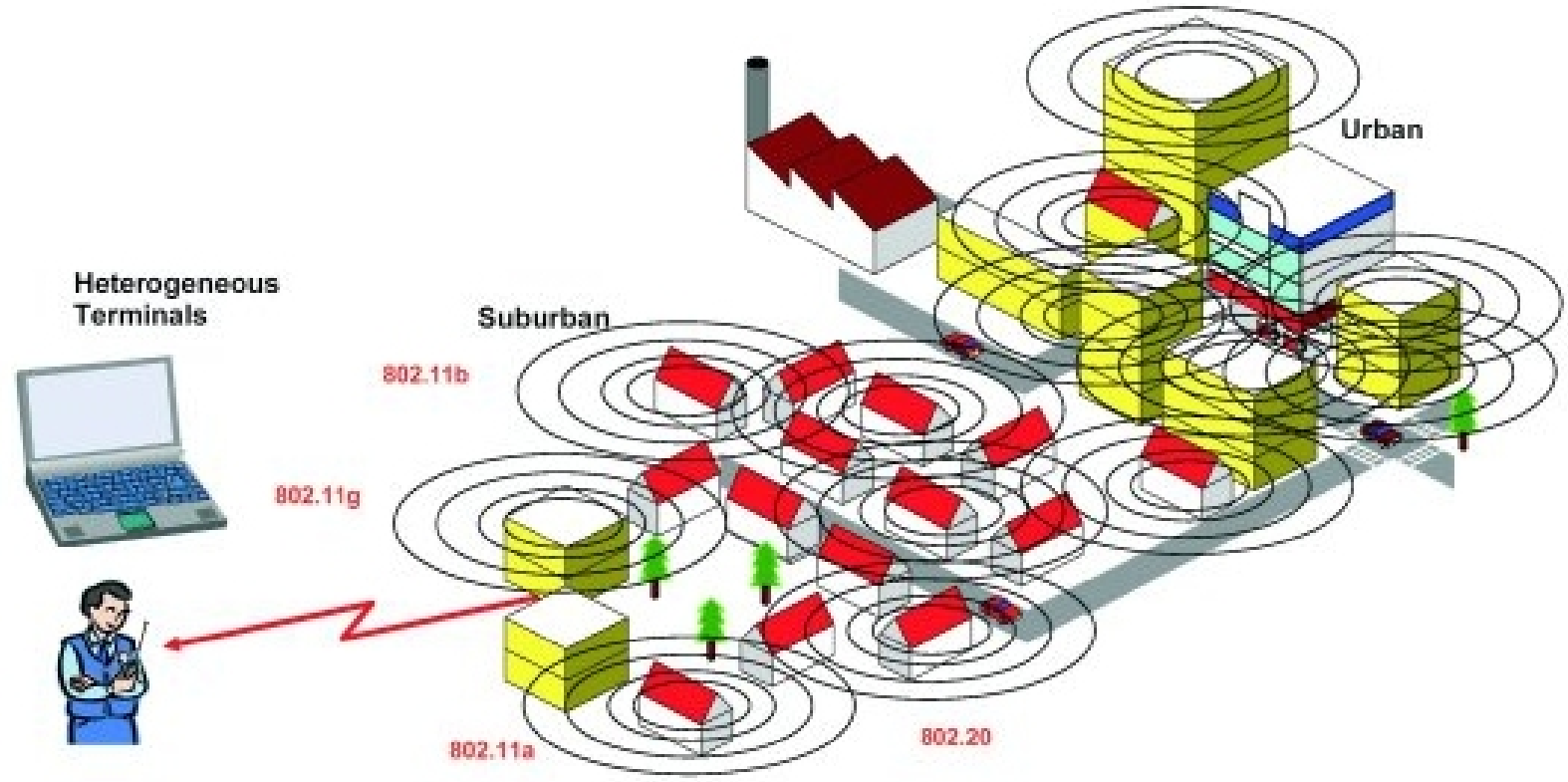
Security Mechanisms to support Real-Time Applications for OBAN

