

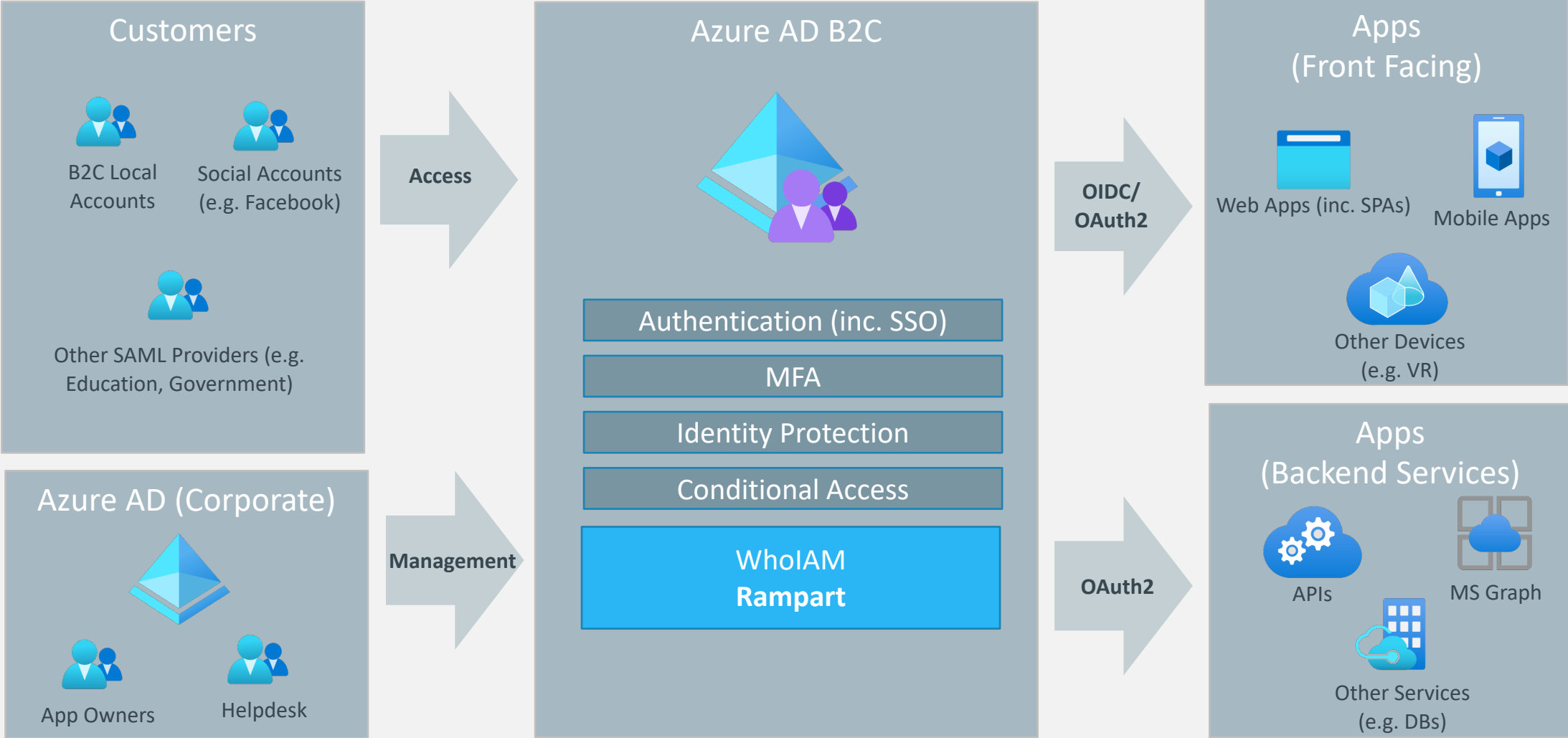
WhoIAM Rampart

Authorization Engine for
Azure AD B2C

WhoIAM Rampart

- WhoIAM Rampart is an **authorization engine** for Azure AD B2C
- Allows the definition of per-application **authorization policies** that enforce:
 - **Restricted application access** (e.g. by invitation only)
 - **Application permissions** (e.g. roles)
- **Managed** by users of an Azure AD tenant, for example a corporate tenant, using either:
 - A web management portal
 - PowerShell cmdlets

