



# KEY2B

## EINFACH VERSCHLÜSSELN, SIGNIEREN UND AUTHENTIFIZIEREN

### Worum geht's?

- E-Mail-Verschlüsselung
- Digitale Unterschriften
- Verbesserung und Absicherung von Geschäftsprozessen

Ohne E-Mail und IT geht heute in den meisten Unternehmen nichts mehr, doch die zunehmende Digitalisierung ist nicht ohne Risiko: Die Gefahren durch IT-basierte Angriffe, Computerkriminalität und Wirtschaftsspionage steigen und mit ihnen die gesetzlichen Anforderungen an IT-Sicherheit und Datenschutz. Verschlüsselung ist eine wirksame Möglichkeit die eigene Kommunikation zu schützen, doch entsprechende Lösungen eigneten sich bisher nur für IT-Experten und große Unternehmen. Mit Key2B gibt es jetzt erstmals eine professionelle Verschlüsselung für kleine und mittlere Betriebe. Sie eignet sich auch für Computernutzer ohne Fachkenntnisse und Betriebe ohne IT-Abteilung. Technologie und Verfahren sind bereits bei tausenden Nutzern erfolgreich im Einsatz.

Mit Key2B-Schlüsseln können Unternehmen gesetzliche Vorgaben einfach erfüllen und gleichzeitig ihre Betriebsabläufe verbessern. Nutzer können verschlüsselte und/oder signierte E-Mails versenden und empfangen. Zusätzlich lassen sich Dokumente mit Standardsoftware elektronisch unterschreiben und archivieren. So können Unternehmen zum Beispiel interne und externe Prozesse wie Urlaubsanträge, Zeiterfassung, Auftragsänderungen oder Freigabeprozesse digital abbilden. Zusätzlich können Benutzer sich in geeigneten Web-Anwendungen sicher einloggen – ganz ohne komplizierte Passwörter.

### Was ist Key2B?

- Laientaugliche Software zur Schlüsselerzeugung und Installation

### Für wen eignet sich Key2B?

- Freiberufler
- Kleine und mittelgroße Unternehmen

### Vorteile:

- Erfüllung von Datenschutz- und Compliance-Anforderungen dank standardkonformer S/MIME-Zertifikate
- Beschleunigung von Betriebsabläufen
- Fortgeschrittene digitale Signatur für Rechnungen und andere Dokumente

### Was unterscheidet Key2B von anderen?

- Höchste Sicherheitsstufe durch Identitätsprüfung
- Echte Ende-zu-Ende-Verschlüsselung: Nur Absender und Empfänger sehen den Inhalt der E-Mails
- Usability by Design - Laientauglichkeit
- Einfache Integration: Nutzung bestehender E-Mail-Infrastruktur
- Zertifikate made in Germany

### Systemvoraussetzungen:

- Betriebssysteme: Windows, macOS\*, iOS\*
- Mail-Clients: Outlook, Thunderbird, Apple-Mail\*, Lotus Notes\*
- Webbrowser: Internet Explorer, Firefox, Chrome, Safari\*

\* Schlüssel müssen zurzeit noch auf einem Windows-Gerät erzeugt werden. Sie können dann exportiert werden, um sie auf Geräten mit anderen Betriebssystemen oder über eine Netzwerk-basierte Anwendungen zu nutzen.

*Fraunhofer-Institut für Sichere  
Informationstechnologie SIT*

*Kontakt:  
Oliver Küch  
Rheinstraße 75  
64295 Darmstadt*

*Telefon 06151 869-213  
Fax 06151 869-224  
oliver.kuech@sit.fraunhofer.de*