Thomas J. Wilke

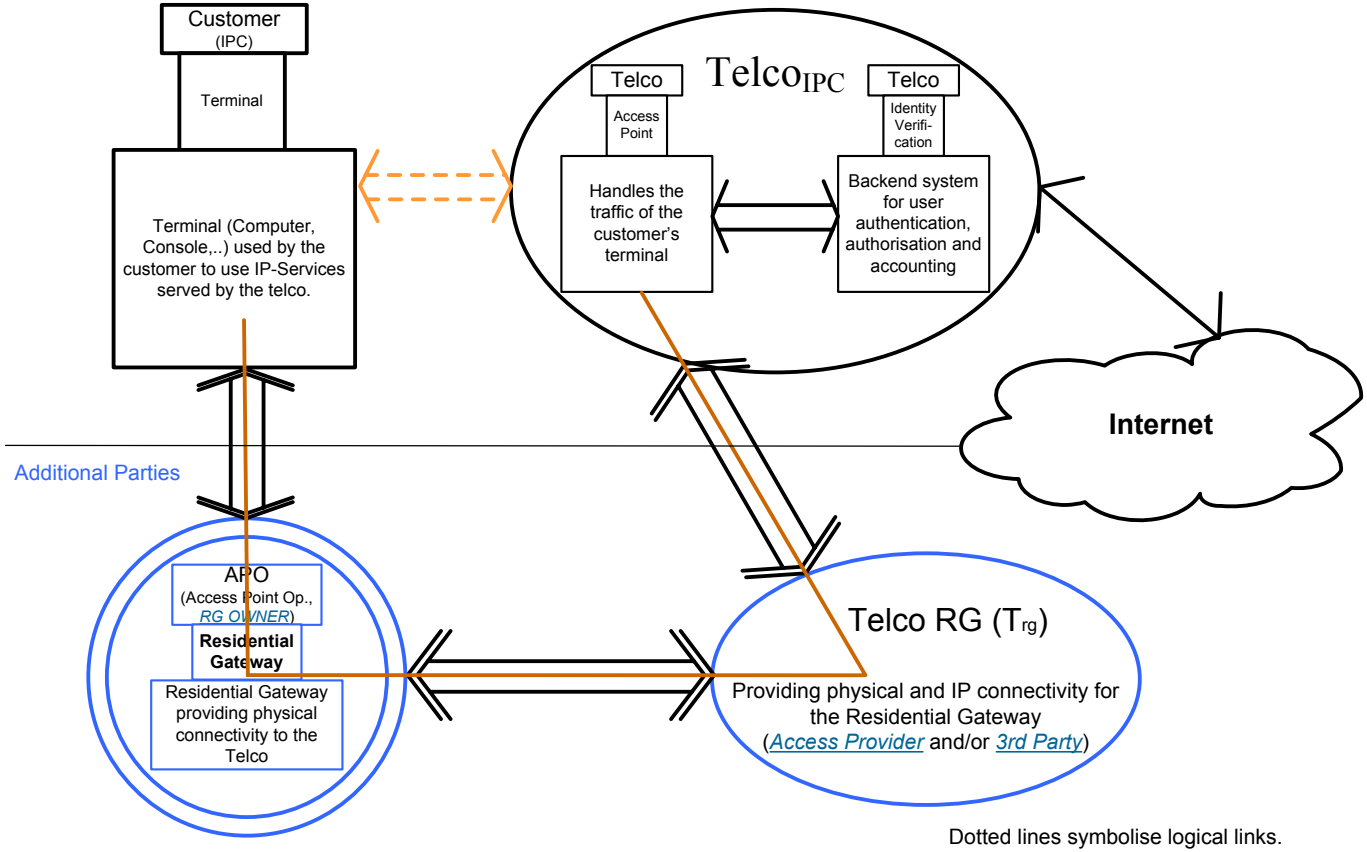
Contents

- OBAN Approach
- Security Goals
- Fast Handover and the Timing Problem
- Problem Solution: Time Shifted Security Computing
- Fast Handover Security Enforcement Mechanism
- Conclusion

