

Liebe Userin, lieber User!

### Gebrauchsinformation für den/die AnwenderIn:

Bitte lesen Sie diese Gebrauchsinformation sorgfältig durch bevor Sie den PrivacyDongle anwenden, da sie wichtige Informationen darüber enthält, wie Sie bei der Verwendung von **PrivaSEC forte** vorgehen sollten. Heben Sie die Packungsbeilage auf. Vielleicht möchten Sie diese später noch lesen.

**PrivaSEC forte** wurde Ihnen persönlich verschrieben. Sie können **PrivaSEC forte** aber auch jederzeit weiterschicken.

Weitere Exemplare von **PrivaSEC forte** sind bei der UBIT Wien unter [ubit@wkw.at](mailto:ubit@wkw.at) erhältlich.



# PrivaSEC forte

PrivacyDongle  
Wirkstoff: Browser für TOR-Netzwerke

### Anonymes Surfen auf Rezept:

Beim Surfen im Internet hinterlassen Sie einen digitalen Fußabdruck, der es anderen ermöglicht, Ihre Aktivitäten zu verfolgen oder zu rekonstruieren. Die Europäische Menschenrechtskonvention und somit auch die österreichische Verfassung sichern Ihnen ein Recht auf Privatsphäre zu, das natürlich auch für das Internet gilt. Das Brief- und das Fernmeldegeheimnis sind wichtige Bürgerrechte, die auch im Internet gewahrt werden müssen.

Ihr Recht auf Privatsphäre wird durch neue technische Möglichkeiten und damit zusammenhängende Gesetze ausgehöhlt. Der PrivacyDongle ermöglicht Ihnen, das Internet anonym zu verwenden, und sichert Ihr Recht auf Privatsphäre. Er verhindert unter anderem zuverlässig, dass aus Ihrem Verhalten im Internet Rückschlüsse über Ihre Vorlieben oder Ihr Kaufverhalten u.a. gezogen werden können.

### Anwendung:

Die Anwendung von **PrivaSEC forte** ist einfach. Der kleine USB-Stick beherbergt eine Version des Browsers Firefox, mit der eine anonyme Kommunikation ohne vorherigen Installationsaufwand möglich ist. Der Dongle wird einfach in den USB-Port des Rechners am Arbeitsplatz (sofern die private Nutzung der Rechner nicht verboten ist), bei Freunden oder in einem Internetcafé gesteckt. Dann wählen Sie den Stick an, klicken auf das Programm-Icon und schon kann es losgehen.

Sobald Sie auf das Programm-Icon klicken, wird ein adaptierter Firefox-Browser geöffnet. Dieser verbindet sich sofort mit dem TOR-Netzwerk und ermöglicht so das unerkannte Surfen. Sie können den **PrivaSEC forte** mit Windows-, Linux- und Apple-Systemen verwenden. Sie können Ihre Installation sogar von einem Betriebssystem zum anderen „mitnehmen“ und ihre Browser-Umgebung so über die Systemgrenzen „wandern lassen“.

Bei fremden Rechnern sollten Sie Ihren Dongle nach der Benutzung wieder entfernen und mitnehmen.

### Wirkungsprinzip:

Der Einsatz von **PrivaSEC forte** schützt Sie gegen die Analyse Ihrer Zugriffsdaten, indem

- der auf dem USB-Stick installierte Firefox-Browser auf dem verwendeten Rechner keine Daten ablegt und Sie damit keine nachträglich auswertbaren Spuren hinterlassen;
- der Zugang zum Internet über das TOR-Netzwerk erfolgt, das Ihre Anfragen im Internet nicht mehr rückverfolgbar macht.

Das TOR-Netzwerk schützt gegen die Auswertung Ihrer Internetnutzung, bei der durch die Analyse des Netzverkehrs ermittelt wird, wer mit wem über ein öffentliches Netzwerk kommuniziert. Diese Form der Auswertung findet sowohl aus kommerziellem als auch aus politischem Interesse verstärkt statt. Bei der Verwendung von **PrivaSEC forte** werden Ihre Kontakte mit dem Internet in verschlüsselter Form so über mehrere TOR-Server gesendet, dass die Rückverfolgung zum Ausgangspunkt so gut wie ausgeschlossen ist. Für den Zielserver Ihrer Kommunikation gilt der letzte TOR-Server als Ausgangspunkt der Abfrage.



