SECURE MOBILE IPv6 REQUIREMENTS & SOLUTIONS

Deploying IPv6 Networks, Paris

Friday December 5th 2003

Thomas Scheffler
T-Systems - Systems Integration

T-Systems

Agenda

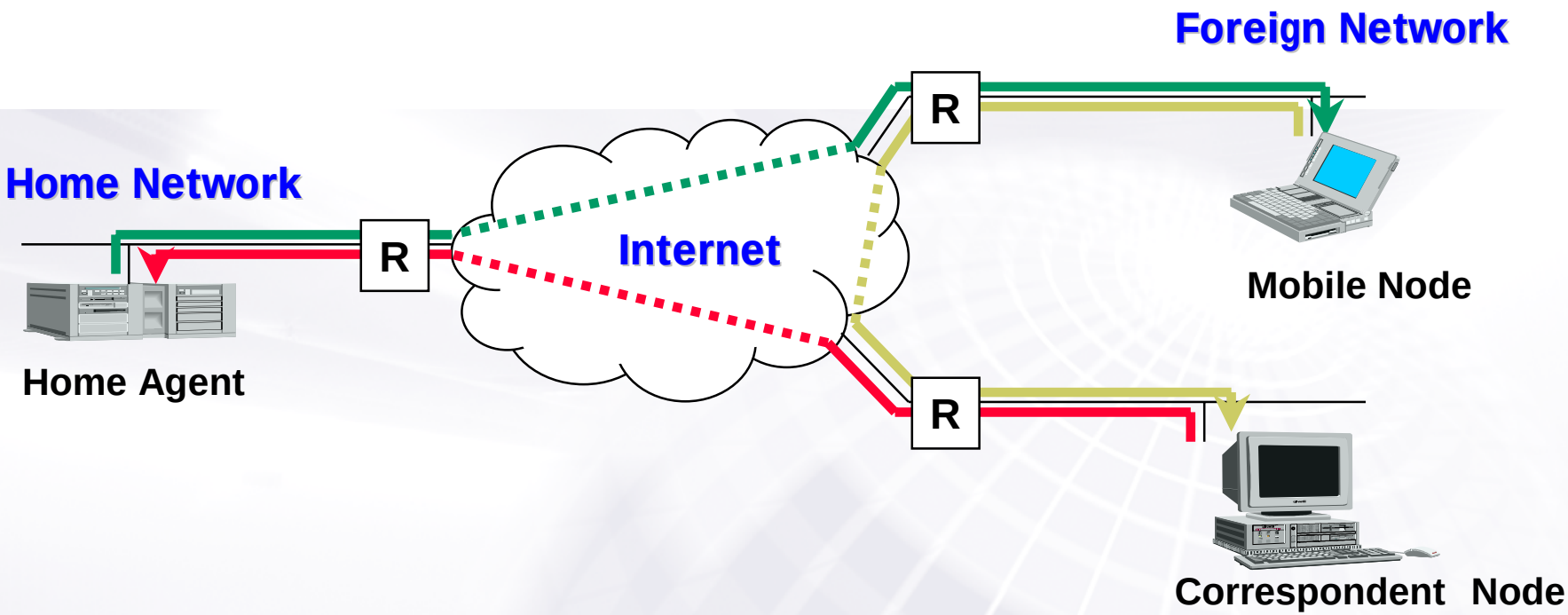
- Requirements for a Mobility Protocol
- Mobile IPv6 Basics
- Security Analysis of Mobile IPv6
- Status of Implementations
- Proposed Security Architecture for ‚Closed Systems‘
- Requirements revisited
- Work ahead – The SEINIT Project

Mobile IPv6 Security Architectures
Requirements

Requirements for a Mobile Protocol:

- Small Footprint (on the wire, implementation wise)
- Fast Handover (Minimum Delay, Packet Loss during Handover)
- Secure Operation
- Privacy Issues for the foreign network and the visiting mobile node
- Coexistence of Mobile IPv6 and Transition Mechanisms