Architectural Overview



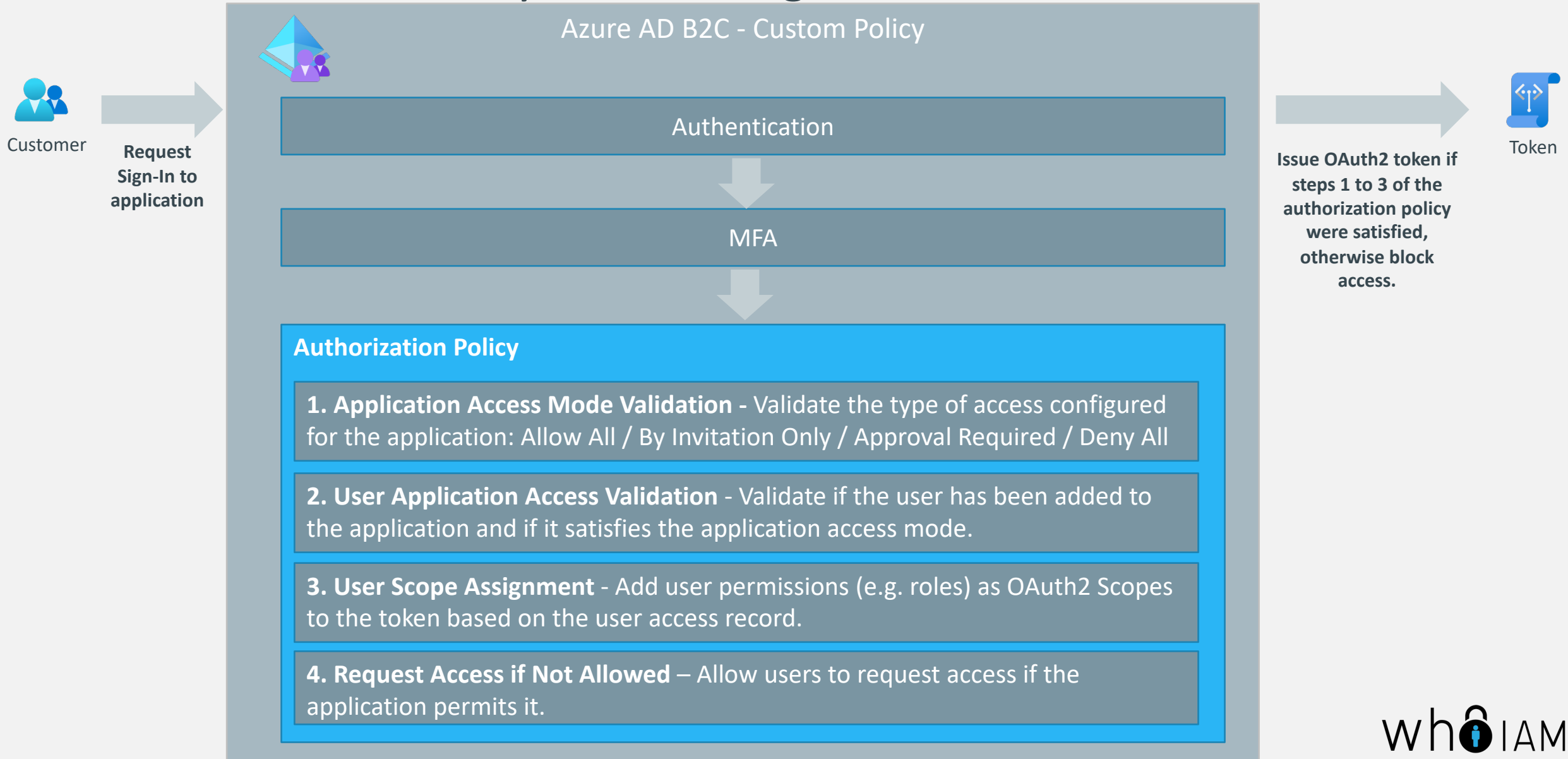
Restricted application access

- Rampart supports the following application **access modes**:
 - **Allow all** – All users registered within the B2C tenant can access the application without restriction.
 - **By invitation only** – Only users who have been invited to the application can access.
 - **Approval required** – Users can request access but it has to be approved by an application Administrator. Approvals can be configured to expire after a set period of time.
 - **Deny all** – No user can access the application.

Application permissions

- Rampart allows the definition of application specific **permissions** (i.e. scopes).
 - Each **user** can be assigned one or multiple permissions.
 - Permissions are included in the **access token** that B2C issues.
- A **single place** to manage all application and user permissions (instead of defining them separately within each application).


Authorization Policy Flow – Sign In




Architectural Components



Rampart Policy Execution




Azure B2C Custom Policies
(e.g. Sign In/Signup)




Authorization Policy Execution Functions


Rampart Management and Helpdesk




Web Portal (SPA)



PowerShell Cmdlets



API




MS Graph




Corporate Azure AD
(Employees)



Rampart Data




Authorization DB




Application Insights

Infrastructure Services



SendGrid



Azure Storage