ISEC7 THE DIGITAL WORKPLACE COMPANY | Hypergate

MOBILE SIGN-IN WITH HYPERGATE

Cloud-like experience. On-prem sovereignty.

Hypergate brings Kerberos single sign-on to Android and iOS, against the Active Directory you already run. ISEC7 integrates and operates the solution.



Kerberos SSO
for Android and iOS

No additional server
directly against your domain controllers

On premises
authentication and data stay in your own data centre

Through your UEM
delivered as a managed app

CHALLENGE

Two changes hit the same spot in the network: how a work phone signs in, and how it reaches the file shares. Microsoft is phasing out NTLM step by step, and Acronis Cyber Files receives no security updates after 31 December 2026.

The replacements Microsoft builds for NTLM exist for Windows. Smartphones and tablets that reached the intranet, internal web applications and file shares over NTLM need a route via Kerberos.

CAPABILITIES

Hypergate, a Swiss vendor from Zug, closes both gaps. Hypergate Authenticator signs Android and iOS devices in via Kerberos, directly at the existing domain controllers, with a user certificate distributed by your UEM or with user name and password. Hypergate Files then opens the existing shares with the NTFS permissions you have already set.

THE SOLUTION & USP

- Kerberos single sign-on on Android and iOS, without a password prompt in every app
- No cloud identity required: authentication and data stay in your own data centre
- No additional server between device and domain controller
- File access via SMB2 and SMB3 to Windows shares and NetApp, in the native Files app of the device
- Delivered as a managed app through Microsoft Intune, Ivanti, Omnissa Workspace ONE, BlackBerry UEM, SOTI or 42Gears
- No data on the device: files stay on your servers, nothing is cached locally, and the DLP rules of your UEM apply

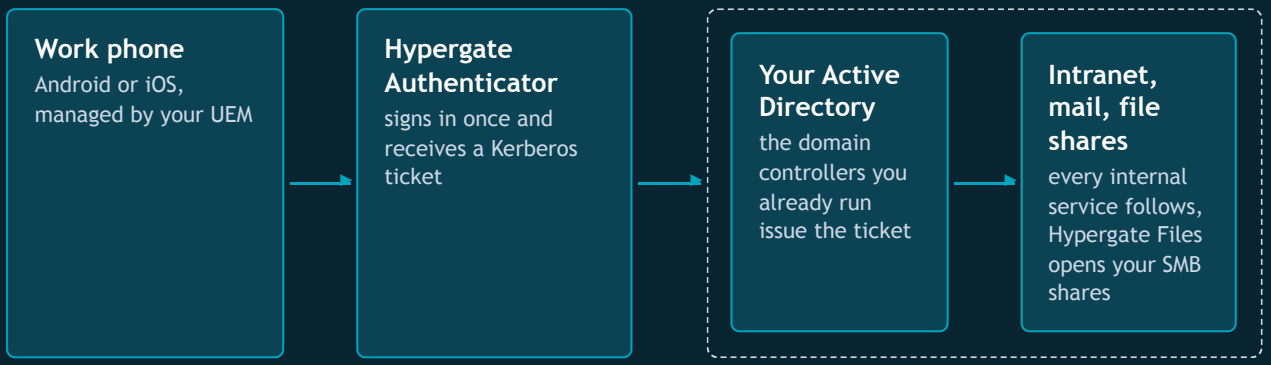
WHO DOES WHAT

Hypergate makes the software. ISEC7 is a Hypergate partner, integrates the apps into your UEM, operates them and is your contact for support. A proof of concept runs for about 30 days, is free of charge and needs no change to your infrastructure.

Since 2003, the ISEC7 Group has run Digital Workplace and Managed Mobility Services for public authorities, international enterprises, operators of critical infrastructure (KRITIS), companies that handle classified information and other organizations with strict compliance requirements. Over 700 customers worldwide, among them governments, police forces and armed forces. ISEC7 is headquartered in Germany, with locations in the USA, Australia, New Zealand and Poland.

ISEC7 | Hypergate

Authenticate once. Access everything.



Everything inside the frame runs in your own data centre.

TARGET GROUP

- Endpoint managers and administrators with Android and iOS fleets
- CISOs for whom a cloud identity is not an option as the sign-in route
- Public authorities, defence, financial services, insurance and healthcare
- Organizations that have to replace Acronis Cyber Files

AREAS OF APPLICATION

- Single sign-on to the intranet and internal web applications
- Access to file shares from the smartphone and tablet
- Leaving NTLM on mobile devices
- Replacing Acronis Cyber Files

WHERE TO START

First find out which devices and services still use the old sign-in method. ISEC7 SPHERE gives you that inventory. On the network side, the devices need Kerberos (port 88) to the domain controllers and SMB (port 445) to the file servers, over your existing VPN. ISEC7 MAIL supports sign-in with Hypergate.

FIND OUT MORE

www.isec7.com/en/hypergate-migration

ISEC7 THE DIGITAL WORKPLACE COMPANY
Schellerdamm 16, 21079 Hamburg, Germany ■ isec7.com ■ sales@isec7.com ■ +49 40 325076 0