Using Cryptographically Generated Adresses for securing Mobile IPv6

Seminarvortrag

Olaf Christ

Fakultät Technik und Informatik
Hochschule für Angewandte Wissenschaften Hamburg

01.12.2006

Übersicht

Warum Cryptographically Generated Addresses?

- Unkomplizierte Authentifizierung
- Sicherung der Nachrichten
- Handover-Latenz bei einfachem Mobile IPv6 meist zu groß für Echtzeitanforderungen
- Testplattform für CGAs: FTS

IPv6 Adressen

- Länge: 128 Bit
- vordere 64 Bit: Prefix
- hintere 64 Bit: Interface Identifier
- Kein CIDR (Classless Interdomain Routing)
- Stateful (DHCP) oder Stateless Adresskonfiguration (RA)
- DAD (Duplicate Address Detection)

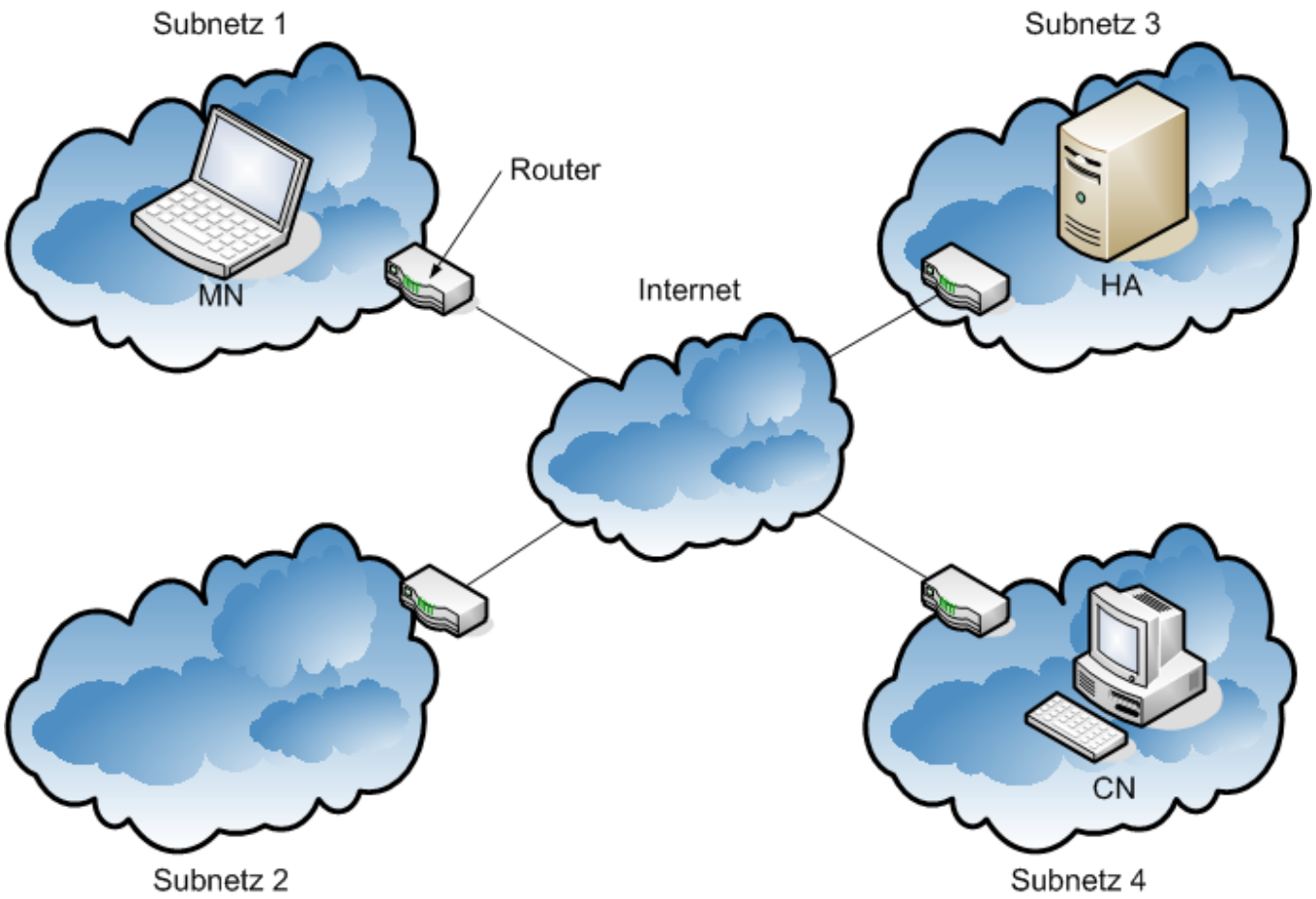
Beispiel

$$\underbrace{1:2:3:4}_{\text{Prefix}}:\underbrace{x:x:x:x}_{\text{Interface Identifier}}$$

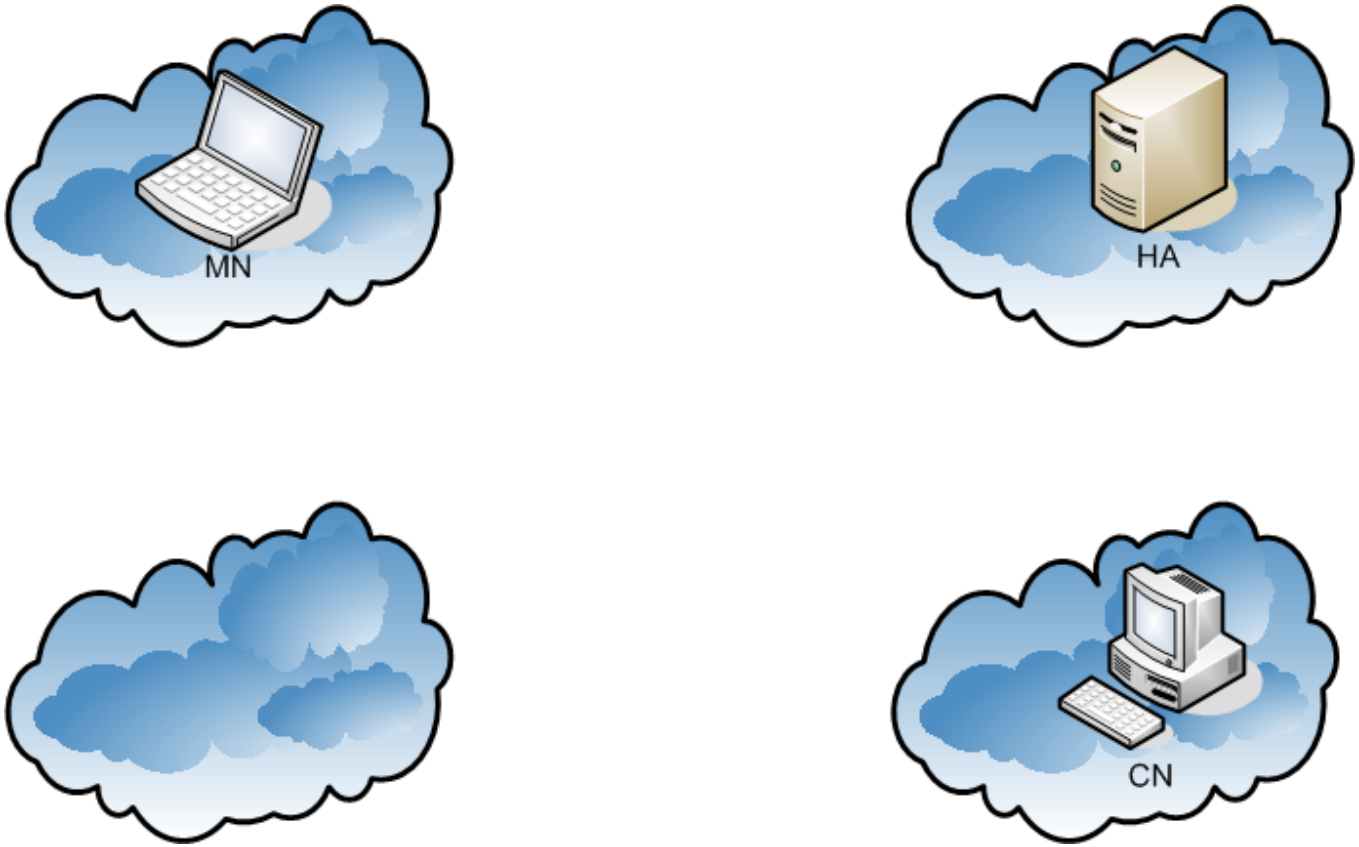
Warum Mobile IPv6?