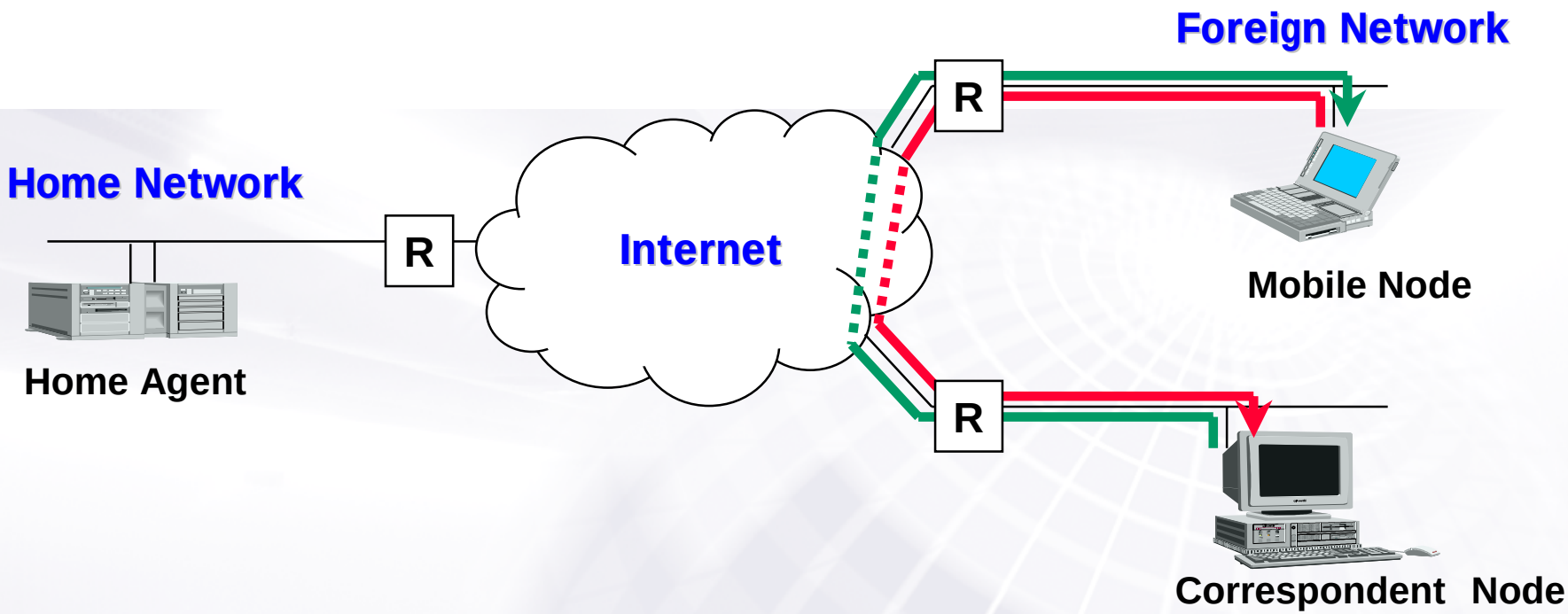
Mobile IPv6 - Basics



Procedure:

- The Mobile Node gets an IPv6 care-of address (CoA) in the Foreign Network (via auto-config)
- Registers CoA with Home Agent, who routes packets destined for the Mobile Node via a Tunnel (similar to Mobile IPv4)

Mobile IPv6 - Basics

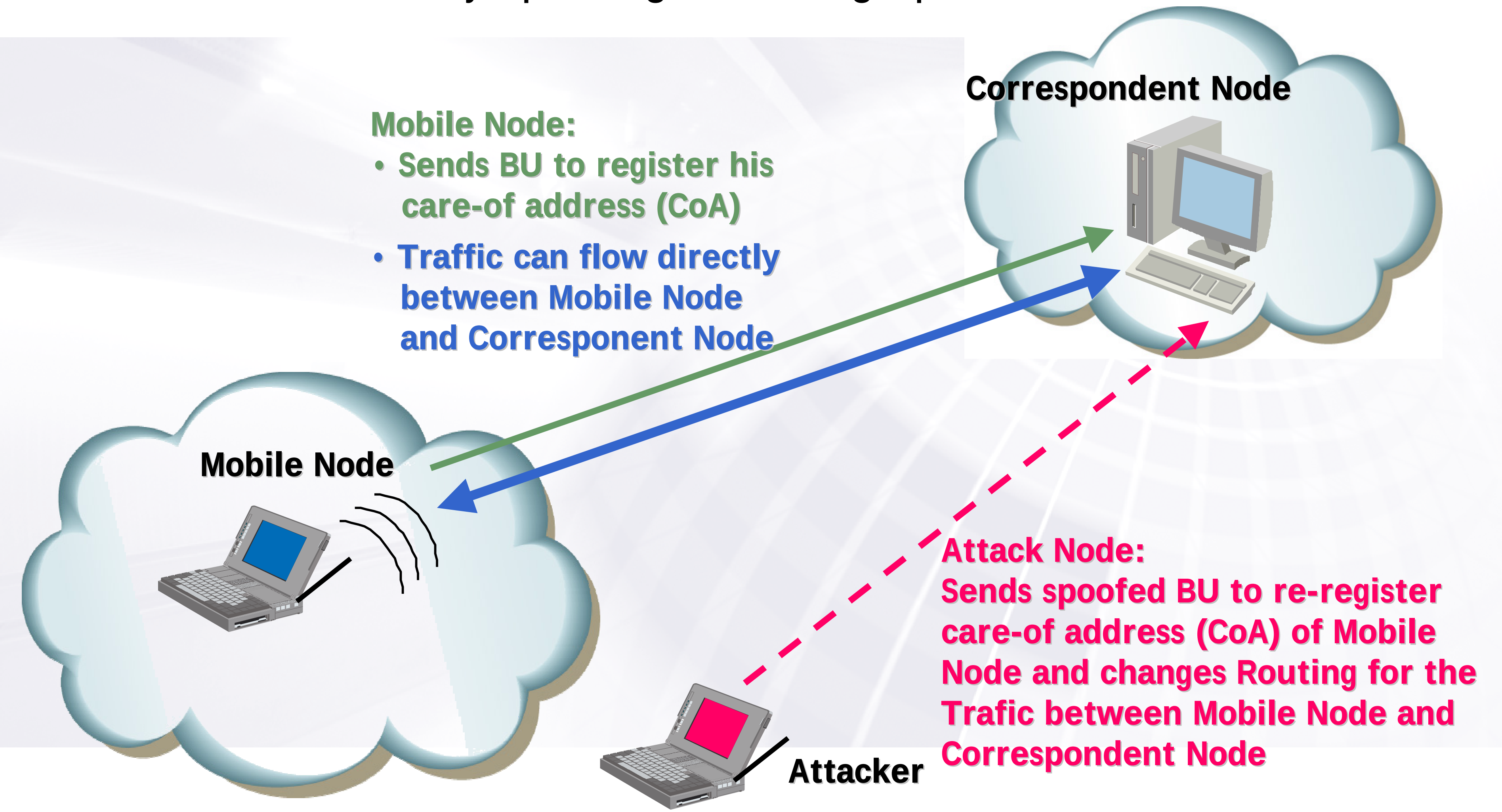


Procedure:

- Route Optimisation allows short-cut routing.
- The Mobile Node informs the Correspondent Node of its current address on the Foreign Network via a Binding Update

Security Analysis of Mobile IPv6
Possible Attack Scenario (1/2)

Mobile IPv6 Attack by Spoofing of Binding Update

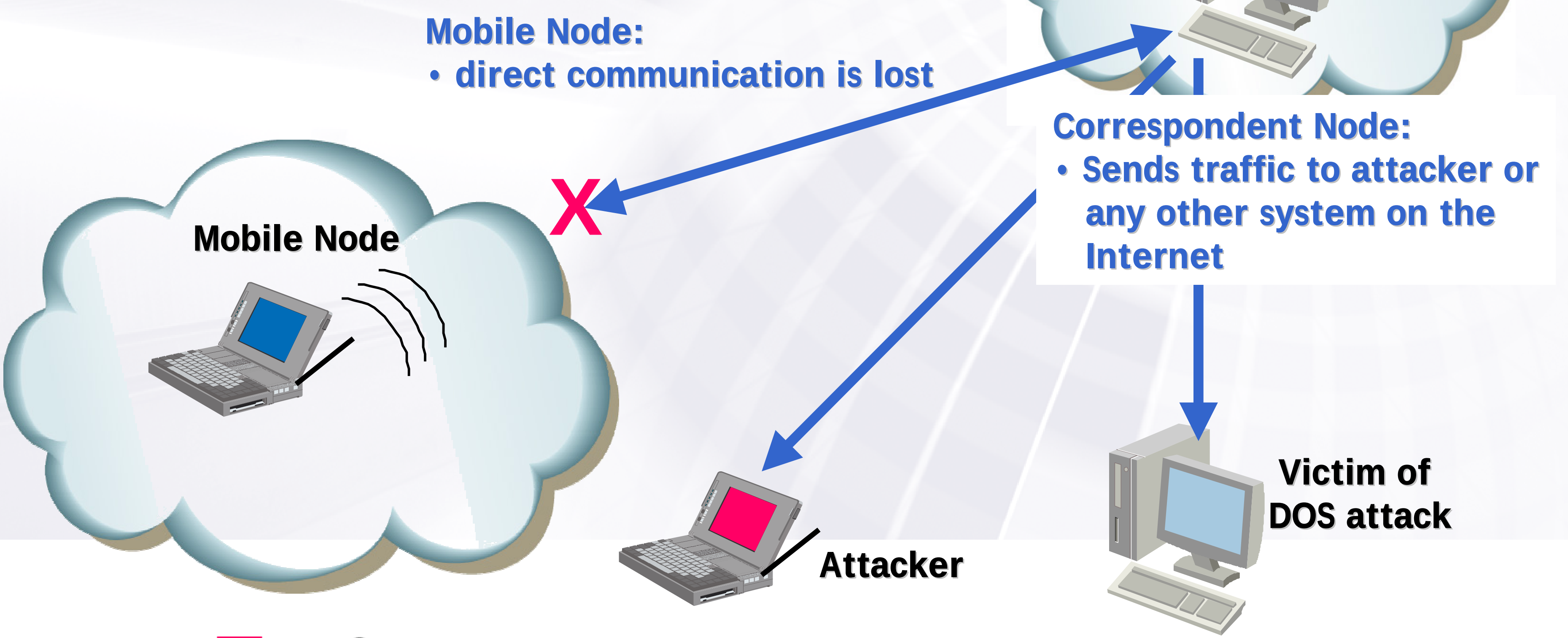


Security Analysis of Mobile IPv6
Possible Attack Scenario (2/2)

Mobile IPv6 Attack by Spoofing of Binding Update

Can be used as:

- DOS Attack (against Mobile Node and/or 3rd Party)
- Redirect Traffic
- Compromise Data



