Multilateral Security for IP-Service Provisioning in Open Broadband Access Networks

Thomas J. Wilke, Research Associate
PRZ,
Technische Universität Berlin
Berlin, Germany
tjw@prz.tu-berlin.de

Tor Hjalmar Johannessen, Security Advisor

Telenor R&D
Fornebu/Oslo, Norway
torhjalmar@telenor.com

***Abstract*—Enabling the vision of the 3G and 4G mobile communications is one of the most demanding challenges in terms of technologies, investment strategies and business models for the today's communication and service provider. This paper deals with a security architecture for a new approach of IP-Service/Internet Service Provisioning, called OBAN, utilising privately operated facilities enabling a high communication service quality for the public. The concept of the OBAN approach and its distinguished features in respect to the common service provisioning practice today is introduced, followed by a discussion of the new security issues, which are implied by the OBAN approach. Finally, a multilateral security oriented architecture design is presented which solves the OBAN security issues by implementing new security paradigms such as binding transparency, enhanced privacy and data protection.**

I. Introduction

Utilisation of existing infrastructure resources is the approach of “Open Broadband Access Networks” (OBAN) as a technological option to realise the vision of future 3G and 4G mobile communication. OBAN is a research project part of the 6th framework program hosted by the EU Commission.

The idea is to build an open access network upon “privately owned” wireless LANs and users' access lines enabling a high coverage of IP-Service provisioning for the public. Unused fixed broadband access network resources and facilities operated are offered to public in order to benefit the private operator, public users, fixed network operators and mobile broadband access network operators. Such private operators are enabled to fund additional resources, which they might need to have to handle their peek traffic requirements. Fixed network operators may increase their utilisation of their networks and therefore be more cost efficient. Users Public will get a very high coverage and access availability for advanced mobile services. Mobile communication service providers will be enabled to solve the challenges of 3G/4G mobile communication with respect to technological and financing feasibility.

Next to the benefits of the approach there are some immanent impacts especially with respect to security concerning integrity, authentication, access control, data integrity and confidentiality, and not least accountability for the involved parties. This is due to the fact, that the service provisioning technically involves additional parties with different ambitions than only the service provider and his subscribers.

II. IP Service Provisioning: Common Approach in Contrast to OBAN

IP-Service provisioning for world wide communication is nowadays commonly done by Internet Service Providers (ISP) operating an access infrastructure and networks which transports data between network nodes located in the provider's networks and other public networks. Part of the ISPs access infrastructures are access points which are used by their customers (IP-Customers, IPCs) to connect their LANs to exchange data with the Internet. Therefore in the common IP Service Provisioning approach the contracting parties (ISPs and their IPCs) exchange data over technical infrastructures they are responsible for self. In this scenario it is a common practice that the technical connection of the contracting partners are assumed to be secure in terms of confidentiality, accountability and access control with respect to the usage of physical or virtual dedicated data transportation paths.

In contrast the OBAN approach can imply that the facilities and services for the access and communications are under the responsibility of additional parties which may have other intentions than the contracting parties (ISP and IPC).

One of these parties can be the operator of the residential gateway (RG), also called Access Point Operator (APO). Another party can be a separate ISP (ISP_{RG}) that serves IP-Services for the RG. The different intentions of the additional parties may be a result of business models proposed for the OBAN approach. One category of these models wants to motivate APOs to offer their RG and bandwidth for other users, referred to as visiting users (VU). Next to the VUs the RG owners may use the gateway themselves. This kind of users is called home users (HU). Like commercial hotspots today, potential business will motivate APOs to open up their RGs for public use.

Figure 1 shows the physical connection and dataflow of the common approach with (pink double line) as well as the potential additional parties of the OBAN approach (coloured blue). The physical dataflow of the OBAN approach is coloured orange.

