrade.

Alignment with PIV-level authentication represents a major step up from standard civilian methods. It can be thought of as military grade authentication for energy infrastructure and many other global businesses requiring the strictest security. authID is now one of the first organizations offering an out-of-the-box biometric security solution that incorporates the methods and processes associated with the PIV security framework and applies them to civilian operations, locking down SCADA consoles, privileged engineering accounts, and contractor access to operational environments without the need for passwords or physical tokens.

"We cannot overstate the level of security needed for these locations," commented Rhon Daguro, CEO of authID. "Interruptions to gas, water, or electricity delivery can cause widespread chaos. Nuclear facilities are especially sensitive. Our biometric identity verification solution ensures only authorized access to these critical systems, by binding an identity to a live human, and defending against spoofs, deepfakes, and imposters. There is no other platform offering that out of the box. We provide a scalable path to higher trust without user friction, and on Day One our clients can operate with confidence and security without the vulnerability of legacy tools."

Three other authID solutions contribute to this unique biometric security platform: IDX, PrivacyKey and authID Mandate. IDX enables central management of identities across the ecosystem of a standard utility that includes not only employees but many contractors, vendors, and other third parties. PrivacyKey utilizes cryptographic keys to identify returning users, providing the most accurate biometric verification while achieving user privacy and strong compliance with laws prohibiting the storage of biometric data. Mandate locks down Agentic AI, allowing only authorized users to launch AI agents while providing the audit trail linking users to the agents they invoke.

Daguro added, "According to the U.S. Energy Information Administration, the top US energy suppliers are natural gas at 40%, nuclear at 18%, coal at 17% and renewables at about 24%. authID can provide the most impactful security for all of them. With the aggressive investment now flowing to the energy sector, we expect to lead the way on securing this vital infrastructure."

For a copy of authID datasheets on how to lock down access to critical utility sites, contact sales@authid.ai.

About authID Inc.

authID® (Nasdaq: AUID) ensures enterprises “Know Who's Behind the Device™” for every customer or employee login and transaction through its easy-to-integrate, patented, biometric identity platform. authID quickly and accurately verifies a user's identity, to enable only legit users. Leveraging a 1-in-1-billion False Positive Rate for the highest level of assurance, coupled with industry-leading speed and privacy-preserving technology, authID provides the most secure digital identity experience. Our IDX and authID Mandate solutions secure the distributed workforce of employees, contractors, and vendors, as well as bring authorization and accountability for AI agents. authID’s PrivacyKey ensures compliance with laws on personal data storage while protecting user privacy. By creating a biometric root of trust for each user, authID stops fraud at onboarding, prevents account takeover, detects and stops deepfakes, eliminates password risks and costs, and provides the fastest, frictionless, and most accurate user identity experience in the industry. For more information, please visit www.authID.ai.

Investor Relations Contacts

authID Investor Relations
investor-relations@authID.ai