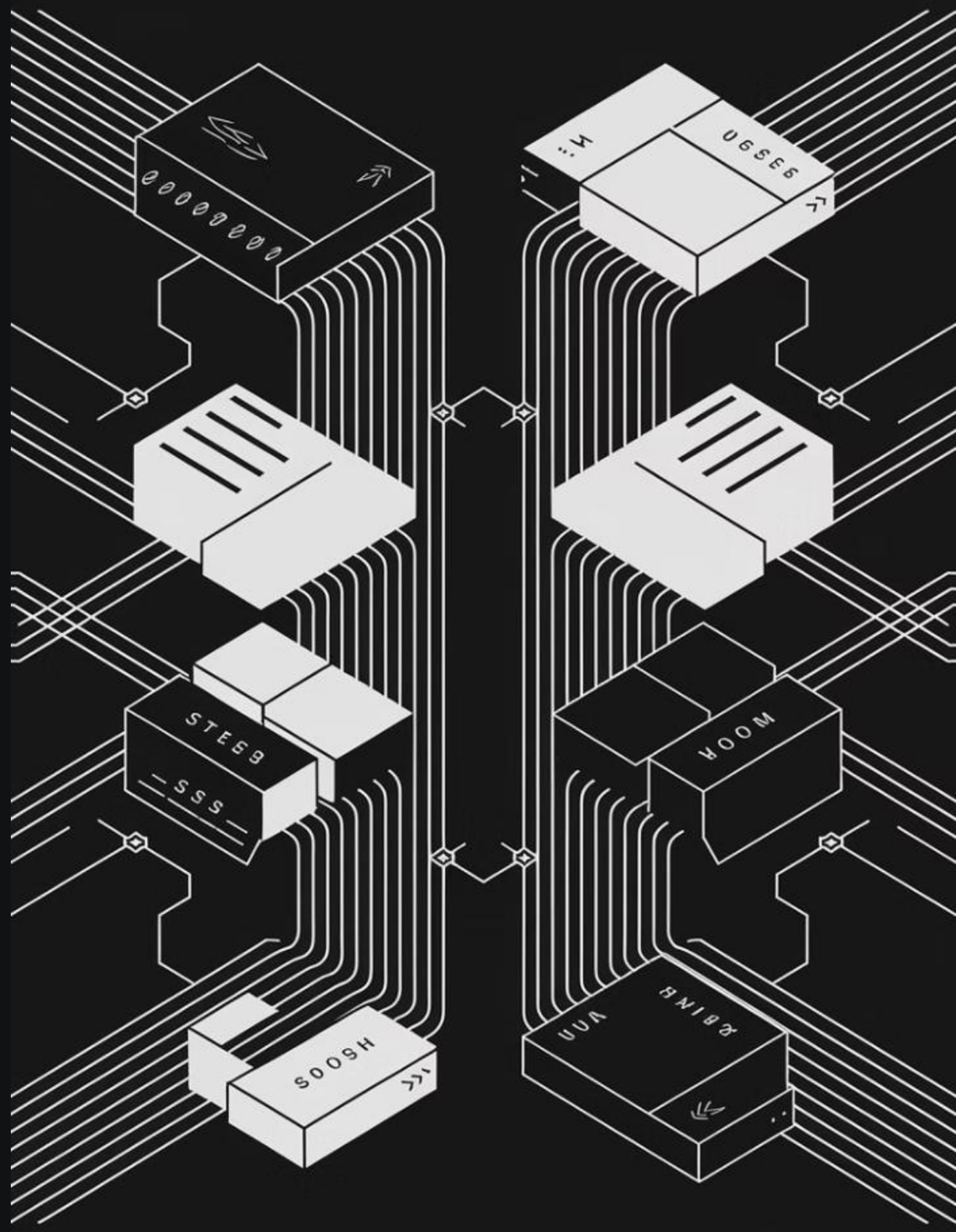
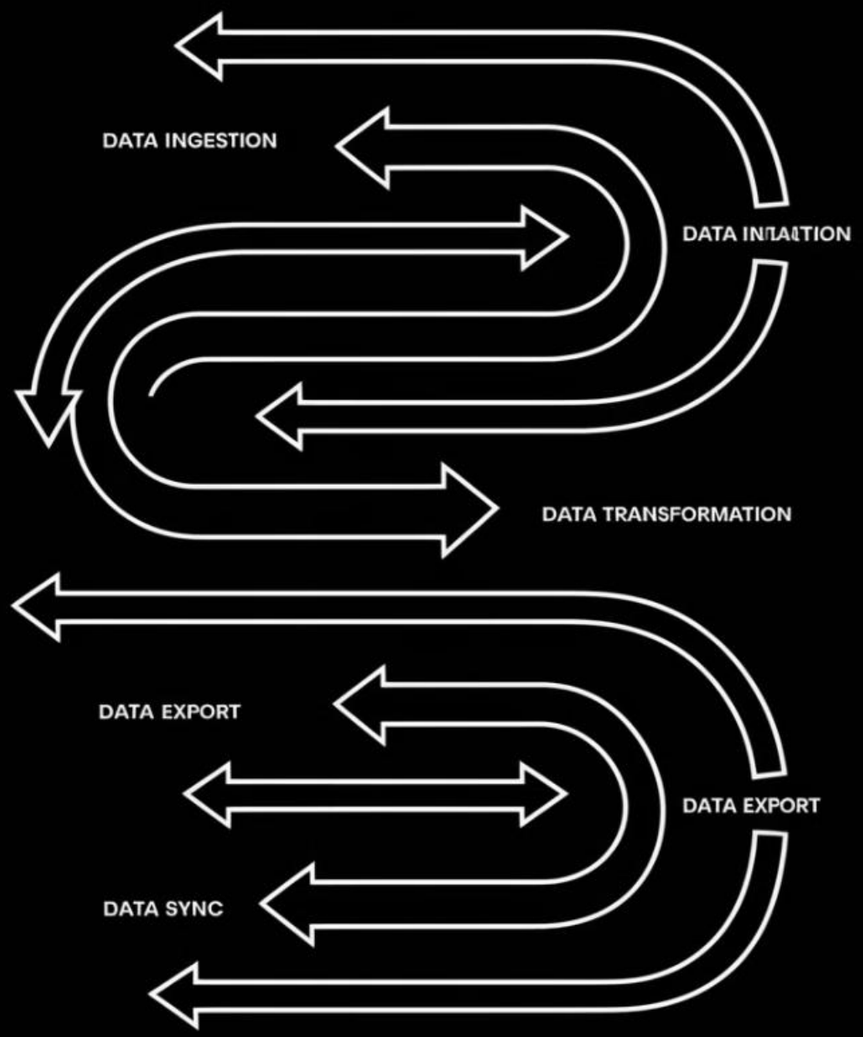
# Architecture of Identity Provisioning