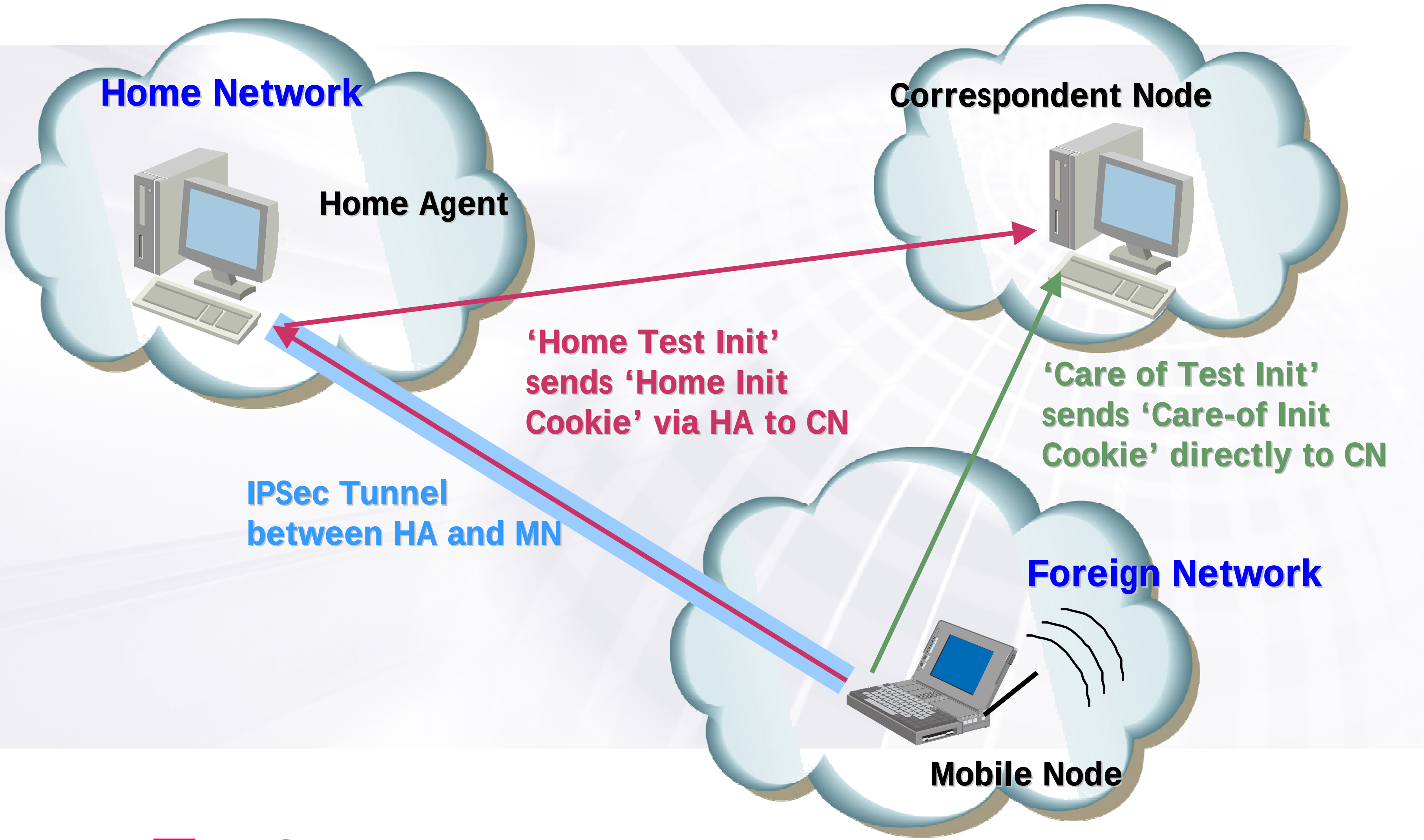
Security Analysis of Mobile IPv6
Proposed Security Measures

Standardisation Status: IETF Draft 24 (draft-ietf-mobileip-ipv6-24.txt)

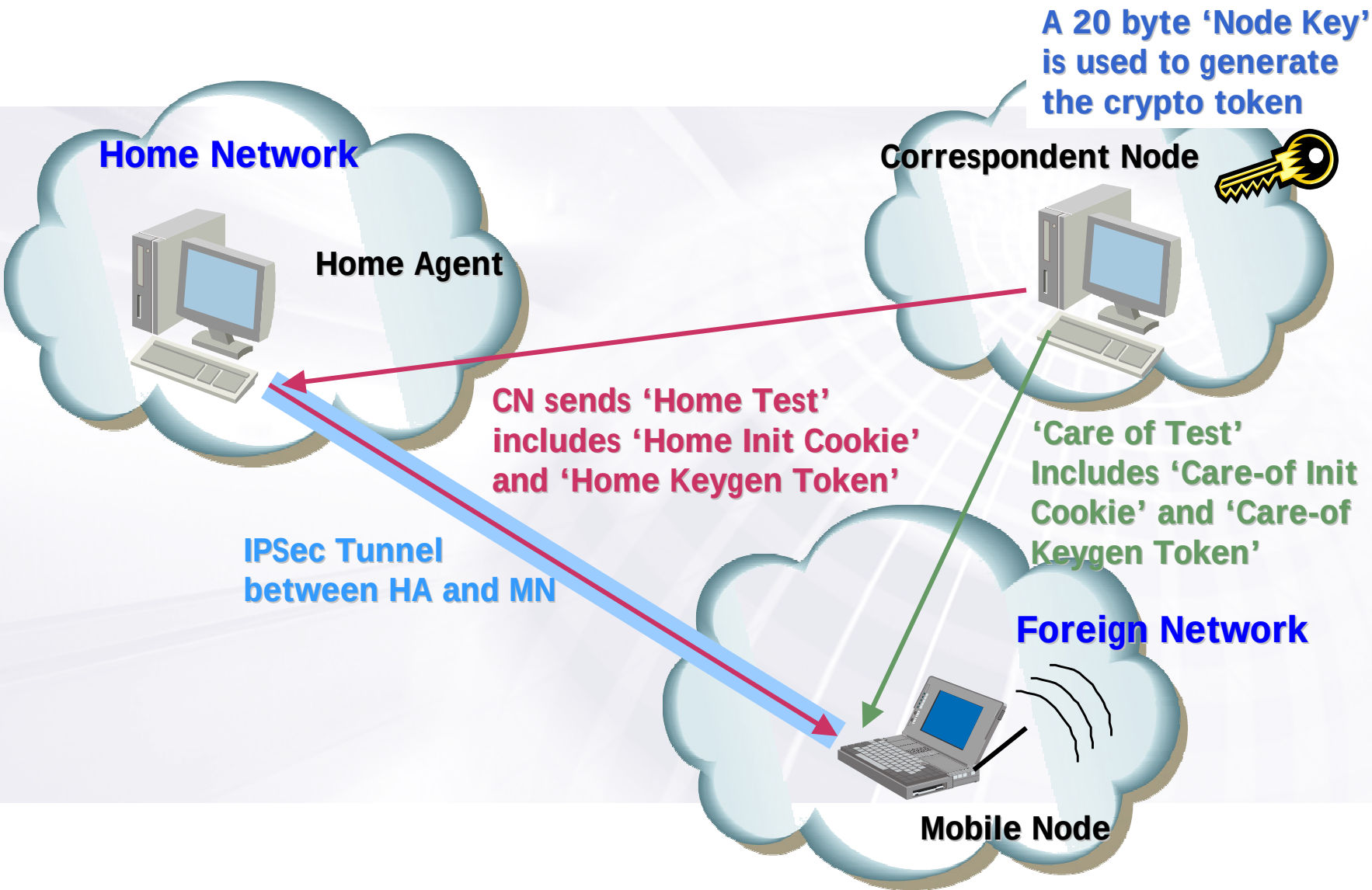
Requires the use of security mechanisms:

- Protection of Mobile IPv6 Signaling between Mobile Node and Home Agent (draft-ietf-mobileip-mipv6-ha-ipsec-06.txt)
  - Registration of Care-Of Address with Home Agent secured via IPSec
  - Return-Routablity Test for the authentication of Binding Updates send to the Correspondent Node
- Payload Packets
  - Payload packets exchanged with mobile nodes can be protected in the same way as stationary hosts can protect them

Security Analysis of Mobile IPv6
Return Routability: Step 1



Security Analysis of Mobile IPv6
Return Routability: Step 2



T-Systems

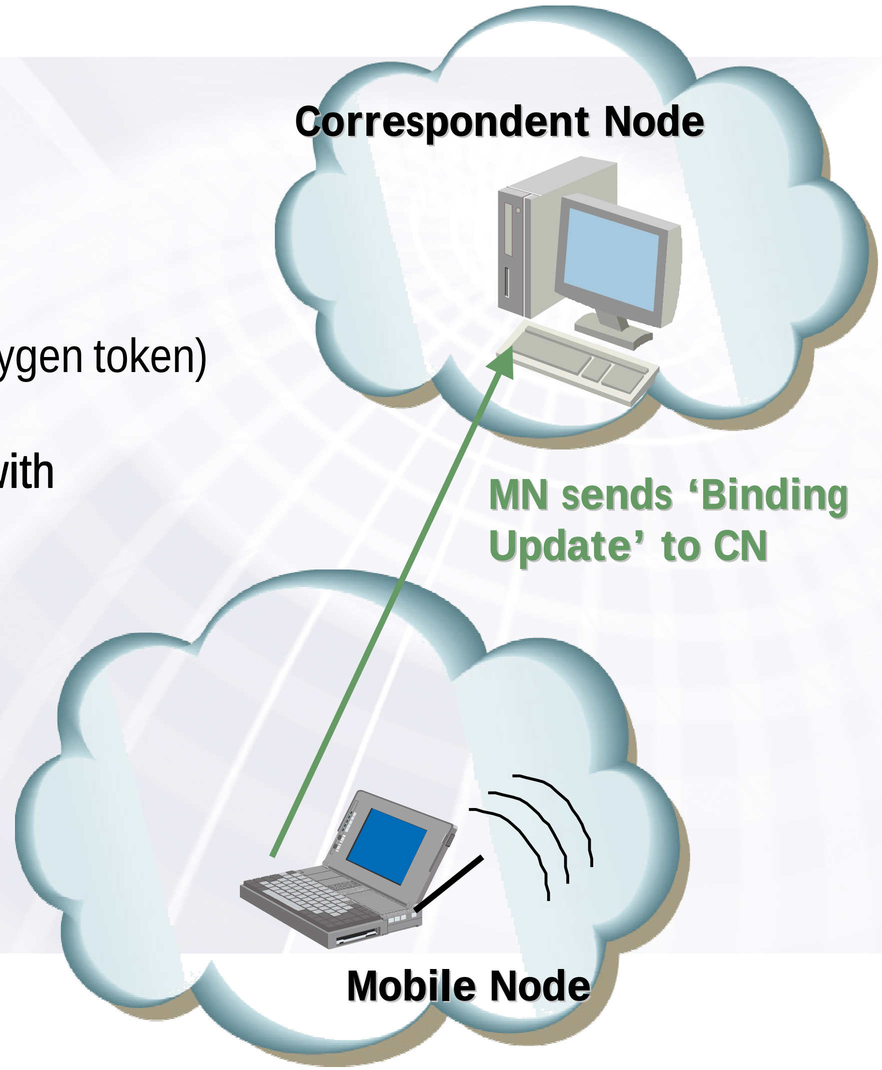
Security Analysis of Mobile IPv6
Return Routability: Step 3

