Peer to Peer Settlement for Next Generation IP Networks

Using the ETSI OSP Protocol (ETSI TS 101 321) for Cascading Peering Settlements

Table of Contents

1 Introduction

It has been proven that the benefit of a network for its users increases as the number of interconnected networks increases. Therefore open interconnection, or peering, among IP networks benefits all users. However, it is also an economic reality for network operators that interconnection has a cost. In addition, all networks do not benefit, or recover the costs, from interconnection equally. For network operators, open interconnection without a fair and reliable cost recovery mechanism is a very risky business prospect. Network operators are more likely to connect with other networks when interconnect costs can be managed and a clear business case can be proven based on the benefits. To encourage ubiquitous interconnection among networks, an efficient interconnect cost recovery mechanism is needed. The inter-network cost recovery mechanism is known as clearing and settlement of interconnect fees.

In the Public Switched Telephone Network (PSTN) and Mobile phone networks, clearing and settlement of interconnect and roaming transactions are commonly processed by a central third party clearinghouse. The multi-lateral clearing and settlement model prevails in the telecom industry because of the efficiencies and economies of scale that a central trusted clearinghouse can provide to carriers.

The growth of next generation networks (NGNs) and the growing IP interconnection among those networks drives the need to identify an efficient model for managing clearing and settlement of inter NGN transactions – whether they be voice, video, content, gaming or other IP based communication transactions. This paper describes how the ETSI Open Settlement Protocol (OSP) provides a solution for clearing and cascading settlement of NGN peering transactions.

2 Requirements

Before describing the proposed solution, the first step is to understand and define the requirements for NGN clearing and settlement. Those requirements are defined here.

1. Standards based: Clearing and settlement solution must be based on a recognized, international standard to ensure widespread vendor support and global adoption.
2. Use proven technology: Clearing and settlement of transactions is a well defined problem which has been solved in many times in different industries. The NGN clearing and settlement solution should be based on proven techniques and not require the development of new technology.
3. Flexible and adaptive: Clearing and settlement solution must offer the flexibility to be extended for new IP based services as they are developed.
4. Competitive solutions: The model for inter-carrier clearing and settlement must be a model that benefits carriers and their customers without the risk of centralized control that could impede the freedom of NGN operators. The model must enable open competition between competing clearing and settlement solution providers so carriers benefit from lower costs and rapid innovation.
5. Secure: Clearing and settlement model must be secure.
    a. Secure authentication of transacting parties (NGN carriers)
    b. Secure authorization of NGN interconnect or roaming transactions
    c. Ensure data integrity of NGN accounting records
    d. Non-repudiation of NGN interconnect transactions
    e. Auditable

3 The ETSI Open Settlement Protocol

The ETSI Open Settlement Protocol (OSP) was developed by ETSI TIPHON and is officially known as the Open Settlement Protocol (OSP) for Inter-Domain pricing, authorization and usage exchange - Technical Specification 101 321. Version 4.1.1 was released on 2003-11.

The OSP protocol is a set of XML (eXtensible Markup Language) messages defined for transmission over HTTP (Hyper Text Transaction Protocol). As the title describes, the OSP set of messages are defined for authorizing and accounting for inter-domain transactions. The vast majority of current OSP implementations manage interconnection among VoIP networks. However, the OSP standard anticipated future applications and V.4.1.1 is fully functional for clearing and settling services such as video and new, yet to be defined, services.

OSP was created to utilize the proven security features available from Public Key Infrastructure (PKI) technology to ensure secure transactions. While PKI technology is not part of (or required by) OSP, the OSP implementation examples in this paper include the PKI techniques to ensure secure clearing and settlement.

4 How OSP Settlement Works

The business model benefits of a central, trusted clearinghouse providing multi-lateral clearing and settlement of transactions for a large network of trading peers has been

proven in many industries, including the legacy PSTN. Therefore, the OSP standard was created to support a clearinghouse model for clearing and settlement of NGN transactions. This section describes the basics for enabling a trusted third party clearinghouse to clear and settle IP transactions among of group of next generation networks.

4.1 Establishing a Trusted Infrastructure

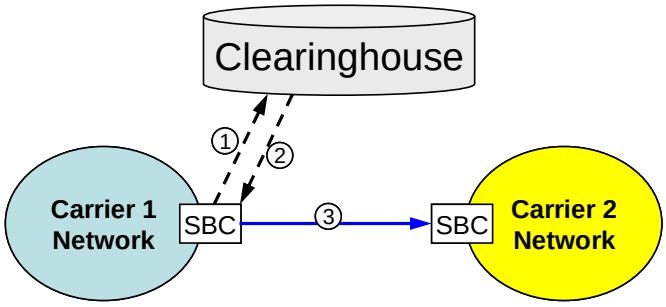
The first implementation task is to create a trusted relationship between the central clearing and settlement authority (clearinghouse) and each NGN peer. While each NGN is a discrete IP domain, the role of the clearinghouse is to create a single, trusted *administrative* domain for a network NGN peers. Since PKI techniques are well known, the steps to create a trusted infrastructure using asymmetric PKI services are discussed only briefly.

