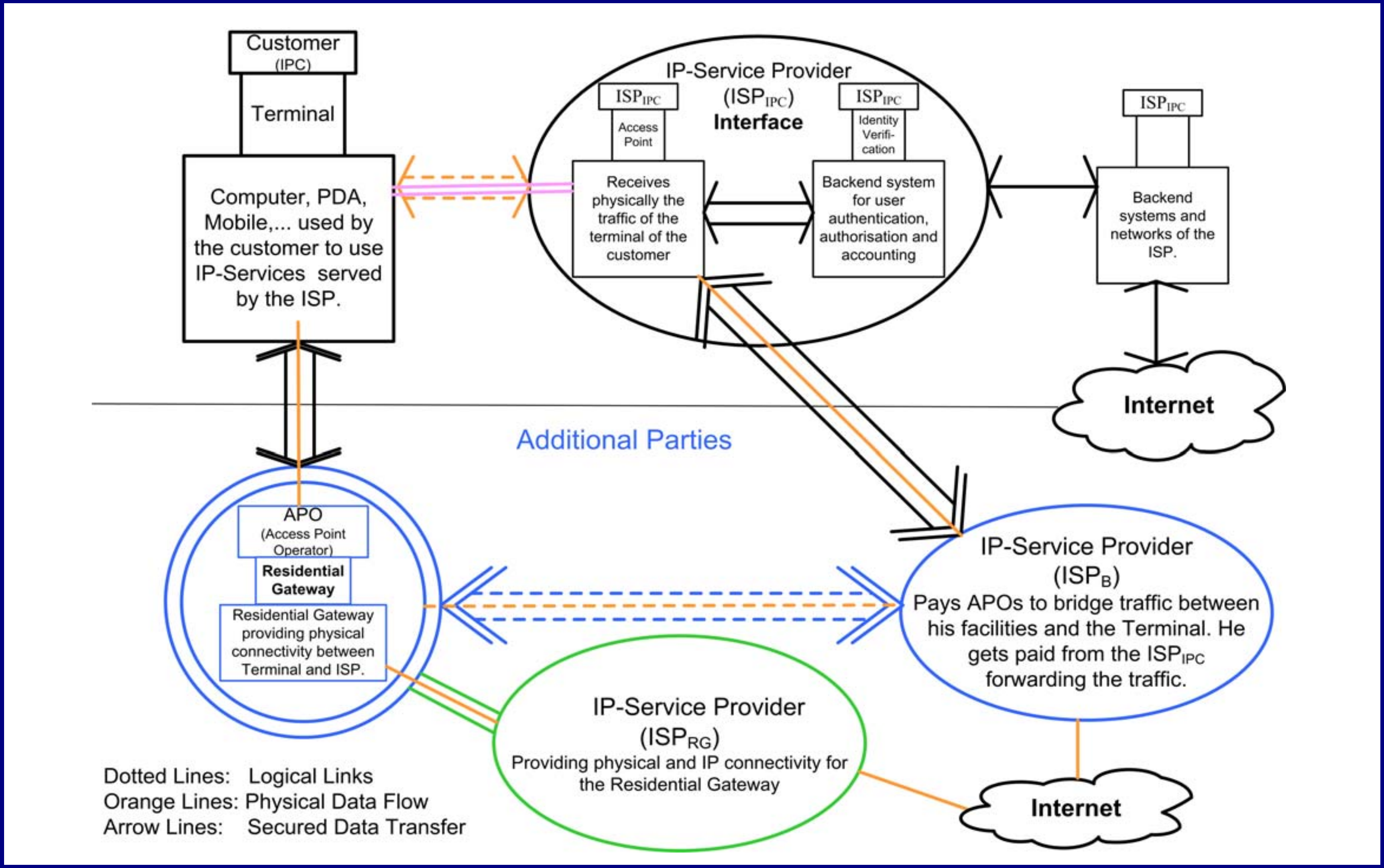
OBAN Specific Security

Thomas J. Wilke

Contents

- Common Approach versus OBAN Approach
- Security Goals for OBAN
- Security Problem Model
- Security Architecture
- Conclusion

