

Open IN Service Provider Access

Dr. Audun Jøsang

*Department of Telematics
The Norwegian University of Science and Technology
N-7149 Trondheim
Norway
email: ajos@item.ntnu.no*

Abstract

Open IN service provider access means that a public telecommunication network operator lets other companies have access to special parts of the public network in order to provide added value services such as for example freephone or premium rate services to subscribers of the public network operator. European regulators have stated that this type of access is needed in order to achieve free competition in the telecommunications sector. It is however not evident how this type of interface should be implemented, and this paper discusses possible solutions. We conclude that an interface based on the INAP protocol on top of the TCP/IP protocol stack combined with an interworking function is the best solution.

1 Introduction and background

It is generally accepted today that the business of providing plain old telephony is different from the business of providing value added services to telephony. However, in practice this is not as evident as it may sound. The development of telecommunications during the past decades has resulted in a monolithic structure for Intelligent Networks (IN) where speech path swithing and service logic have been closely integrated, and opening up networks to external service logic operators does not come naturally in this context. In the following we will use the term *Public Network Operator* (PNO) to designate the company providing subscriber access and network facilities, and the term *Service Provider* (SP) to designate the company providing IN services through the network of a PNO. The access point to the public network will be called *IN Service Provider Access Interface* (SPAI). However technically challenging it may be, there are strong reasons for creating open access to public networks in order to provide IN

services. IN service provision is already a huge market, and if only PNOs were allowed to provide IN services it would create an undesirable monopoly. The market regulators are already aware of this situation and are trying to enforce free competition in the IN service market. The European Commission has for example issued the Interconnection Directive[1] which has the purpose of ensuring universal service and interoperability for both fixed and mobile networks. The Interconnection Directive states that “*fixed and mobile operators with significant market power must meet all reasonable requests for access to their network ...*” (Art.4.2). The term “reasonable” means that access should be granted if it is required for offering a service, if it is technically possible, and if it does not threaten the network integrity. Guidelines for the operational aspects of network integrity are given in the recommendations on network integrity [5] published by the European Committee for Telecommunications Regulatory Affairs (ECTRA).

Furthermore, the Interconnection Directive states that interconnection agreements between the involved parties should be non-discriminating, meaning that no discrimination in own use and third party use is allowed, and that the same conditions shall be offered to all the parties asking for interconnection (Art.6.a). Interconnection agreements shall also be transparent, meaning that the agreements must be open and made available for all interested parties (Art.6.c). It is further stated that interconnection agreements shall be cost-oriented, meaning that the interconnection tariffs must be based on the associated costs of offering the interconnection (Art.7.2).

Finally, the Interconnection Directive states that adherence to relevant technical standards may be made compulsory (Art.13). On this background, cost-orientation would imply that the additional cost for service providers when connecting to a network that deviates from existing standards has to be covered by the network operator. Non-standard solutions would in addition break the principle of non-discrimination because it for example would favour interconnecting equipment from the vendor that delivered the network equipment. In the absence of relevant standards, the principles of cost-orientation and non-discrimination are severely weakened, and regulation such as the Interconnection Directive alone will not be sufficient to give SPs access to public networks. The existence of relevant standards is thus crucial, and this will be discussed below.

Another EU directive that specifically targets IN SP access is the Revised Voice Telephony Directive[2] (RVTD) which has the purpose of ensuring the availability throughout the EU of good quality fixed telephone services and to define the set of services to which all users should have access in the context of universal service at an affordable price. The RVTD states for example (Art.16) that “*National regulatory authorities shall ensure that organisations with significant market power in the provision of fixed public telephone networks deal with reasonable requests from organisations providing telecommunications services for access to the fixed telephone network at network termination points other than the commonly provided network termination points*”. This type of access is also referred to as *Special Network Access* (SNA), and Art.16 of the RVTD really constitutes the regulatory basis for open IN service provider access.

