

## **Zertifizierung von Mixbetreibern (JonDonym)**

Die Identität der Betreiber von JonDonym-Mixen wird durch Certification Authorities zertifiziert. Neben der JonDos GmbH bietet auch die German Privacy Foundation e.V. diesen Service. Dabei wird zwischen dem Betreiber und der GPF folgender Vertrag geschlossen (Stand 10.03.2009):

Vereinbarung zur Zertifizierung eines Mix-Betreibers  
zwischen der

German Privacy Foundation e.V.  
Berliner Straße 69  
13189 Berlin

Kontakt:

Webformular: JonDonym-CA.msg  
E-Mail: jondonym\_ca (at) privacyfoundation.de  
(OpenPGP: 0x8A1737D5)

und dem Mix-Betreiber

### **§ 1 Gegenstand der Vereinbarung**

1. Der Betreiber kann Nutzern der Software JonDo sogenannte Mix-Server (im folgenden Mixe genannt) als Dienst anbieten. Soweit er diese Dienstleistung im Rahmen einer Zertifizierung durch die German Privacy Foundation e.V. erbringt, verpflichtet er sich zur Einhaltung der hier genannten Vereinbarung, um die Sicherheit und Leistungsfähigkeit seiner Dienste so weit wie möglich zu gewährleisten.
2. Der Austausch von Leistungen oder die Abrechnung über Leistungen ist nicht Gegenstand dieser Vereinbarung.
3. Ausgehend von dieser Vereinbarung ist der Betreiber eigenverantwortlich für den Betrieb seiner Mixe und für die Bereitstellung seiner Dienstleistung an die JonDo-Nutzer. Insbesondere ist er unabhängig von der German Privacy Foundation e.V.

### **§ 2 Definitionen**

Ein Mix ist diejenige Software, welche die IP-Pseudonymisierung für JonDonym erbringt. Mit Mix-Server wird die Betriebssystemumgebung bezeichnet, in der ein Mix läuft. Als Mix-Rechner wird das physische Gerät bezeichnet, auf dem diese Betriebssystemumgebung installiert ist. Einzel-Mixe oder Mix-Kaskaden, zu denen sich JonDo-Nutzer verbinden können, werden als Dienste bezeichnet.

### **§ 3 Zertifizierung**

1. Der Betreiber muss den Nutzern seiner Mixe alle wesentlichen Informationen zu seiner Identität als natürliche oder juristische Person offenlegen.
2. Zu den wesentlichen Informationen zählen:

- der vollständige Name des Betreibers bzw. seiner Organisation,
- das Land, in dem der Betreiber seinen Sitz oder Wohnsitz hat,
- eine gültige und regelmäßig abgerufene E-Mail Adresse,
- die Adresse einer offiziellen Website des Betreibers.

3. Der Betreiber stellt der German Privacy Foundation e.V. einen Certificate Signing Request (CSR) nach dem Standard X.509v3 bereit. Der CSR muss die gleichen Signaturalgorithmen verwenden wie das Zertifikat der German Privacy Foundation e.V. Die GPF prüft und signiert diesen CSR und sendet das gültige X509-Zertifikat an den Betreiber zurück. Voraussetzung ist, dass folgende wesentlichen Informationen zur Identität des Betreibers zuzüglich zu den oben genannten Daten nachgewiesen wurden:

- eine gültige postalische Adresse (kein Postfach)
- eine telefonische Kontaktmöglichkeit

4. Die Zertifizierung ist kostenfrei. Es steht dem Betreiber offen, mit einer freiwilligen Spende die German Privacy Foundation e.V. zu unterstützen.

5. Die Gültigkeit des Zertifikates ist auf drei bis zwölf Monate beschränkt. Die German Privacy Foundation e.V. verpflichtet sich, mindestens eine Woche vor Ablauf des Zertifikates ein neues Zertifikat auszustellen, wenn der Betreiber dies mindestens drei Wochen vor Ablauf des Zertifikates beantragt.

6. Die German Privacy Foundation e.V. kann ein Betreiber-Zertifikat vorzeitig als ungültig markieren, wenn:

- der Verdacht des Missbrauchs besteht.
- der Verdacht auf Kompromittierung durch unbefugte Dritte besteht.
- diese Vereinbarung gekündigt wurde.
- der Betreiber eine der Voraussetzungen nicht mehr erfüllt.