- Mobile Node ist immer über gleiche IP-Adresse erreichbar
- TCP-Verbindungen bleiben trotz Adress-Wechsel bestehen

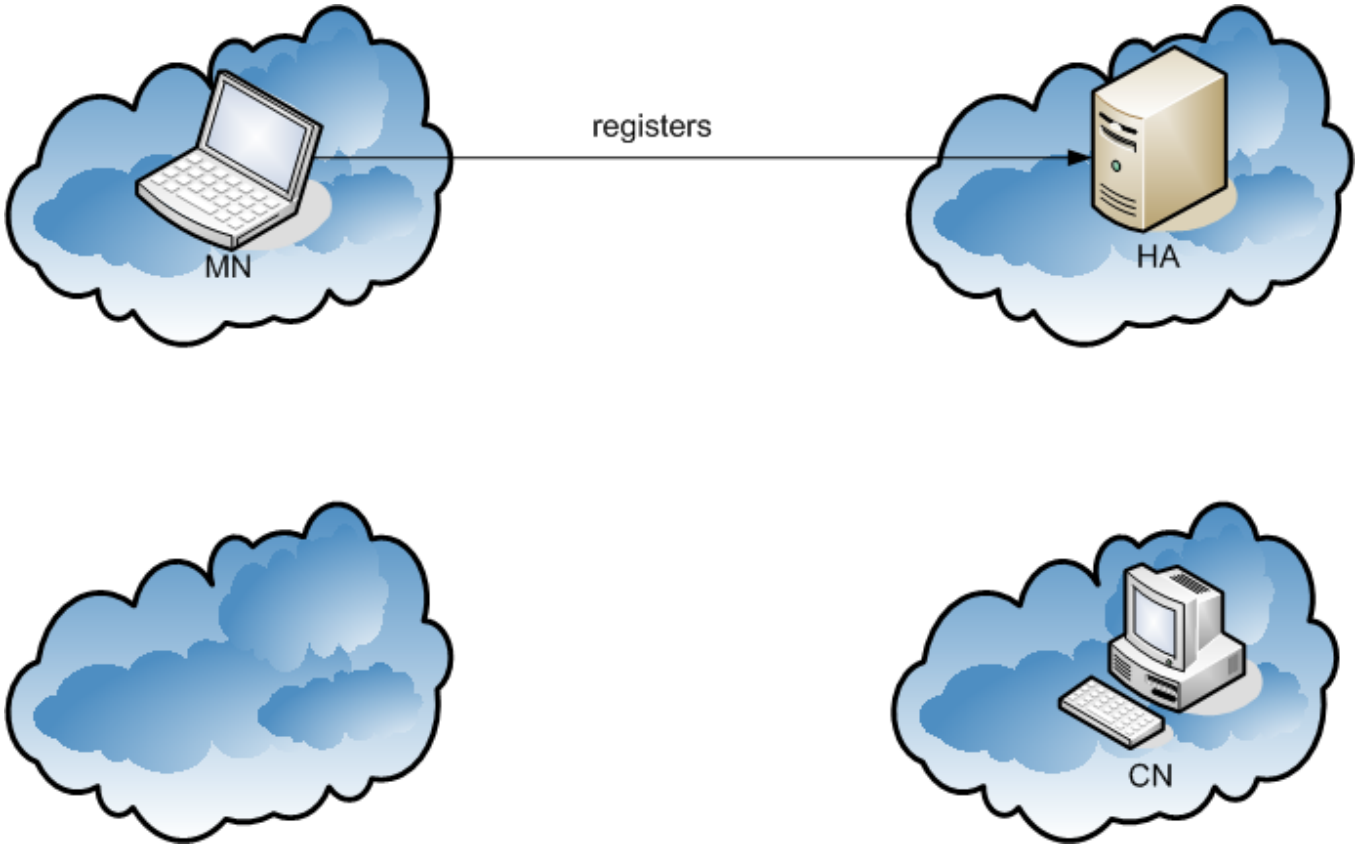
Beispiel-Netzwerk



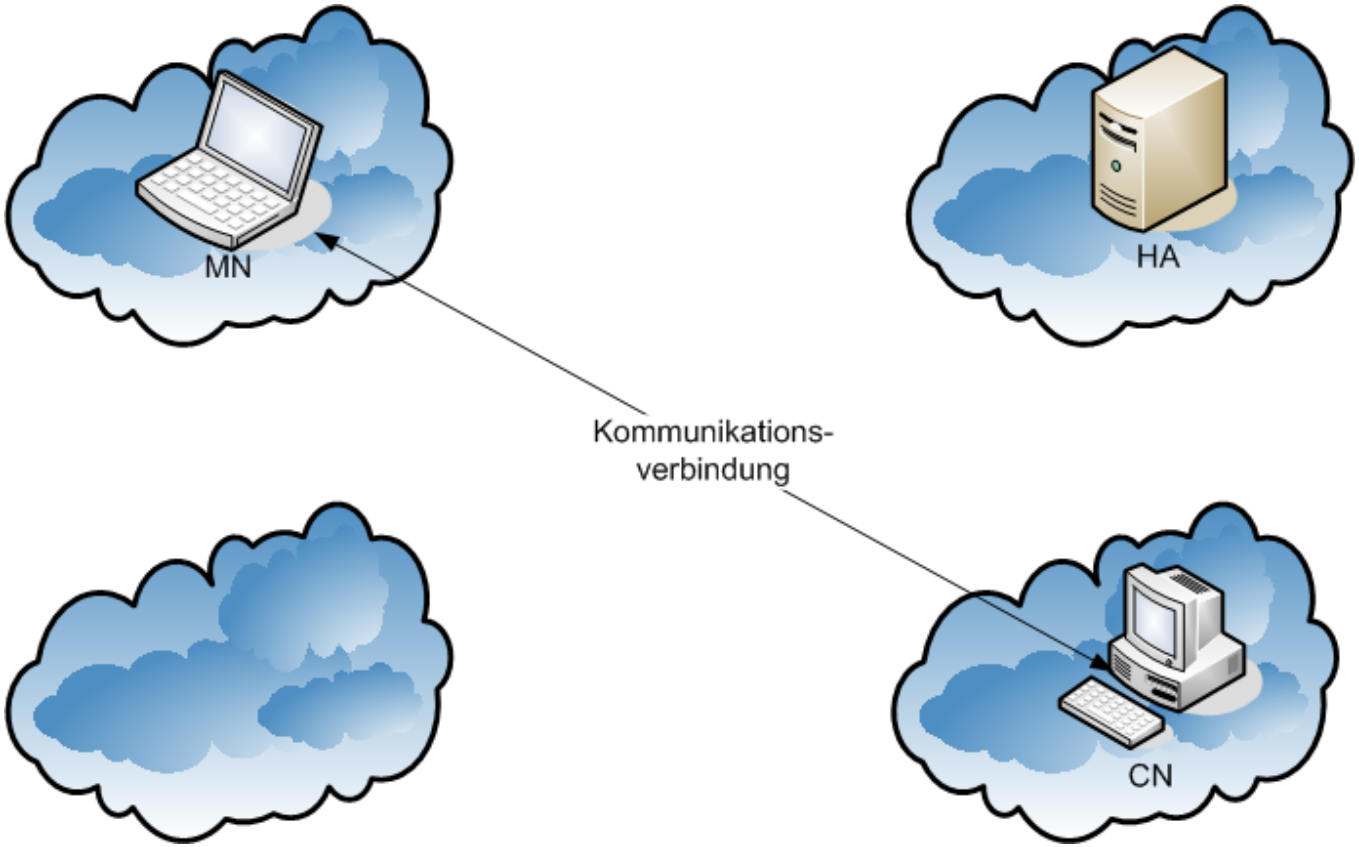
