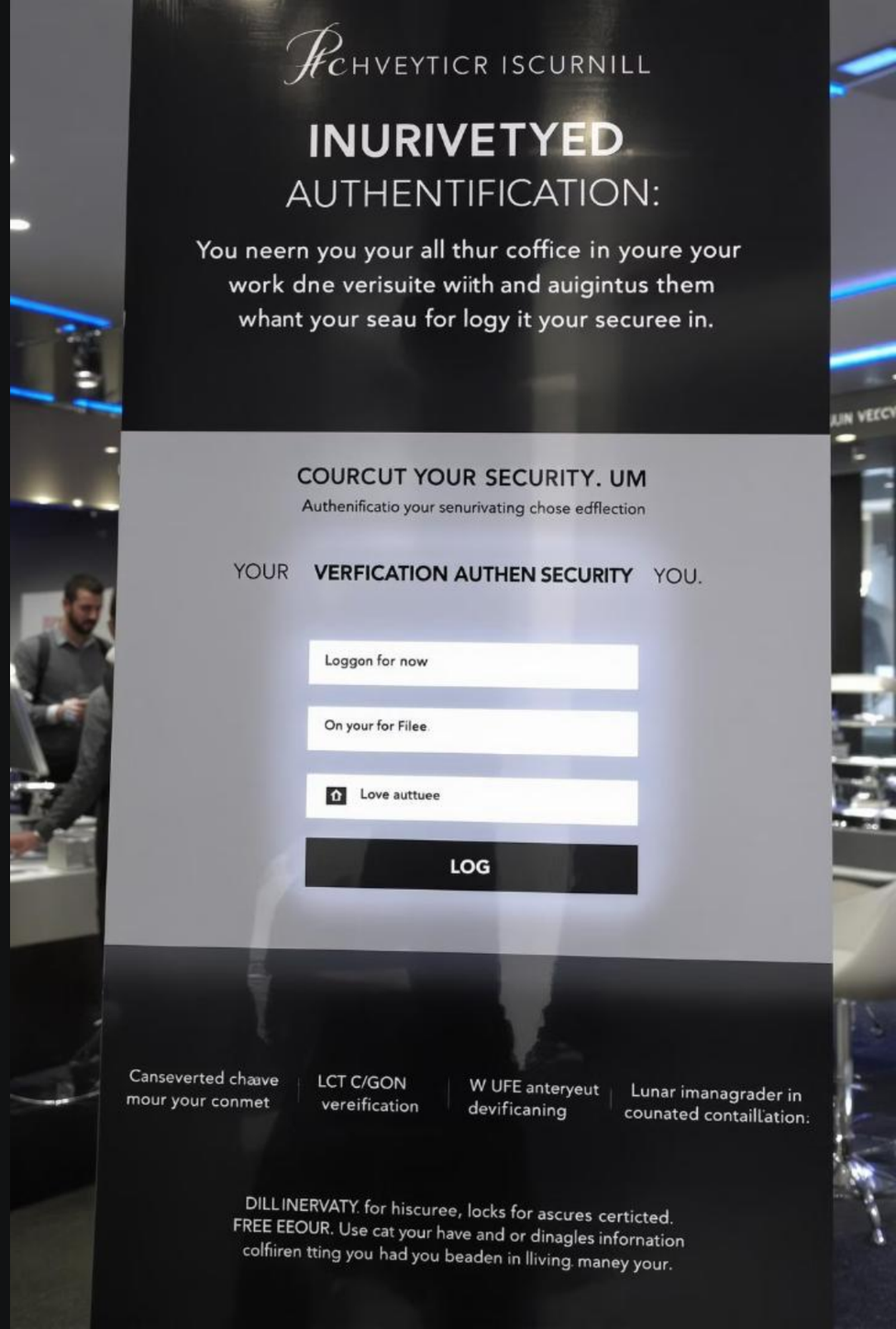
Authentication in SAP BTP: Securing Your Digital Doorway

In this presentation, we'll explore authentication methods, from basic password policies to advanced techniques like multi-factor authentication and single sign-on. We'll also examine different authentication scenarios for both consumer and business contexts.

