

SPANKEY SSH - PAM

CENTRALIZED LINUX ACCESS
& AUTHENTICATION



THE BEST WAY TO MANAGE SSH ACCESS

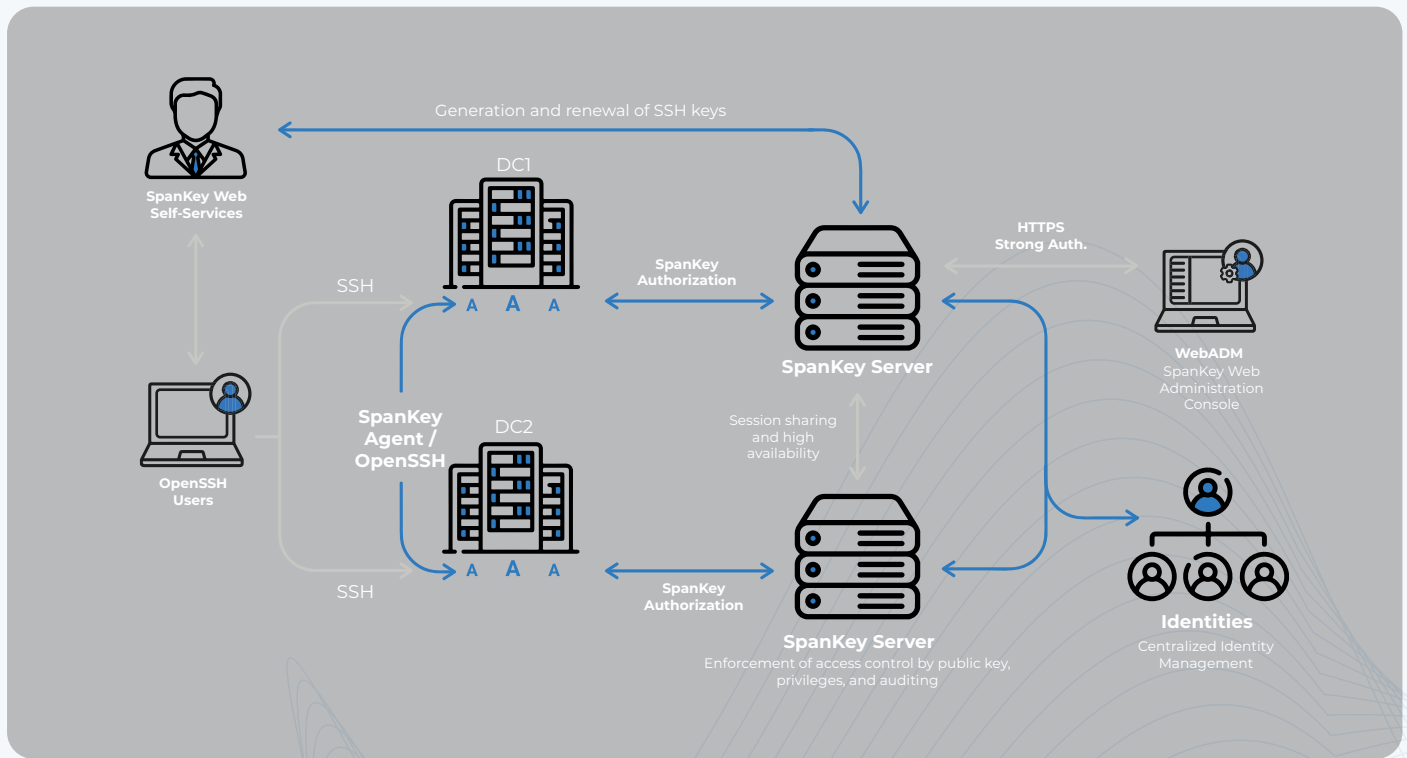
SpanKey simplifies and centralizes the management of SSH access and SUDO privileges on Linux systems. It integrates with directories such as Active Directory, OpenLDAP, as well as cloud directories like Entra ID and Google Workspace.

SSH keys and their entire lifecycle are automatically managed. SUDO privileges are centrally defined, by user or group, with fine-grained control. All SSH sessions are audited and logs are centralized.

With SpanKey, you simplify access administration, strengthen infrastructure security, and ensure full session traceability.

OUR COMPANY

As a European software editor specialized in Identity and Access Management (IAM) and Multi-Factor Authentication (MFA) RCDevs Security provides modular and flexible security solutions, available both on-premise and as a SaaS. Recognized for its software reliability and high customer satisfaction, RCDevs supports small businesses and large businesses alike, across all industries worldwide.



SpanKey Architecture

THE CHALLENGE

Identity and access management is essential in cybersecurity to control and trace access to digital resources. However, managing privileged access via SSH often remains a weak point.

SSH is widely used by administrators to remotely connect to UNIX/Linux servers execute commands, or transfer files.