Common Approach versus OBAN Approach



Common Approach versus OBAN Approach

Common

- Physically direct connected devices of IP- Customer and his IP Service Provider
- Data exchange between customer and provider takes place only over devices which are under the responsibility of parties having a legal contract with each other

OBAN

- Physically NOT direct connected devices of IP- Customer and his IP-Service Provider
- Data exchange between customer and provider takes place over devices of additional parties. The data flow path does not correspond to the contract relations of the involved parties.

Common Approach versus OBAN Approach

Security Impacts of the OBAN Approach:

- Higher technical and organizational complexity of the IP-Service provisioning process.
- Involved parties may have conflicting intentions due to possible business models.
- Not corresponding technical and legal structures may endanger monetary and legal interests of the involved parties.

Security Goals for OBAN

Main Directives:

- The OBAN approach should be as secure or insecure as the common approaches
- The OBAN Security Architecture should primarily only address security issues resulting of the specific OBAN structure

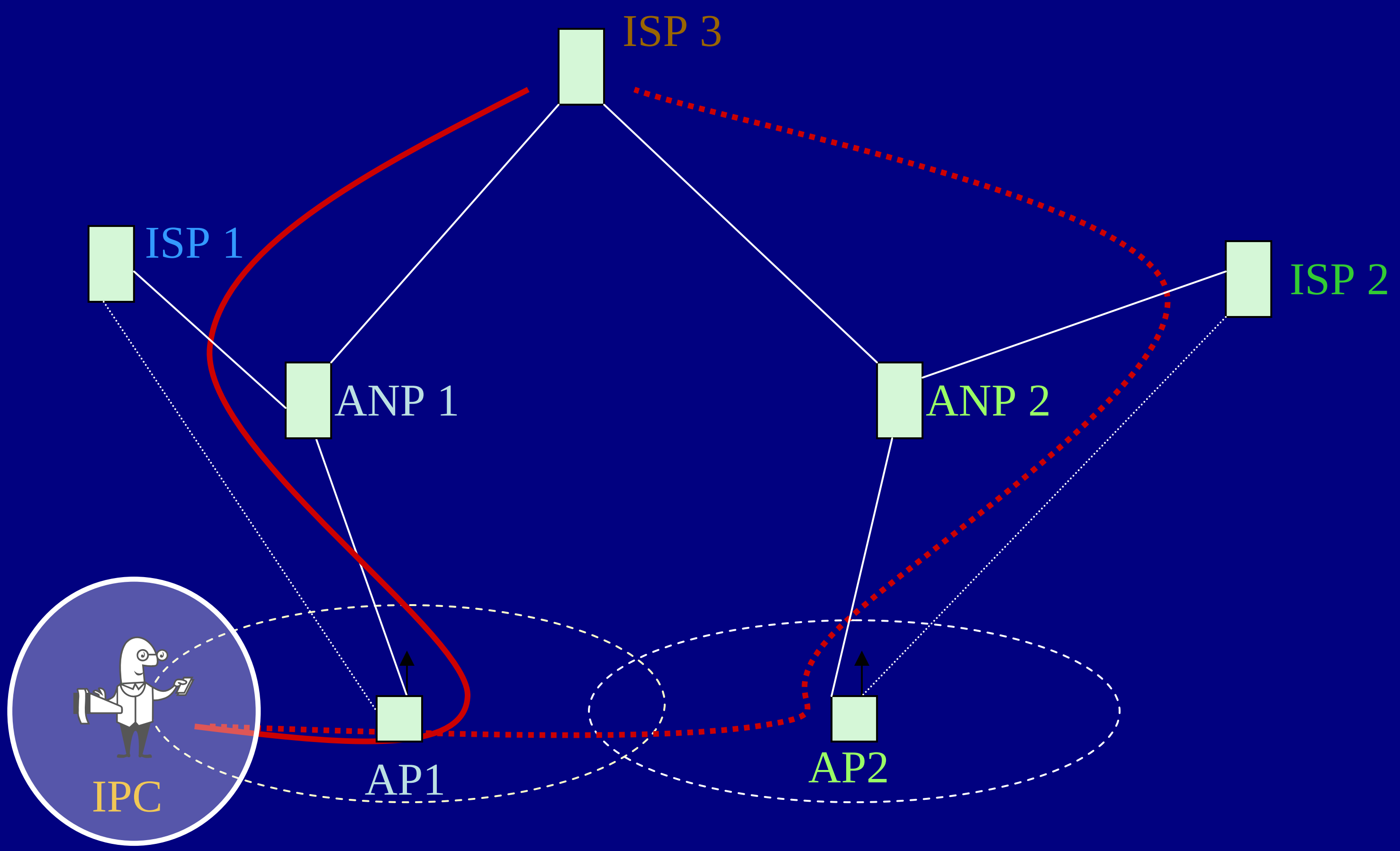
Security Goals for OBAN

- Multi Lateral Security.
  Protection of the legitimate interests of each party involved within OBAN
- Binding Transparency.
  Consistent and authentic traceability of the path of actions taking place within the OBAN IP-Service Provisioning processes
- Enhanced Data Protection and Privacy.
  Strategic data distribution and processing to ensure that each involved party only holds and accesses the information required to fulfill their legitimate tasks

Security Problem Model

Party	Description
IPC	IP Customer: consuming IP-Services of his ISP_{IPC} via ISP_{RG}
HU	Home User: operates the RG he uses
VU	Visiting user: uses RGs of varying APOs and ISP_{RG}s
APO	Access Point Operator: operates the RG using an ISP_{RG}
ISP	Internet Service Provider, providing IP-Services
ISP_{IPC}	service provisioning to subscribed IPCs
ISP_{RG}	service provisioning to APO & IPC having a contract with
Others	All others which do not belong to the parties above