In order to define a standardized IN service provider access interface a set of requirements must first be defined, and ETSI NA6 is presently finalising two documents that define the basic requirements that must be met by the IN SPAI. The first document called *Service provider access requirements*[3] has as scope to present generic functional requirements regarding service provider access, as seen from the SP's point of view. A second document called *Network operator's requirements for the delivery of service provider access*[4] presents similar generic functional requirements, but this time as seen from the PNO's viewpoint in order to create a balance. The former document focuses on necessary functionality for creating services whereas the latter focuses on network integrity, security, charging and related aspects. Both documents are supposed to be finalised in 1999, and will constitute the input to the protocol groups within ETSI that will develop the standardised protocol. The ETSI protocol groups are ETSI SPS1 (ISUP), SPS3 (INAP) and SPS5 (DSS1), with between brackets examples of their current work. Formally, It is still open whether a new interface (e.g called SPAI) or a combination of enhancements to the existing interfaces is to be developed. However, our view is that enhancing current interfaces is the only practical way forward in order to limit investment costs and meet time constraints.

It is not at all evident that standardisation in this field will be successful because of the powerful market players that might find that it is in their interest to define their own solutions. Broadly speaking, PNOs are interested in limiting or carefully controlling the functionality of the SPAI as well as delaying its introduction as long as possible. SPs on the other are interested in a flexible and powerful SPAI but do also see the advantage of limiting its functionality in the first phase in order to have a functioning SPAI as soon as possible. Regulators in many countries have already asked PNOs to provide SPAI on request from SPs, but these interfaces have usually been based on routing calls from the PNO to the SP and back via trunks or normal subscriber lines, which in the definition of the RVTD can not be called special network access. The very fact that circuit related SPAIs exist and are expected to be used in the future has for example resulted in ETSI NA6 defining separate functional requirements for so-called circuit related service provider access in the mentioned documents [3] and [4].

In parallel to the standardisation activities, both manufacturers and operators are proposing and implementing solutions for SPAI, and if one particular implementation is made open and gets sufficient market acceptance it can be called a de facto standard and will satisfy the requirement of non-discrimination as stated in the Interconnection Directive. On the other hand, if many solutions continue to co-exist, it will result in discrimination and cost-ineffectiveness.

It can also be questioned whether a standard SPAI is achievable at all and whether it is to anyone's advantage. Telecommunication networks are in constant evolution, and every innovation opens up for a multitude of new possibilities. A standardised SPAI will in many ways be relatively frozen and not allow a SP to take advantage of new innovations as long as it has not been included in the standard. The very concept of special network access is defined as " ... *not commonly provided* ..." (RVTD [2] Annex II, part 1), and that can hardly be said about a standardised interface that is commonly used by SPs. In that sense, a PNO should therefore deal with any request for access to all parts of its

network, through standardised and non-standardised interfaces, as long as it can be judged reasonable. In the imaginary situation where for example INAP (Intelligent Network Application Part) and SS7 (Signalling System Nr.7) were standardised as the SPAI it would still not allow SPs to implement services that are not based on INAP such as for example handling SMS (Small Message Service) messages. The concept of special network access is therefore more illusive that one should think at first glance and indeed seems to be something that can not be captured once and for all within a standard.

2 Technical solutions for open IN service provider access

In this section we will discuss a set of possible solutions for implementing open IN service provider access, of which some are already in use or under implementation. All network elements in the IN architecture illustrated in Figure 1 can in principle have a SPAI, but some are more suitable than others.

