Maximum security at the smallest possible workplace

SINA Mobile: Simple, flexible, well-designed

App on, unwanted audience out

The smartphone has become an integral part of our daily lives. However, in a professional context, security has always been a concern.

What if sensitive data ends up on the phone and attackers intercept or manipulate it? This concern is especially relevant when classified information is involved. SINA Mobile provides the solutions.

Work like you're in the office, without working in the office

With SINA Mobile, you can chat, call, email, and work from anywhere. The application suite for Samsung Knox Native and Apple iNDIGO ensures everything is secure—with German national RESTRICTED (VS-NfD) approval[1] from the German Federal Office for Information Security (BSI). The SINA VPN Stack enables a secure connection to the organizational network. Since no data is stored persistently on the device, your information remains safe even if the smartphone is lost.

SINA Mobile is easy for users to operate. Access to the internal network and data occurs within the secure environment of the app. Outside the app, the smartphone can be used normally and even privately.

When connected to a monitor, mouse, and keyboard, the smartphone becomes a full-fledged workstation thanks to the supported desktop mode. The smartphone camera can be used for video conferences.

Edit documents without exposing data

Writing emails, opening and editing documents, accessing the intranet, managing projects, or booking hours—all of this is possible with SINA Mobile from your smartphone. In the app's browser, all applications and programs with a web interface can be used, such as Outlook Web Access.

The secure browser supports virtual desktop infrastructures and virtual mobile infrastructures. This way, specific specialized procedures of your organization can also be used. The computing power of the virtual infrastructures comes from the backend.

[1] currently in the approval process

Applications scale optimally to large screens. Useful feature: Because the computing power comes from the backend, SINA Mobile provides employees with a high-performance workstation regardless of the smartphone they use.

Work simply without worrying about security

The core element of the solution is the proven SINA VPN Stack, already integrated into other SINA solutions. This provides additional security, as SINA Mobile does not rely on the operating system's standard VPN.

Together with the approved hardware security anchor (the embedded Secure Element for SAMSUNG and the Secure Enclave for Apple), the device can connect to the appropriate SINA Gateways to establish a secure communication tunnel to a data center.

SINA Mobile complements the existing SINA infrastructure for even more flexibility and convenience. The application suite is managed via a mobile device management. The necessary hardware security anchors for the devices are administered in the same management environment as all other SINA components.
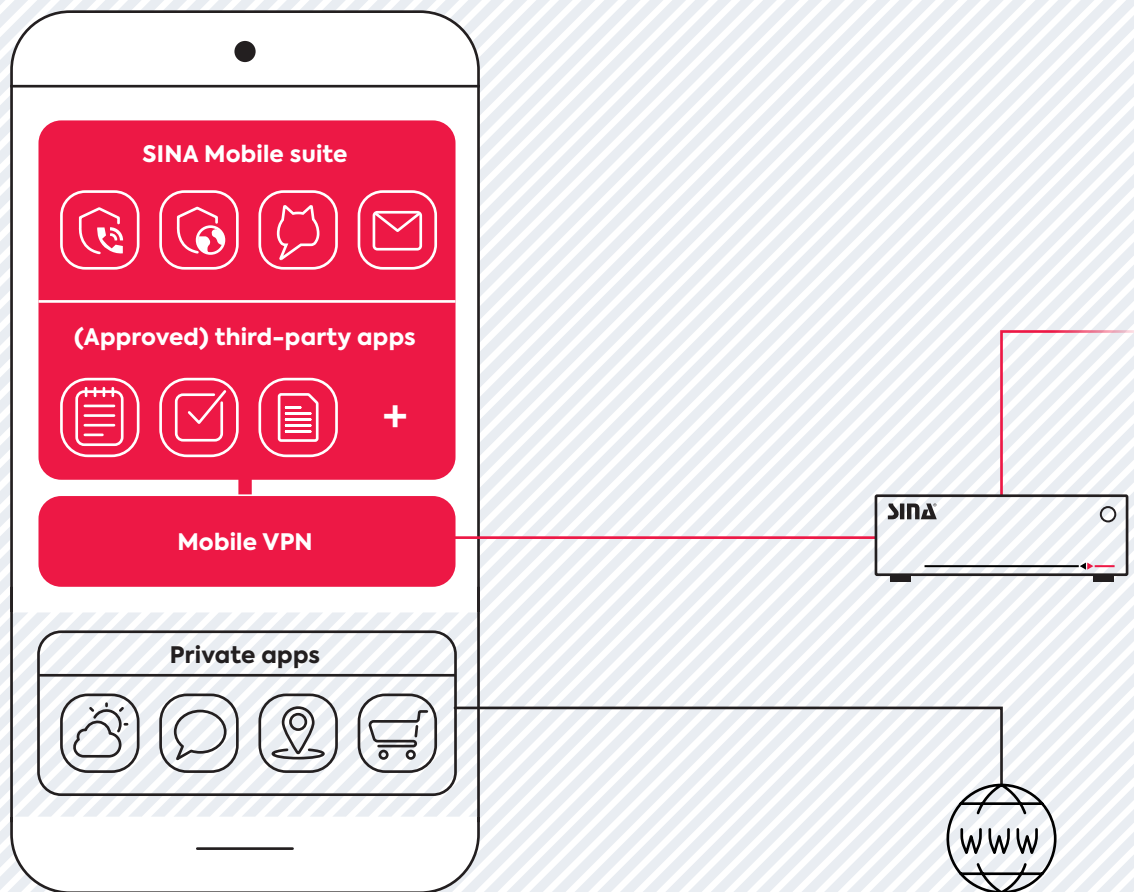
An all-in-one solution without limitations