1. The clearinghouse is the PKI certificate authority for the network of NGNs. The clearinghouse publishes its certificate which includes its public key.
2. Each NGN peer obtains the certificate and public key of the clearinghouse.
3. Each NGN peer generates its own public/private key pair.
4. Each NGN peer sends a certificate request to the clearinghouse.
5. The clearinghouse signs each certificate request with its private key and returns each signed certificate to the respective NGN peer.

With the completion of these steps, the clearinghouse establishes a trusted relationship with each peer. More importantly, this trusted relationship can be used to securely authorize and account for IP transactions among any two peers, even if the two peers are anonymous to one another. The clearinghouse and its network of NGN peers become a trusted administrative domain for secure clearing and settlement of inter-domain IP sessions.

4.2 Authorizing an Inter-Domain Session

This section describes how a central clearinghouse can use the OSP protocol and standard PKI services to authorize an inter-domain session between two NGN peers. The diagram below presents two NGN peers and a central clearinghouse which is the trust authority for inter-NGN clearing and settlement. In this diagram, Carrier1 is requesting authorization for an interconnect session with Carrier2.



0. The first step, which is not included in the diagram above, is route discovery. Carrier1 must determine that Carrier2 is the destination network for the IP

session. There are a wide variety of route discovery options. For example, the destination can be determined from 1) static route tables configured in Carrier1, 2) an ENUM query to a route server, 3) a SIP INVITE to a redirect server or 4) an OSP query to a route server. (While an OSP AuthorizationRequest can be used for route discovery, the focus of this paper is on clearing and settlement.)

1. Once Carrier1 has determined the destination NGN for an IP session, Carrier1 sends an OSP AuthorizationRequest to the Clearinghouse. Transmission of the OSP AuthorizationRequest can be encrypted using TLS/SSL (Transport Layer Security/Secure Sockets Layer). Typically the OSP AuthorizationRequest would be sent from a device at the edge of the NGN such as a session border controller (SBC), but this is not required. Below is an OSP AuthorizationRequest example for a VoIP call between Carrier1 and Carrier2.

```
<?xml version="1.0"?>
<Message messageId="11703738491" random="1170373849">
<AuthorizationRequest componentId="11703738490">
  <Timestamp>2005-05-12T17:32:57Z</Timestamp>
  <CallId encoding="base64">Call ID</CallId>
  <SourceAlternate type="transport">[Carrier1 IP address]</SourceAlternate>
  <DestinationAlternate type="transport">[Carrier2 IP address]</DestinationAlternate>
  <Service>voice<Service/>
</AuthorizationRequest>
</Message>
```

   This OSP AuthorizationRequest includes the minimum detail needed for secure session authorization and accounting:
   - The Call ID, or session ID for the call.
   - The source IP address for the session which may be different from the IP address of the device which sends the OSP AuthorizationRequest.
   - The destination IP address for the session
   - The service type requested – voice in this example.

2. When the Clearinghouse receives the OSP AuthorizationRequest, it can securely authenticate the message using TLS/SSL authentication. The Clearinghouse then authorizes the interconnect session and returns an OSP AuthorizationResponse to Carrier1. The OSP response may be encrypted using TSL/SSL. Below is an example OSP AuthorizationResponse.

```
<?xml version='1.0'?>
<Message messageId='11703738491' random='21655'>
<AuthorizationResponse componentId='11703738490'>
  <Timestamp>2005-05-12T18:32:59Z</Timestamp>
  <Status>
    <Description>SUCCESS</Description>
    <Code>200</Code>
  </Status>
  <TransactionId>Transaction ID</TransactionId>
  <Destination>
    <CallId encoding='base64'>Call ID</CallId>
    <DestinationSignalAddress>[Carrier2 IP Address]</DestinationSignalAddress>
    <Service>voice<Service/>
    <Token encoding='base64'>OSP Authorization Token</Token>
    <ValidAfter>2005-05-12T18:27:59Z</ValidAfter>
    <ValidUntil>2005-05-12T18:37:59Z</ValidUntil>
  </Destination>
</AuthorizationResponse>
</Message>
```

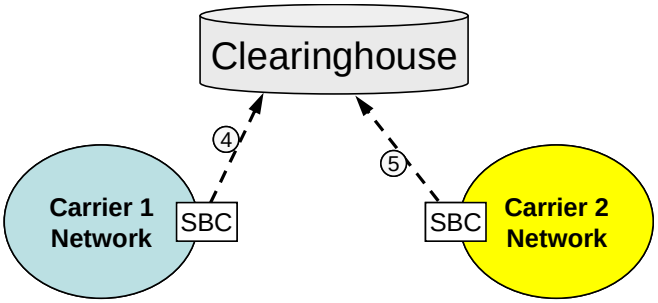
This OSP AuthorizationResponse includes the minimum detail needed for secure session authorization and accounting:

- A unique Transaction ID issued by the Clearinghouse
- The Call ID from the OSP AuthorizationRequest
- The destination IP address from the OSP AuthorizationRequest
- The service type requested – voice in this example.
- OSP Authorization Token which is digitally signed by the Clearinghouse. The token includes the Clearinghouse Transaction ID and session data, such as Call ID, Source IP Address and service type, which can be verified by the destination device from the call setup.