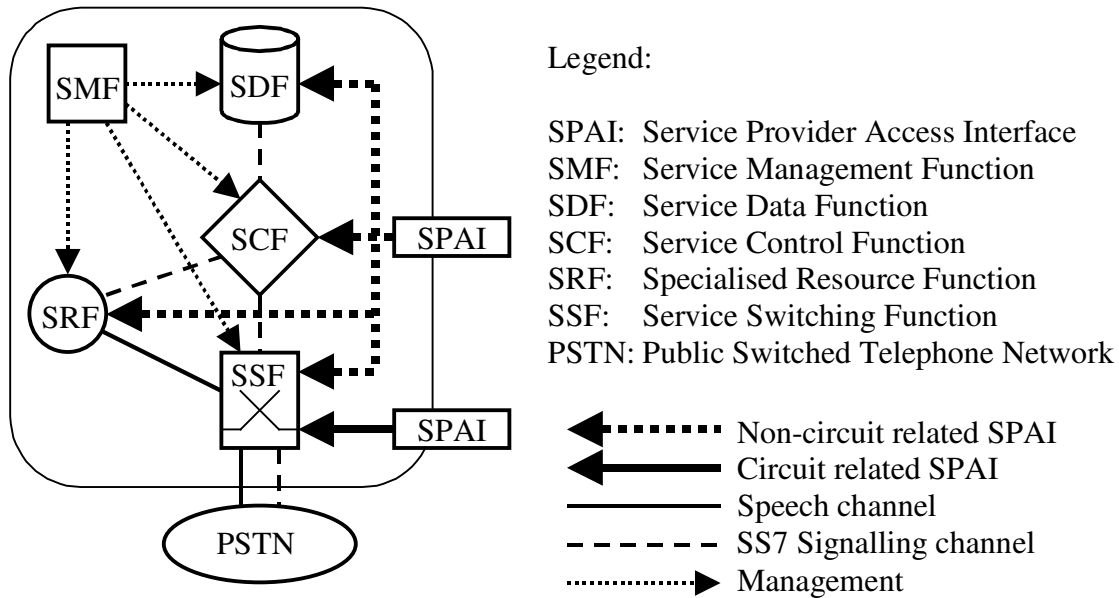


Figure 1. Single operator IN architecture with proposed SPAI points

We will assume that the non-circuit related SPAI will be on the SCF or the SSF using INAP or a similar protocol, and that the circuit related SPAI will be on the SSF using for example ISUP (ISDN User Part) trunk signalling, DSS1 (Digital Signalling System 1) subscriber signalling, or some older pre-ISDN signalling protocol.

2.1 Service provider access through middleware

Middleware is the general term used for SW that provides platform and location transparency for distributed applications, i.e. that the applications do not have to worry

about where or on what type of SW platform a particular resource can be accessed, as it is all sorted out by the middleware. The CORBA (Common Object Request Broker Architecture) defined by the OMG (Object Management Group) is the most prominent example of middleware and is presently implemented in a multitude of applications.

2.1.1 SPAI based on CORBA middleware

CORBA could for example be used as middleware between equipment respectively at the PNO's and the SP's premises, as well as between equipment within the PNO's internal network as shown in Figure 2. A more detailed description can be found in [6].

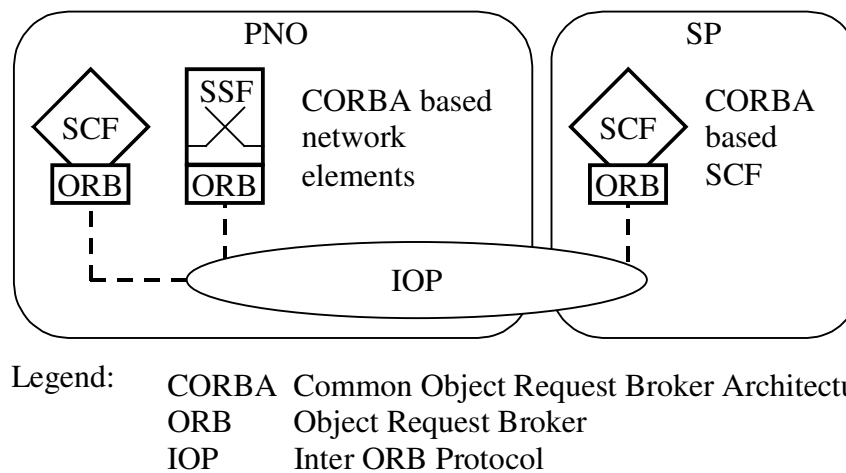


Figure 2. SPAI based on CORBA and IOP

The ORB (Object Request Broker) is the functional SW entity that identifies the location of a needed resource and that provides it to the application through the IOP if it is located in another network element. The IOP (Inter Orb Protocol) is the protocol connecting the different ORBs. In this way, the application does not need to know where the resource is located. The protocol stack carrying the IOP can for example be SS7 or any other protocol stack that provides reliable transport service.