por Mayko Silva






# Operation Overview

The identity provisioning process involves taking user information from one or more sources, applying transformations, and then customizing it for target systems. This transformation is critical - it maps user attributes from source systems to standardized attributes in SAP BTP.

When user data flows through the system, it undergoes standardization to ensure consistency across all connected platforms. This creates a unified identity framework that maintains data integrity while supporting diverse system requirements.

1

## Source Data

User information extracted from original systems

2

## Transformation

Mapping attributes to SAP BTP standards

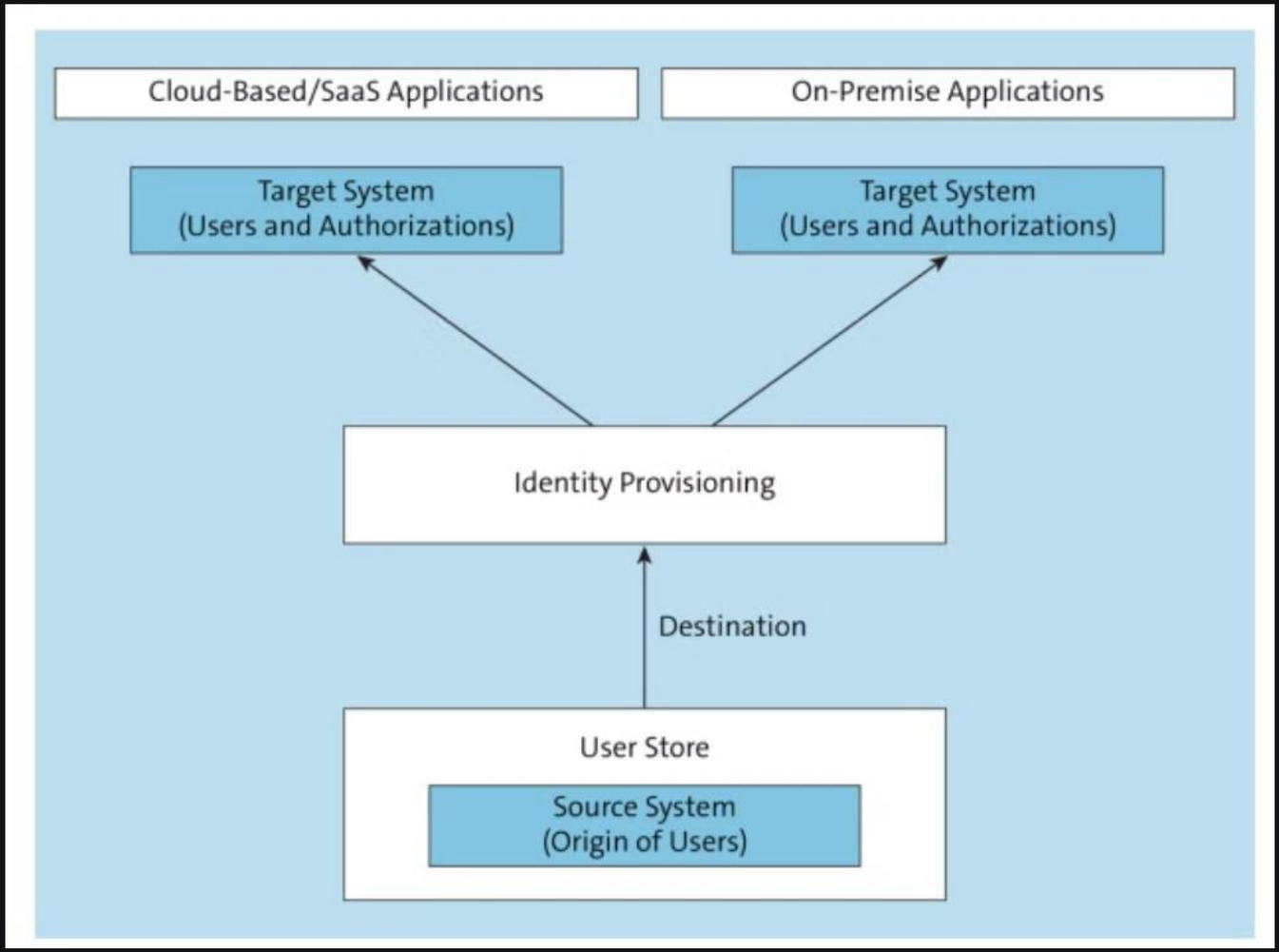
3

## Customization

Adapting standardized data for target systems

# Source Systems

Source systems serve as the origin points for user identity data. Typically, these are your company's existing user stores, such as Microsoft Active Directory, which can be either cloud-based or on-premise. The Identity Authentication service can also function as a source system.