7. Jedem Mix ist vom Betreiber ein individuelles, gültiges Mix-Zertifikat zuzuweisen, welches mit seinem Betreiber-Zertifikat signiert wurde. Die im Mix-Zertifikat gespeicherten Angaben über den Standort des Mix-Rechners müssen der Wahrheit entsprechen.

8. Die privaten Keys der Mix- und Betreiber-Zertifikate sind vor dem Zugriff unberechtigter Dritter zu schützen. Auch die German Privacy Foundation e.V. zählt nicht zu den Zugriffsberechtigten. Betreiber-Zertifikate sind mit einem starken Passwort zu sichern.

#### **§ 4 Verwendung der Mix-Software**

1. Der Betreiber kann die Quellcodes der JonDo- und Mix-Software von der JonDos GmbH beziehen. Die German Privacy Foundation e.V. ist nicht für die Wartung und Entwicklung der Software zuständig.

2. Der Betreiber ist gehalten, ihm bekannt gewordenen Aktualisierungen der Mix-Software unverzüglich einzuspielen und regelmäßig Änderungen zu prüfen.

3. Stellt der Betreiber Veränderungen des Codes durch nicht autorisierte Dritte fest oder Änderungen, die offensichtlich dazu gedacht sind, die Sicherheit des Dienstes negativ zu beeinflussen, so hat er dies unverzüglich an die Entwickler der Software zu melden und darf diese Software nicht einsetzen.

## § 5 Weiterleitung und Speicherung von Daten

1. Der direkte oder indirekte Austausch bzw. die Weiterleitung von Nutzer- und Verbindungsdaten zwischen den Betreibern, Mixen, Mix-Servern und Mix-Rechnern ist nur innerhalb der Mix-Software standardmäßig aktivierten Protokolle gestattet.
2. Das Speichern von Verkehrsdaten, Kommunikationsinhalten, Informationen über den inneren Zustand eines Mixes und die anonymisierten Verbindungen oder das Übermitteln dieser Daten an Dritte ist untersagt, soweit die folgenden Absätze nichts anderes bestimmen.
3. Die verdachtslose Speicherung von Kommunikationsdaten der Nutzer im Rahmen der Vorratsdatenspeicherung (§113a TKG) oder vergleichbarer Bestimmungen ist untersagt. Die German Privacy Foundation e.V. wird die Zertifizierung als ungültig markieren, wenn der Betreiber gegen diese Regelung verstößt.
4. Eine kumulative, anonymisierte Speicherung von statistischen Daten bedarf der schriftlichen Zustimmung der German Privacy Foundation e.V. Die Speicherung darf maximal für einen Monat erfolgen und nur folgende Daten umfassen:
  - Herkunftsland der Nutzer
  - Kategorien von aufgerufenen URLs
5. Die jeweils geltenden nationalen Vorschriften bleiben unberührt.

## § 6 Organisation von Mixen in Kaskaden

1. Definitionen
  - Eine Kaskade ist ein Zusammenschluss von zwei oder mehr Mixen.
  - Mixe einer Kaskade sind geografisch verteilt, wenn deren Mix-Rechner nicht bei demselben Host betrieben werden.
  - Der Betreiber ist unabhängig von anderen Betreibern, wenn keine verwandtschaftlichen Beziehungen, Anstellungsverhältnisse, direkte oder indirekte Weisungsbefugnisse bestehen, wenn keine persönlichen, organisatorischen oder finanziellen Abhängigkeiten bestehen und wenn keine vertraglichen Abhängigkeiten bestehen. Der Betreiber ist verpflichtet, solche Verhältnisse unverzüglich offenzulegen.
  - Eine Kaskade gilt als international wenn der Sitz der Betreiber der Mixe in verschiedenen Ländern gemeldet ist und die Standorte der Mix-Rechner einer Kaskade nicht in denselben Ländern liegt.
2. Mixe müssen in geografisch verteilten, internationalen Kaskaden ohne Datenspeicherung betrieben werden. Stehen keine vollständig geeigneten Mix-Server im Sinne von § 6(1) zur Verfügung, so sollen beim Aufbau eines Dienstes die Kriterien gemäß § 6(1) in der angegebenen Reihenfolge eingehalten werden.
3. Die Namen von Mixen und Kaskaden dürfen keine Ortsbezeichnung enthalten, nicht länger als 40 Zeichen sein und nicht gegen deutsche Gesetze und die guten Sitten verstoßen.