CORBA is an object oriented architecture and it is therefore suitable to use a modern object oriented language like Java for implementing this solution. By using a Java Virtual Machine as SW platform in each network element all application programs become portable. However, this will require all network elements to be CORBA and/or Java enabled, which is impossible to combine with legacy network elements. This solutions is therefore judged to be premature.

2.1.2 SPAI based on an INAP/CORBA gateway

A major concern for many PNO is how to protect or shield their SS7 network from SPs because it in their view would give SPs more flexibility than strictly needed from the SPAI. One way to do this is to map INAP messages to CORBA operations which then can be reached by other CORBA based platforms as illustrated in Figure 3 and also described in [6]. The gateway also avoids implementing CORBA in existing network elements in the PNO's domain.

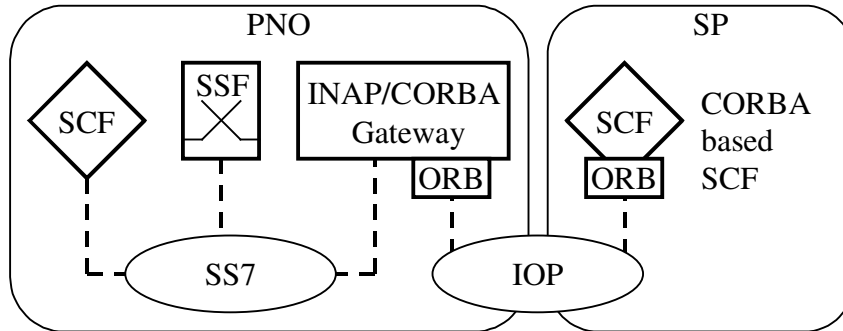


Figure 3. SPAI based on INAP/CORBA gateway

This and the previous solution can make service creation by the SP very simple because CORBA hides the fact the SSP is a remote unit, and makes it seem as if the SSP was local. On the other hand, the SP does only get access to the functionality available through the mapping in the gateway, and this is functionally equivalent to an API which will be described next.

2.2 SPAI based on API

This solution as illustrated in Figure 4 is very similar to the INAP/CORBA gateway described in the previous section. The difference is that it is using an application protocol interface (API) not necessarily based on CORBA. The Parlay API [7] is one such

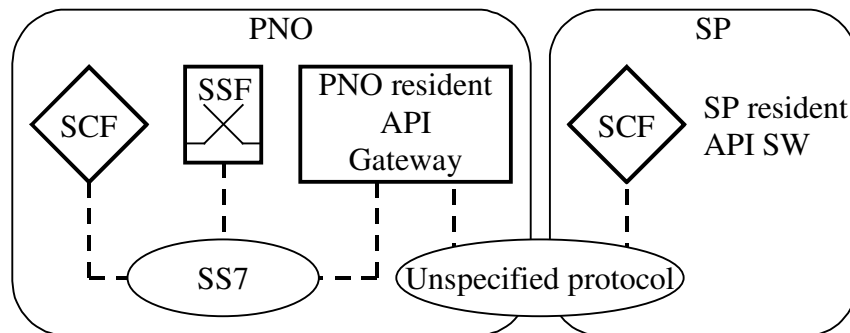


Figure 4. SPAI based on API

example, which explicitly does not specify the physical connection and the protocol to be used.

The network resident part of the API consists of a gateway which offers a given set of functions, and is connected to SS7 in the PNO's network. The API can provide the necessary security facilities in order to protect the PNO's network from failure in the SP's service logic.