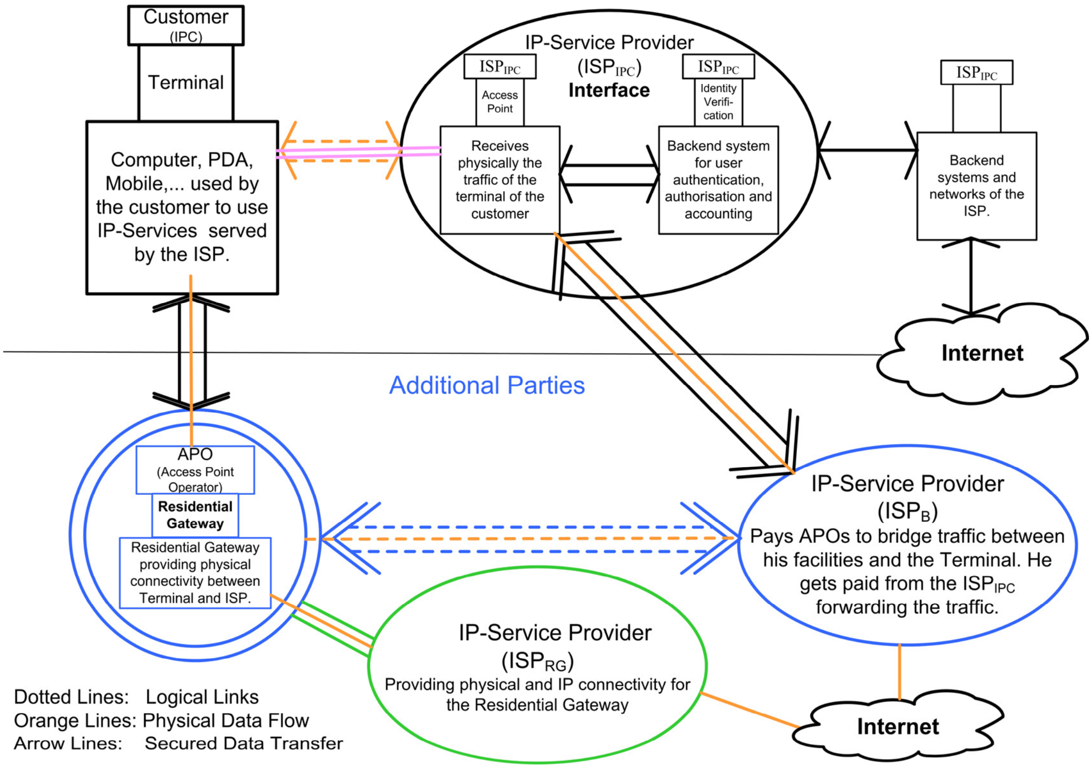
Customer
(IPC)
Terminal
Computer, PDA, Mobile,... used by the customer to use IP-Services served by the ISP.
IP-Service Provider
(ISP$_{IPC}$)
Interface
ISP$_{IPC}$
Access Point
Receives physically the traffic of the terminal of the customer
ISP$_{IPC}$
Identity Verifi-cation
Backend system for user authentication, authorisation and accounting
ISP$_{IPC}$
Backend systems and networks of the ISP.
Internet
Additional Parties
APO
(Access Point Operator)
Residential Gateway
Residential Gateway providing physical connectivity between Terminal and ISP.
IP-Service Provider
(ISP$_B$)
Pays APOs to bridge traffic between his facilities and the Terminal. He gets paid from the ISP$_{IPC}$ forwarding the traffic.
IP-Service Provider
(ISP$_{RG}$)
Providing physical and IP connectivity for the Residential Gateway
Internet
Dotted Lines: Logical Links
Orange Lines: Physical Data Flow
Arrow Lines: Secured Data Transfer

Figure 1: Data flow and parties of the OBAN approach

The OBAN approach decouples the physical connection between the ISPs and their IP-Customers. The contractual partners are no longer directly connected to each other, but through additional parties. This leads to a higher technical and business flexibility but it also increases the overall system complexity in terms of a rising number of technical components, functionality and parties with varying intentions. Especially the additional parties with their different trust relations based upon contractual agreements imply the need of security mechanisms that enable each party to preserve and enforce their monetary and legal interests. Since the dedication of OBAN is to be used by a large number of individuals within many different and distributed applications, which might not be known in advance, the security mechanisms should not only be effective for known incidents but also for incidents which appear when the system is established and operated.