## **§ 7 Betrieb und Administration von Mixen**

1. Unbefugten ist der Zugang zu den Mix-Rechnern zu verwehren. Berechtig sind nur diejenigen Personen, die für den Betrieb des Mixes erforderlich sind und denen gegenüber der Betreiber weisungsbefugt ist.
2. Die Mix-Server sind nach dem aktuellen Stand der Technik zu konfigurieren und zu administrieren.
3. Auf dem Mix-Rechner darf nur die Software installiert werden, die für Betrieb und Wartung des Mixes notwendig und sinnvoll ist. Insbesondere untersagt ist der Betrieb anderer von außerhalb des Mix-Servers erreichbarer Proxies, Webserver oder Anonymisierungsdienste.

## **§ 8 Überprüfungen**

1. Der Betreiber ist verpflichtet, einer von der JonDos GmbH oder der German Privacy Foundation e.V. beauftragten und zur Verschwiegenheit verpflichteten Kontrollinstanz zur Überprüfung obiger Zusicherungen Einblick in die dafür notwendigen Unterlagen und Rechnersysteme zu gewähren. Diese Instanz kann ein Rechtsanwalt, ein vereidigter Gutachter, eine Datenschutzbehörde oder ein von beiden Seiten akzeptierter Dritter sein.
2. Betreiber von ausschließlich kostenfreien Mixen tragen keine Kosten für die Überprüfung. Betreiber kostenpflichtiger Mixe tragen die Kosten zu gleichen Teilen mit der beauftragenden Instanz, maximal jedoch 5% des letzten Jahresumsatzes mit den Mixen.
3. Es sind Überprüfungsverfahren anzuwenden, bei denen der Betreiber nicht die unbeaufsichtigte oder nicht-nachvollziehbare Kontrolle über seine Mix-Rechner der Kontrollinstanz überlassen muss. Die Anonymität der Nutzer darf durch die Kontrolle nicht beeinträchtigt werden.
4. Vorgenommene Prüfschritte und Ergebnisse werden öffentlich einsehbar gemacht. Mängel sind innerhalb eines Monats zu beseitigen.
5. Überprüfungen, die von der JonDos GmbH vorgenommen wurden, werden von der German Privacy Foundation e.V. anerkannt.

## **§ 9 Haftung**

1. Der Betreiber ist selbst für alle Folgen seines Mixbetriebs verantwortlich. Die German Privacy Foundation e.V. kann nicht für Schäden oder Vergehen haftbar gemacht werden, die direkt oder indirekt mit dem Mixbetrieb in Verbindung stehen. Der Betreiber haftet direkt gegenüber dem Betroffenen.
2. Der Betreiber haftet selbst für alle kausal verursachten Schäden, die auf grobe Fahrlässigkeit oder Vorsatz von ihm selbst, Vertretern oder Erfüllungsgehilfen zurückzuführen sind.
3. Die German Privacy Foundation e.V. gewährt keine Garantie auf Dienstleistungen, Produkte oder Software, die im Rahmen der Erbringung von Diensten für Mix-Kaskaden

genutzt werden.

4. Die German Privacy Foundation e.V. verpflichtet sich, die Abläufe im Rahmen der Zertifizierung nach besten Kräften abzusichern. Sie haftet nicht für Schäden, Verdienstauffälle und Leistungsminderung innerhalb der Mix-Kaskaden, sofern diese nicht grob fahrlässig oder vorsätzlich herbeigeführt wurden.

## **§ 10 Kündigung**

1. Diese Vereinbarung wird auf unbestimmte Zeit geschlossen und kann von beiden Parteien durch Erklärung in Schriftform gekündigt werden.

2. Die Kündigungsfrist beträgt für beide Parteien vier Wochen zum Ende des Monats, wobei das Recht zur Kündigung aus wichtigem Grund im Sinne des § 341(1) BGB, insbesondere bei Verstoß gegen wesentliche Vertragspflichten, den Parteien unbenommen bleibt.

3. Ein wichtiger Grund liegt insbesondere vor, wenn der Betreiber gegen eine der in dieser Vereinbarung genannten Vorschriften grob fahrlässig oder vorsätzlich verstößt.

4. Mit der wirksamen Kündigung dieses Vertrages erlischt die Zertifizierung des Betreibers.

## **§ 11 Abschließende Bestimmungen**

1. Für diesen Vertrag gilt das Recht der Bundesrepublik Deutschland.

2. Gerichtsstand für alle Streitigkeiten aus diesem Vertrag ist Berlin. Die German Privacy Foundation e.V. ist darüber hinaus berechtigt, den Betreiber an seinem allgemeinen Gerichtsstand zu verklagen.