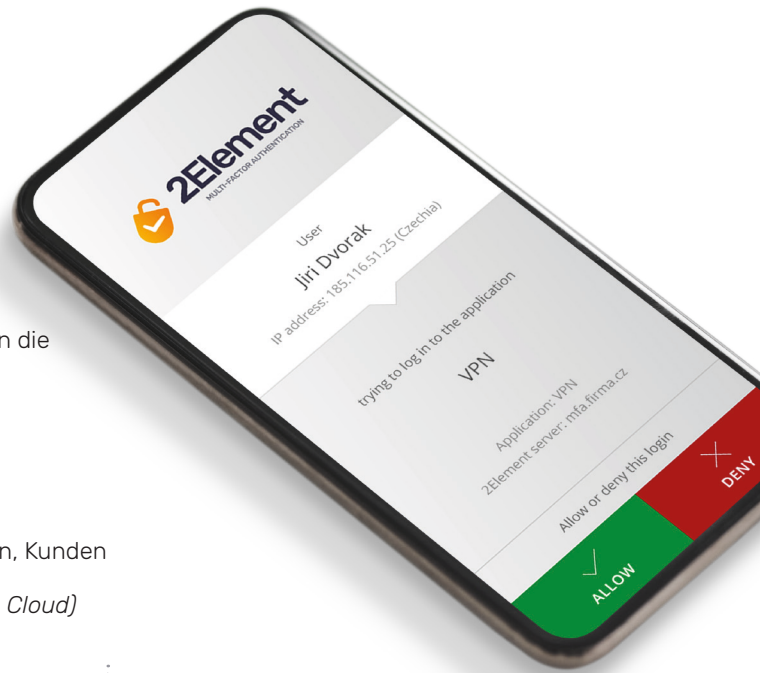
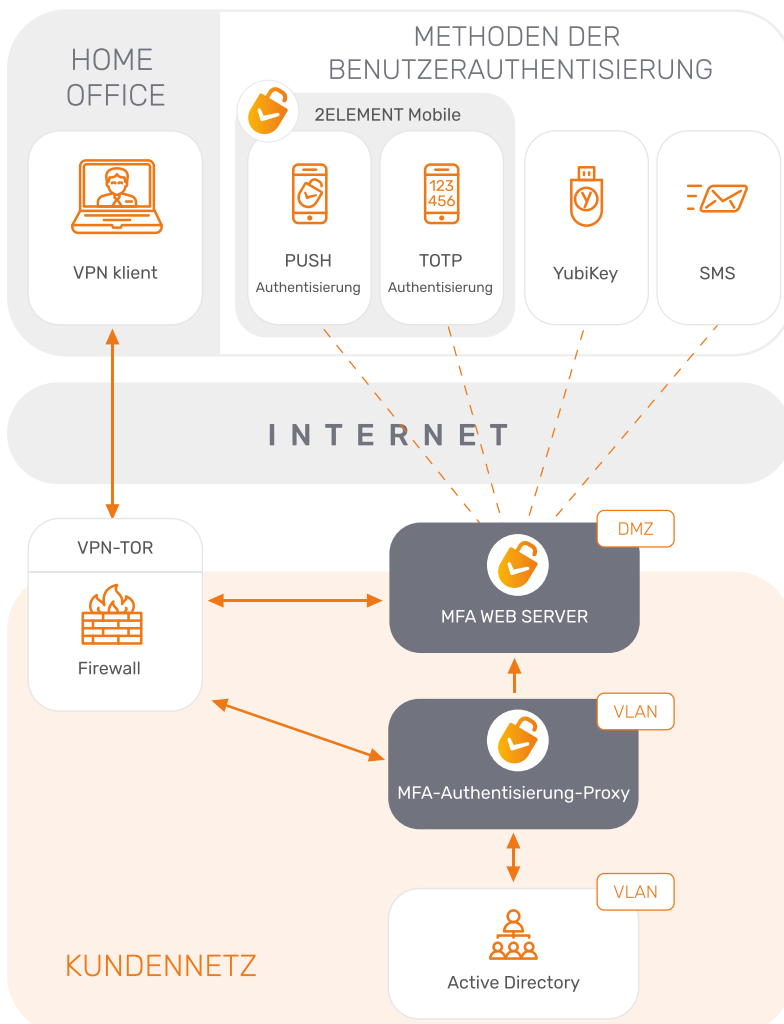