III. Security Problem Model

OBAN specific elements are additional organizational structures and technologies which enable the more efficient and flexible way of provisioning IP-Access and IP-Services. To identify the security needs, generic party constellations are of interest. The trust relation of each party relationship will constitute the security needs for the design, implementation and operational environment of the OBAN security architecture. The relationships and associated intentions within these relationships of the OBAN parties are modelled in the security problem model.

A. IP-Customer (IPC) and IP-Service Provider (ISP)

Service consuming and provisioning are the main characteristics of the IPC and ISP relationship. This may implicate that the intentions of the IP-Customer and the ISP are conflictive. The IPC wants to get the services as cheap as possible, whereas the ISP wants to get a maximal paid for his services. Main values to protect for both sides are the accounting parameters describing the services provisioned - from the ISP side - nd for the services consumed from the IPC side. In the OBAN scenario the parties are not physically connected to each other but via other devices not being in their responsibility (see Figure 1). That is why special efforts is employed on items such as identity proof, service delivery proof to a specific identity as well as service provisioning protection against other parties. Service like non-repudiation, data and privacy protection and also protection against illegal traffic analysis are needed. An additional interest of the IPC is that the ISP should in general not be able to locate the IPCs access point he consumes IP-Services from, if not the IPC explicitly wants the ISP to know this. Finally, a common interest of both parties is to avoid any non-intended interference by other parties concerning the service provisioning and service consuming actions.

B. IP-Customer (IPC) and Access Point Operator (APO)

Technically, these have a direct relationship and legally, they have indirect relationship. The business intention of the APO is that he gets paid for the data traffic he conveys between his ISP and the IPC. Therefore he must be able to prove to against his ISP how much traffic he has transferred from Terminals through his access point. In case an IPC causes illegal or technical problems, the APO must be able to disconnect it. If the IPC causes legal and/or financial damage to the APO, the APO must be able to prove the course of events and the identity of the IPC later on. The IPC, on the other hand, may want to operate anonymously to the APO, which he has normally no direct contractual relationship with. It has to be ensured that the identity of the IPC is only accessible to legitimated entities in any situation. Moreover the data the IPC exchanges over an RG should not be accessible to the APO. The IPC has the interest to be able to prove from where, how much and which quality of traffic he consumes from a specific RG in case of dispute.

C. Access Point Operator (APO) and IP-Service Provider (ISP)

The ISP_{RG} provides IP-Services to the RG only, and will be paid for the provisioned services. The RG bridges the data from the Terminals to another IP-Service Provider, which is called ISP_B. The ISP_B forwards the bridged Terminal from the RG to the IPCs ISP. This ISP will pay the ISP_B for his services and the ISP_B pays the APO for the bridged data. The APO might not only bridge for one but for several different ISP_Bs. One simplifying condition is given when the ISP_B has the responsibility for the RG. A more complex situation can be designed where any of the IPC, ISP and APO configurations can be applied in any cascading way. This might be of interest for technological or business relevant cases to achieve higher access coverage, availability, bandwidth and so on.

In all these cases the APO must be able to prove the amount of the traffic from a IPCs Terminal that has been bridged to an ISP. It is also in the interest of the APO to get a cost absorption confirmation from an ISP for the bridging services he is going to deliver for an IPC. The APO will have to request a confirmation from an ISP since he has normally no contractual relationship with the IPCs.

The ISPs intention is to bridge only traffic, delivered from RGs they can trust i.e. that the RGs work properly and/or that they have a contract with APOs of the RGs. Moreover in a legal case the ISP must be able to prove in a binding way to the other ISP that the operations take place while a service provisioning session of an IPC session is bridged. That is why the ISP needs to identify the relation of RGs, IPCs, services provisioned, as well as service provisioning confirmation of the IPCs ISP.

D. IP-Service Provider and IP-Service Provider

IP-Service Provider normally provides IP-Services. But ISPs can also be a consuming entity in the OBAN approach. Some ISPs may offer IP-Services to other ISPs. Therefore the ISP must relate consumed IP-Services from own customers as well as the consumption from foreign ISPs on behalf of own customers. The party of ISPs can be divided into 2 major groups:

- **ISP_{RG}**: is an IP-Service provider who serves IP-Services directly for interfaces (RGs) and is specific for the OBAN approach. The ISP_{RG} has a contract with the RG operator (APO) defining the rules for the IP-Service provisioning for the RG.
- **ISP_B:** is an IP-Service provider who bridges the data traffic between a RG and an ISP_{IPC} and is also specific entity of the OBAN approach. The ISP_B is paid for the data transported between the ISP_{IPC} and its' IPC. The ISP_B pays the APO of the RG for the bridged traffic.