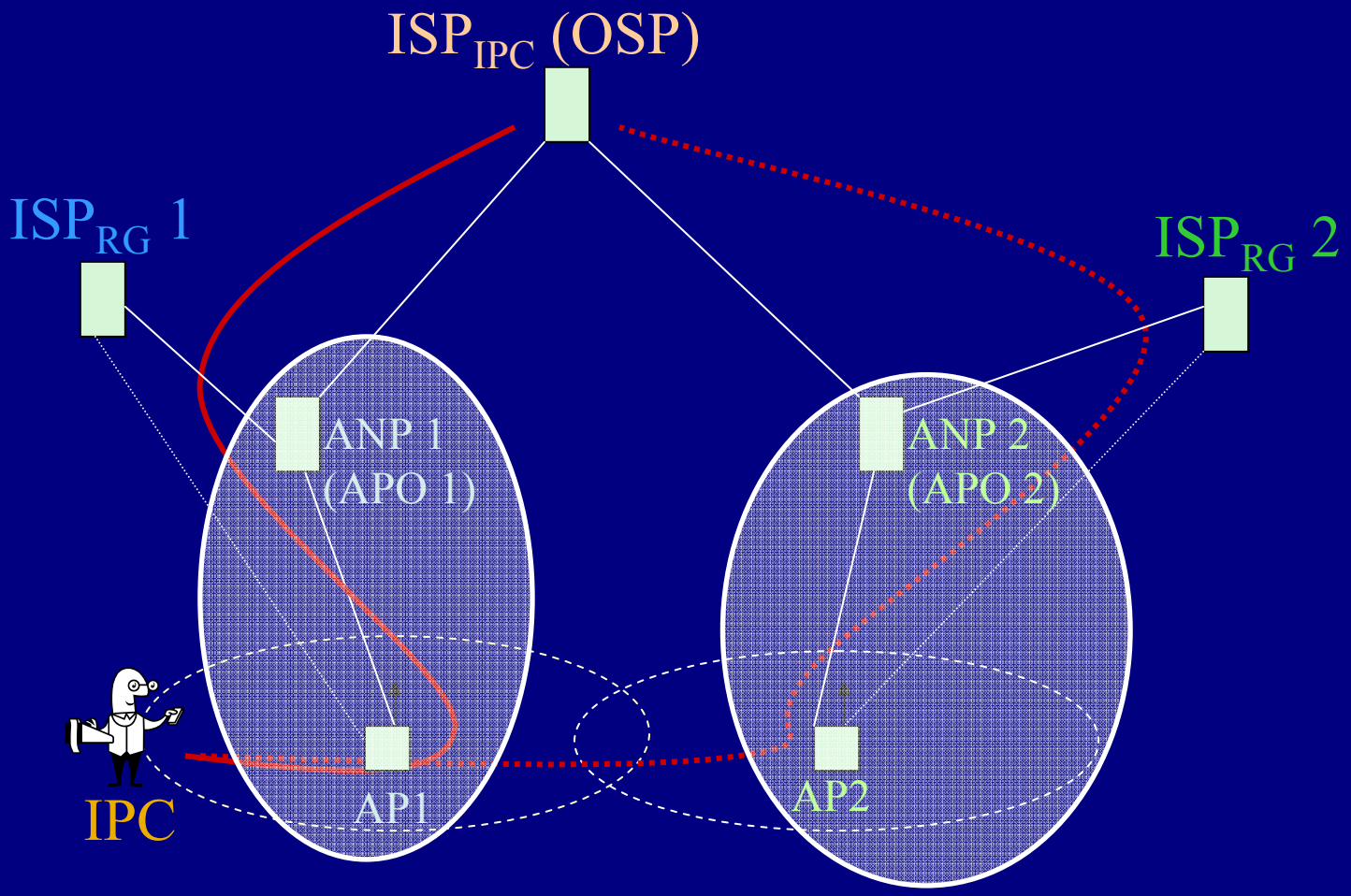
The OBAN Approach



OBAN Approach: Parties



OBAN Parties: Mobility



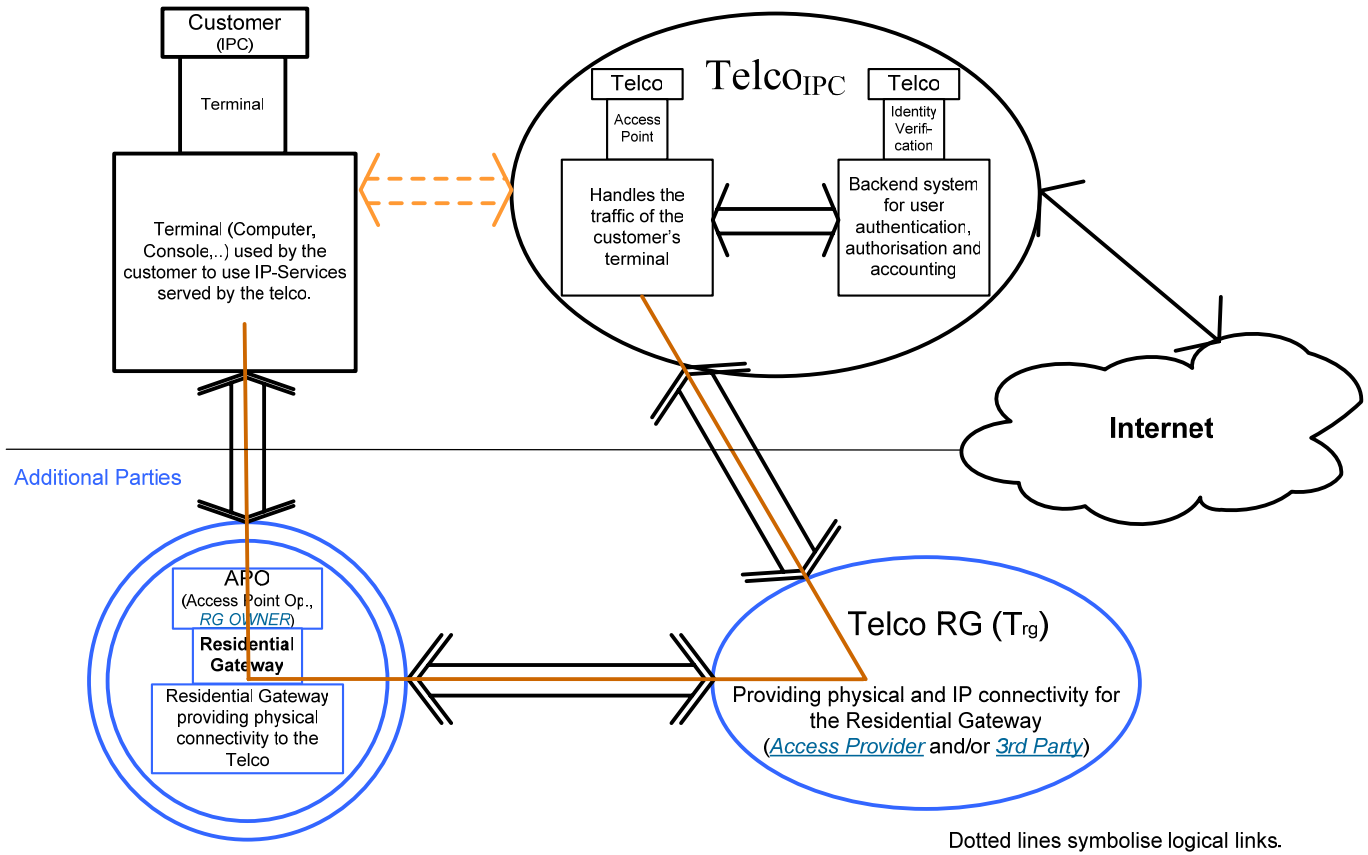
OBAN Security Goals

- Authentication
- Confidentiality
- Accountability
- Non-Repudiation
- Data Integrity
- Access Control
- Enhanced data protection and privacy
- Binding transparency