Security Problem Model

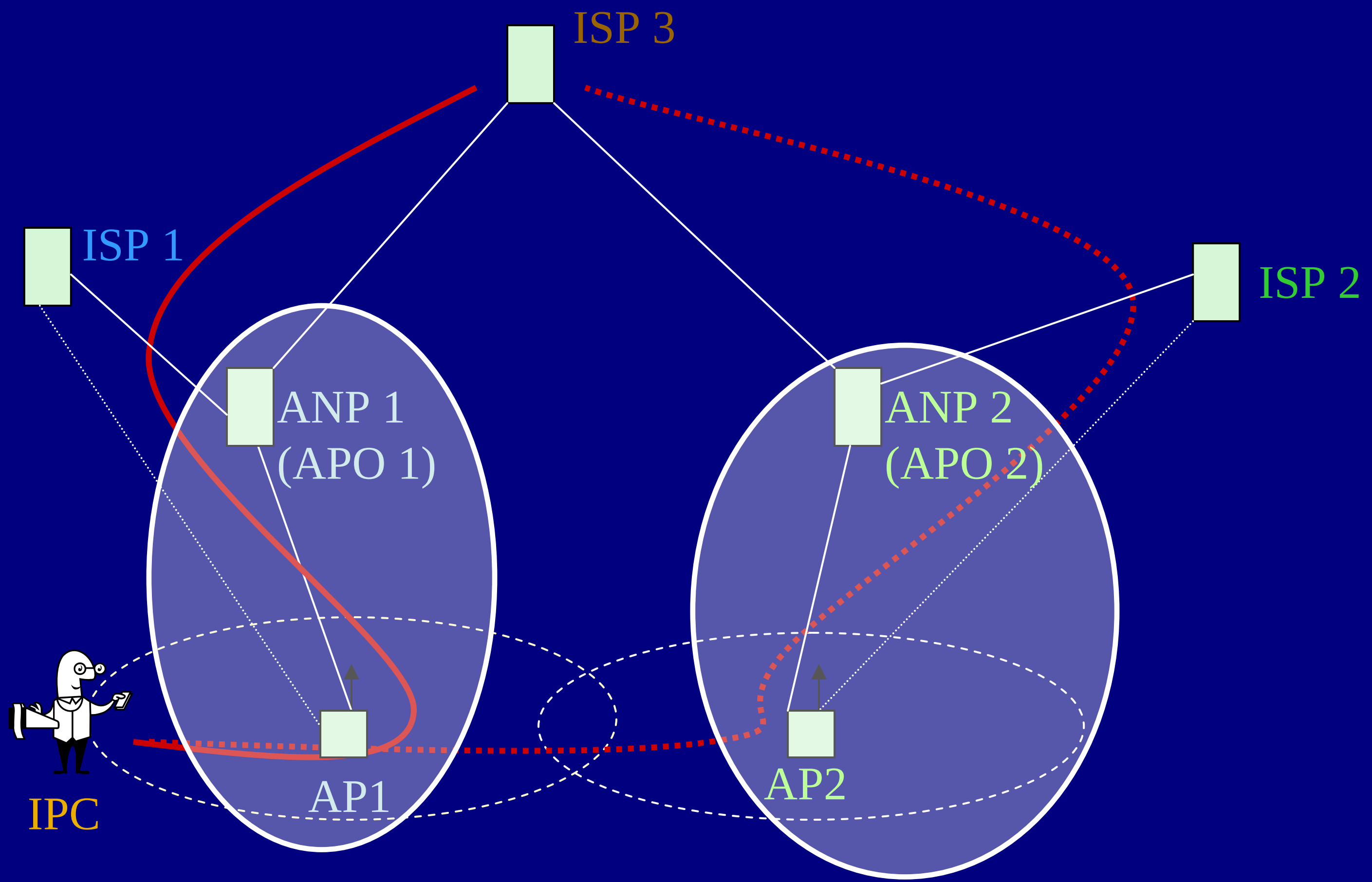


Security Problem Model

Intentions, IP-Customer

- Consuming IP-Services
- ability to prove consumption
- Non interference by other IPCs
- Home User: non interference by APOs
- Visiting User: privacy against APO & ISP$_{RG}$