One ISP consuming services from another ISP is interested in Privacy and data protection as well as integrity of the customer's identity, payload and signalling data exchange. He must be able to prove the amount of consumed services for each customer session. In order to prevent unwanted service provisioning and charging, the ISP_{IPC} must confirm an each service provisioning offer originating from other ISPs on the base of an approved IPC services requests. On the other hand, to assure payments for the services provided from one ISP to another ISP, the ISP must be able to prove the consumed services in relation to ISP IPCs sessions and the involved RGs as well as receive confirmation from the service consuming ISP that the IPC's service request will be accepted.

E. IP-Customer (IPC) and IP-Customer (IPC)

IP customers are IP-Service consuming entities. As in the common IP-Service Provisioning Scenario, IP Customers of the OBAN approach use a Terminal (PC, PDA, mobile phone…) in a direct or indirect way to exchange data between their Terminals and other network nodes via an interface that the Terminal is connected to. It has to be ensured that IP-Customers cannot interfere with their communication and Terminal functionality by using RGs or additional ISPs. Especially, aspects such as usability, correctness of accounting, but also session security in terms of privacy and integrity are important issues. This has a special meaning for the relationship of Home Users and Visiting Users. Home Users operate the same RG that they use for network services. Therefore they have a special ability and may have the interest to influence the sessions of the Visiting Users who are using their RG to make an illegitimate profit.

F. Access Point Operator and Access Point Operator

The APOs are paid for bridging traffic between Terminals and IPCs. Therefore, each APO has the interest that its RG is handling the traffic load efficiently. It is therefore necessary that the proportioning of the requesting Terminals between the available RGs is fair. It has to be ensured that the APO cannot manipulate their RGs in such a way that they manipulate other RGs, the Terminals or the ISPs in a manner that other RGs are excluded from fair requesting Terminal proportioning.

G. Rest of the World (Others)

Entities, which are not part of the formerly described parties, are categorized as "Others". Their intentions may vary very much and produce conflicts.

The doted lines in Figure 1 represent virtual dedicated data flow paths which should ensure at least integrity and confidentiality.

IV. SECURITY ARCHITECTURE FOR OBAN

The security mechanisms and procedures employed in the architecture will solve the identified security needs of the security problem model. Main aspects are the gaps of trust between physically connected party pairs, enabling each party to be protected against each other in order to enable them to safeguard their interests.

A. Basic Mechanisms

The basic approach of the architecture is to get confirmations from those party elements, which have a direct trust relation to accept requests or enable services provisioning with the party elements that they have no such direct trust relation with.

Principle: if A and B both have a trust relation with C, but not with each others, the AC and BC relations can be utilised to establish indirect trust also between A and B, and, furthermore, proof for consumption of resources. The model mechanisms provide this in a fashion that also maintains anonymity between A and B if needed. Trust relations imply mutual knowledge of true identity for the entities directly involved (here: A-C and B-C) in the trust relation.

Encryption, digital signing as well as strategic data distribution is employed to provide data protection and privacy. The basic strategy is to give each party just the information enabling them to perform their task and the proofs they need to claim their legal rights. Therefore, the confirmations are digitally signed by the confirming party. Parts of the information given in the confirmations may also be encrypted.

Normally, identity or other relevant information will be accessible between party elements having a direct and mutual trust relation. The party elements, which do not have a direct trust relation can use this encoded confirmations to prove the action taken place by handing them over to party elements, which have access to the encrypted data. The confirmations build the basic anchor for the binding transparency. Logs documenting the actions that have taken place will also relate to the confirmation as well as the accounting and signalling processes. Access control decisions are based on the existence of the correct confirmations as well as data transport protection mechanisms like VPNs.