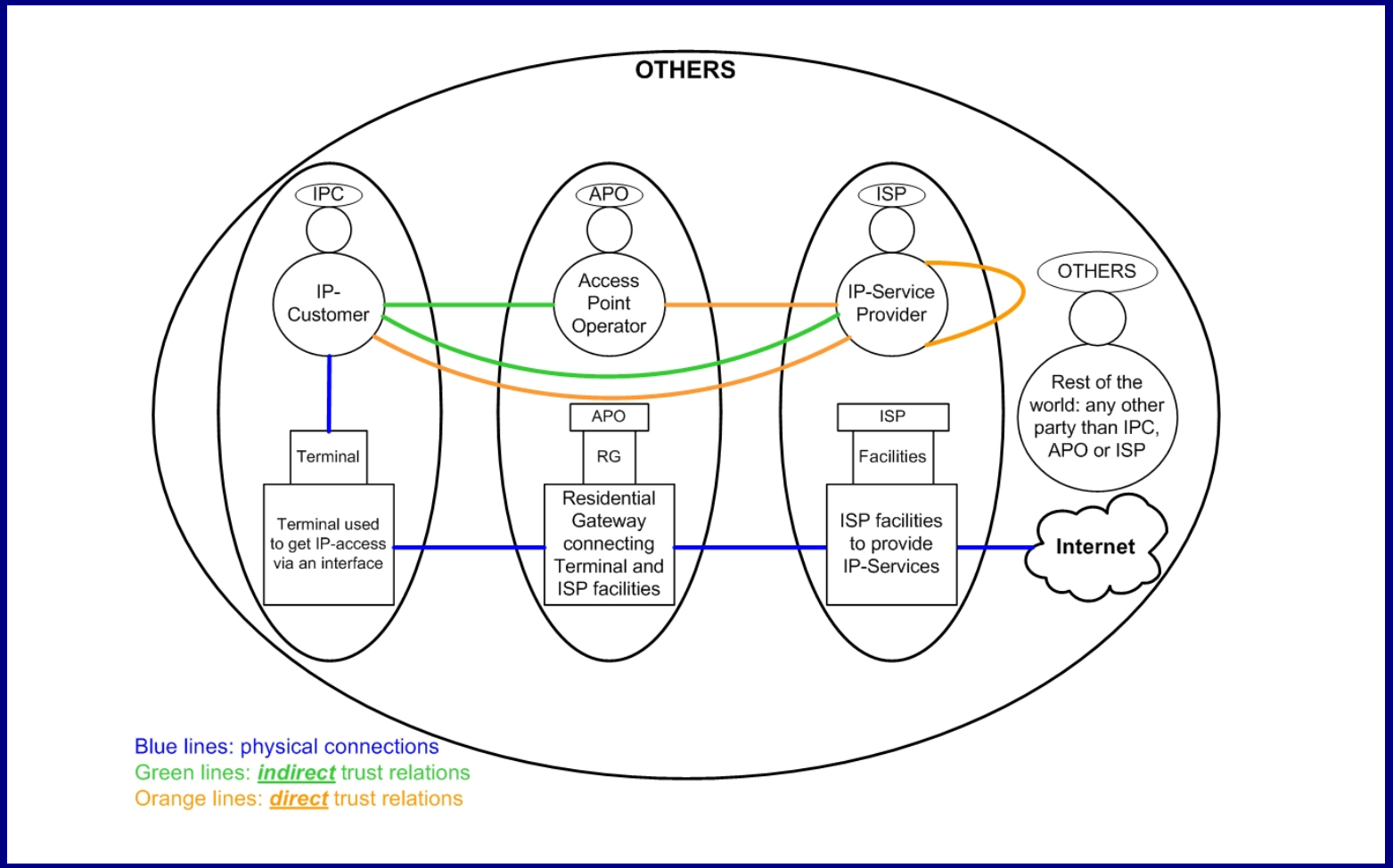
Specific for Handover:

- Bridging Policy Enforcement

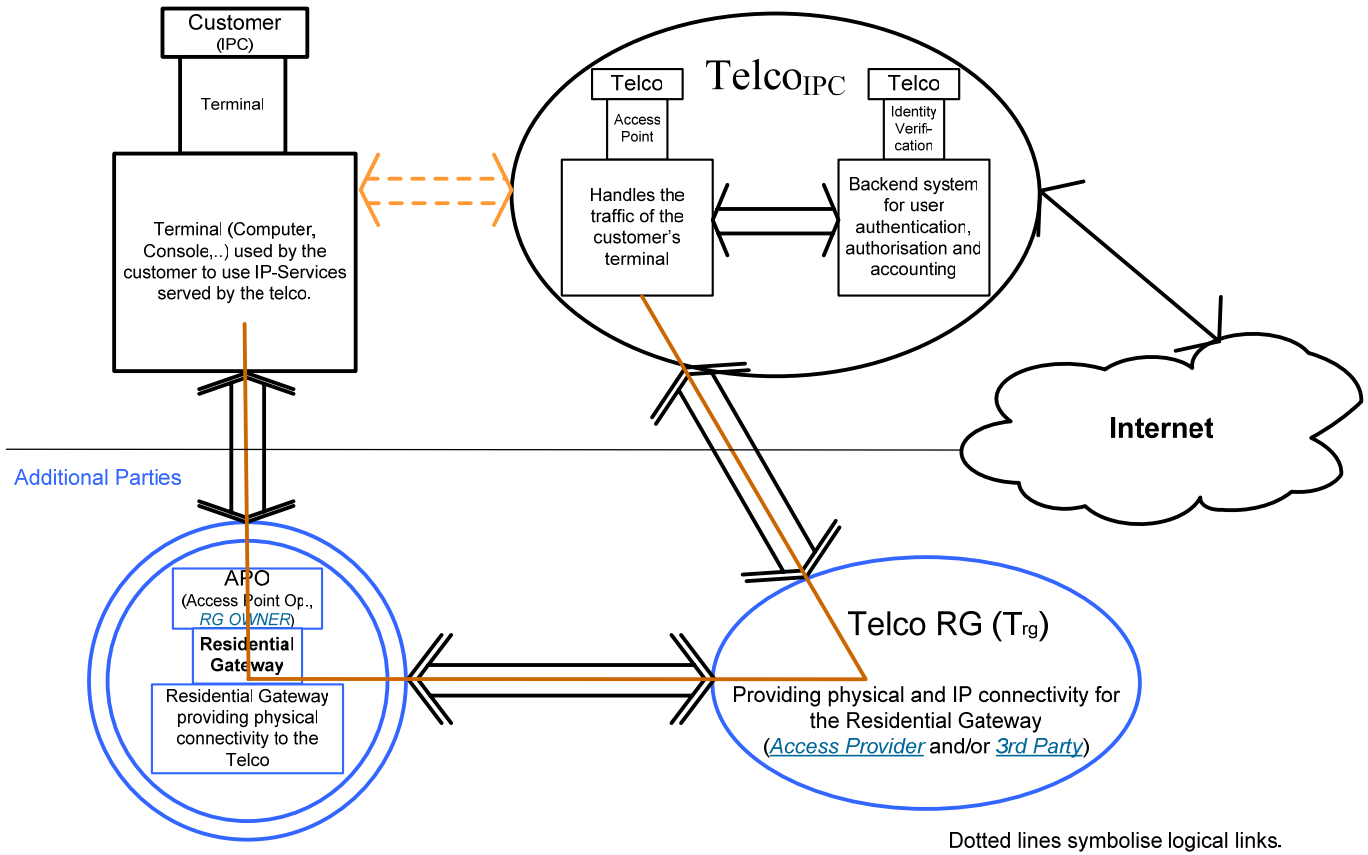
OBAN Approach: Security Requirements



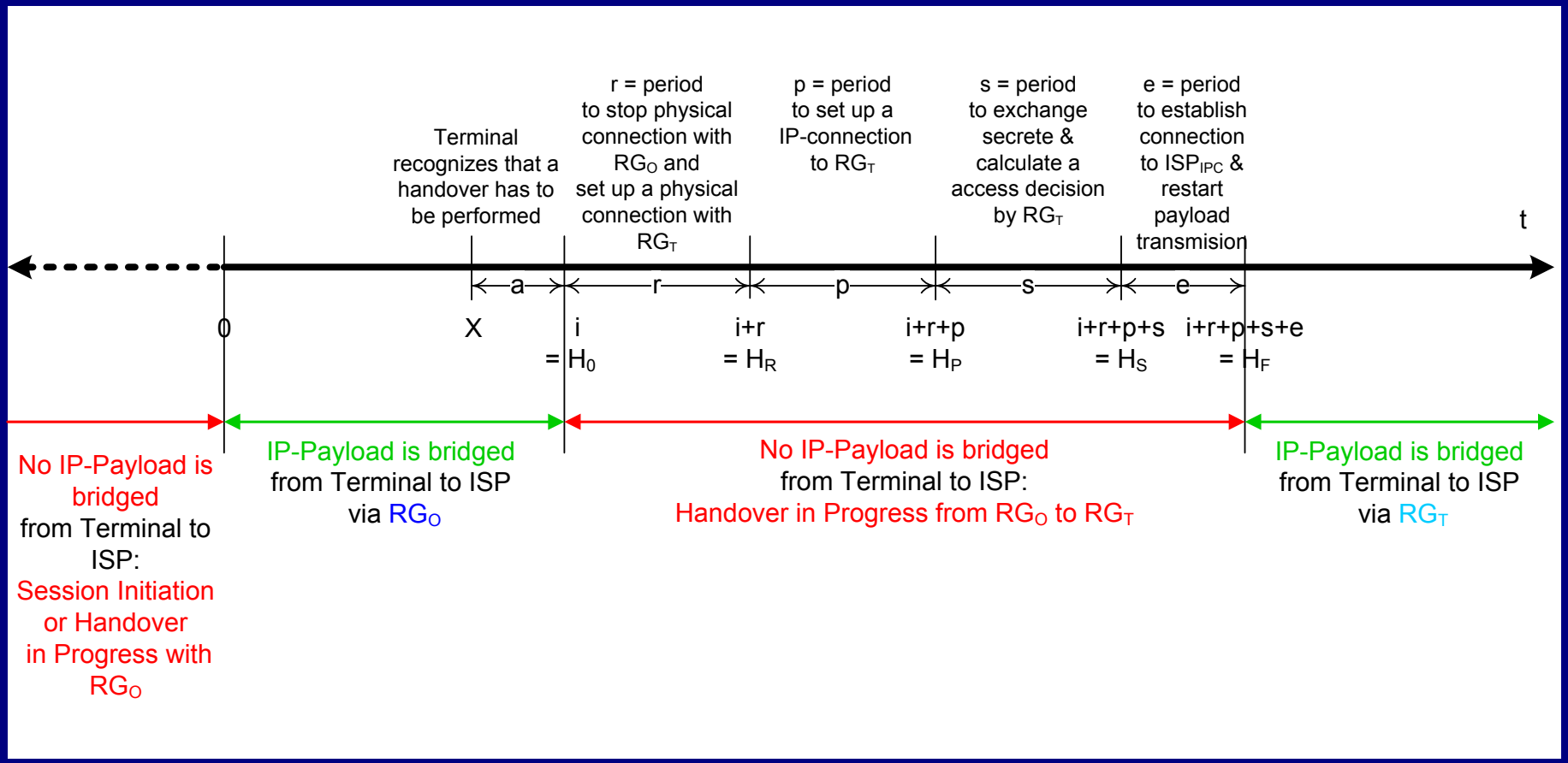
OBAN Approach: Party Trust Relations



OBAN Approach: Mutual Authentication



Fast Handover and the Timing Problem



Problem Solution: Time Shifted Security

2 Step divided security functionality processing:

- **Complex Security Functionality Processing:**
  Resource and time consuming are performed in parallel to other computations to prepare Real-Time Security Processing.
- **Real-Time Security Processing:**
  Very resource and time efficient processing performed based upon data computed ahead or after the Real-Time Processing event.

Fast Handover Security Enforcement Mechanism: pre- & post-processing

