grc outlook

Leveraging Passkeys for Strong Authentication of Dynamic Teams of Enterprise Users

By Sarbari Gupta, CISSP, Electrosoft Inc

In various disaster response and emergency scenarios, users from different enterprise organizations (such as nonprofits and state, local, and federal government entities) form dynamic teams to perform critical, time-sensitive operations in tactical, often challenging environments. These teams transcend organizational boundaries to pool the collective expertise, resources, and perspectives of members. Such collaboration fosters synergy, efficient problem-solving, and effective solutions.

To accomplish their short-term mission, dynamic team members must securely share data and access common online applications. Often, based on the sensitivity and criticality of the shared information, it becomes crucial for purposes of integrity and data confidentiality for these users to authenticate strongly to online tools and services, validating their identity and their rightful position on the team.

Typical identity authentication options for dynamic teams include passwords, often supplemented with one-time password (OTP) mechanisms delivered via SMS, email, or authenticator apps. However, these solutions are considered weak at best due to vulnerabilities such as password reuse, phishing, and malware attacks. Stronger authentication methods, such as biometrics or cryptographic tokens, are recommended for enhanced security and protection against unauthorized access.

Strong authentication solutions often come with high costs, time-consuming implementation processes, and complexity, however. It is often impractical to institute such solutions for short-term, rapidly forming teams of individuals from different organizations.

The FIDO (Fast Identity Online) Alliance developed passkey technology to enhance online security and authentication. Passkeys utilize public-key cryptography where the private key remains securely stored on the user's device and the public key is registered with service providers. This approach enables strong authentication while reducing the risk of password-related attacks and breaches. Major vendors, including Google, Microsoft, and Apple, have actively participated in the FIDO Alliance to promote this technology. As a result, passkey support exists on most traditional and mobile operating system platforms (such as iOS, MacOS, Android, Windows) as well as popular browsers (such as Chrome, Edge, Firefox), making it easy for users to generate and use passkeys for online applications that allow their use.

Enterprise users typically undergo moderate to strong levels of identity proofing to obtain organizational identity credentials. Such identity credentials, which often include multifactor authentication techniques, enable users to access their organizational email accounts and other organizational applications and services.

A novel approach leverages organizational users' existing identity credentials to generate new passkeys for use within dynamic teams, thereby combining the strength of organizational identity proofing with the strength of FIDO passkeys. The proposed workflow would involve the dynamic team leader establishing the required online applications/services as usual but with support for passkey-based authentication. The team leader would do so by identifying dynamic team members through existing methods, requesting their enterprise email IDs, and validating their IDs as consistent with their organizational affiliation. Then, the team leader would send a short-lived, one-time use link to the members' email IDs requesting that they sign up for passkey access to the online service established for them.

Then, dynamic team users would individually authenticate to their organizational IT environment using their existing credentials for accessing their email. Using their own mobile or traditional computing device, they would retrieve their individual link for passkey creation designed for online authentication to the team applications/services. The link would guide them through the process of new passkey creation on their device. Typically, users would also be prompted to establish a biometric factor or PIN to unlock their new passkey.

Subsequently, each time users require access to dynamic team online services, they will authenticate using the unique passkey established above. Depending on usability factors and

the criticality of the application involved, users may need to unlock their passkey for each use or only on an intermittent basis. Notably, using a biometric modality as the second factor facilitates use in a fast-paced tactical environment.

The benefits of this approach are:

- **Fast Rollout:** Since most user devices already possess functionality for passkey generation and usage, rolling out a passkey-based system is fast, low-cost, and relatively simple. Leveraging the existing identity proofing of organizational users makes the issuance of the passkey quick and painless while increasing the assurance that the team member (user) is indeed who they claim to be.

- **Increased Security:** A primary advantage of passkeys is their ability to enhance security. Traditional password-based authentication systems are susceptible to various threats such as brute-force attacks, phishing attempts, and password reuse. Passkeys eliminate these vulnerabilities by leveraging cryptographic algorithms and multifactor authentication techniques. Since passkeys are stored on separate devices, they are less prone to compromise than passwords stored on servers or transmitted over networks. In addition, use of biometric authentication methods, such as fingerprints or facial recognition, further strengthens the security of passkeys.

- **Streamlined User Experience**: Passkeys not only bolster security but also offer a streamlined user experience. Compared to the hassle of remembering complex passwords, passkeys provide a more seamless authentication process, as users only need to physically possess their cryptographic key (typically stored on their device) and follow simple steps to authenticate their identity.

When the dynamic team is no longer needed, the online service and users' access can be managed as appropriate.

In the realm of online services for short-lived dynamic teams comprised of users from multiple organizations, passkeys offer a significant advancement in authentication security. By eliminating reliance on traditional passwords and introducing cryptographic keys, passkeys fortify the authentication process, reducing the risk of unauthorized access and enhancing overall security. Moreover, passkeys streamline the user experience by simplifying the authentication process and mitigating the burden of password management. These advantages, coupled with the ability to anchor the passkey issuance to existing identity credentials that are based on established identity proofing processes, make passkeys an invaluable tool for securing online access for dynamic teams built to address disaster or other critical scenarios.