Next to the dynamic base – the confirmations – there is a static base called trustable identity descriptors. Each element of the parties IPC, APO and ISP has a unique identity descriptor, which can be verified by cryptographic methods. These identity descriptors have to be handled very carefully by the elements, which are described by them, since these descriptors have significance like a passport. Processes have to guarantee that only the legitimated elements have access to the identity descriptor in terms of use, as well as in terms of the descriptor mapping to real identities. Therefore, not only the process of identity descriptor use has to be protected, but also the processes of identity descriptor creation and distribution.

B. Trust Relations

In the OBAN approach different parties with different intentions will have to cooperate in order to enable the desired goal and thus fulfil their intentions. In order to ensure that the cooperation between the parties can be enforced in an way the parties have agreed to, so-called trust relations have to be established between them. In the architecture design two kinds of trust relations are used.

- Direct Trust Relations (DTR) are established by organisational procedures like contract conclusions, formal agreements and so on. The involved parties do know each other and determine the base as well as rights and duties of their cooperation. Upon these rules violations will be handled legally. The coverage of the direct trust between parties relates to these rules.
- Indirect Trust Relations (ITR) are ad hoc established trust relations between parties who do not know each other explicitly. The issuer of the confirmation certifies against the other party he has a Direct Trust relation with, that he will guarantee the rules and duties defined in the confirmation.

Indirect Trust Relations are a basic security mechanism to establish technical connectivity as well as to collect accounting information and prove actions taken place.

Using Indirect Trust Relation for the OBAN security architecture implicates that Direct Trust Relations are established between *IPC and* ISP_{IPC}, *APO and* ISP_{RG}, *APO and* ISP_{B}, ISP_{IPC} *and* ISP_{B}.

To establish a service session between the IPC and his ISP_{IPC} indirect trust relations have to be established between *IPC and APO*, *IPC and* ISP_{RG}, *IPC and* ISP_{B}, *IPC and* ISP_{B}, *APO and* $ISP_{IPC.}$

The devices, physically connected to each other enabling the direct data flow for an IP-Service session are *Terminal – RG*, *RG – ISP access point facilities* and *ISP – ISP IP service provisioning facilities* via Internet or dedicated lines.

The correlation of physical connection and direct trust relations provides operations to establish indirect trust relation in order to enable a trustable IP-Service provisioning. Figure 2 shows the correlation of the Trust Relation Types in relation to the path along which data are exchanged.

C. Trusted Points

The concept of establishing dynamic trust relations (Indirect Trust Relations) as well as the strategic information distribution is based upon processing instances which can be trusted to operate the way they are dedicated for. These instances are called Trusted Points. Trusted Points are devices with a functionality proven to be correct. These functions include mecha-

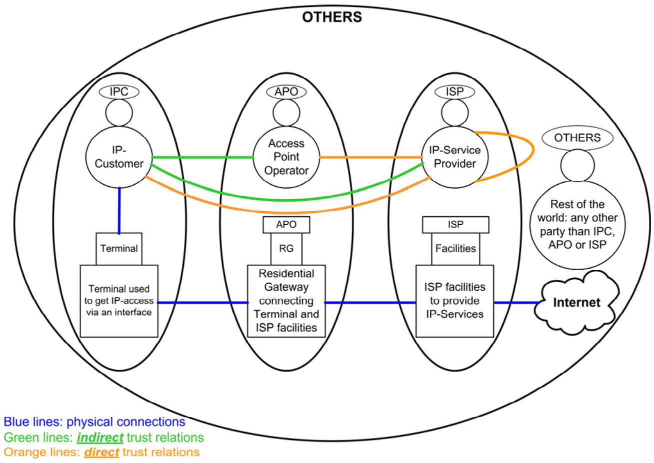
OTHERS
IPC
IP-Customer
APO
Access Point Operator
ISP
IP-Service Provider
OTHERS
Rest of the world: any other party than IPC, APO or ISP
Terminal
Terminal used to get IP-access via an interface
APO
RG
Residential Gateway connecting Terminal and ISP facilities
ISP
Facilities
ISP facilities to provide IP-Services
Internet
Blue lines: physical connections
Green lines: indirect trust relations
Orange lines: direct trust relations

Figure 2: Direct and indirect Trust Relations of the parties

nisms to verify their integrity during runtime. Trusted Points have to be placed at several locations within the system in a way that regularised system operations can only be performed involving one or several of them. Typically, Trusted Points perform security critical tasks like calculating policy decisions, enforce decisions, keeping identity descriptors, and perform also encryption and digital signing.