## Risiken und Nebenwirkungen:

**PrivaSEC forte** führt keine Verschlüsselung Ihrer Daten durch. Das TOR-Netzwerk setzt Verschlüsselung nicht dazu ein, um Ihre Kommunikation abhörsicher zu machen. Die Verschlüsselung besteht nur innerhalb des TOR-Netzwerks. Zwischen dem von Ihnen verwendeten Rechner und dem Zugangspunkt im TOR-Netzwerk sowie dem letzten Server im TOR-Netzwerk (dem „TOR-Ausgangsknoten“) und dem von Ihnen adressierten Webserver sind die Daten so gut oder schlecht geschützt wie bei einer normalen Verbindung. Nur die Herkunft Ihrer Verbindung ist verschleiert (die Verbindung scheint vom TOR-Ausgangsknoten zu kommen), nicht die Inhalte.

Sie bleiben deshalb nur so lange anonym, bis Sie Ihren eigenen Namen irgendwo eingeben oder sich in ein Forum o.Ä. einloggen. Damit Ihre Verbindung bis zum Webserver abhörsicher wird, müssen Sie weiterhin „https“-Verschlüsselung nutzen. Sensitive Daten, zum Beispiel beim Online-Banking, könnten sonst irgendwo zwischen dem TOR-Ausgangsknoten und dem Webserver abgehört werden.

Die Möglichkeit, sich anonym im Internet zu bewegen, bringt auch Verantwortung mit sich. Wie überall sonst im Leben erleichtert auch hier die Anonymität ein im weitesten Sinne asoziales Verhalten. Anwender müssen sich ihrer Verantwortung gegenüber anderen bewusst sein, um sich korrekt verhalten zu können (und zu wollen!).

Sobald in Österreich das Gesetz zur Vorratsdatenspeicherung in Kraft tritt werden auch die TOR-Server diesen Vorschriften unterliegen. Bei einer gesetzlich begründeten Analyse des vollständigen Datenverkehrs im TOR-Netzwerk kann aufgrund von Nutzungsprofilen die Anonymität nicht immer vollständig gesichert werden.

## Kontraindikation:

Verwenden Sie **PrivaSEC forte** auf keinen Fall, wenn Sie

- Angst vor Unterstellungen haben, dass Sie als PrivacyDongle-NutzerIn hätten etwas zu verbergen, und
- Sie befürchten, dass Sie Ihren Anspruch auf Privatsphäre im Zuge möglicher Ermittlungsverfahren nicht ausreichend argumentieren können;
- dem Art. 19 der Allgemeinen Deklaration der Menschenrechte über die Informationsfreiheit oder
- dem Art. 10 der Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK), dem Recht der freien Meinungsäußerung oder
- dem Art. 8 der Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK), dem Gebot der Achtung der Privatsphäre nur geringe bis keine Bedeutung beimessen
- Wert auf die externe Nachvollziehbarkeit bestimmter Internetkontakte legen.

## UBIT und Datenschutz:

Die UBIT als gesetzliche Interessensvertretung der Wiener Dienstleistungsunternehmen in der Informationstechnologie und die IT-Security Experts Group der UBIT stellen die PrivacyDongles bereit und betreiben für zunächst zwei Jahre insgesamt drei leistungsfähige TOR-Server in Österreich. Als Anerkennung für die Softwareentwicklung wurde dem FoeBuD e.V. eine Spende übermittelt.

Die österreichischen IT-AnwenderInnen sind KundInnen der UBIT-Mitglieder, die darauf vertrauen können, dass ihre privaten Daten bei den IT-Dienstleister gut aufgehoben sind. Mit dieser Aktion betont die UBIT die hohe Bedeutung des Datenschutzes und stellt klar, dass die Informationsdienstleister die Interessen ihrer Kunden wahren.

## Credits:

Die UBIT Wien dankt allen, die zu diesem Projekt beigetragen haben, sehr herzlich. Im Internet sind die Initiatoren mit umfangreichen weiteren Informationen vertreten unter:

<https://www.foebud.org/>

<http://www.privacydongle.com/>

<http://www.torproject.org/>

<http://www.vibe.at/>

<http://www.ubit.at/wien/>

<http://www.itsecurityexperts.at/>

## Impressum:

Fachgruppe UBIT

Unternehmensberatung und Informationstechnologie

Rudolf-Sallinger-Platz 1

A-1030 Wien

Telefon: +43 1 514 50 2262 oder 2263