Security Problem Model

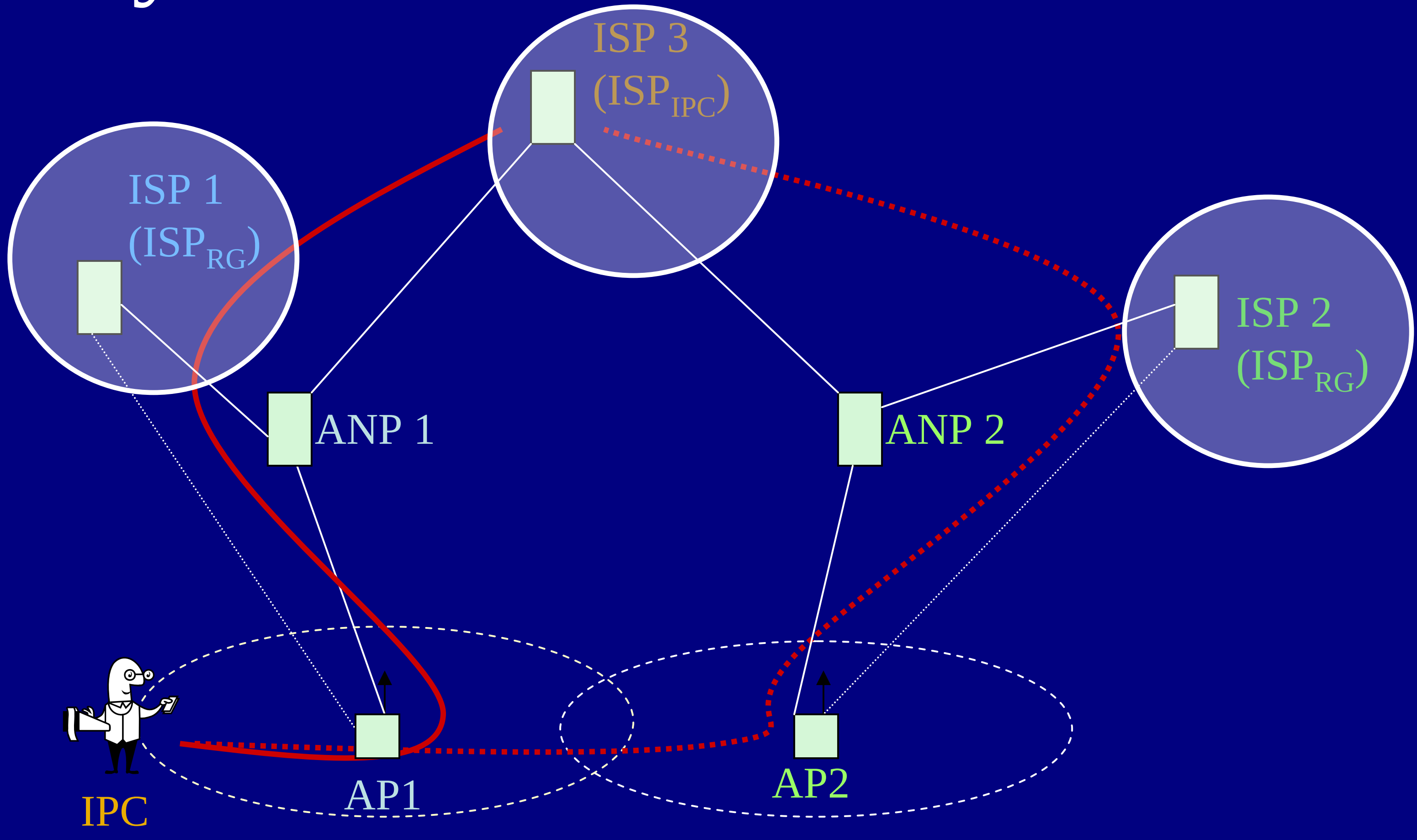


Security Problem Model

Intentions, APO

- maximize bridged traffic
- cost absorption confirmation from ISP
- non repudiation of bridged traffic
- non interference by IPC & APO
- ability to identify the IPC using his RG

Security Problem Model



Security Problem Model

Intentions, ISP

- Optimise network utilisation
- Max. service provisioning efficiency & subscription numbers
- Non interference by other IPCs
- Non repudiation of service consumption by the customers
- ISP_{IPC}: proof of consumed services of ISPs
- ISP_{RG}: maximize bridged traffic