Beispiel-Netzwerk



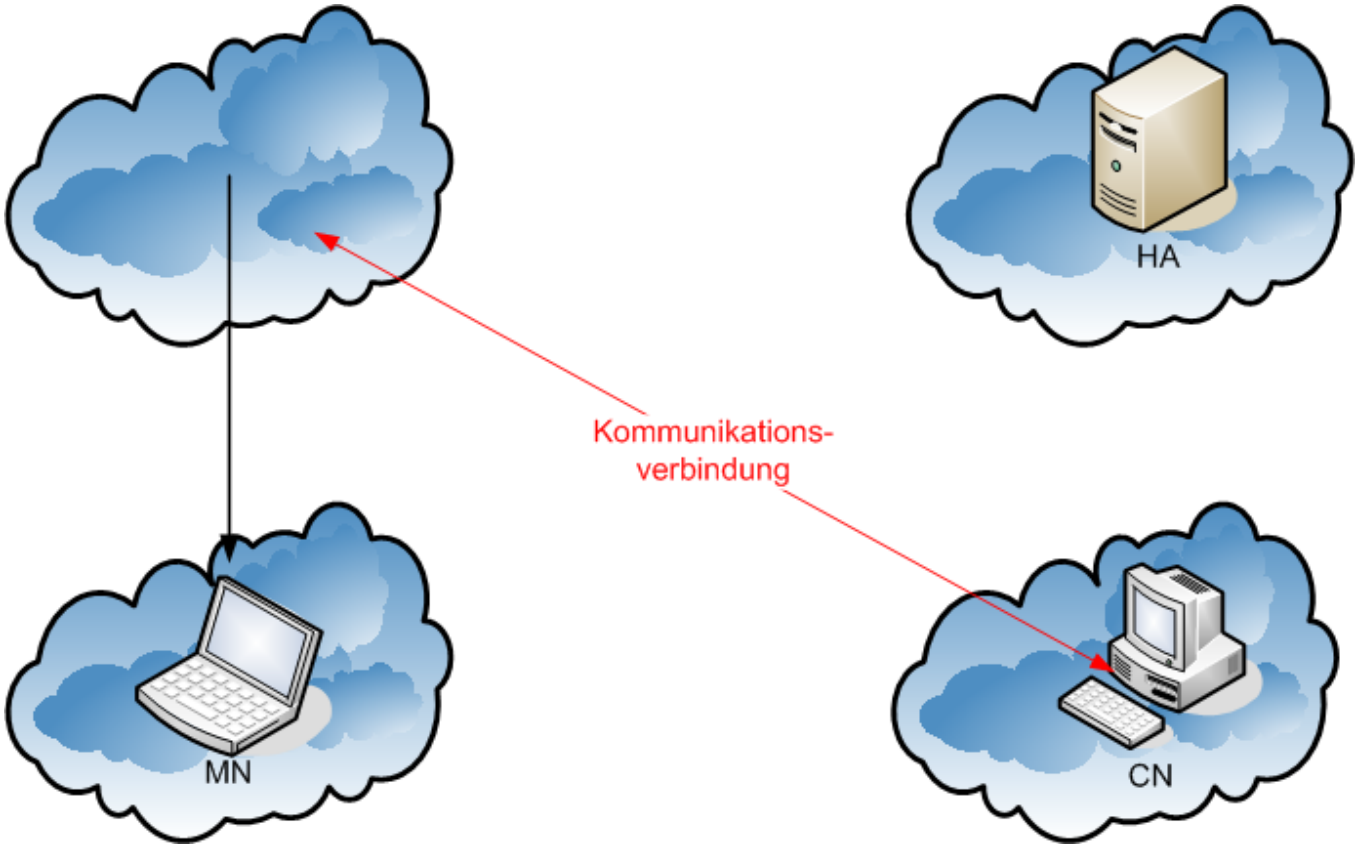
Mobile Node registers



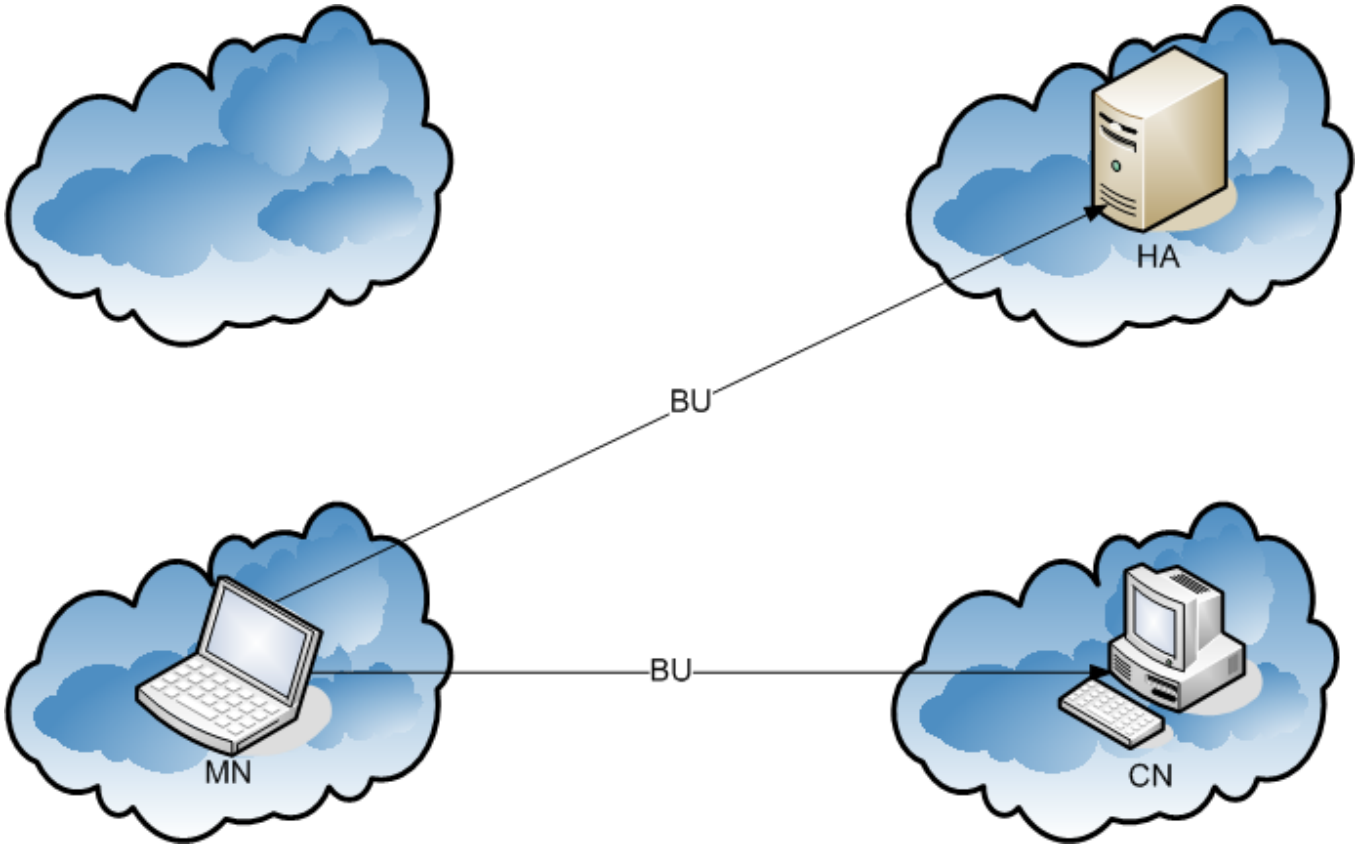
Bestehende Kommunikation



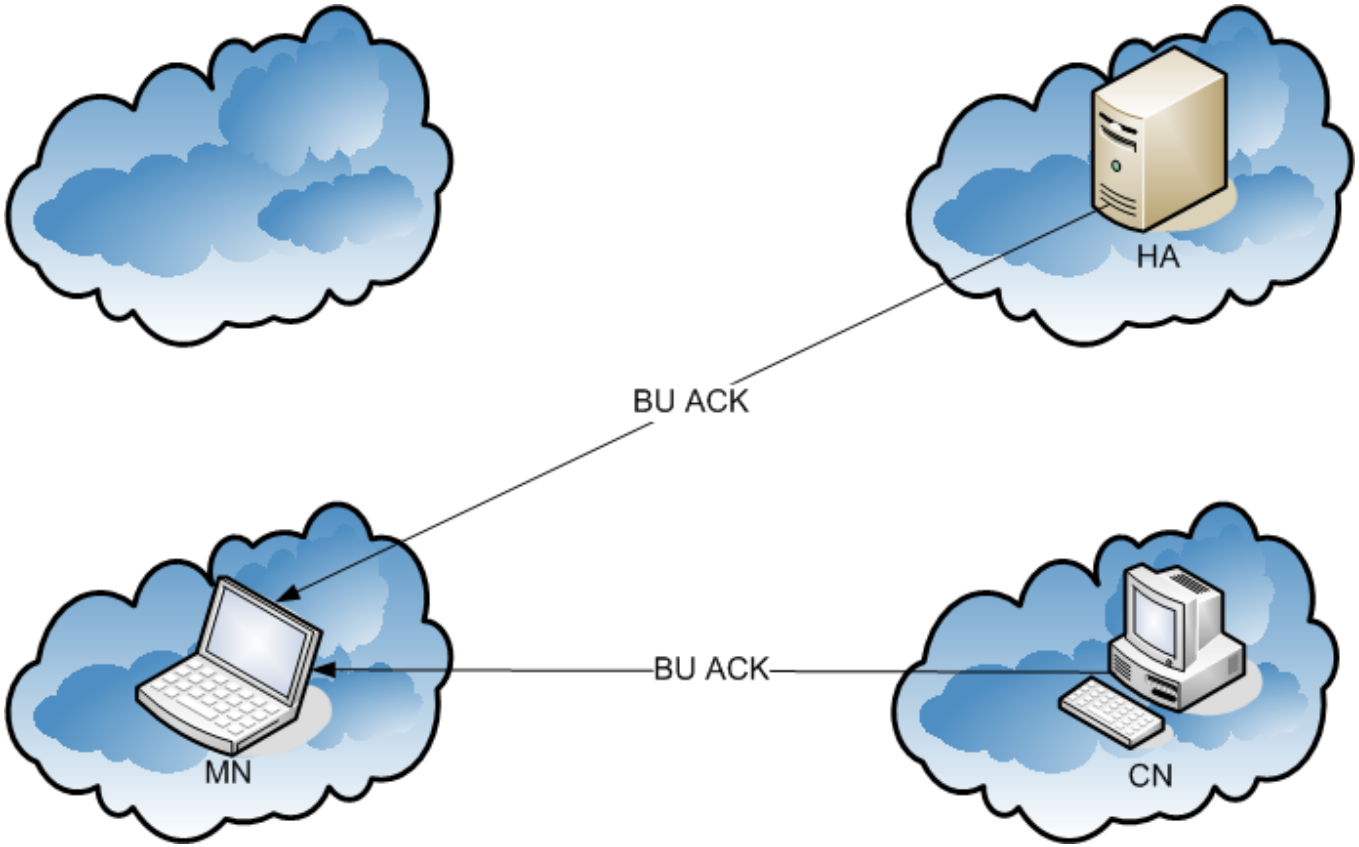
Mobile Node bewegt sich in neues Subnetz