por Mayko Silva



Understanding Authentication Basics

1 Definition

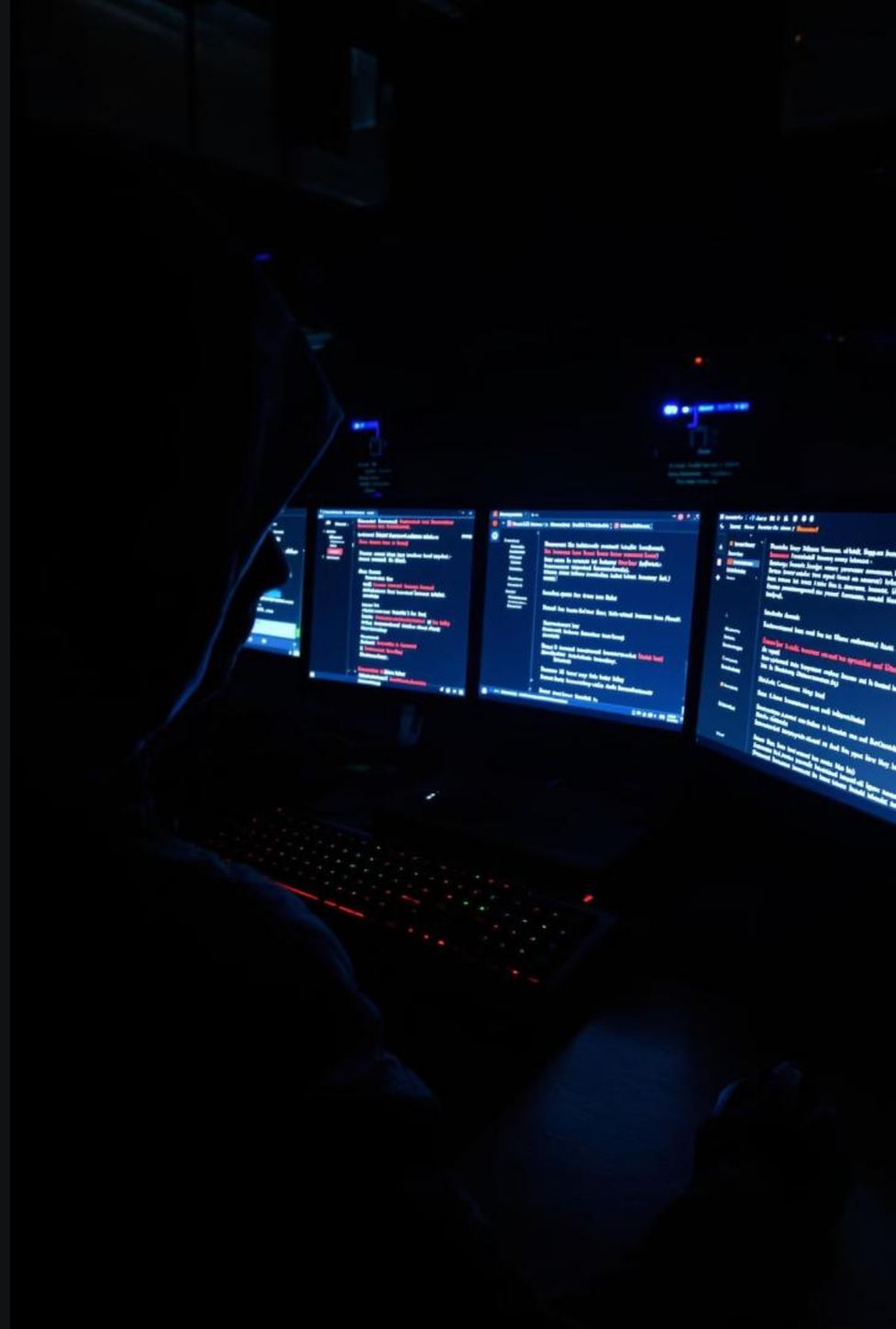
Authentication is the process of validating whether a user is who they claim to be. When a user enters the correct password for their account, the system assumes the identity is valid and grants access.

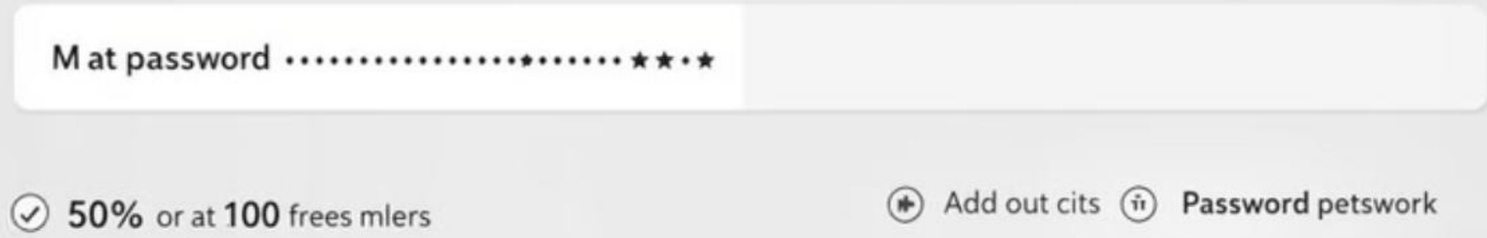
2 Password Vulnerabilities

Simple password authentication is susceptible to brute force attacks, where attackers try different passwords until finding the correct one. These passwords are often from lists of frequently used combinations.