  cost absorption confirmation from

  proof of received traffic from APO

Security Architecture: Mechanisms

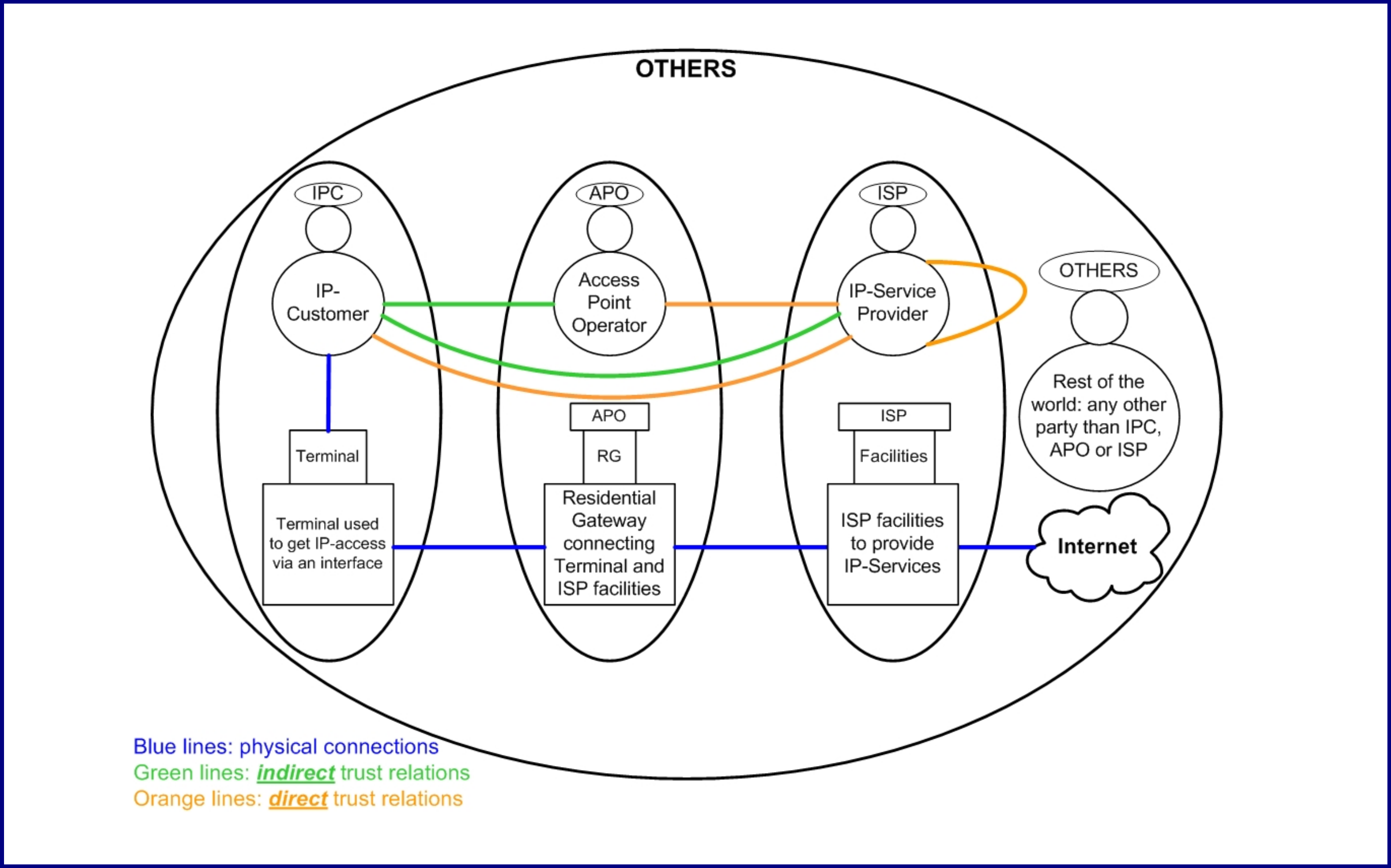
- Confirmations
- Payload and signaling communication protection: using cryptography
- Data Access Protection: using asymmetric cryptography
- Multi control and verification of signaling data
- Trusted point based rule enforcement