SINA Mobile offers a comprehensive solution for business phones. It supports an open app ecosystem: third-party apps already approved by the BSI can communicate via the SINA VPN once signed by secunet. Even non-approved apps can be virtualized from the backend and used just like local apps.

Since SINA Mobile also builds on the approved platforms Apple iNDIGO and SAMSUNG Knox Native, mail, calendar, and contacts can even be used offline.

Make calls without anyone listening in

Using the integrated VoIP telephony app, employees can make encrypted calls with others in the organization up to the confidentiality level German RESTRICTED. Thanks to the secure VPN tunnel, there is no need to worry about unauthorized eavesdropping.

The other party does not necessarily need a SINA Mobile device: calls can also be received via the SINA Workstation or SINA Communicator.

Chat without anyone reading along

Employees can chat securely using the integrated stashcat app. This business messenger is not only EU-GDPR compliant within the SINA Mobile environment but also approved up to German RESTRICTED classification level.

With stashcat, you can exchange not only text messages and images but also conduct video conferences directly through the messenger. Additional features such as a calendar, file storage, and polls further facilitate collaboration.

stashcat can be used as an app or in a browser on other devices such as the SINA Workstation. The user license for stashcat is included with SINA Mobile.

With stashcat, the team is always up to date.

SINA.
Holistic concepts.
Simply done.

SINA Mobile seamlessly integrates into the SINA infrastructure

Like other SINA devices, the smartphone connects to the network via the SINA VPN Stack, with gateways managing secure data traffic. All SINA users and components are managed through central SINA Management.

Users no longer need to do much to ensure data protection with SINA. They can fully enjoy the benefits of the digital work environment, always in compliance with German classified information directive (VSA) standards. Another advantage of the SINA ecosystem is that the devices are perfectly aligned and complement each other optimally.

With the proven **SINA Workstation**, employees work securely and in a user-friendly manner in their familiar environment. On their laptop, they can access their data from anywhere. **SINA Mobile** provides a highly mobile complement to the Workstation.

The **SINA Communicator** is designed for desktop use and suitable for classified calls. Calls can be securely made between various devices—whether from a smartphone, the Workstation or the SINA Communicator.

Need to quickly check an application on the road, but your computer is in the office? No problem with SINA Mobile.

SINA Workstation

SINA Mobile

SINA Communicator

SINA was developed as a holistic security system that protects entire digital infrastructures. At its core, perfectly coordinated network components and clients ensure effective encryption and separation of differently classified data – both locally and during transfer via open networks.

With more than 250,000 installations, SINA is the leading security architecture in Germany and is trusted by governments, critical infrastructures and industry worldwide.

secunet – protecting digital infrastructures

secunet is Germany's leading cybersecurity company. In an increasingly connected world, the company's combination of products and consulting assures resilient digital infrastructures and the utmost protection for data, applications and digital identities. secunet specializes in areas with unique security requirements – such as cloud, IIoT, eGovernment and eHealth. With security solutions from secunet, companies can maintain the highest security standards in digitisation projects and advance their digital transformation.

Over 1,000 experts strengthen the digital sovereignty of governments, businesses and society. secunet's customers include federal ministries, more than 20 DAX-listed corporations as well as other national and international organisations. The company was established in 1997, is listed at the German Stock Exchange and generated revenues of around 393 million euros in 2023.

secunet is an IT security partner to the Federal Republic of Germany and a partner of the German Alliance for Cyber Security.

secunet Security Networks AG
Kurfürstenstraße 58 · 45138 Essen · Germany
T +49 201 5454–0 · F +49 201 5454–1000
info@secunet.com · secunet.com

More information:
secunet.com/en/products-consulting/sina-mobile