

Der sichere Arbeitsplatz

für hochmobile Einsatzszenarien bis VS-NfD



SINA Mobile ist eine Thin-Client Lösung für mobile Endgeräte wie Smartphones und Tablets.

SINA Mobile ist eine Applikations-suite mit vier Anwendungen:

- MobileVPN
- MobileWeb
- MobileCall
- MobileScreen

Vorteile

- Sehr hohe Sicherheit, aller Traffic terminiert im Backend
- Sehr gute Skalierung der Rechenleistung
- Sehr gute Wartbarkeit, Backups einfach möglich
- Investitionsschutz, da Endgeräte nicht viel Rechenleistung und Speicher benötigen
- Gerät beliebig austauschbar und einfachst personalisierbar
- Bei Verlust des Endgerätes kein Sicherheitsrisiko und leicht ersetzbar
- Desktop-Mode um einen zweiten Arbeitsplatz zu simulieren (auch Performance lastige Applikationen und Anwendungen können ausgeführt werden, da die Rechenleistung vom Backend kommt)



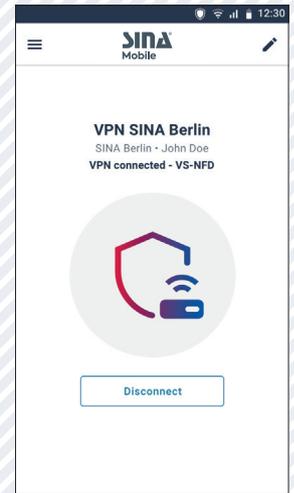
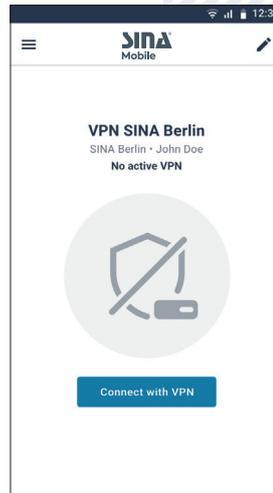
MobileVPN

Das Kernelement der Lösung bildet der MobileVPN. Dieser besteht aus einem eigen entwickelten TCP/IP-Stack und der VPN Komponente die in SINA verbaut ist, sowie einem Hardware-Sicherheitsanker.

Der Sicherheitsanker wird derzeit noch als microSD Token realisiert, jedoch ist die Zielstellung, schon bald auf embedded Secure Elements zurückzugreifen.

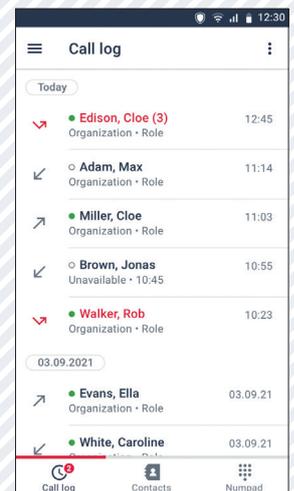
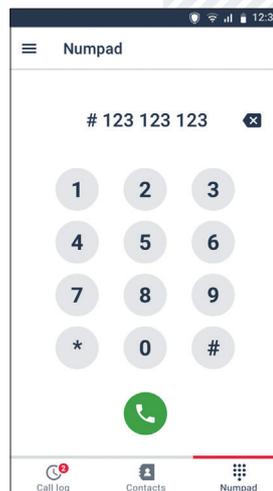
Mit MobileVPN ist das mobile Endgerät in der Lage, sich an eine SINA L3 Box anzubinden und einen sicheren Kommunikationskanal zum Rechenzentrum aufzubauen.

Somit profitieren Sie von einer bereits bestehenden SINA Infrastruktur.



MobileCall

Die zweite Anwendung ist MobileCall. Mit ihr ist es möglich, über den aufgebauten VPN-Tunnel verschlüsselte Telefonanrufe bis VS-NfD Niveau mit anderen Teilnehmern im Netzwerk zu führen. Netzübergreifende Gespräche sind derzeit in Planung und Entwicklung.



MobileWeb

Mit MobileWeb können VS-NfD Daten über gängige HTML basierte Webanwendungen wie z. B. Outlook Webaccess bearbeitet werden.

Der Browser ist selbst gehärtet und verfügt über eine von uns geschaffene Daten-Diode. Diese ermöglicht es uns, Input durch Sensoren und Aktoren des Gerätes hineinzureichen, ohne dass Informatio-

nen wieder zurück zum Endgerät abfließen können. Sie werden lediglich in dem gehärteten Browser angezeigt und können auch nur dort weiterbearbeitet werden.

Damit kann mit allen Diensten und Applikationen auf dem Endgerät bis VS-NfD gearbeitet werden, die ein einfaches Web-Interface anbieten.



MobileScreen

Der MobileScreen ist die innovativste Anwendung unserer Suite. Hierbei wird ein virtualisiertes Android im Rechenzentrum für jeden Endnutzer personalisiert gehostet.

Durch die sichere VPN-Verbindung werden hier die Sensoren und Aktoren vom Endgerät an die virtuelle Instanz durchgereicht. Die grafische Oberfläche des virtuellen Betriebssystems wird auf das Endgerät gespiegelt.

Dadurch sieht es für den Anwender so aus, als würde er weiterhin auf seinem nativen Endgerät arbeiten, obwohl er eigentlich von remote auf seine persönliche virtuelle Instanz zugreift.

Der Unterschied zu MobileWeb besteht darin, dass hier native Android Anwendungen sicher im Rechenzentrum betrieben werden können.

MobileScreen bedarf damit einer Hostingumgebung (heute Secustack), wohingegen die MobileWeb Anwendung ohne zusätzliche Hostingumgebung auskommt.

Da diese Anwendung noch so innovativ ist, hören wir häufig die Frage nach der Latenz.

Die Latenzen bewegen sich bei einer schnellen 5G / LTE Verbindung im Rahmen von 20-50 Millisekunden, wodurch keine spürbare Verzögerung wahrgenommen wird.

Derzeit ist die Gesamtlösung SINA Mobile nur auf Android Geräten verfügbar. Pläne bezüglich einer Realisierung auf iOS sind vorhanden und der Roadmap zu entnehmen.

Es ist eine VS-NfD Zulassung für das Produkt in 2023 angestrebt.

Design-Prinzipien / USPs

- Keine lokal auf dem Gerät persistent gespeicherten Daten
- Transportverschlüsselung mit SINA Technologie (Anbindung an SINA-Infrastruktur)
- Nutzung eines zugelassenen SEs (SINA Smartcard, perspektivisch eSIM)
- Keine Einschaltung durch unflexible Container-technologien
- Möglichst flexibles App-Angebot in der Virtualisierung ohne Neu-Zulassung

Unterstützte Hardware-Modelle

Derzeit werden alle Geräte unterstützt die Android 12 oder neuer als Betriebssystem haben und über einen microSD Kartenslot verfügen.

Im Rahmen der VS-NfD Zulassung wird in Zukunft auf ausgewählte Geräte (Smartphones und Tablets) zurückgegriffen. Weitere Informationen können der Roadmap entnommen werden.

secunet Security Networks AG

Kurfürstenstraße 58 · 45138 Essen

T +49 201 5454-0 · F +49 201 5454-1000

info@secunet.com · secunet.com

Weitere Informationen:
secunet.com/sina

secunet