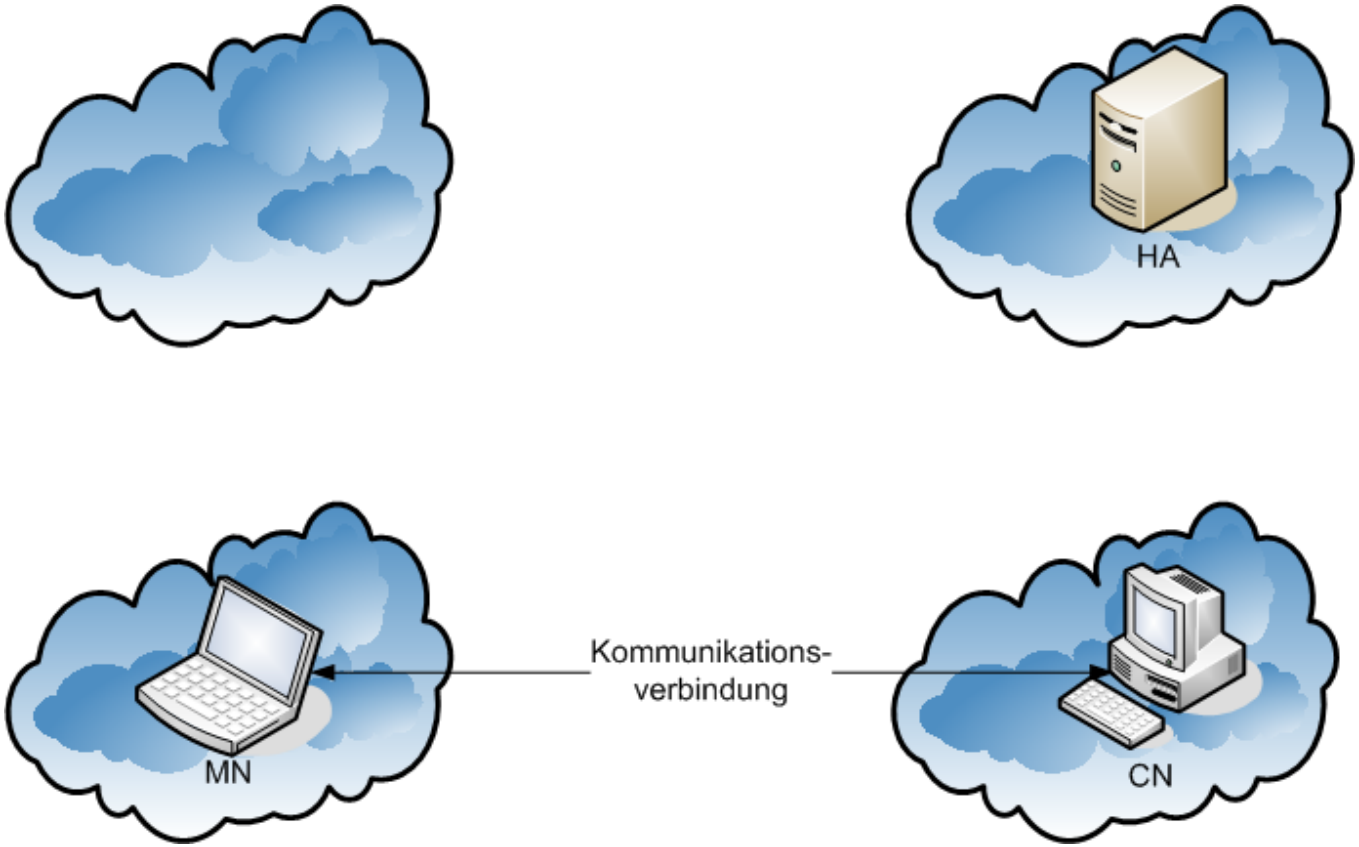
Binding Updates



Binding Update Acknowledges

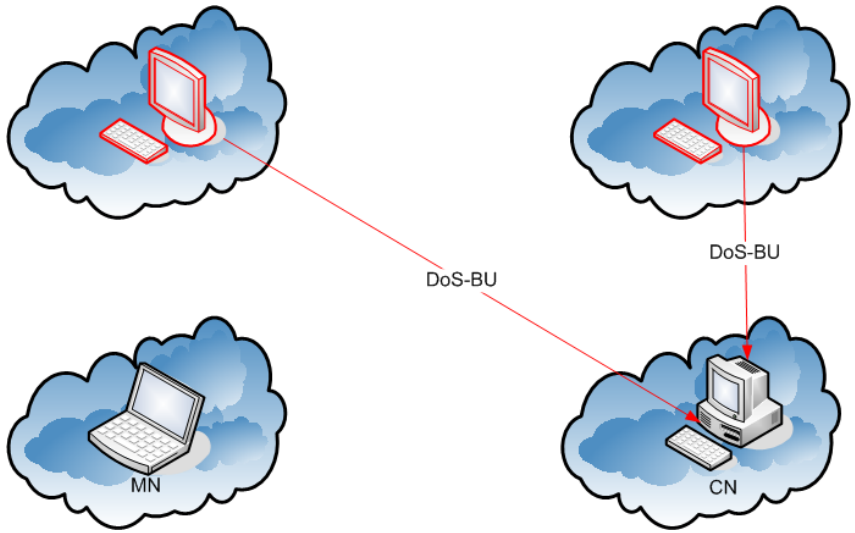


Binding Update Acknowledges

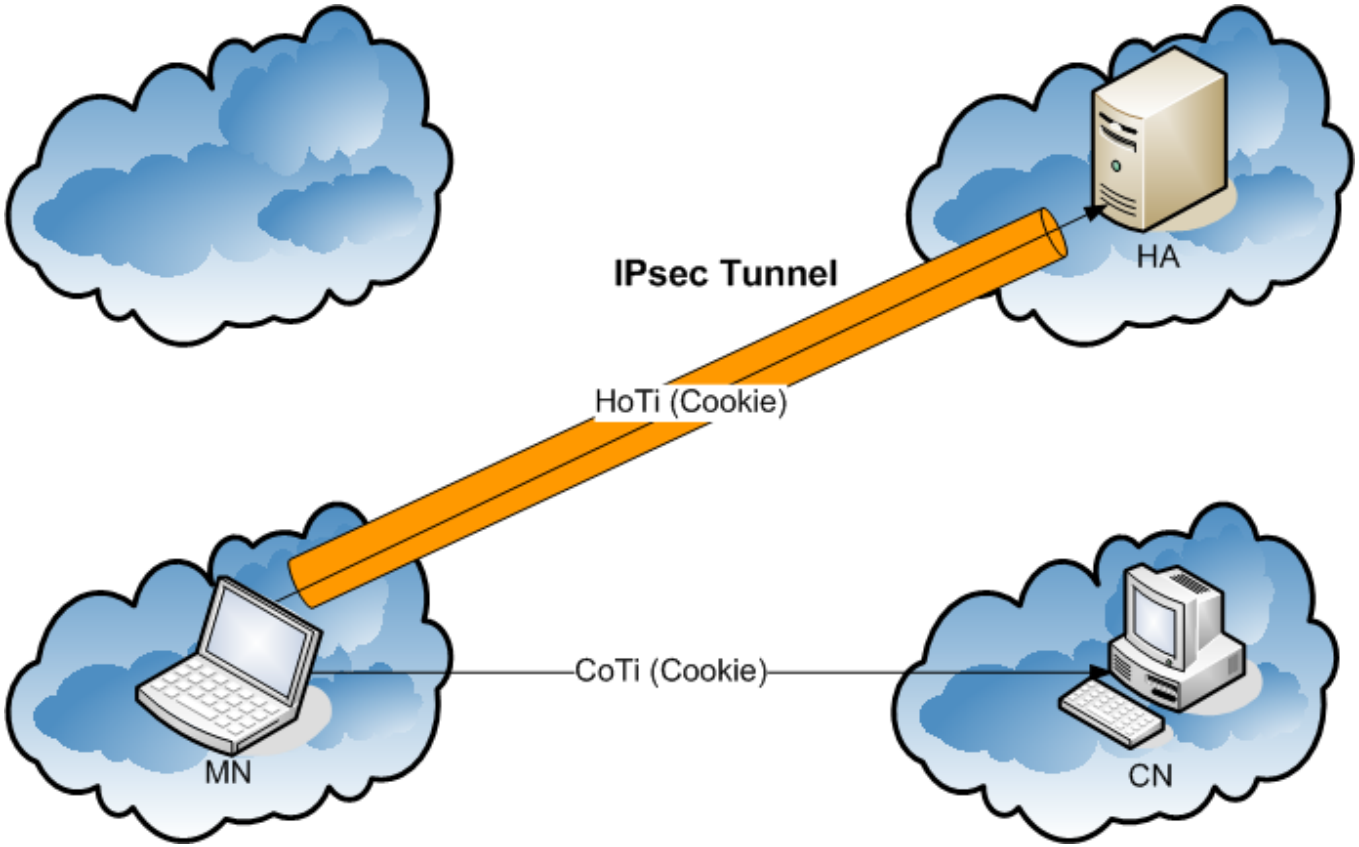


