yubico

TECHNOLOGY BEHIND PASSWORDLESS AUTHENTICATION

KEYTOS

KEYTOS

TABLE OF CONTENTS

/ INTRODUCTION

As technology continues to advance, the need for secure authentication methods has become increasingly important. Traditional passwords have proven to be vulnerable to attacks such as phishing and brute force, leading to the development of new methods such as Smartcard and FIDO2 (Fast Identity Online 2) authentication. While these technologies have been around for many years, they have only been used in high security scenarios by governments and critical infrastructure.

In 2021, over 6 billion credentials were leaked, and more than 60% of breaches were caused by stolen credentials. While this might not seem like a critical issue, no organization is immune from cyber-attacks. Last year, over 90% of organizations reported being targeted by phishing campaigns.

Now that passwordless authentication is gaining wider adoption, new tools had to be created to increase end-user adoption, reduce onboarding friction, and ultimately make passwordless authentication easy for ALL businesses. This is where Keytos, in collaboration with the Yubico team, has created a seamless and secure onboarding experience that allows users to self-service onboard new credentials even from remote locations while giving organizations the security and attestation that is required for these high privilege actions.

/ Technology Behind Passwordless Authentication

Smartcard Authentication

Smartcard authentication uses a physical card with a built-in chip that stores the user's authentication credentials (X509 Certificate). The chip is tamper-resistant, making it difficult to copy or manipulate the private key stored on the card. Smartcard authentication is a two-factor authentication method, which means it requires something the user has (the card) and something the user knows (a PIN code). This method significantly reduces the risk of unauthorized access, especially in environments where high-security levels are required.

FIDO2 Authentication

FIDO2 authentication is a newer authentication method that uses public key cryptography to authenticate users. This method relies on the use of hardware security keys, such as YubiKeys, to verify the user's identity. When the user wants to authenticate, the hardware key generates a public-private key pair, with the private key stored securely on the key and the public key sent to the service provider. The user then proves their identity by providing a biometric identifier or a PIN code, which is used to unlock the private key stored on the hardware key. The private key is then used to sign a challenge sent by the service provider, verifying the user's identity.

FIDO2 + Smartcard = Better Together

While some organizations might prefer one over the other either because of regulations, requirements, or personal preference, we recommend using both when possible since some experiences are better served by the more modern FIDO2 and some other scenarios such as un premises authentication are better supported by Smartcard authentication.
One of the main advantages of EZSmartCard is how when a user requests an identity, they do not have to specify if they want a certificate for smartcard authentication or a FIDO2 key. Instead, we automatically create the ones that have been set up by the administrator, giving the user the credentials they need with a single, simple workflow.

yubico + KEYTOS Advantage

YubiKeys are the most popular hardware authentication tool for a reason, they are the most convenient and easy to use key available in the market. Keytos enhances that amazing technology by creating an easy way to distribute and onboard YubiKeys both in person and for remote workers.

Easy Distribution

From our years working in the passwordless space, we understand that one of the most challenging parts of deploying a hardware-based authentication system is managing the inventory of keys. This has become even more difficult with the modern distributed workspace which is why EZSmartCard offers 3 different ways to manage inventory.

Self-Distribution

If you have the experience distributing keys or will be distributing them in an office building, EZSmartCard's inventory management system will enable your team to easily manage the inventory as well as gives your users an intuitive UI/UX where they can request and manage the keys.

Yubico Enterprise Delivery (Coming Q2 2023)

To help with the overhead that comes with shipping YubiKeys worldwide, Yubico offers the Yubi Enterprise Delivery program where it helps organizations get their YubiKeys to their employees around the world. EZSmartCard connects to Yubico's program to automatically request a new YubiKey when the new request is created.

Keytos Delivery System

For organizations that do not qualify for the YED program but would still like to offboard the inventory management for their keys, Keytos offers a key delivery service where we assign and send the keys to your users when a new key is requested. This allows your team to focus on other pressing security tasks while your users get their keys.

Easy Onboarding

Once the YubiKey is delivered to the user, the user must create the passwordless Identities. For this, we have 3 ways to authenticate the user: government ID and face validation, existing account onboarding, and PUK unblock for when the user identity is validated in person.

Government ID and Face Validation

When creating the first user's identity, your organization must first validate the user's physical identity. In the past this was done by security when the employee first walked into the building and was given a badge. Now that remote onboarding is more popular, this is no longer feasible. This is why we offer an option where the user can scan their government ID and their face, and EZSmartCard validates that information and matches what the organization already has on the user. Once this information is validated, the user can create their identity.