With the functions of the Trusted Points it can be verified that all pieces of information that each OBAN party holds fits to each other and therefore proves the action(s) taken place in a binding way. In the OBAN approach Trusted Points have to be placed in the Terminal, Residential Gateway as well as in the access facilities of the ISPs.

D. Basic Operations of the parties and devices

The intention for the OBAN security is to enable at least the same quality of the security like the common IP-Service provisioning practice today. Therefore the OBAN security architecture has to solve additional problems concerning the session establishment and also session operations including handovers and session termination.

1) Session establishment

Before an RG can bridge it has to be enabled by the ISP_B. The ISP_B validates the RG and postulates the RGs integrity by sending an Access Request Destination Ticket (ARDT). The ARDT proves the identity of the RG as well includes information for the Terminals how to contact the $ISP_{B.}$

a) Terminal – RG

The Terminal RG access starts with establishing a physical connection between the Terminal and the RG. Physical and organisational compatibility tests are performed. Success implies that the ARDT that the RG has sent to the Terminal has been verified (by the Terminal). If the tests and verification have been successful the Terminal generates and sends an identification token TID_{RG} to the RG which is unique for each RG.

$$TID_{RG} = sign_{Term}(enc_{PbK\text{-}IPC}(ID\_IPC, ID\_Sub) + ID\_P\text{-}IPC)$$

This is to ensure that the RG can recognize but not track the IPC. The token describes the ID of the Terminal and IPC as well as the Identity (ID_P-IPC) to the entity that can resolve the encrypted IDs. Based upon the ARDT and TID_{RG} a protected Service Level negation is performed between RG and Terminal resulting in a Request Origin Ticket (ROT), encrypted by the Terminal and an Access Service Level Suggestion (ALS)

$$ROT = enc_{PbK\text{-}ISP\_B}(TID_{RG}+ARDT+PbK_{Term}+Timestamp)$$
$$ALS = sign_{RG}(TID_{RG}, Parameter, IP\text{-}C_B, Timestamp)$$

b) Terminal – ISP_B

In the next step the Terminal starts the negotiation with the ISP_B. Using the address provided within the ARDT the Terminal will send a Service Level Request (SLR) to the ISP_B via the RG.

$$SLR = sign_{IPC}(ROT, ALS, Timestamp)$$

The ISP_B decodes the received SLR and verifies the encoded information to ensure that the IPC is a valid customer of an ISP that the ISP_B has a Direct Trust Relation with. Next to the IPC the RG is verified in relation to the information coded in the ROT. In case all verifications are successful the ISP_B opens up a Terminal session generating a Bridging Session Suggestion (BSS)