Denial of Service

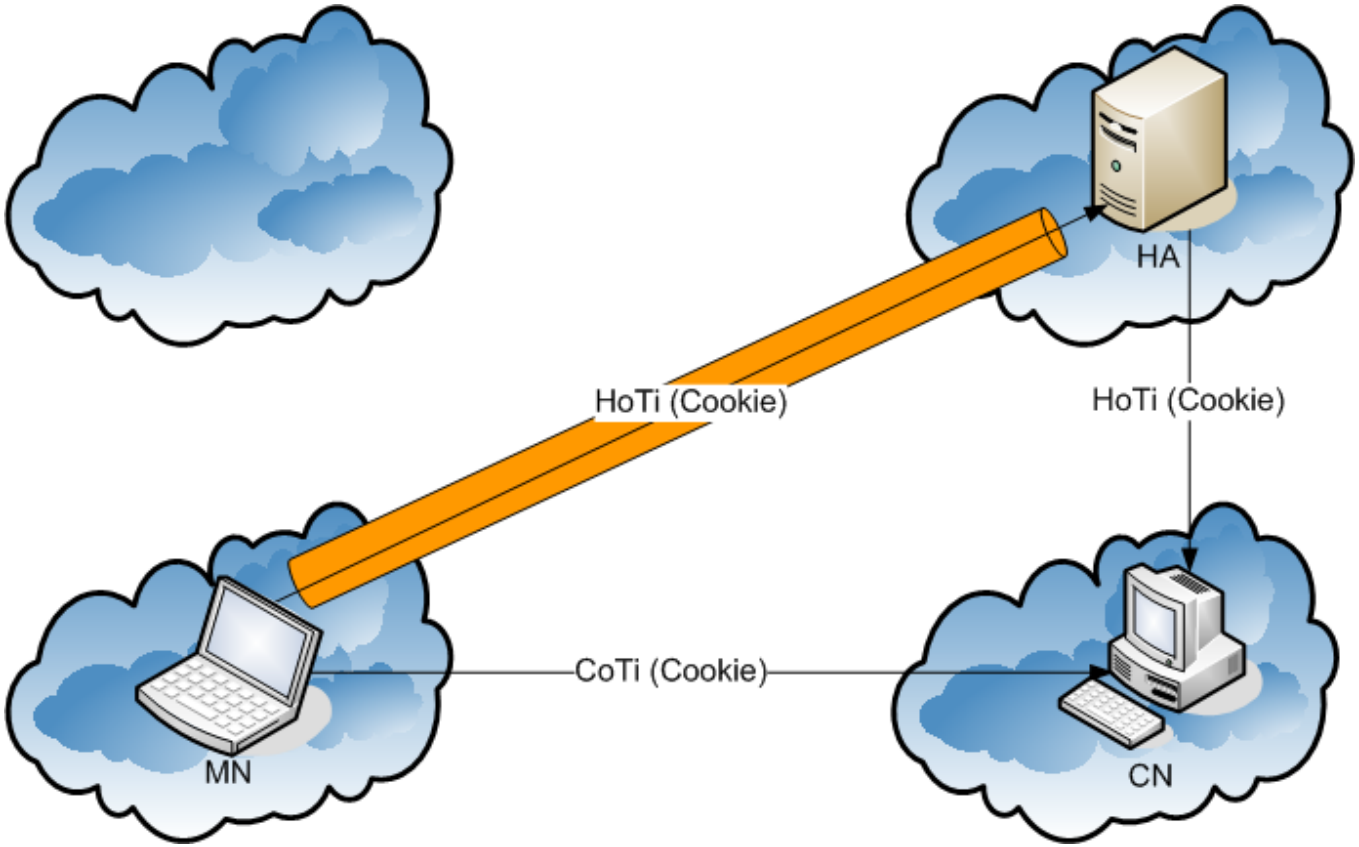
- BUs sind weder verschlüsselt noch authentifiziert
- BUs können von jedem Rechner gesendet werden
- Gefahr einer Denial of Service-Attacke