Combination of 2 time shifted computing variants leading to 3 step computation mechanisms

- **1 step: Pre-Processing** (payload is bridged in parallel)
  - ISP_{IPC}: Identifying candidate ISPs and RGs
  - ISP_{IPC}: Terminal authorization
  - ISP_{RG}: Authorization of candidate RGs
  - ISP_{RG}: Terminal identity and authentication indication

Fast Handover Security Enforcement Mechanism: pre- & post-processing

Combination of 2 time shifted computing variants leading to 3 step computation mechanisms

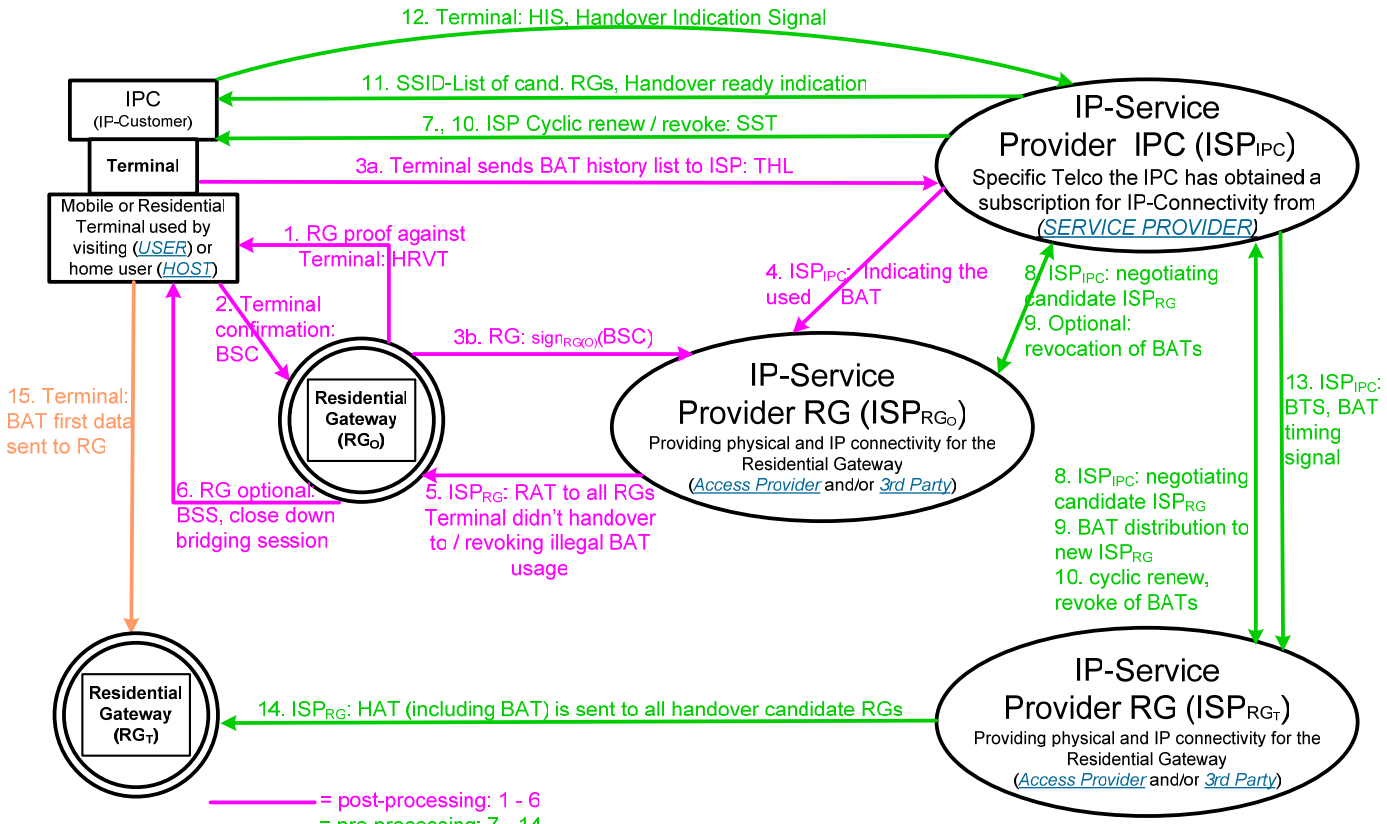
- **2 step: Real-Time-Processing** (no payload is bridged in parallel)
  - RG: Terminal identification
  - RG: Terminal access decision and enforcement