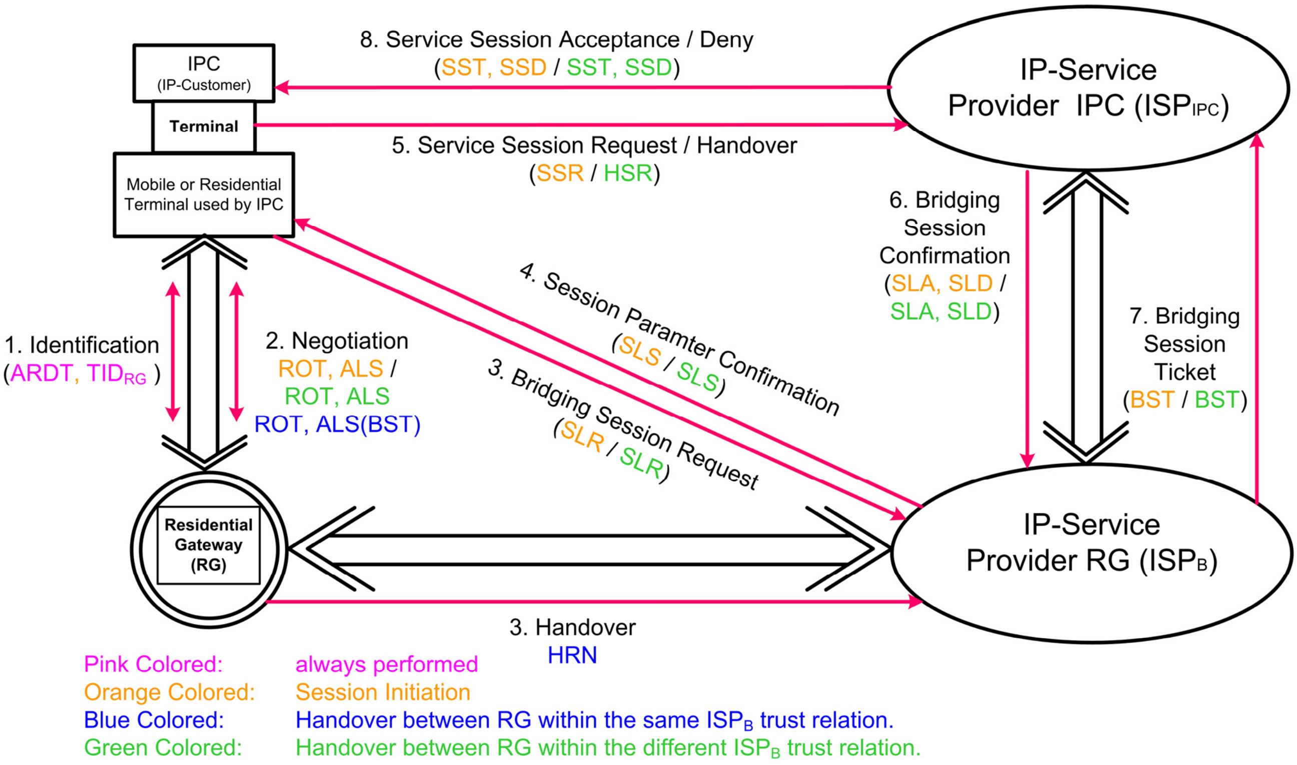
8. Service Session Acceptance / Deny
(SST, SSD / SST, SSD)
IPC
(IP-Customer)
Terminal
Mobile or Residential Terminal used by IPC
IP-Service Provider IPC (ISPIPC)
5. Service Session Request / Handover
(SSR / HSR)
6. Bridging Session Confirmation
(SLA, SLD / SLA, SLD)
4. Session Paramter Confirmation
(SLS / SLS)
3. Bridging Session Request
(SLR / SLR)
1. Identification
(ARDT, TIDRG)
2. Negotiation
ROT, ALS /
ROT, ALS
ROT, ALS(BST)
7. Bridging Session Ticket
(BST / BST)
Residential Gateway (RG)
IP-Service Provider RG (ISPB)
3. Handover
HRN
Pink Colored: always performed
Orange Colored: Session Initiation
Blue Colored: Handover between RG within the same ISPB trust relation.
Green Colored: Handover between RG within the different ISPB trust relation.

Figure 3: Session Initiation and Handover

BSS = (ID-ISP$_B$, SessionParam, Timeslot, Validity)

which is associated to the ROT. The “Timeslo”t parameter is used instead of a timestamp in order to ensure that a Terminal can not be tracked by the RGs. In addition to the BSS, the ISP$_B$ generates an IP-Address (IP-H$_B$) for the Terminal which is associated with the IP-Address (IP-C$_B$) that the RG has assigned to the Terminal. All information needed by the Terminal and IPCs is coded into the Service Level Suggestion:

SLS = enc$_{\text{PbK-Term}}$(sign$_{\text{ISP-B}}$(AST, BSS, SLA, SLD, Timestamp, Validity))

This includes an Access Session Ticket (AST):

AST = sign$_{\text{ISP\_B}}$(ROT, SessionParameter, Timestamp, Validity)

which enables the Terminal to have signal communication with IPC’s ISP via the RG. The Service Level Acceptance and Service Level Denial

