



---

## Projektgruppe Zugang, Struktur und Sicherheit im Netz

### 3 Fragen zum Thema „IPv6 - Sicherheitsaspekte“

---

#### Fragen an Herrn Gert Döring

- Können „Privacy Extensions“ echte Anonymität garantieren, wenn gleichzeitig andere Teile der Adressen eine Rückverfolgung und zumindest grobe geografische Lokalisierung des Standorts zulassen?
- Gibt es unter Berücksichtigung dessen eine sinnvolle Lösung, und wie hoch ist der technische Aufwand für Provider?
- Die Vorteile sowohl fester, identifizierbarer IP-Adressen als auch dynamischer, komplett anonymisierter IP-Adressen sind bekannt. Ist es denkbar, dass diese Vorteile, unter Ausschluss der Nachteile, gleichzeitig in der selben kleinen Software (Browser) nutzbar sind?

## Fragen an Herrn Gert Döring

### **1. Können “Privacy Extensions” echte Anonymität garantieren, wenn gleichzeitig andere Teile der Adressen eine Rückverfolgung und zumindest grobe geografische Lokalisierung des Standorts zulassen?**

Die “Privacy Extension” verhindern wirksam eine eindeutige Identifikation eines bestimmten Endgerätes anhand seiner IPv6-Adresse.

Anhand des vom Provider zugeteilten Adressraums ist bei statischer Prefix-Vergabe trotzdem nach wie vor eine Wieder-Erkennung eines bestimmten Kundenanschlusses möglich – aber nicht des genutzten Endgerätes oder gar der handelnden Person, und ohne Mitwirkung des Providers auch nicht die Identifikation des Anschluss*inhabers*. Bei einer dynamischer Prefix-Vergabe ist die Identifikation des verwendeten Providers möglich, und je nach Netzstruktur dieses Providers kann auch eine Zuordnung des Teilnehmers in eine geographische Region oder Stadt möglich sein.

IPv6 mit “Privacy Extensions” bietet hier also ein zu IPv4 mit NAT vergleichbares Anonymitäts-Niveau.

### **2. Gibt es unter Berücksichtigung dessen eine sinnvolle Lösung, und wie hoch ist der technische Aufwand für Provider?**

Nachdem durch IPv6 (mit Privacy Extensions) hier kein Problem neu entsteht, ist die Lösung auch nicht bei IPv6 als Transporttechnik zu suchen.

Möchte man die Wieder-Erkennbarkeit eines Teilnehmeranschlusses verhindern, kann die dynamische Zuteilung von Prefixen auf zeitlicher Basis oder “auf Knopfdruck” ein nützliches Hilfsmittel sein.

Will man vollständige Anonymität auf Basis des bestehenden TCP/IP- Protokollstacks, muss man deutlich weitergehende Massnahmen ergreifen, etwa die Verwendung anonymisierender Proxy-Kaskaden (TOR etc.) – und vor allem in den Applikationen ansetzen, denn das Verhalten der üblichen Web-Browser identifiziert sehr viel präziser den einzelnen Benutzer als nur die Wiedererkennung eines Geräts oder Anschlusses über die IP-Adresse.

Der Aufwand für die Provider, dynamisierte IPv6-Prefixe zur Verfügung zu stellen, ist vergleichsweise gering – geringer als die Verwaltung statisch zugewiesener IPv6-Prefixe.

Der Aufwand, einem Anschluss gleichzeitig ein statisches und ein dynamisches Prefix zuzuteilen, ist allerdings als durchaus hoch einzustufen, weil hierfür noch keine automatischen Verfahren existieren, d.h. es muß der Router (CPE) beim Teilnehmer manuell konfiguriert

werden. Bei nur einem Prefix pro Anschluß (statisch oder dynamisch) kann die Konfiguration des CPE komplett automatisch beim Verbindungsaufbau erfolgen.

**3. Die Vorteile sowohl fester, identifizierbarer IP-Adressen als auch dynamischer, komplett anonymisierter IP-Adressen sind bekannt. Ist es denkbar, dass diese Vorteile, unter Ausschluss der Nachteile, gleichzeitig in der selben kleinen Software (Browser) nutzbar sind?**

Die Verwendung fester und dynamischer IP-Adressen ist völlig unterschiedlich – für Server- und für Client-Dienste. Ein Browser ist eine typische Client-Anwendung, insofern ist die Verwendung von statischen Adressen dort nicht vorteilig. In unterschiedlichen Programmen auf dem selben Rechner ist das natürlich wünschenswert.

Geht man von einem Endkundenanschluss mit gleichzeitiger Verwendung eines dynamisch und eines statisch zugewiesenen Prefix aus, ist die gleichzeitige Verwendung je nach Zweck beim heutigen Stand zwar möglich, aber nicht “bequem”, d.h. es muss im System manuell konfiguriert werden, welches der vom Router übermittelten Prefixe für welchen Typ Verbindungen bevorzugt werden soll.

Um dennoch direkt die Frage zu beantworten: es spricht prinzipiell nichts dagegen, per Browser-Auswahlmenü zwischen “Surfen mit statischer IPv6-Adresse” und “Surfen mit dynamischer IPv6-Adresse” zu wählen. Die grundlegende Funktionalität “IPv6-Adresse für eine abgehende Verbindung festlegen” unterstützen alle gängigen Betriebssysteme – die Schwierigkeit liegt also vor Allem darin, zu erkennen, welches der vorhandenen Prefixe statisch und welches dynamisch ist.