Fast Handover Security Enforcement Mechanism: pre- & post-processing

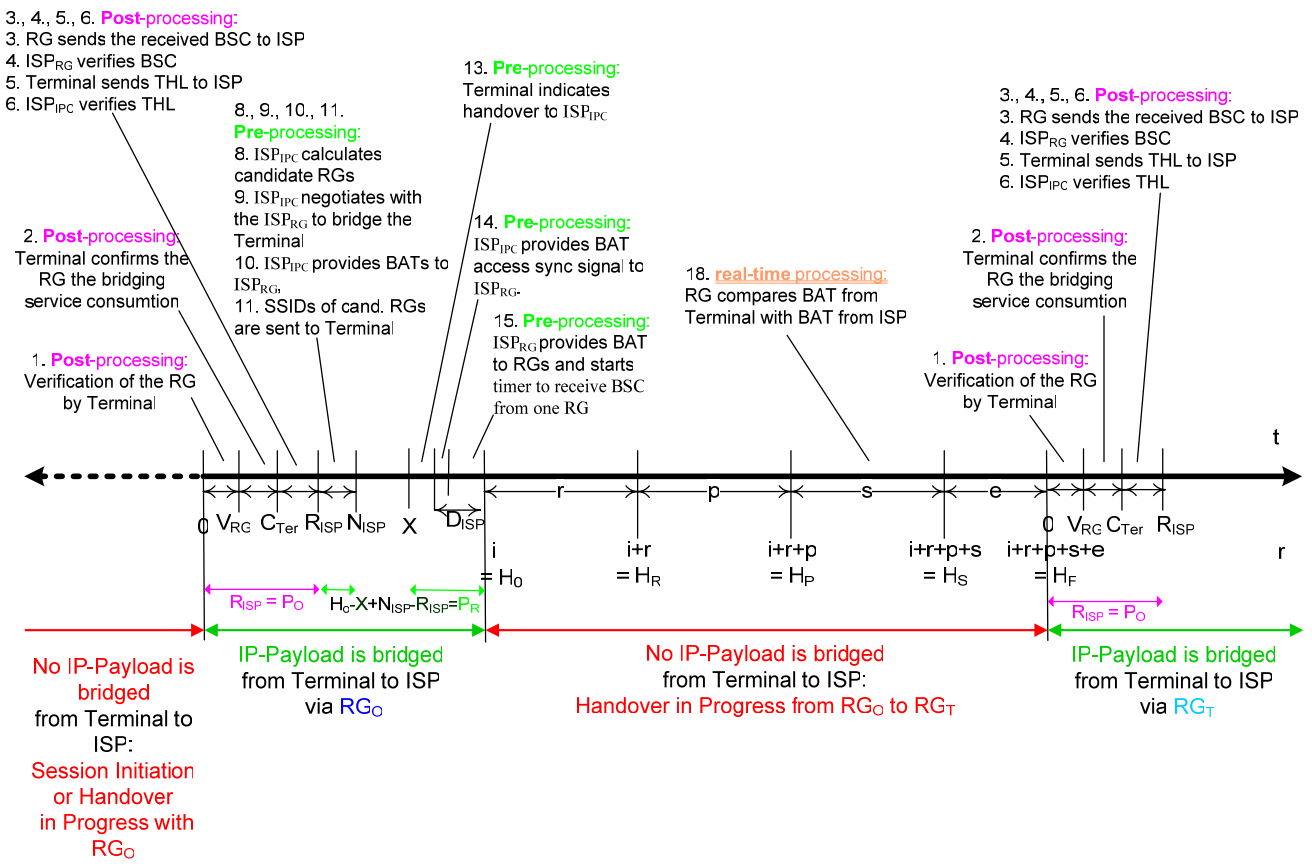
Combination of 2 time shifted computing variants leading to 3 step computation mechanisms