2.3 SPAI based on INAP and SS7

The most straightforward solution is to implement the SPAI by giving SPs access to INAP/SS7. In order to maintain integrity and security an *Interworking Function* (IWF) will be needed between the PNO's and the SP's domains, in practice implemented both in the PNO's and the SP's domain, as illustrated in Figure 5.

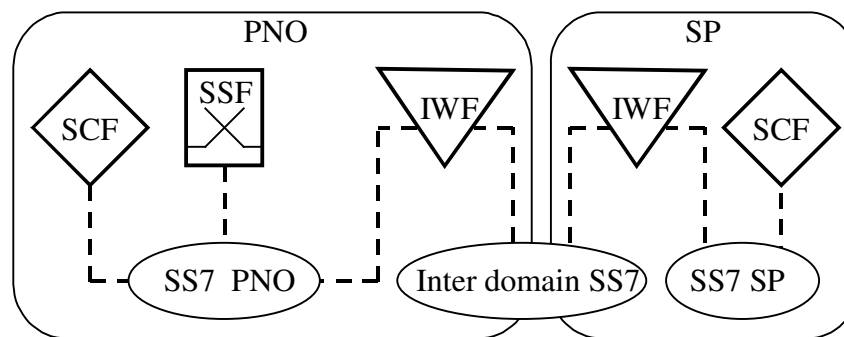


Figure 5. SPAI based on INAP and SS7

The IWF acts as a firewall between the external and the internal SS7 networks and thereby splitting SS7 into separate networks that can only be reached through the IWF.

Using SS7 in the SPAI imposes several problems. Platforms that implement the SS7 protocol stack have been limited to pure telecom applications and remain relatively expensive compared to for example TCP/IP based platforms. New service providers that do not have legacy equipment can in fact choose any other protocol that provides a reliable transport service and use that instead of SS7. The TCP/IP protocol is the most obvious choice, and that will be described next.

2.4 SPAI based on INAP and TCP/IP

Without exception, new SPs will have LANs that are connected to the Internet and will have IT equipment using the TCP/IP protocol stack. Most likely they will not have legacy equipment based on SS7. It will therefore be much easier to purchase and install service

logic on new network elements based on the TCP/IP protocol stack. Figure 6 illustrates how the Internet can be used as transport medium between the PNO and the SP.

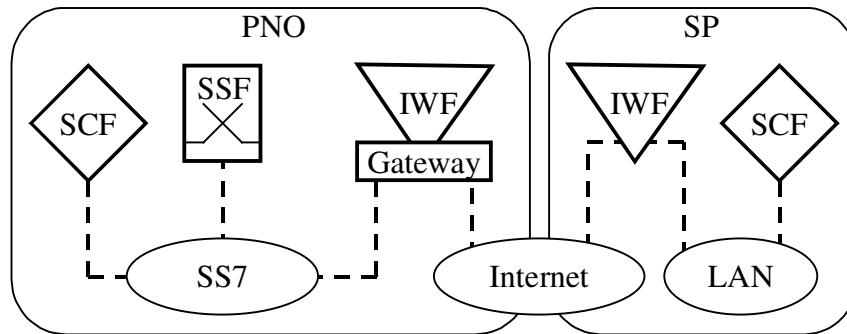


Figure 6. SPAI based on INAP and TCP/IP

The network elements of the PNO must be protected against externally induced failures and inappropriate usage. For this purpose the IWF plays an important role by providing security services including:

- **Data integrity:** Only authorised agents shall be able to create, delete or modify messages. Data integrity can be obtained by message authentication codes, by encryption, by authentication or by digital signatures.
- **Confidentiality:** Only authorised agents shall be able to read messages. Confidentiality is implemented by encryption.
- **Authentication:** The recipient of a message shall be able to verify the identity of the sender. Authentication is implemented by the means of protocols consisting of a sequence of messages.
- **Non-repudiation:** The sender of a message shall not be able to deny having sent the message. In the same way, the recipient of a message shall not be able to deny having received the message. Non-repudiation is implemented by using digital signatures.
- **Accountability:** It shall be possible to trace all actions to identified agents, and agents shall be made responsible for their actions.