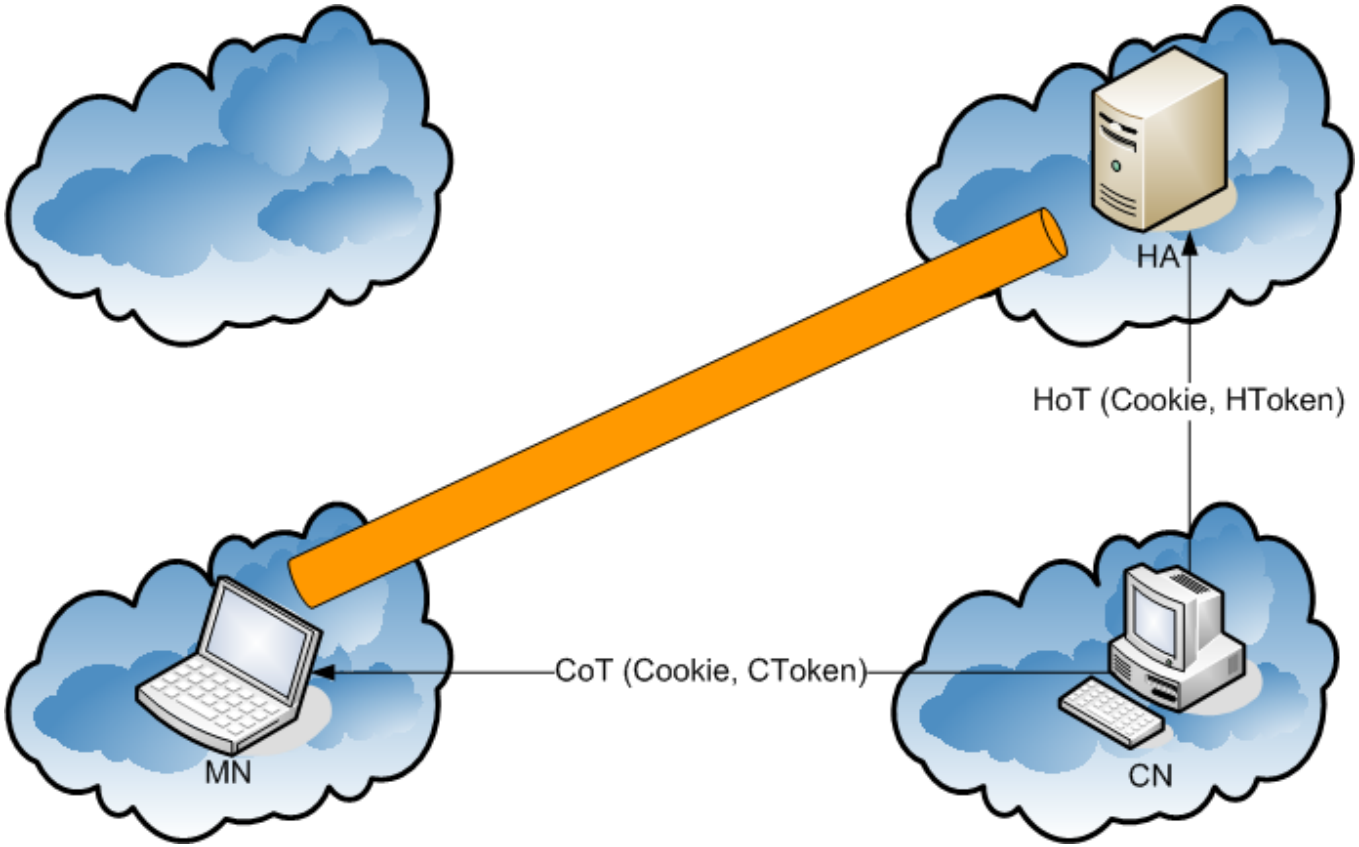
Return Routability Procedure



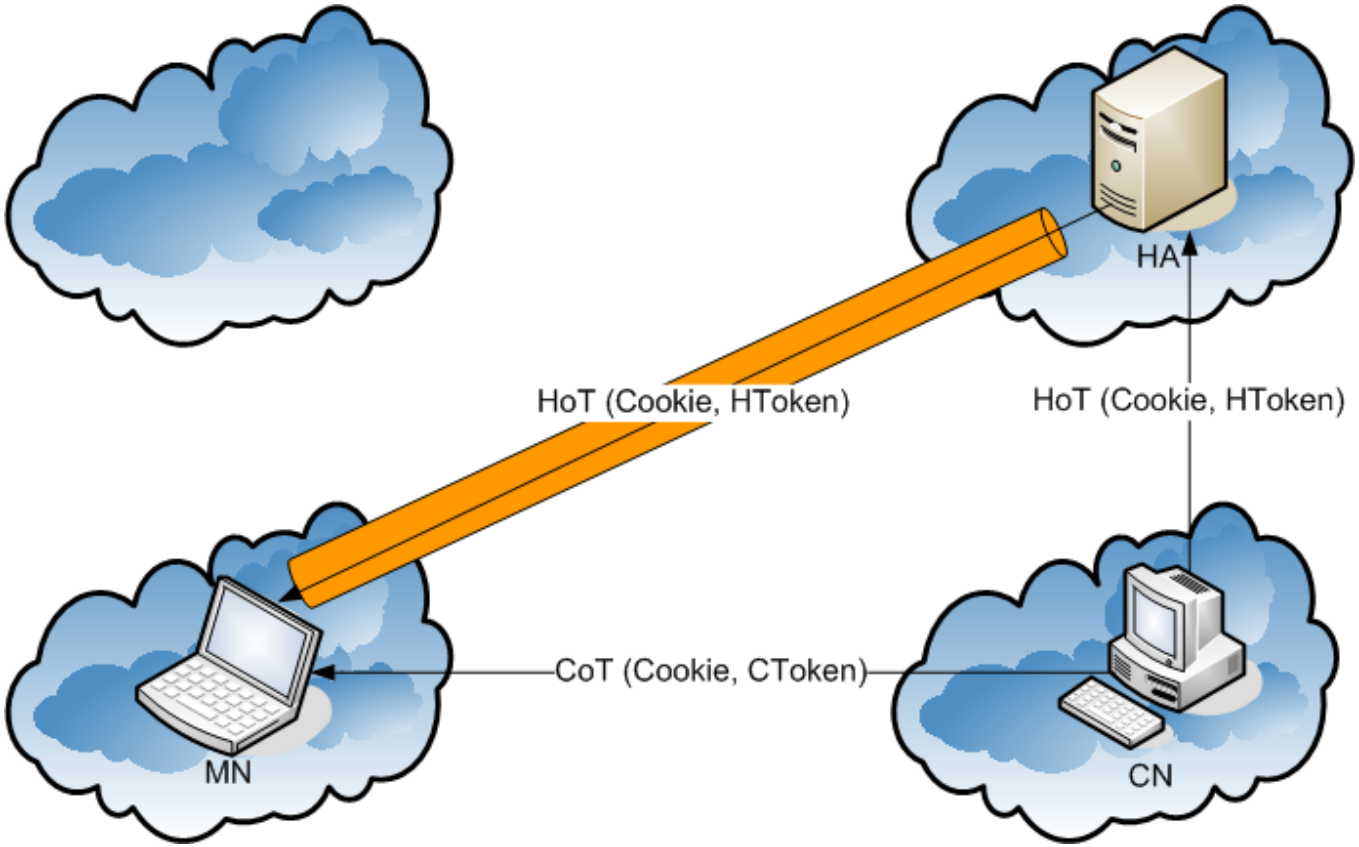
Return Routability Procedure



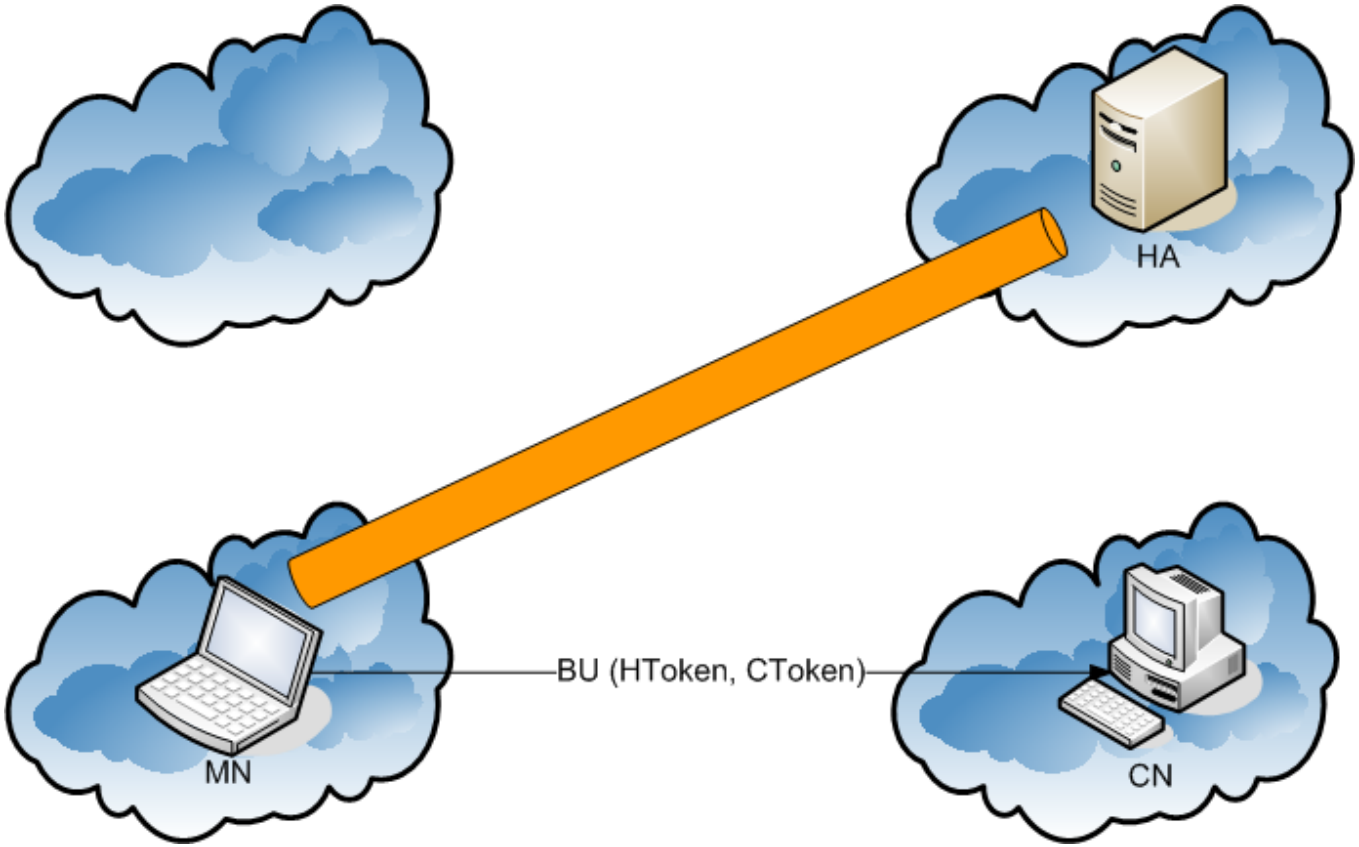
Return Routability Procedure



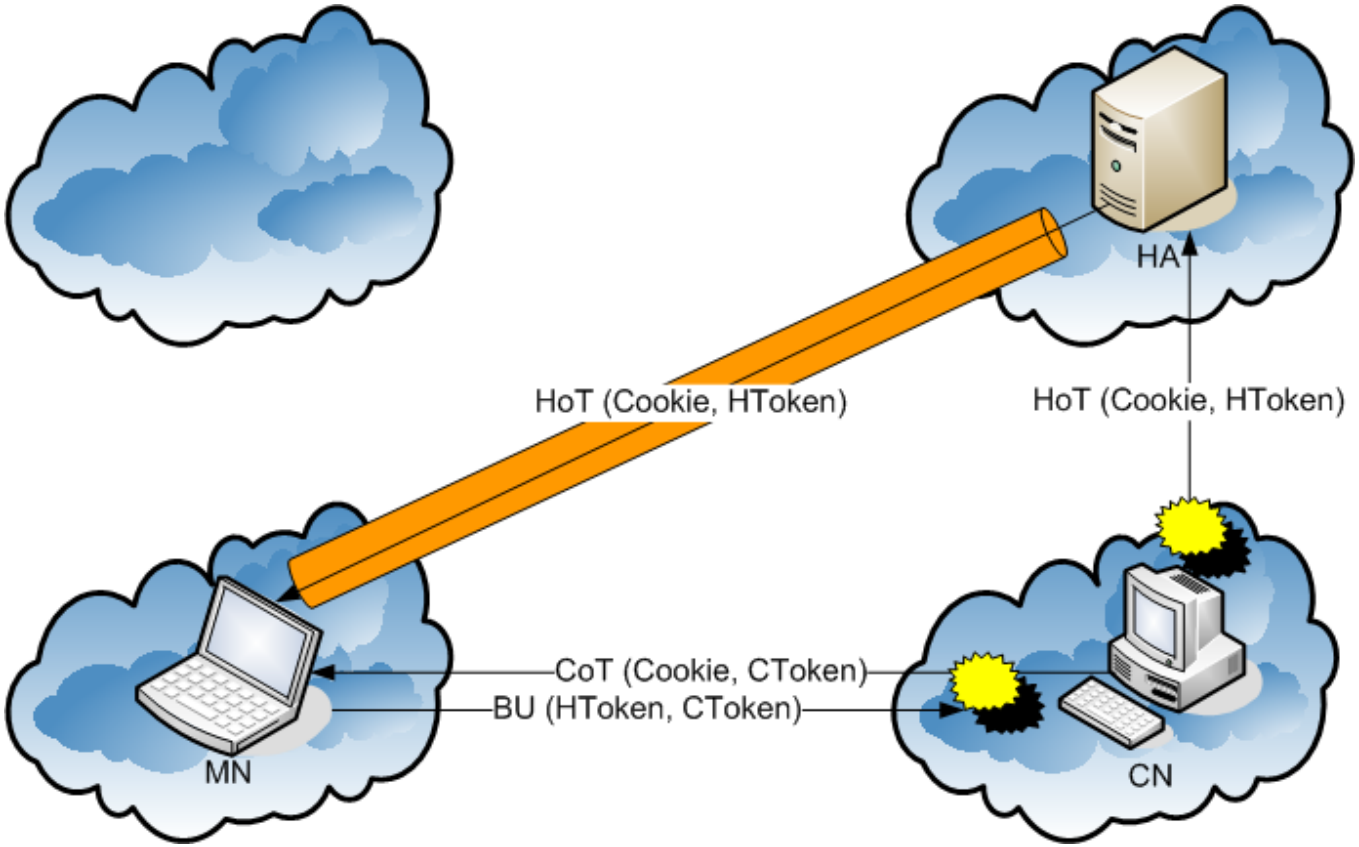
Return Routability Procedure



Return Routability Procedure



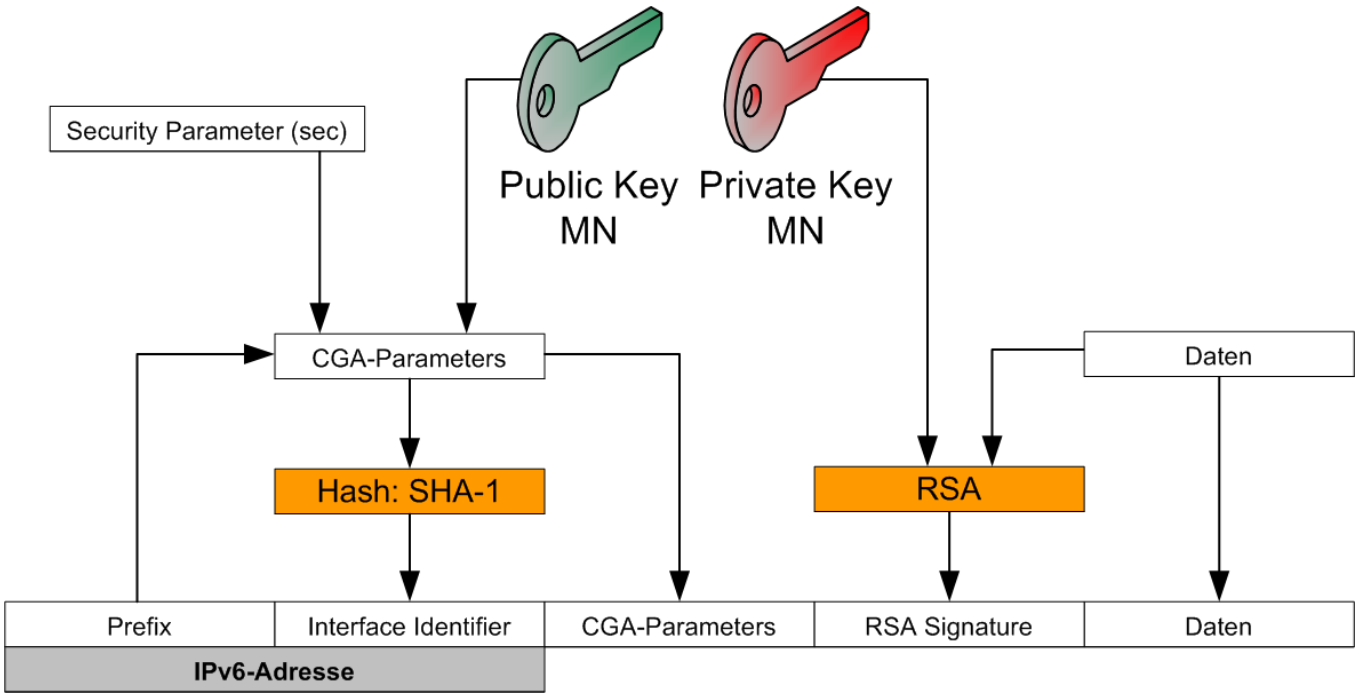
Man in the Middle