# Source System's Limit

There's a limit of up to 20 source systems that can be connected simultaneously. Your available options may vary depending on your specific license bundle.

### Common Source Systems

- Identity Authentication
- Microsoft Active Directory
- SAP SuccessFactors

### SAP BTP Sources

- SAP BTP account members (Neo)
- SAP BTP Java/HTML5 apps (Neo)
- SAP BTP extended services (Cloud Foundry)

### SAP Cloud Sources

- SAP S/4HANA Cloud
- SAP Marketing Cloud
- SAP Work Zone

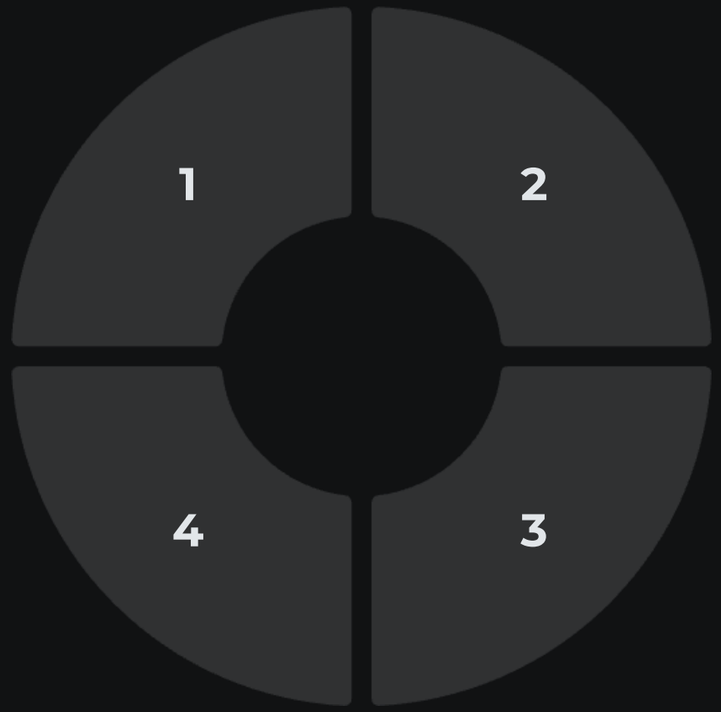
# Target Systems

Target systems are the destinations where identities from your source systems are created or customized. These systems receive the transformed identity data that has been standardized through the provisioning process. You can connect up to 50 target systems simultaneously.

All systems that can serve as sources can also function as targets. Additionally, specialized systems like SAP Analytics Cloud and SAP Sales Cloud (analytics and AI) can be used exclusively as target systems.