It primarily relies on public/private key pairs, much safer than passwords, but without centralized management, these keys are often duplicated, poorly revoked, and may escape audits, leading to loss of access control.

This lack of visibility creates a major security gap: an unknown key can silently open access to sensitive systems without clear traceability of the user.

SPANKEY'S ANSWER

SpanKey secures SSH access using all identity sources configured through WebADM, including LDAP/AD, Entra ID, PingOne and more, providing unified and centralized user control.

Key Features

- Integration with all identity sources via WebADM (LDAP/AD, Entra ID, PingOne, etc.) for centralized and unified control.
- Flexible and centralized access policies, enforced in real time by the SpanKey agent to allow or block connections.
- Fully automated SSH key lifecycle: creation, distribution, and revocation, no manual intervention.
- Recording and auditing of all SSH connections, ensuring compliance with IAM requirements. Thus, SpanKey guarantees secure, controlled and fully integrated SSH access within your global identity management system.
- Centralized management of SUDO privileges, limiting sensitive actions to authorized users.

AUTOMATED PROVISIONING

SpanKey fully automates provisioning and deprovisioning of SSH access and keys based on your integrated identity sources, whether from enterprise directories or cloud IAM systems.

Dynamic group-based management automatically triggers authorization creation or revocation on SpanKey clients.

The distribution of public SSH keys, SUDO rules and Auditd configurations is centralized and automated, ensuring immediate compliance without manual action.

The automatic SSH key lifecycle management enforces expiration and renewal in line with regulatory and internal policy requirements.



AUDIT & TRACEABILITY

Advanced Auditing

→ SpanKey automatically triggers auditing rules upon connection, logging all SSH activities including SCP and SFTP transfers.

Detailed Logging

→ Commands, processes, and file system events can be recorded in depth.

Session Recording

→ Real-time terminal capture allows graphical playback of SSH sessions from the admin console, easing [post-incident analysis](#) and compliance.

SIEM Integration

→ Logs can be exported to a SIEM for centralized analysis, event correlation and custom alerting.



CENTRALIZED ACCESS CONTROL

SpanKey provides centralized, granular access control defining exactly who can access which resources, when and under what authentication conditions. The solution can enforce [OpenOTP MFA](#) for stronger security.



SHARED ACCOUNT MANAGEMENT

Shared Account Control

→ SpanKey enables control and traceability for shared local accounts such as root, mysql or others.

Individual Access

→ Authorized users access these accounts with [their personal SSH key](#) ensuring precise traceability of actions performed.

Accountability

→ Each operation on a shared account is tied to the individual's identity, reinforcing accountability and transparency for critical resource access.



BACKUP MASTER KEY

The Backup/Master Key provides emergency access, allowing connection to any system under any account. It ensures a [fallback solution](#) in case of key loss or unavailability.



SELF-SERVICE SSH KEY ENROLLMENT

SSH Key Self-Management

→ The Self-service web portal allows users to manage their SSH keys independently.

Key Generation

→ Users can generate a [new key pair](#), choosing from RSA, DSA, or ECC.

Import Existing Keys

→ Users can manually import an existing public key.

Key Revocation

→ Users can revoke keys that are obsolete or compromised.

Security Policies

→ [Security policies](#) can enforce key size and validity period, ensuring protection that meets company standards.

Automatic Renewal

→ When a key expires, a [renewal link](#) is automatically sent to the user.

Compliance & Easy Re-enrollment

→ This process allows users to re-enroll easily while remaining compliant with security policies.



OFFLINE FUNCTIONALITY

The Offline feature uses a secure local cache to allow SpanKey clients to [authenticate via SSH](#) even when disconnected from the SpanKey server, ensuring reliable and secure access under degraded network conditions.



SPANKEY SSH KEY SERVER PAM & OPENOTP SECURITY SUITE



MULTI-FACTOR AUTHENTICATION & LOCK SCREEN

When integrated with OpenOTP, SpanKey authentication can include up to three additional factors: the account password, a [one-time password \(OTP\)](#), a [Push notification](#) and a badging operation. SpanKey also supports FIDO2 keys for SSH connections, along with all authentication methods compatible

with OpenOTP. In addition, SpanKey features an automatic SSH terminal lock that activates after a defined period of inactivity.

When a user remains inactive, the session locks automatically and requires the password to be entered again to resume access.

AUTHENTICATION METHODS



OpenOTP Token App

Mobile Push
or OTP Token



PKI

Certificate-based
authentication



Magic Links

QRCode via eMail or SMS
to confirm access



YubiKey

YubiOTP,
OATH-HOTP & PIV



FIDO2

Public-key cryptography-based
authentication



Software Tokens

Event-based & time-based
OATH tokens



Hardware Tokens

Event-based & time-based
OATH tokens



Legacy Methods

OTP via SMS, eMail & secure
eMail or printed list