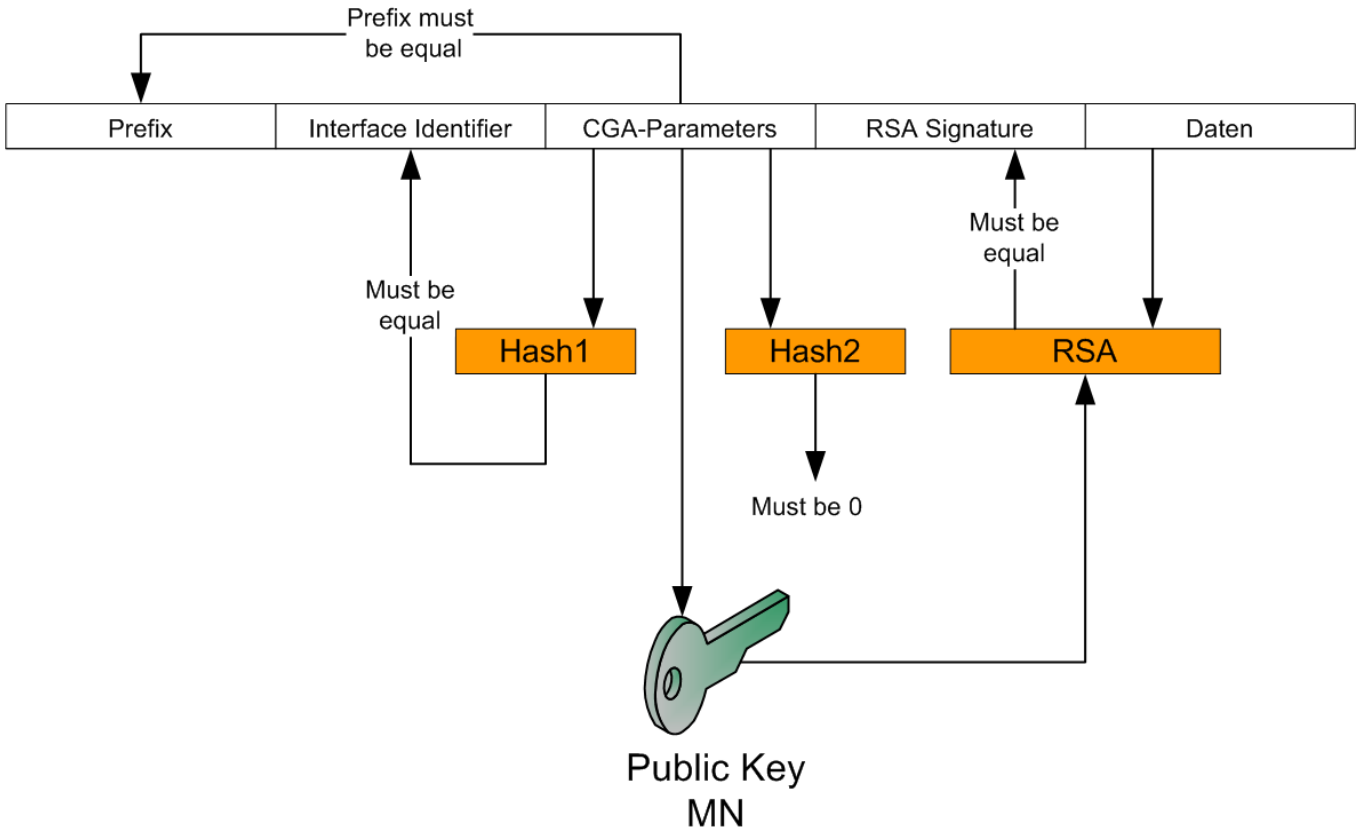
Cryptographically Generated Addresses

- MN muß beweisen, dass er legitimer Besitzer der HoA ist.
- Aufsetzen einer PKI (Public Key Infrastructure)
  - Kostspielig
  - Administrationsaufwand
- Idee der CGAs
  - Interface Identifier ist kryptographisches Merkmal
- Paketauthentifizierung
  - ohne Shared Secred
  - ohne vorherigen Public Key-Austausch