Binding Update:

- Returned tokens are used to generate binding management key:
  Kbm = SHA1(home keygen token | care-of keygen token)

- The binding update is generated and signed with Kbm

- The Correspondent Node can evaluate the Received Binding Update



T - -Systems-

Security Analysis of Mobile IPv6
Standardisation Issues:

Challenges:

- IPSec Configuration:
  - Traffic between must be routed via IPSec: Strict Filtering on Mobile IP-Message Level
  - Currently only loose integration of Mobile IP and IPSec implementations, can not filter Home Address Destination option
  - IPSec not generally deployed

- Draft requests an IPSec API to redirect Security Associations as Mobile Host moves – potential security hole

- Computational burden:
  - Conflict with 3G Mobile Node requirements
  - Home Agent must be scalable and performant

Security Analysis of Mobile IPv6
Implementation Status

	Open Source	Draft Status	Security	Platform	Future Support
Ericsson/Telebit	No	?(13)	No	Router	?
Microsoft	No	?(12)	Yes	Windows	?
MIPL	Yes	24	partially	Linux	Yes
Kame	Yes	?(15)	Yes	BSD	?
NEC	Yes	?(13)	Yes	BSD	?
6WIND	No	20	partially	Router	Yes
Cisco	? (was Announced for Q4/2002)				

- Not yet stable standardisation process has deterred implementers
- Securing of control messages is left to IPSec – currently no tight integration
- Scalability issues due to lack of 'Global PKI' and complex provisioning

Proposed Architecture for Mobile IPv6 Deployment
'Closed System Architecture'

What is our definition of a closed system?

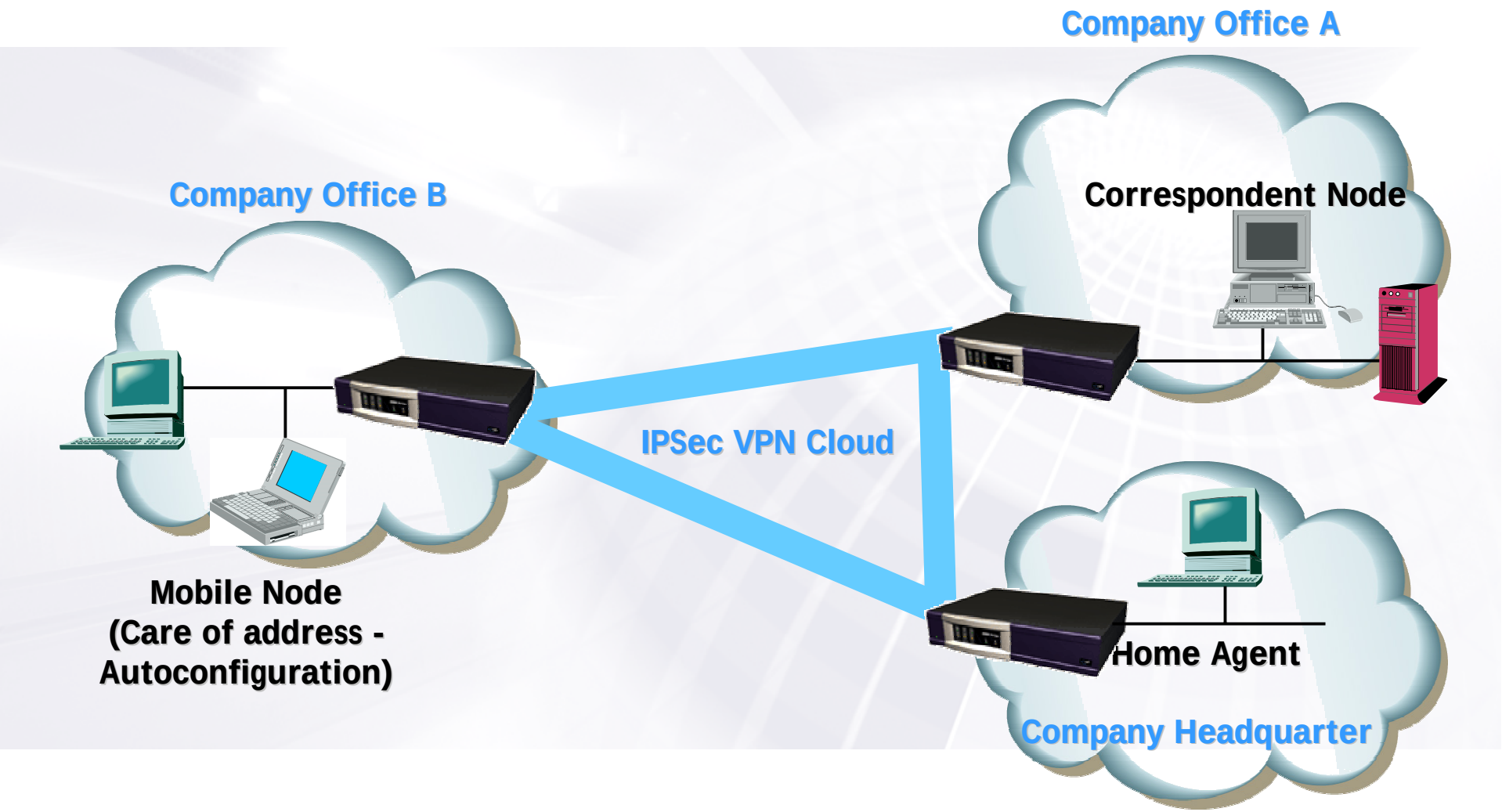
- One administrative domain
- Users/machines are known in advance
- Single use policy
- Dedicated software environment

