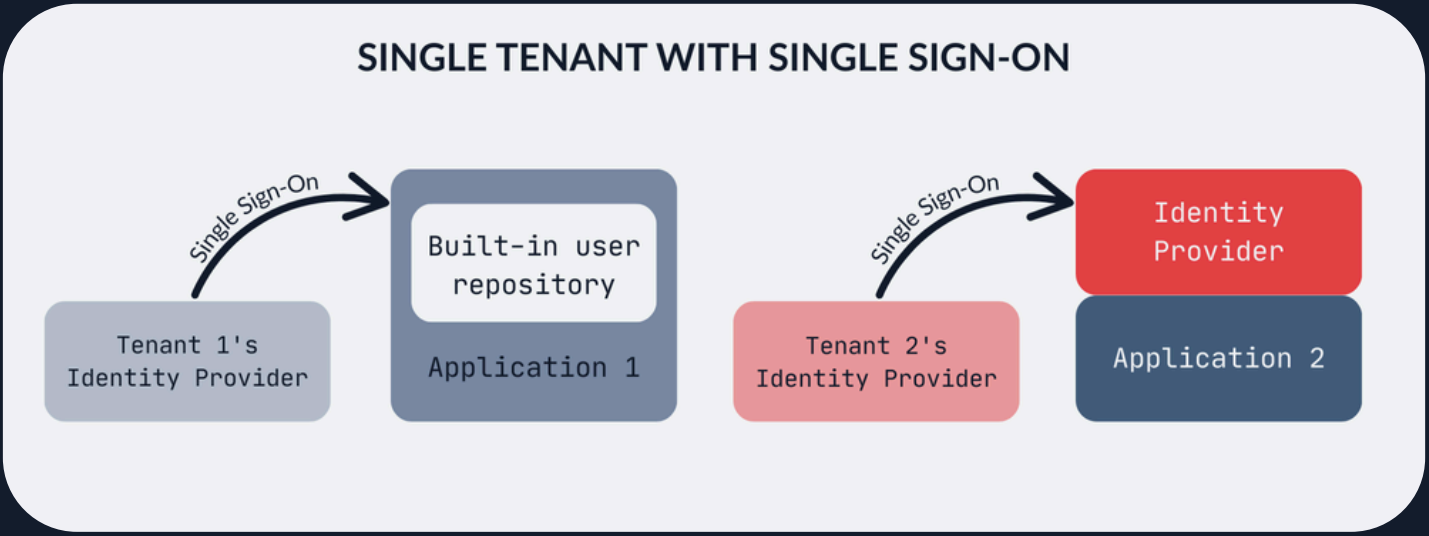
SECURING SOFTWARE-AS-A-SERVICE: IDENTITY AND ACCESS MANAGEMENT THREAT MODEL

securing

SSO EXPERT
Natalia Trojanowska-Korepta

1. Single Tenant



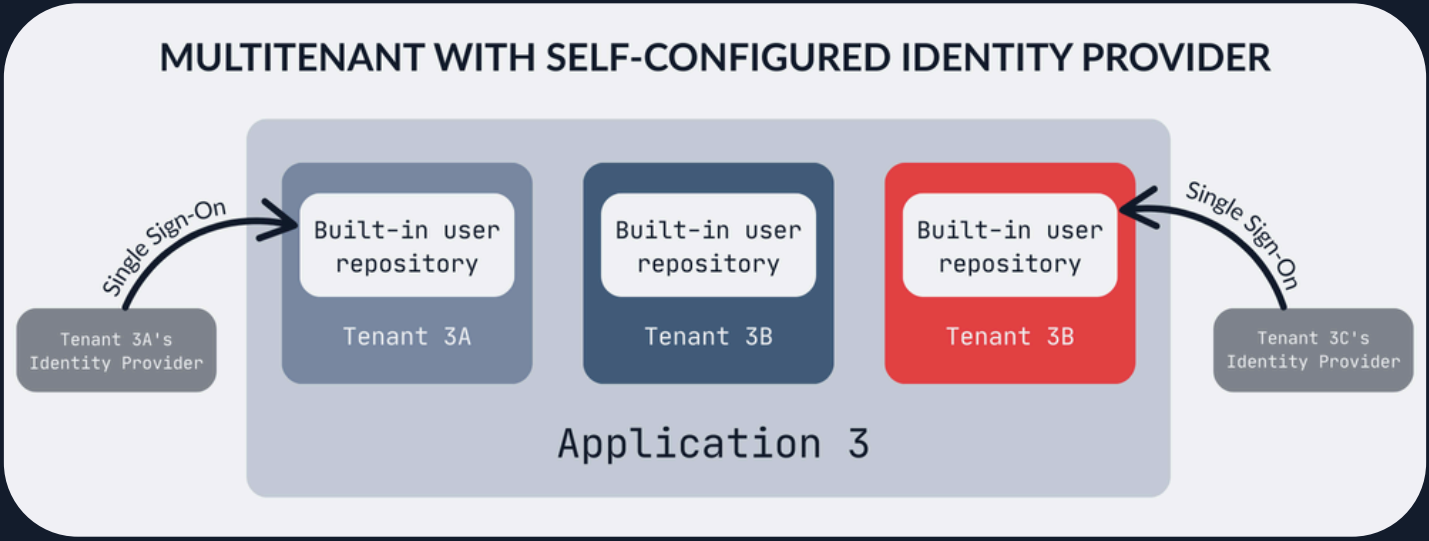
Threat actors

- Anonymous attacker.
- Low privileged user.

Key threats

- Authentication bypass or MFA bypass.
- Account takeover, e.g., via insecure password reset process.
- Privilege escalation, e.g., via manipulating own permissions.
- Gaining access to the user management panel to create new high-privileged users.

2. Multitenant with self-configured Identity Provider



Threat actors

- Anonymous attacker.
- Low privileged user.
- **Administrator of a malicious tenant.**

Key threats

1. Single Sign-On

- Modification of another organization's SSO configuration (tenant takeover).
- Deletion of another organization's SSO configuration (Denial-of-Service).
- Accidental global enforcement of an SSO configuration (e.g., one tenant's SSO configuration works for every organization in the application).
- Vulnerabilities in the implementation of SAML or OIDC.
- Account pre-hijacking (e.g., creating an account using a victim's email address before the victim signs up, potentially gaining backdoor access if the victim uses Single Sign-On in the future).

2. User synchronization (Just-In-Time, SCIM, or manual)

- Insufficient offboarding.
- Hijacking a different tenant's user.
- Provisioning a user to another tenant.

3. User in multiple organizations

- Abuse of the context switcher to gain access to a different tenant.
- Modification of a user from a different tenant after inviting them to your tenant (e.g., changing their password).
- Improper evaluation of authentication context (e.g., if the user logged in using a specific tenant's SSO, they should not be able to switch tenants).
- Improper permission management for a user in multiple organizations (e.g., if a user is high-privileged in one tenant and low-privileged in another).

4. User management

As an administrator of a malicious tenant:

- Creating a user account in a different tenant.
- Creating a user with the same username or email as in a different tenant leading to account takeover.