In order to provide these security services we propose to use the Secure Socket Layer protocol (SSL) [9] or its standardised version the Transport Layer Security protocol (TLS) [10] between the INAP and the TCP layers. The proposed protocol architecture for the INAP/SSL/TCP/IP solution is illustrated in Figure 7 and compared with the SS7 protocol layers as well as with the OSI reference model.

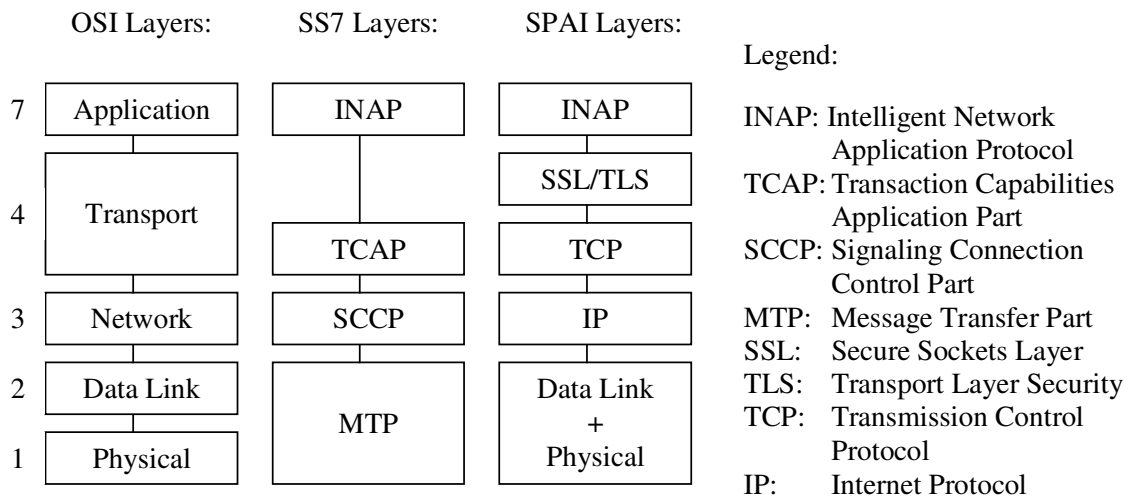


Figure 7. Proposed SPAI protocol architecture for the INAP/SSL/TCP/IP solution

SSL which is based on public/private key cryptography and on public key certificates is already implemented in many applications and have received widespread acceptance in the Internet community. In the context of public key cryptography a certificate is a digital signature on the public key of for example the PNO or the SP, issued by a CA (Certification Authority), guaranteeing the binding between the public key and the identity of its owner. In that way, a SP can use its private key to sign INAP messages sent to the PNO. The PNO will then have the ability to perform authentication by verifying the message with the corresponding certified public key, and will be assured that the messages can be traced and not subsequently be repudiated.

If disputes are to be settled efficiently, the CA will play crucial role by guaranteeing the authenticity of public keys and mediating between parties. The X.509 standard [8] for exchanging public key certificates is already used by commercial CAs, and is the natural choice for establishing a secure infrastructure for open IN service provider access.

2.5 SPAI based on circuit connection

All solutions discussed so far were based on signalling and did not require a physical speech path connection passing through the SP's domain. The typical IN service consists of creating a connection between two arbitrary parties possibly combined with a Specialised Resource Function for user interaction, digit collection etc. The SP will be able to provide this functionality by physically forwarding calls or connecting two separate calls where the SP is either the called or the calling party.

This solution is expensive in operation because two legs are used for each call setup, but also very simple because a standard PBX can play the role of SSF which will require

relatively small investments to start up a business as SP. This solution can be based on 2Mbps trunks (= 30 channels) with ISUP/SS7 signalling or with pre-ISDN channel associated trunk signalling protocols such e.g. R2. This solution can also be based on subscriber lines such as ISDN PRAs (Primary Rate Access = 30 B-channels + 1 D-channel) with DSS1 signalling on the D-channel. The architecture for this solution is illustrated in figure 8 below.