Security Architecture: Trust Relations

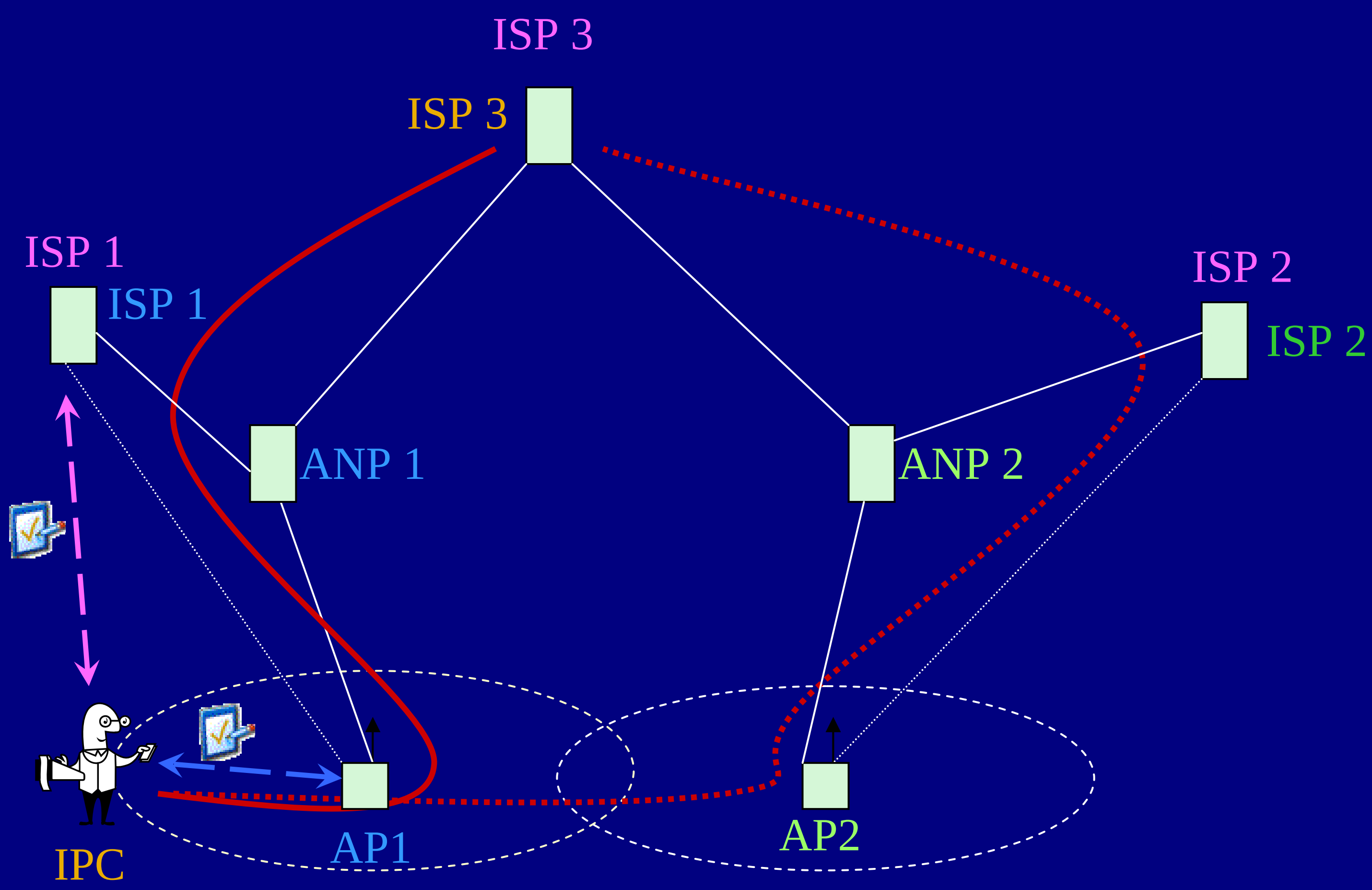
- Direct Trust Relations (DTR):
  Static trust relations established by organizational procedures like contract conclusion, formal agreements and so on.

- Indirect Trust Relations (ITR):
  Dynamic trust relations established between parties not knowing each other using confirmations issued by parties which have established direct trust relation

Security Architecture: Trust Relations



Security Architecture: Trust Relations



Conclusion

A security architecture for a physically decoupled service provisioning approach has been presented which

- Enables to enforce operation rules between parties which do not know each other a priori
- Enables to prove the actions taken place between the parties within a service session in a legally binding way
- Enables to ensure non-repudiation between the parties involved within a service session
- Enables to provide enhanced data protection and privacy for the involved parties of a service session

Contact:

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