SLA = sign$_{\text{ISP\_B}}$(ROT, IP-H$_B$, DeliveryParamter, BSS)
SLD = sign$_{\text{ISP\_B}}$(ROT, IP-H$_B$, DeliveryParamter, Message),

are used by the ISP$_{\text{IPC}}$ to indicate the ISP$_B$ whether the BSS is accepted or not. After the Terminal has received the SLS from the ISP$_B$ it verifies the signatures and the encoded BSS and generates a Service Session Request (SSR):

SSR = enc$_{\text{PbK-ISP\_IPC}}$(sign$_{\text{IPC}}$(SLA, SLD, ID-IPC, ID-Subscription, ID-Terminal, Parameter, Timestamp, Validity))

c) Terminal – ISP$_{IPC}$

Using AST the Terminal will be enabled via the RG to send SSR to the IPC’s IPC. The ISP$_{\text{IPC}}$ will verify the signatures and the IPC subscription parameter to correlate with the Session parameter indicated within the BSS of the SLA. If the ISP$_{\text{IPC}}$ accepts the SSR it associates the Terminals IP-H$_B$ IP-Address to the home address of the IPCs subscription IP-H$_{\text{IPC}}$. In case it does not accept the SSR a Service Session Denial (SSD) is sent back to the Terminal immediately:

SSD = sign$_{\text{P-IPC}}$(ROT, Timestamp, Message)

d) ISP$_{IPC}$ – ISP$_B$

Due to the ISP$_{\text{IPC}}$ decision the ISP$_{\text{IPC}}$ will respond to the SSR by sending either a signed SLA or SLD token to the ISP$_B$. In case the ISP$_B$ receives the SLA he will send back a Bridging Session Ticket (BST) = sign (BSS). If a SLD is received the signalling session between Terminal and ISP$_{\text{IPC}}$ is closed.

e) ISP$_{IPC}$ – Terminal

After the ISP$_{\text{IPC}}$ has received the signed BST from the ISP$_B$ it verifies whether it correlates to the BSS and generates a Service Session Ticket (SST)

SST = enc$_{\text{PbK-IPC}}$(sign$_{\text{P-IPC}}$(ID_Session, ID-SST, Session-Paramter, Timestamp, Validity, BST))

If the BSS does not correlate a SSD is sent to the Terminal. When the Terminal receives the SST or SSD it ends the signalling session. In case it has received a SST it establishes a VPN connection to the ISP$_{\text{IPC}}$. IP-Services Session is established and IPC can consume IP-Services from his ISP.

2) Session Operation

The main aspects of the session operation to be discussed are handovers between RG of the same ISP$_B$ and different ISP$_B$s. Both handover types start with the actions like the session initiation. Considering the ARDT, the Terminal can identify if it is connected to an RG it that it has a valid BST for or not.

a) Handover to a RGs of an already authenticated ISP$_B$

In case the Terminal has a BST which relates to the ARDT of the RG to handover to, it generates a ROT and a BST instead of negotiating with the RG. The RG verifies the BST and will grant access if the BST is valid and the Session Parameter described in the BST can be offered. The RG sends Handover Recognition Notice (HRN) = sign$_{\text{RG}}$(ROT, ALS, BST, Timestamp) to the ISP$_B$.

b) Handover to an RGs of an ISP$_B$ “not authenticated”.

This handover type requires all session initiation actions to be performed till the communication between Terminal and ISP$_{\text{IPC}}$ is established. Instead of the SSR the Terminal sends a Session Handover Request (SHR) to the ISP.

SHR = enc$_{\text{PbK-ISP\_IPC}}$(sign$_{\text{IPC}}$(SLA, SLD, ID-IPC, SST))

According to the session initiation the confirmation is sent to the ISPB and the Terminal will receive a new SST with an increased ID-SST.

3) Session Termination

Any party can terminate a session by sending a session close ticket.

V. CONCLUSION

Security requirements and architecture have been presented enabling a Broadband Access Network with new parties between customers and ISPs without sacrificing security.

[1] Thomas J. Wilke, Tor Hjalmar Johannessen, “Open Access Environment Architecture”, Deliverable D5, IST 6 Project OBAN, 2004, pp. 36–48, 67–87.

[2] E.. Edvardsen, “Fixed and Mobile Convergence” Proc. BroadBand Europe 2004., Belgim, December 2004,.