## UNIVERSALLÖSUNG FÜR MULTI-FAKTOR-AUTHENTISIERUNG MULTI-FAKTOR-AUTHENTISIERUNG (MFA)

- Universallösung für Organisationen und Firmen
- MFA ergänzt problematische Passworte mit weiteren Faktoren
- **MFA wird vor allem für folgende Kontos verwendet:**
  - **Privilegierte Kontos** (*verschiedene Administratorberechtigungen*)
    - für alle Zugriffstypen
    - VPN, Anmeldung in Server, Verwalter der Passworte,...
  - **Benutzerkontos** – vor allem für Zugriffe aus dem Internet in die Organisation (*oder in Cloud*)
    - VPN, Remote Desktops (RDP), ...
- Unterstützung der tschechischen und englischen Sprache (*weitere Sprachen können ergänzt werden*)
- Flexible Lösung für Authentisierung – von Angestellten, Partnern, Kunden
- Mögliche On-Premise-Installation (*ganz nur beim Kunden, ohne Cloud*)



### Beispiel der Anmeldung des VPN-Klienten (*typisch für Heimbüros*)



### UNTERSTÜTZTE FAKTOREN DER AUTHENTISIERUNG

- **Mobile Anwendungen 2Element**
  - PUSH-Authentisierung
  - TOTP-Authentisierung
  - Unterstützung für iOS und Android
  - Unterstützung TouchID/FaceID
- **Hardware tokens**
  - Yubikey für OS Windows, MacOS und Linux
- **SMS-Nachrichten**
  - Unterstützung für SMS-Cloud-Dienste und SMS-Gateways

Es entspricht der Empfehlung von



CYBERSECURITY  
& INFRASTRUCTURE  
SECURITY AGENCY



## ANBINDUNG AN AD ODER ADFS

- Anbindung an Active Directory, einschl. der Einstellung, welche Benutzerbäume oder -gruppen zu synchronisieren sind und wie.
- Gleichzeitige Unterstützung sowohl der lokalen Gruppen und Benutzer, als auch der Gruppen und Benutzer, die aus AD übergeben werden.
- Der Betrieb ist auch ohne Anbindung an AD möglich. Lokale Benutzer können auch direkt in MFA-SERVER gespeichert werden. Geeignet für Installationen ohne AD, oder für Benutzer, die sich nicht in AD befinden.
- Möglich ist auch die Unterstützung weiterer kompatibler LDAP-Verzeichnisse.
- Integration in ADFS-Anmeldung – auf diese Weise wird das ganze Ökosystem um MFA einfach erweitert, das die ADFS-Anmeldung und kettenweise auch SAML unterstützt.

## MÖGLICHKEITEN DER MFA-INTEGRATION

- Offene API für Integration in Applikationen von Dritten
- Anbindung an ADFS und SAML (z. B. *Cloud-Dienste des Kunden*)
- RADIUS-Unterstützung (z. B. für VPN)
- SMS-Tore
- Verwalter der Passworte – schlüsselfertige Lieferungen sind möglich

## UNTERSTÜTZTE PLATTFORMEN

VPN mittels RADIUS





Hardware Tokens




## TYPISCHE DIENSTE UND APPLIKATIONEN FÜR MFA



VPN-Zugriffe (Fortinet, Cisco, CheckPoint, ...)



Administrator RDP-Zugriffe auf MS-Server



Remote Desktops (RDP) für Benutzer, einschl. Terminal-Server Zugriffe



Lokale Anmeldung der Benutzer in PC



ADFS (Active Directory Federation Services) Integration



Cloud-Dienste (O365, ...)



Eigene Applikation des Kunden (Helpdesk, Intranet, ...) mittels API, SAML



Portale und Lösungen für Partner und Kunden



Weitere Integration durch Radius- oder LDAP-Protokolle



## KUNDENLÖSUNG

- Für größere Implementationen bieten wir eine Lösung an, die heutzutage z. B. in Banken unter den Namen KB-Schlüssel, RB-Schlüssel, ... beliebt ist.
- Wir liefern dem Kunden eine angepasste Mobilapplikation, die ganz kompatibel für alle MFA-Zugriffe ist.
- Geeignete Konsolidierung aller Applikationen, die MFA-Authentisierung benutzen sollen.
- „White Label“ Anpassung
  - für Server (*eigene Bezeichnung und eigenes Design*)
  - für Mobilapplikationen (*eigene Bezeichnung und eigenes Design, feste Verbindung mit dem Kundenserver*)

Mehr Informationen: [www.2element.cz](http://www.2element.cz)

Entwickelt von der Gesellschaft:

SONPO, a.s. | Prag | Tschechien  
[www.sonpo.eu](http://www.sonpo.eu) | [sales@sonpo.eu](mailto:sales@sonpo.eu)

