SOLUTION BRIEF

REDCOM Z-AUTH™

MULTI-FACTOR IDENTIFICATION & AUTHENTICATION WITH ZERO-KNOWLEDGE

REDCOM Z-Auth™ is a multi-factor identification and authentication system for vetting access to confidential resources — such as sensitive data and secure communication channels — without the need to store user secrets on the client or server side. This makes REDCOM Z-Auth highly secure against data breaches.

Z-Auth supports a novel combination of security questions related to multiple domains (i.e., what you have, what you know, who you are, or where you are) in the construction of interactive zero-knowledge proofs (ZKP). ZKP is a cryptographic primitive for a prover to convince a verifier of the possession of a secret without revealing it. These proofs are mathematically sound and offer a provable security guarantee.

Z-Auth offers unique capabilities aimed at balancing usability and security

REDCOM Z-Auth supports:

- **Policy-based binding** of the type of security questions to the different confidential levels of access, allowing low-confidential resources to be accessed in a frictionless manner while maintaining high security for others.
- **Unique identification of multiple authenticated devices** on which a user is authenticating, preventing access from unauthorized devices.
- **Secure handling of authentication tokens**, avoiding unauthorized access from compromised user devices.
- **Secure, multi-round, and interactive proofs** with a small set of private information, improving overall usability.
- **Ubiquitous accessibility to public authentication tokens** by integrating ZKP with distributed, decentralized, and immutable data log systems.

Compared to the two-factor authentication protocol, Z-Auth offers users of the system flexibility in whether, how, and to what extent to prioritize usability vs. security in particular scenarios.

REDCOM has confirmed the feasibility of Z-Auth via an established demo along with establishing the correctness of the mathematical concepts used. REDCOM has filed a provisional patent on the designs that enable the aforementioned capabilities. REDCOM is working with security researchers to incorporate Z-Auth into the REDCOM Sigma® C2 platform and the REDCOM Secure Client for Android™ and Windows®.

Use Case in Secure Communications

REDCOM develops C2 communications systems and clients for Android and Windows end instruments that are currently used by various military programs, including the U.S. Army Network Integration Technology Enhancement (NITE) Program.

By incorporating Z-Auth into our call controllers and end instruments, commanders will be able to ensure that only validated personnel can gain access to critical communication resources at various security levels. Z-Auth's flexibility allows it to conform to any local policy. Network resources and applications within Sigma can be configured to hold varying levels of sensitivity, which can require different methods of authentication. For example, in the context of the mission at hand, access to a chat application may be minimally-sensitive while access to a given voice conference may be regarded as highly sensitive. In either case, Z-Auth can be configured to require more stringent authentication for more sensitive resources. Resources of low sensitivity may require authentication mechanisms that are swift, such as an RFID/NFC tag. Highly sensitive resources, however, may require more authentication data of more robust quality: a rifle serial number, a biometric scan, and a known call sign or rotating passphrase, for example.

This concept of varying sensitivity enables routine enforcement of whatever local policy is required for the mission. Z-Auth can also be altered as changes in policy occur, meaning authentication requirements can adapt to any context: from the command post to the battlefield and everywhere between and beyond. When coupled with existing REDCOM platforms, this flexible policy enforcement ensures that critical network resources are only used by those authorized to do so.

Furthermore, with Z-Auth's wide range of possible authentication tokens, end users can quickly authenticate themselves for rapid, frictionless access to critical services and applications provided by REDCOM. Due to Z-Auth's fundamental architecture, this robust authentication is secure even in surveilled environments, as all traffic generated by Z-Auth's mechanisms is completely void of meaningful intelligence for the adversary. These characteristics make Z-Auth the next-generation platform for strategic, operational, and tactical authentication.

Z-Auth Key Differentiators

- **Immune to man-in-middle and replay attacks.** Authentication tokens are randomized public information and only valid in each round of the interactive proofs.
- **Immune to data breaches.** Data breaches are the natural consequence of centrally hosting thousands of user credentials; a problem for many password-based authentication systems. With Z-Auth, no secret, or sensitive personal data is stored in the prover and verifier's devices. Instead, a vector of authentication tokens is stored on devices for proving one's identification, which if compromised, does not release sensitive information of the user.
- **Immune to data manipulation.** When an Immutable Data Log System is deployed to store the public authentication tokens, built-in auditability measures prevent anyone from maliciously changing any data.
- **User-to-user authentication across multiple domains or agencies.** Oftentimes sharing resources between various agencies becomes problematic since each agency wants complete control of the resource. With Z-Auth, users can authenticate directly to other users as long as both can lookup the public authentication tokens from the shared database across the agency. Therefore, no 3rd party service is needed to handle the authentication process.