Existing Account Onboarding

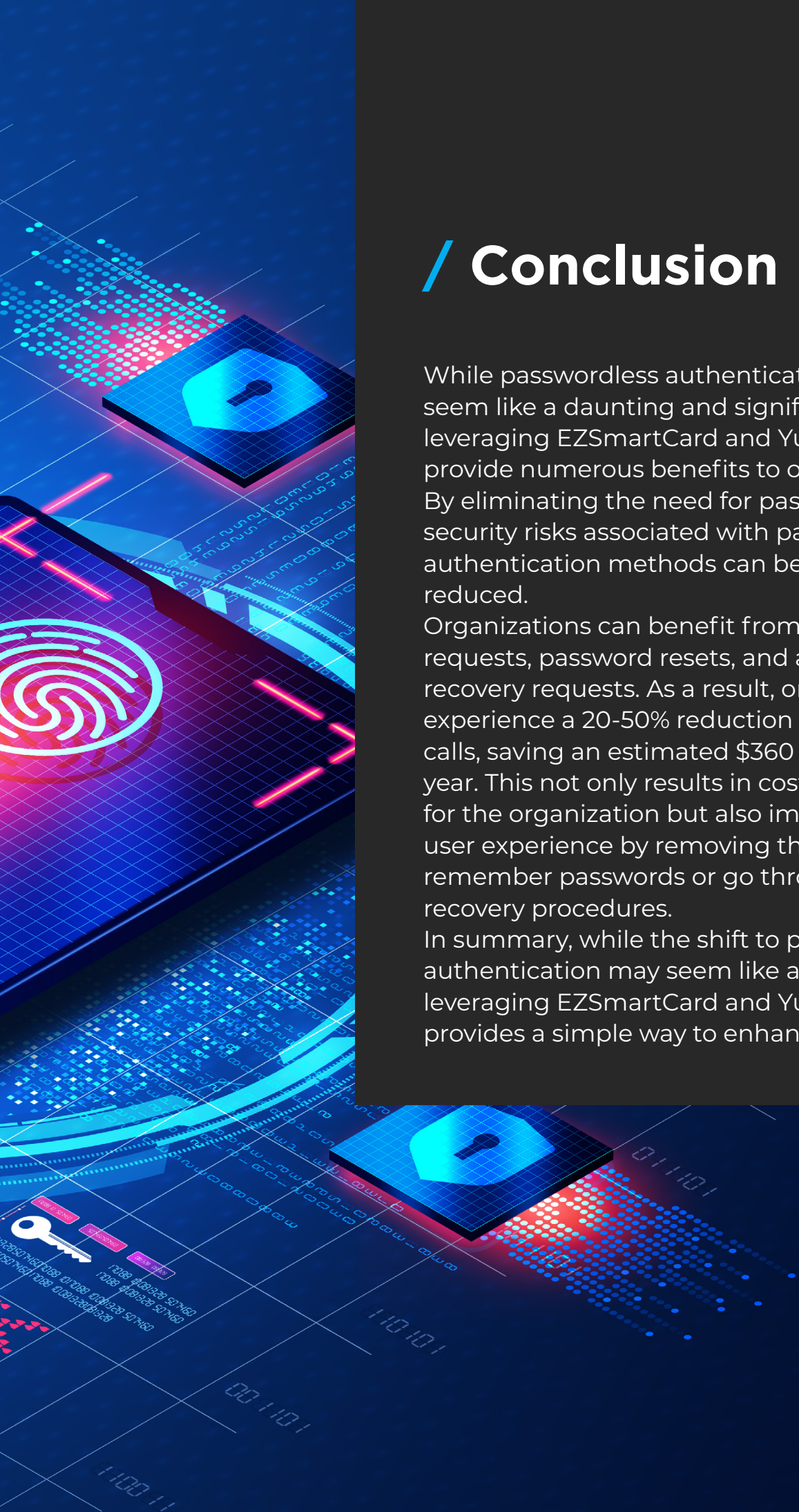
While Government ID + Face is convenient for new users, it is certainly not the ideal method for onboarding existing users. When rolling out YubiKeys for existing users, simply use an existing multi-factor authentication method to validate the user's identity. This feature also allows you to create new identities in other tenants, allowing you to leverage an existing secure identity and device (for example in Keytos our corporate device and corporate identity, to request our production identity).

PUK Unblock

We understand that while the first two methods are very convenient, some organizations must use a physical validation process, if this is the case, EZSmartCard offers the classic PUK unblocking method where the smartcard administrator creates the identity for the user and the user receives a PIN Unblocking Key (PUK) to unblock the smartcard and set their own pin.

Secure Attestation

EZSmartCard and YubiKeys were developed to protect the most critical identities. The YubiKey's Attestation certificate allows EZSmartCard not only to cryptographic validate that the YubiKey being enrolled has not been tampered with, but also allows us to validate that the YubiKey has been assigned to the user that is requesting the account. This adds an extra attestation layer protecting organizations from supply chain attacks that is currently only possible with our two industry leading technologies working together.



/ Conclusion

While passwordless authentication may seem like a daunting and significant step, leveraging EZSmartCard and YubiKeys can provide numerous benefits to organizations. By eliminating the need for passwords, the security risks associated with password-based authentication methods can be significantly reduced.

Organizations can benefit from lower support requests, password resets, and account recovery requests. As a result, organizations experience a 20-50% reduction in help desk calls, saving an estimated $360 per user every year. This not only results in cost savings for the organization but also improves the user experience by removing the need to remember passwords or go through account recovery procedures.

In summary, while the shift to passwordless authentication may seem like a tall task, leveraging EZSmartCard and YubiKeys provides a simple way to enhance security,