- **3 step: Post-Processing** (payload is bridged in parallel)
  - Terminal: RG is authenticated
  - RG: Bridging service consumption confirmation from Terminal
  - $ISP_{IPC/RG}$: Service consumption legitimacy verification

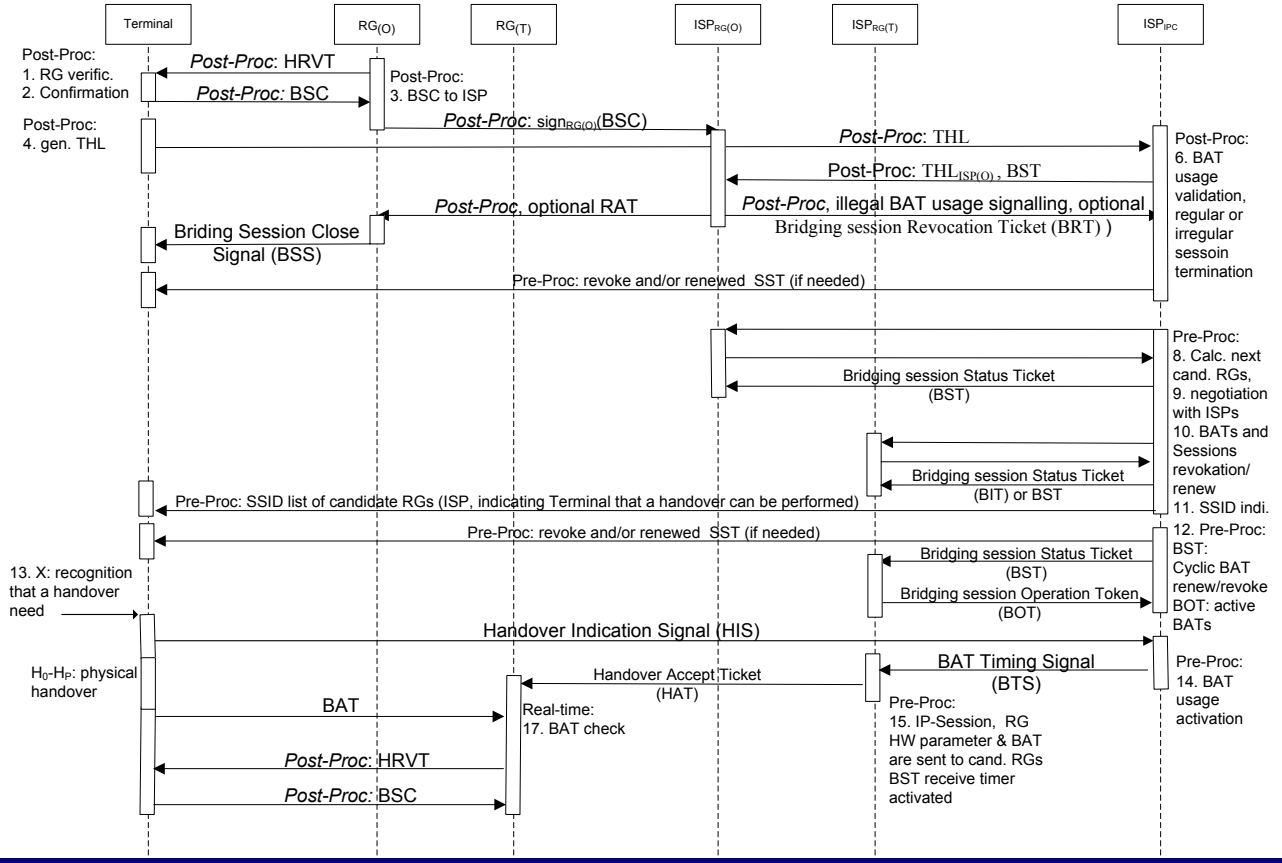
Fast Handover Security Enforcement Mechanism: party perspective



Fast Handover Security Enforcement Mechanism: time-scale perspective



Fast Handover Security Enforcement Mechanism



Characteristics of the Mechanisms

The presented mechanisms can be characterized by the following items:

- A Bridging Access Ticket (BAT) describes a handover in respect of the following aspects:
  - BAT is created and distributed by ISP_{IPC}
  - BAT is only valid for a definite Handover within a limited period,
  - BAT is distributed to 1 or a max. n RGs,
  - BAT can only be used by one Terminal
- Parties controlling the access of a Terminal (in hierarchical order)
  - ISP_{IPC}
  - ISP_{RG}
  - RG

Conclusion

A mechanism has been presented enabling a fast handover solution for OBAN which

- Holds all security goals demanded by the business models (WP1)
- Holds all security requirements defined within the basic OBAN security architecture
- Enables in addition a bridging policy enforcement to ensure a fair and economic resource usage of RGs and ISPs

References

- OBAN Security Architecture, document D10.1
- Document file:
  OBAN-WP1-SCOM-16c_v03-tn2.ppt
- Document file:
  OBAN-WP2-TUB-311d-DIS.pdf

Contact:

Thomas J. Wilke
tub@tjw.li
+49 (30) 314 79496
www.tub.tjw.li