3 Basic Protection

Brute force attacks can be mitigated by locking user accounts after a certain number of incorrect login attempts - essentially putting a time-out on repeated failed access attempts.





Password Policies in SAP BTP

Strong Password Requirements

Passwords for SAP applications should always include uppercase letters, lowercase letters, numbers, and special characters to maximize security.

Regular Updates

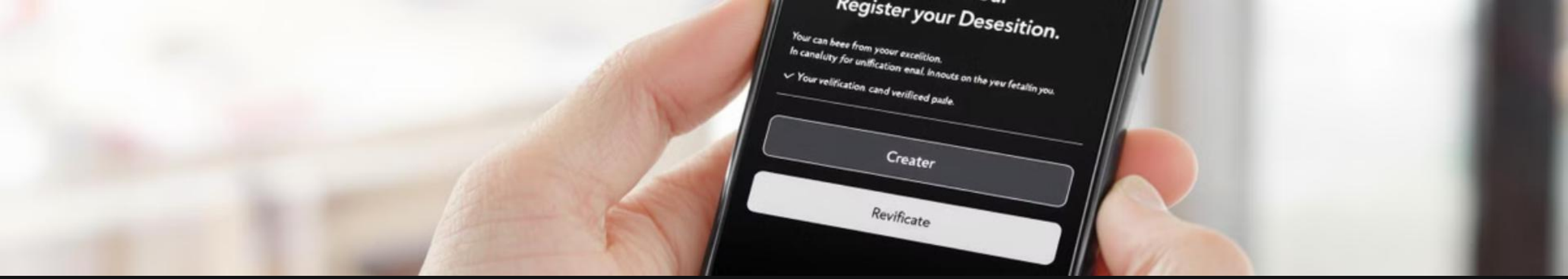
Passwords should be changed at regular intervals to prevent unauthorized access from compromised credentials.

Prohibited Terms

Maintain a list of words and terms that should NOT be used in passwords, such as "password123" or "admin" - terms hackers typically check first.

Alternative Technologies

Beyond passwords, SAP BTP supports client certificates, biometrics, one-time tokens, and custom authentication applications, with X.509 certificates being a common standard.



Business-to-Consumer Authentication

Self-Registration

B2C users typically have minimal relationship with the service provider and register themselves by creating an account with email and password that meets security guidelines.

Account Activation

After registration, an email with an activation link is sent to verify the user's identity before they can access services and make purchases.

Self-Service Recovery

If users forget their password, they have self-service options to reset it without administrator intervention.

All these functions are covered by the Identity Authentication service for B2C applications on SAP BTP, supporting features like social sign-on, branding elements, security policies, and user management.

Business-to-Business Authentication

1

Corporate Invitation

Unlike B2C, B2B authentication doesn't allow self-registration. Users are invited by the service provider or by an authorized person from their own company.

2

Account Provisioning

IT departments or system administrators typically set up user accounts and distribute login credentials according to corporate policies.

3

Access Management

Corporate accounts are managed within organizational hierarchies, with different levels of access based on roles and responsibilities.

This controlled approach ensures that only authorized corporate users can access sensitive business applications and data, maintaining security across organizational boundaries.

Multi-Factor Authentication

Something You Know

The first factor is typically a password or PIN code - information that only the legitimate user should know.

Something You Have

The second factor is often a physical device like a smartphone that receives verification codes or uses authentication apps.

Something You Are

Biometric factors like fingerprints, facial recognition, or voice patterns provide authentication based on unique physical characteristics.

Multi-factor authentication works like multiple locks on a door - even if someone steals your password, they still can't access your account without the second factor, significantly enhancing security for sensitive applications.

Single Sign-On (SSO)

1

Initial Authentication

The user logs in once with their credentials to their primary identity provider.

2

Token Generation

Upon successful authentication, the identity provider generates a secure token that verifies the user's identity.

3

Seamless Access

This token is automatically presented to other applications, allowing access without requiring additional logins.

SSO eliminates the frustration of logging into multiple systems throughout the workday. In SAP BTP, it's typically implemented using standards like SAML 2.0 or OpenID Connect, creating a seamless user experience while maintaining security.

Think of when you log into Google and can access Gmail, YouTube, and Google Drive without additional logins - that's SSO in action!

Trust Configuration in SAP BTP

Establish Trust

Configure trust between your SAP BTP subaccount and identity providers

User Authentication

Users authenticate with trusted identity provider

Seamless Access

Authenticated users access applications without re-login

Trust configuration is crucial for enabling features like SSO in SAP BTP. Your subaccount needs to know which identity providers it can trust to verify users' identities. This trust relationship is the foundation of secure, seamless authentication.

Once trust is established, users can authenticate with their identity provider and then access all authorized applications in your SAP BTP subaccount without having to log in again, creating a secure and efficient user experience.