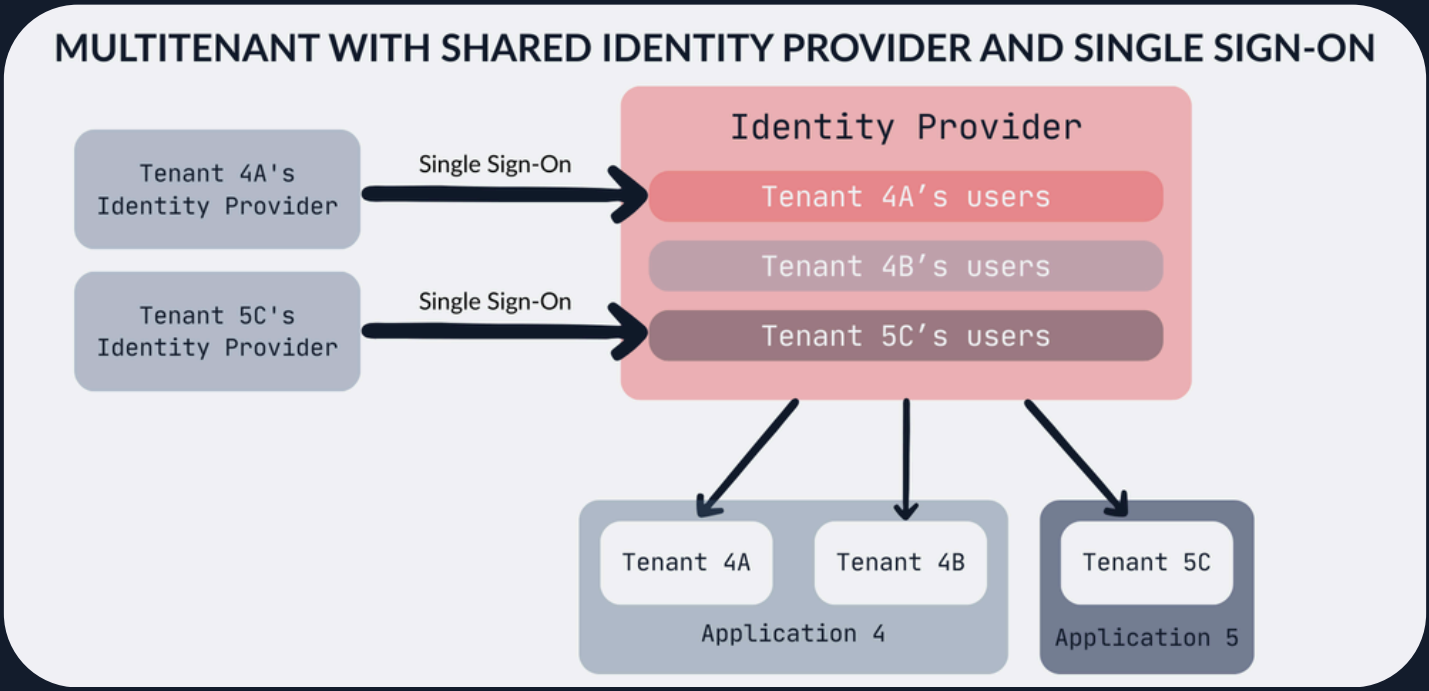
As a low privileged user:

- Privilege escalation, e.g., via manipulating own permissions.
- Gaining access to the user management panel to create new high-privileged users.

5. Authentication without Single Sign-On

- Authentication bypass or MFA bypass.
- Account takeover, e.g., via insecure password reset process.

3. Multitenant with shared Identity Provider



Threat actors

- Anonymous attacker.
- Low privileged user.
- **Administrator of a malicious tenant.**

Key threats

1. Shared Identity Provider

- Accidental global enforcement of SSO configuration (e.g., one tenant's SSO configuration works for every organization in the application).
- Modification of user groups or permissions, which could grant them access to a different tenant.
- Unauthorized access to IdP administration panel (e.g., via improper configuration, usage of default credentials, or credential breach).
- Lateral movement between different Relying Parties (if you use the IdP not only for multiple tenants, but also for multiple applications).

2. User in multiple organizations

- Abuse of the context switcher to gain access to a different tenant.
- Modification of a user from a different tenant after inviting them to your tenant (e.g., changing their password).
- Improper evaluation of authentication context (e.g., if the user logged in using a specific tenant's SSO, they should not be able to switch tenants).
- Improper permission management for a user in multiple organizations (e.g., if a user is high-privileged in one tenant and low-privileged in another).

3. User management

As an administrator of a malicious tenant:

- Creating a user account in a different tenant.

As a low privileged user:

- Privilege escalation, e.g., via manipulating own permissions.
- Gaining access to the user management panel to create new high-privileged users.

LEARN MORE ABOUT OUR SERVICES

Services

The goal of application security testing is to detect application vulnerabilities to potential attacks, or in other words – to find defects that could be exploit...

Securing

https://www.securing.pl

& CONNECT WITH THE AUTHOR ON LINKEDIN

SSO EXPERT

Natalia Trojanowska-Korepta

SINGLE SIGN-ON

CVE-2025-26788: Pas
Bypass in StrongKe

NATALIA TROJANOWSKA-K

2025.02.14 · 5 MIN

SINGLE SIGN-ON

The year in
Sign-On vu

NATALIA TROJ

2025.01.27 ·