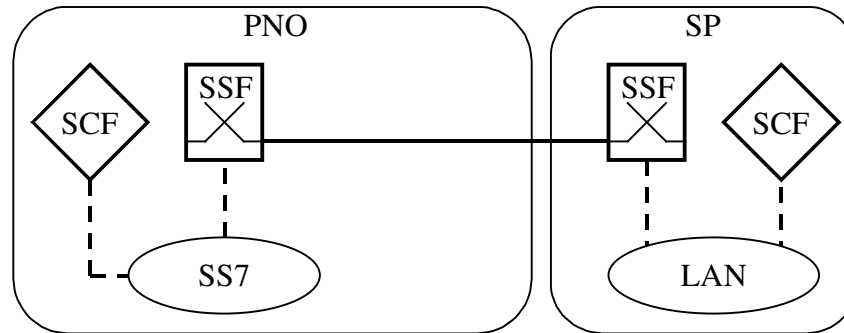


Figure 8. SPAI based on circuit connection

Because of its simplicity this solution has some drawbacks as seen from the SP's viewpoint. In case ISDN PRA with DSS1 signalling is used all call attempts where the SP is the called party must be answered and thereby charged by the PNO, although the IN service might fail and abort so the calling subscriber can not be charged. This solution will also give reduced signalling functionality and thereby limit the range of services that a SP can offer.

3 Conclusion

Service providers can make a significant contribution to the development of new and innovative telecommunication services, can add value to public networks, and can provide users with the freedom of choosing where to buy telecom services. This can only be achieved if the regulatory authorities are willing to enforce the EU directives, and if a good solution for service provider access can be found.

With the multitude of emerging technologies there are several candidates for implementing a SPAI, and many manufacturers and network operators are presently proposing and implementing solutions. PNOs are focusing on the network integrity aspects as well as controlling and possibly limiting the functionality available at the SPAI. The SPs on the other hand are interested in a rich functionality in order to provide competitive and innovative services. Whatever the SPAI will look like it should be as standardised as possible in order to be non-discriminating, but the strong market forces and conflicting interests will make it difficult to reach a European wide consensus in the short term. We have described 6 different solutions, and in our view the best choice is to use INAP with SSL for security on top of TCP/IP.

4 References

1. *Directive 97/33/EC of the European Parliament and of the Council of 30 June 1997 on interconnection in telecommunications with regard to ensuring universal service and interoperability through application of the principle of open network provision (ONP)*, (The Interconnection Directive). The European Commission, 1997.
2. *Directive 98/10/EC of the European Parliament and of the Council of 26 February 1998 on the application of Open Network Provisions to voice telephony and on universal service for telecommunications in a competitive environment*, (The Revised Voice Telephony Directive). The European Commission, 1998.
3. *Service provider access requirements*. DEG/NA-061601. NA6, The European Telecommunications Standardisation Institute, 1999.
4. *Network operators' requirements for the delivery of service provider access*. DEG/NA-061603. NA6, The European Telecommunications Standardisation Institute, 1999.
5. *Recommendation Rec(98)01 - Network integrity*, European Conference Of Postal and Telecommunications Administrations/European Committee for Telecommunications Regulatory Affairs (CEPT/ECTRA), 1998.
6. *Interworking Between CORBA and TC Systems*. The Object Management Group (OMG), 1997. (<ftp://ftp.omg.org/pub/docs/telecom/98-10-03.pdf>)
7. *The Parlay open API specification*. British Telecom, DGM&S Telecom, Microsoft, Nortel Networks and Siemens AG, 1999. (<http://www.parlay.org>)
8. *Recommendation X.509 - The Directory Authentication Framework*, International Telecommunications Union, Telecommunication Standardisation Sector (ITU-T), 1993.
9. *The SSL 3.0 Protocol*, Netscape Communications Corp. Feb.9, 1995.
10. *The TLS Protocol*, RFC2246, Internet Engineering Task Force, January 1999.