### SAP Cloud Targets

SAP S/4HANA Cloud, SAP SuccessFactors, SAP Marketing Cloud




### Analytics Targets

SAP Analytics Cloud, SAP Sales Cloud (analytics and AI)

### On-Premise Targets

SAP S/4HANA on-premise, Microsoft Active Directory

### Identity Targets

Microsoft Azure AD, Identity Authentication, SAP Work Zone

# Proxy System

Proxy systems are specialized connectors designed for hybrid scenarios where cloud systems need to connect with on-premise systems. This architecture eliminates the need for direct connections between disparate environments, enhancing security and simplifying management.

The Identity Provisioning service acts as this proxy, handling critical operations like creating, updating, and deleting entities across system boundaries. This intermediary role ensures smooth data flow while maintaining appropriate separation between environments.

### Cloud System

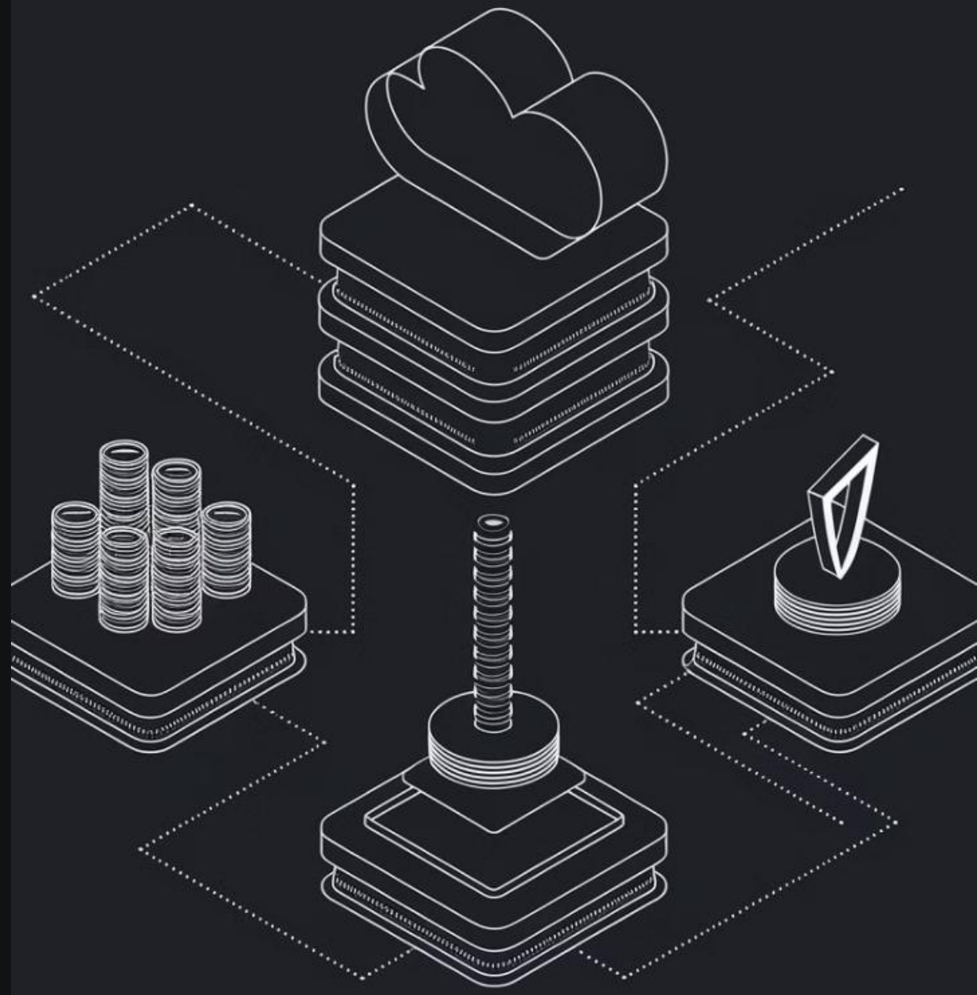
Initiates identity provisioning request

### Identity Provisioning Proxy

Securely manages the connection between environments

### On-Premise System

Receives and implements identity changes



# Licensing

The Identity Provisioning service is available free of charge when bundled with certain SAP cloud solutions, including SAP S/4HANA Cloud, SAP Marketing Cloud, SAP Sales Cloud, and SAP SuccessFactors. Each customer receives two Identity Provisioning tenants per region - typically one for testing and one for production.

When your tenant is bundled with an SAP cloud product, you gain access to all source, target, and proxy systems relevant to that product. Customers with multiple SAP cloud products receive access to all relevant systems across both tenants. Since October 2020, the service is no longer available as a standalone purchase.

**2**

### Tenants Per Region

One for testing, one for production

**20**

### Max Source Systems

Limit per implementation

**50**

### Max Target Systems

Limit per implementation