privacy.boutique
— Privacy first! —

https://privacy.boutique
sales@privacy.boutique

Verbindungsaufnahme und Authorisierung

Trennung der Zuständigkeiten

Zu keinem Zeitpunkt ist irgend einem der beteiligten Prozesse ein Rückschluss auf Ihre Identität als Benutzer des anonVPN möglich.

Die Workflows zur Verbindungsaufnahme und zur Authorisierung zum **anonVPN**	
Workflow A	**Verbinde Benutzer / CryptoRouter mit anonVPN** Dazu benutzt werden Standard OpenVPN Protokolle. Dieser Workflow wird automatisch und immer zuerst ausgeführt. Dabei wird die lokale FIREWALL für den ein- UND ausgehenden Verkehr GESPERRT. Eine einzige Verbindungsmöglichkeit bleibt geöffnet – es ist die Verbindung zum AUTHENTICATOR des **anonVPN**.
Workflow B	**Authentisiere und authorisiere Verbindung zum anonVPN** Dazu benutzt werden proprietäre vpnauth/2- und WebAuth-Protokolle und Programme. Dieser Workflow erfolgt mit den vorkonfigurierten Konto-Informationen Konto-ID und Konto-PW als einzige übermittelte Daten. Der AUTHENTICATOR – ein vom anonVPN völlig getrennter Server – prüft dabei einzig, ob das zu den angegebenen Konto-Informationen passende Ablauf-Datum in der Vergangenheit liegt. Falls dies NICHT der Fall ist, wird an den «Workflow C» ein «OPEN»-Token zurück geliefert. In allen anderen Fällen – Datum abgelaufen oder Konto gar nicht vorhanden – wird KEIN Token zurück geliefert.
Workflow C	**Öffne FIREWALL zum anonVPN** Falls aus «Worflow B» ein «OPEN»-Token resultiert, wird die Firewall und damit der ungehinderte Zugang zum Internet geöffnet. Anderenfalls bleibt die Firewall geschlossen und es erfolgt KEIN Zugang zum Internet.

Weitere Informationen:
- SoC – Separation of Concerns (pb._Flyer_SoC_DE.pdf)
- CryptoRouter Pro (pb._Flyer_CRpro_DE.pdf)
- CryptoRouter Slate (pb._Flyer_CRslate_DE.pdf)

https://privacy.boutique
sales@privacy.boutique

Die Workflows zur Verbindungsaufnahme und zur Authorisierung zum **anonVPN**

Mit dem Ziel: Die private und geschützte Nutzung des Internets