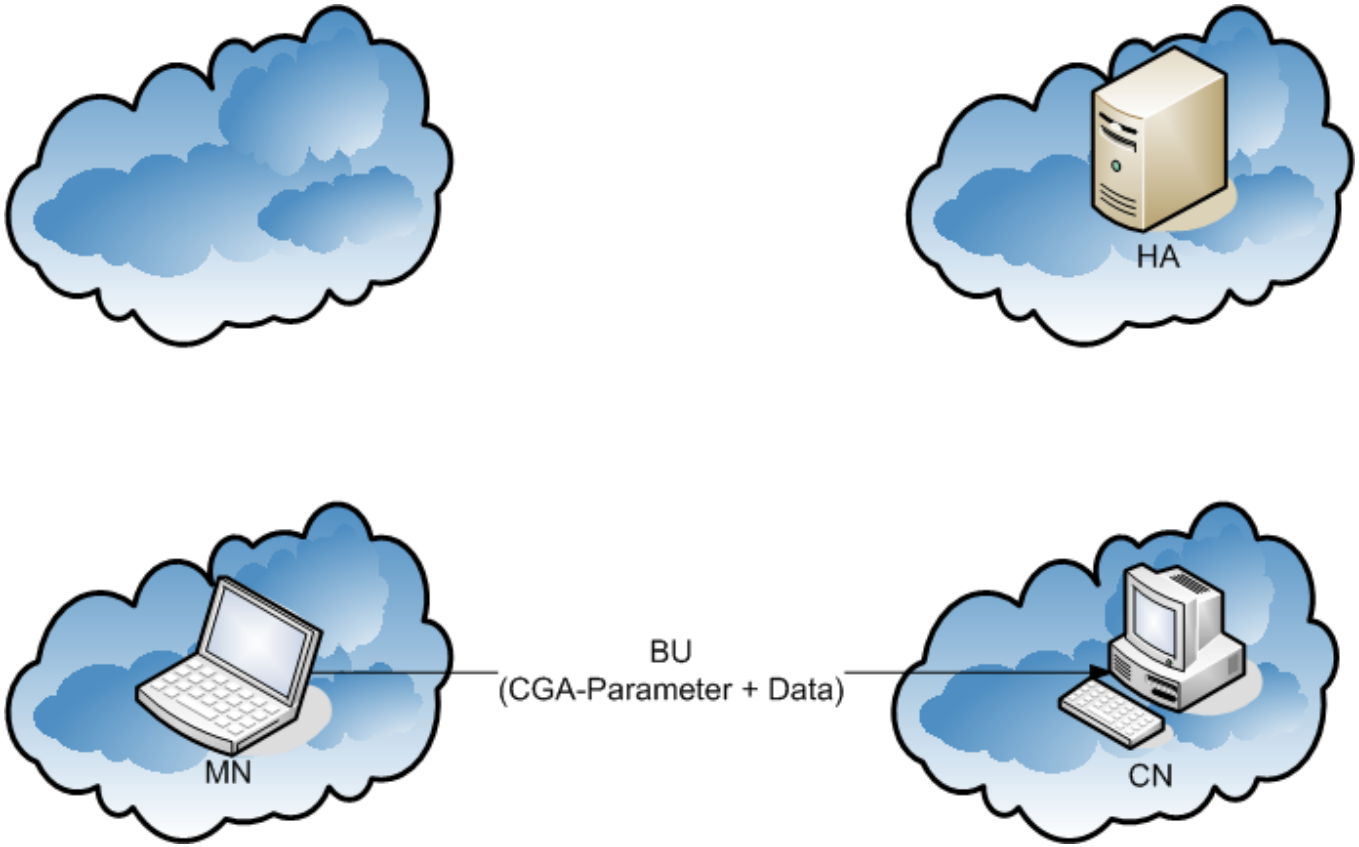
CGA: Encapsulation



CGA: Decapsulation

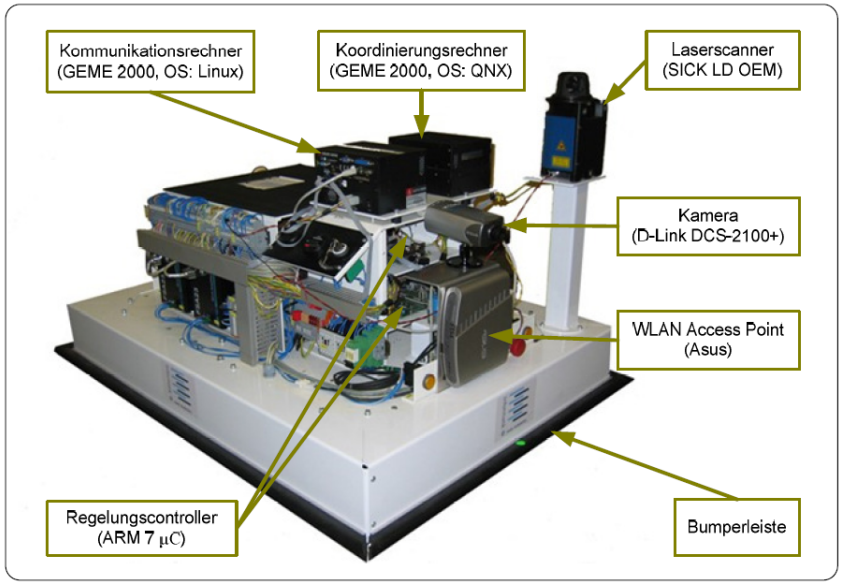


CGA-Authentifiziertes Binding Update



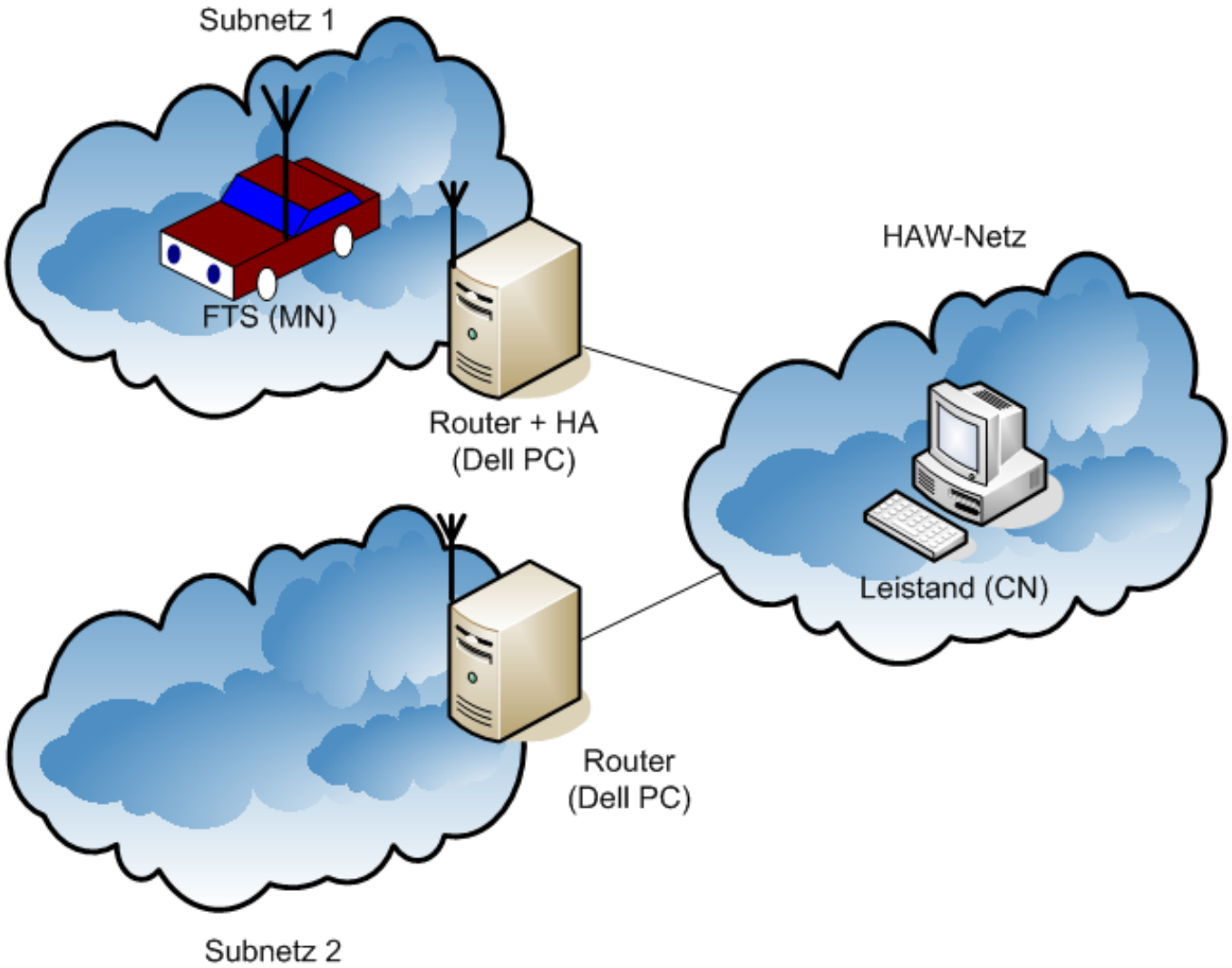
CGA-Authentifiziertes Binding Update

- Handover-Kommunikation wesentlich verringert
  - 1 Paket anstatt von 7 Paketen
- Notwendig für Echtzeitanwendungen, z.B.
  - VoIP
  - Ferngelenkte Transportsysteme



Faust (aus Masterarbeit 2006, A.Pröhl)

CGA-Authentifiziertes Binding Update



Zusammenfassung

- Vermeidung von Denial of Service- und Man in the Middle-Attacken
- Deutliche Reduktion der Handover-Kommunikation
- Nachteil
  - Generierung von CGAs ist rechenaufwendig
  - Sicherheitsstufe einstellbar durch Security Parameter *sec*

Perspektive für die Masterarbeit

- Implementation CGAs und OMIPv6
- Anwendung von CGA auf mobiles Source Specific Multicast
  - Source mobility
  - Sender muss sich ohne Kenntnis der Empfänger authentifizieren

Literatur

T. Aura (Microsoft Research)
Cryptographically Generated Addresses (CGA)
Network Working Group: RFC 3972, 2005
http://www.ietf.org/rfc/rfc3972.txt

J. Arkko (Ericsson Research),
C. Vogt (TH Karlsruhe),
W. Haddad (Ericsson Research)
Applying Cryptographically Generated Addresses and Credit-Based Authorization to Mobile IPv6
Network Working Group: Internet-Draft, 2006
http://www.ietf.org/internet-drafts/draft-ietf-mipshop-cga-cba-01.txt