Characteristics:

- Authentication of users can used predefined tokens (MAC,...)
- Firewalling keeps out the rest
- Threads from within are insignificant and can be neglected
  - Illegitimate use
  - Playful users
- No need to be 100 per cent standards compliant

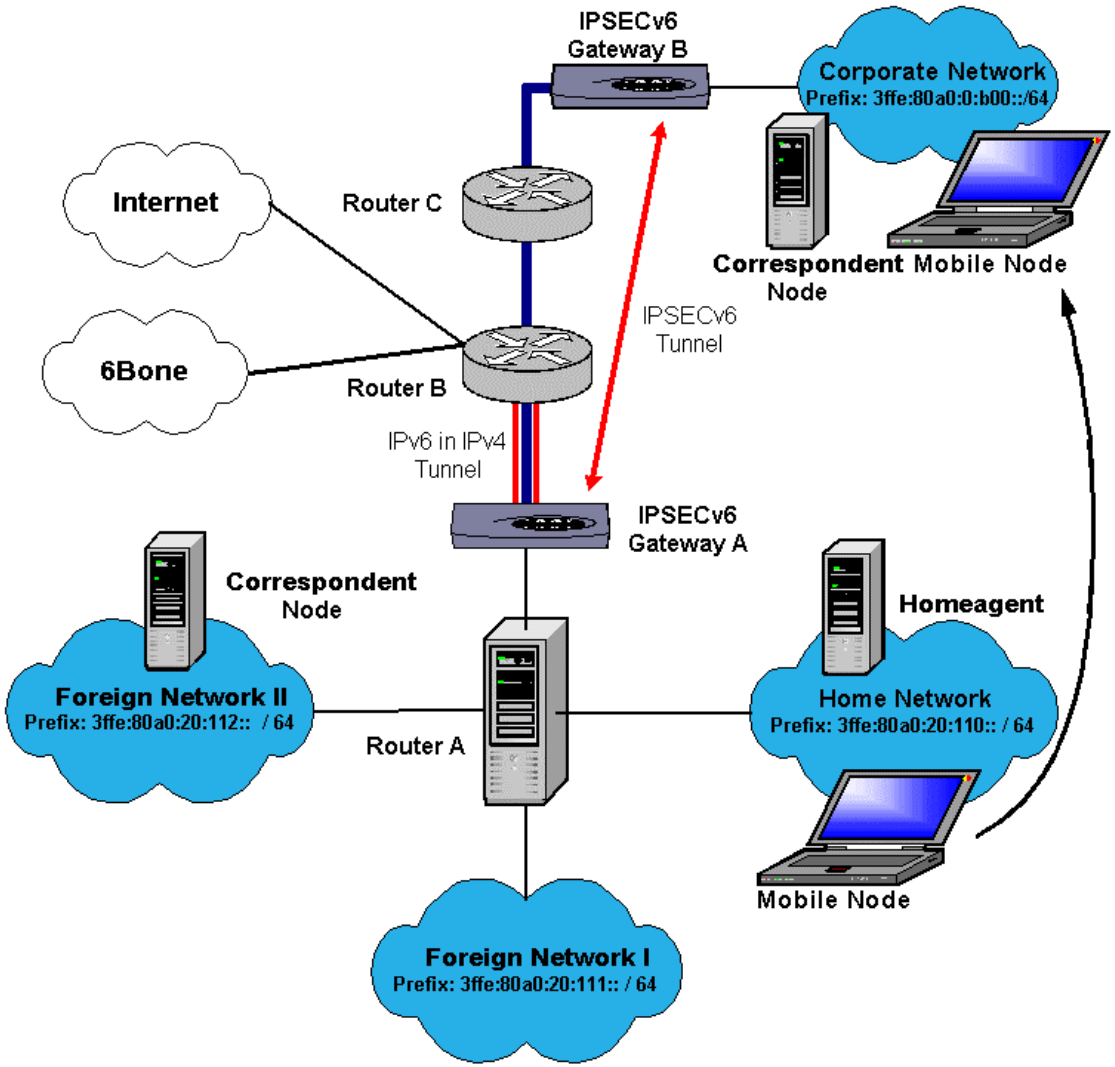
Proposed Architecture for Mobile IPv6 Deployment

'Closed System Architecture'



T-Systems

Lab Setup and Findings



VPN Gateways:

- FreeSWAN Box

Mobile IPv6:

- MIPL

T · · Systems ·

Lab Setup and Findings
Implementation Issues

Status:

- Very little support of security features in implementations
- Interop between implementations regarded as poor
- Integration of IPsec with Mobile IP – Implementations:
  (eg. Check through Home Address Option for the Binding Update – might not be supported by standards IPsec implementations / Processing Order?)
- It seems that implementers have given up on slow progress in IETF
  Danger: very little practical feedback into standardisation
- Integration with AAA and PKI necessary, but not resolved

- Develop and test solutions for Open Mobile IPv6 Szenarios is currently very difficult
- Complexity issues need to be resolved: subset of features for specific usage scenarios

Mobile IPv6 Security Architectures
Requirements revisited

Requirements for a Mobile Protocol:

- Small Footprint (on the wire, implementation wise)
  - current Mobile IPv6 draft is well over 170 pages, still not stable
  - IPSec support required
- Fast Handover (Minimum Delay, Packet Loss during Handover)
  - questionable in the case of IPSec-tunnel setup and teardown
- Secure Operation
  - Filtering, PKI and IPSec configuration still not solved
- Privacy Issues for the foreign network and the visiting mobile node
  - Not in the scope of the standard
- Coexistence of Mobile IPv6 and Transition Mechanisms
  - Not in the scope of the standard

Conclusion: More work needed to bring Mobile IPv6 to market!

Security Expert Initiative

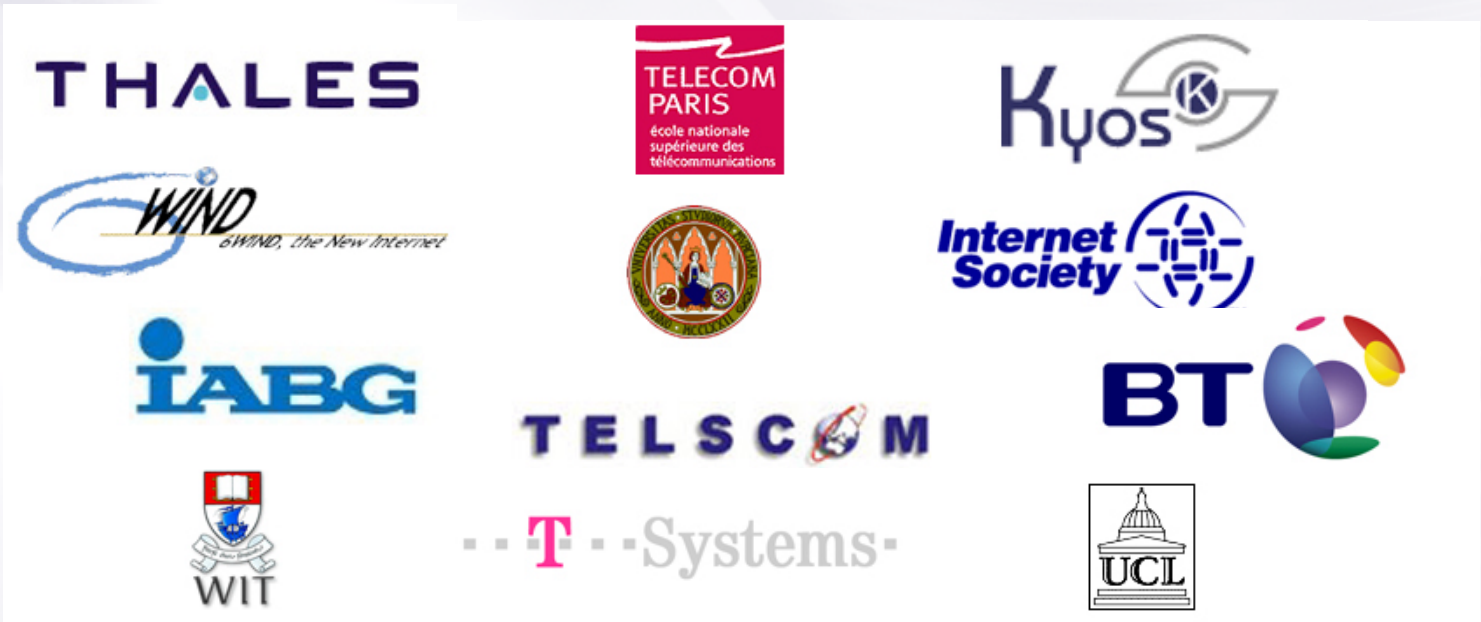
Objective :

- Ensure a trusted and dependable security framework, ubiquitous, working across multiple devices, heterogeneous networks, being organisation independent (inter-operable) and centred around an end-user.

This will be achieve by :

- Defining new trust, security models and security policies that address the current and future threats, and ensure affordable security services, maintaining an adequate security level without infringing a user's right to privacy.
- Specifying components to build the infrastructure, to enforce these policies, select the existing tools and devices, and define the new components to develop.
- Participating to the core research initiatives towards eEurope-2005

IST Project SEINIT:
Project Partners



Project duration:
24 months (Start December 2003)

Project Homepage: www.seinit.org

Project budget:
8 Mio Euro
(3.8 Mio Euro EU contribution)

Information Society Technologies

T Systems

Contact.

Thomas Scheffler
Senior Consultant
Next Generation Networks

T-Systems
Systems Integration
Goslarer Ufer 35
10589 Berlin

Tel. +49 30-3497-2274
Fax. +49 30-3497-2275
Email thomas.scheffler@t-systems.com

T · · Systems