3. The source network includes the OSP Authorization Token in its call setup message to the destination IP address. When the destination device receives the call setup it validates the OSP Authorization Token using the public key of Clearinghouse. (The destination NGN obtained the Clearinghouse public key as described in section 4.1 above.) If the token is validated with the Clearinghouse public key, then the destination can be certain that the specific session (based on source IP address, call ID and service type) was authorized by the clearinghouse. The validated Clearinghouse digital signature on the token is secure proof of the token's integrity and that the Clearinghouse is a trusted party in the authorized interconnect transaction between the two NGN peers, Carrier1 and Carrier2. In addition, the signed token ensures the destination peer that neither the source network nor the Clearinghouse can repudiate the authorized interconnect session request.

4.3 Accounting for an Inter-domain Session

Secure authorization of NGN interconnect transactions is only one half of the secure clearing and settlement process. Secure, reliable call accounting is required for financial settlement between networks. This section describes how the OSP protocol is used by each NGN peer to securely report usage to the Clearinghouse for each authorized interconnect transaction.



4. When the call ends, Carrier1 sends an OSP UsageIndication message to the Clearinghouse. The OSP message can be encrypted and authenticated by the Clearinghouse using TLS/SSL. When the Clearinghouse OSP server receives the OSP UsageIndication message, it returns an OSP UsageConfirmation message which is not shown in this diagram. An example OSP UsageIndication is shown below.

```
<?xml version="1.0"?>
```

```
<UsageIndication componentId="47850982870685430174">
  <Timestamp>2005-05-12T17:33:33Z</Timestamp>
  <Role>source</Role>
  <TransactionId>Transaction ID</TransactionId>
  <CallId encoding="base64">Call ID</CallId>
  <SourceAlternate type="transport">[Carrier1 IP Address]</SourceAlternate>
  <DestinationAlternate type="transport">[Carrier2 IP address]</DestinationAlternate>
  <UsageDetail>
    <Amount>23</Amount>
    <Unit>s</Unit>
  <UsageDetail>
</UsageIndication>
</Message>
```

The OSP UsageIndication message above includes the minimum critical data elements needed for interconnect accounting

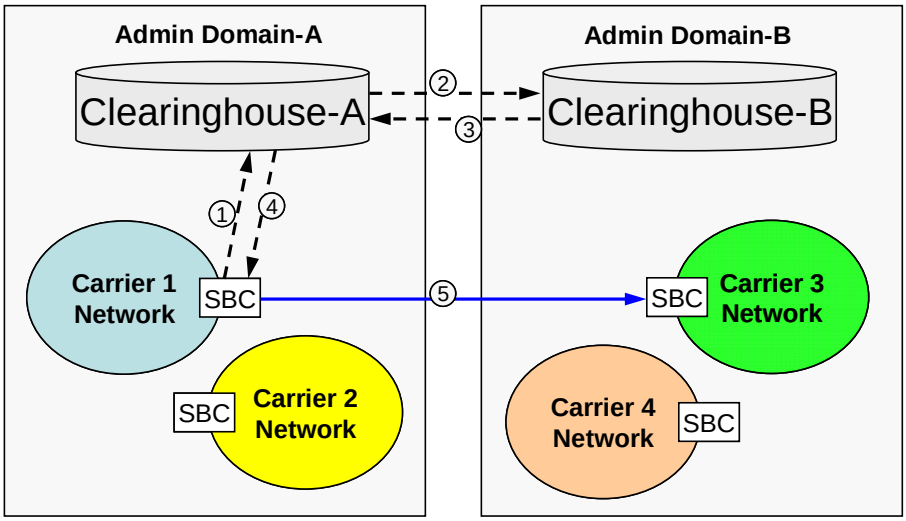
- Element indicating that Carrier1 was the source of the call.
- The Transaction ID from the OSP AuthorizationResponse.
- The Call ID for the call.
- The IP address of the source peer.
- The IP address of the destination peer.
- Usage details of the call duration, 23 seconds in this example.
- In addition to these data elements, OSP defines many other data fields (such as session details and quality of service) that may be reported in a UsageIndication message.

5. Carrier2 sends an OSP UsageIndication to the Clearinghouse as described in step 4 above.

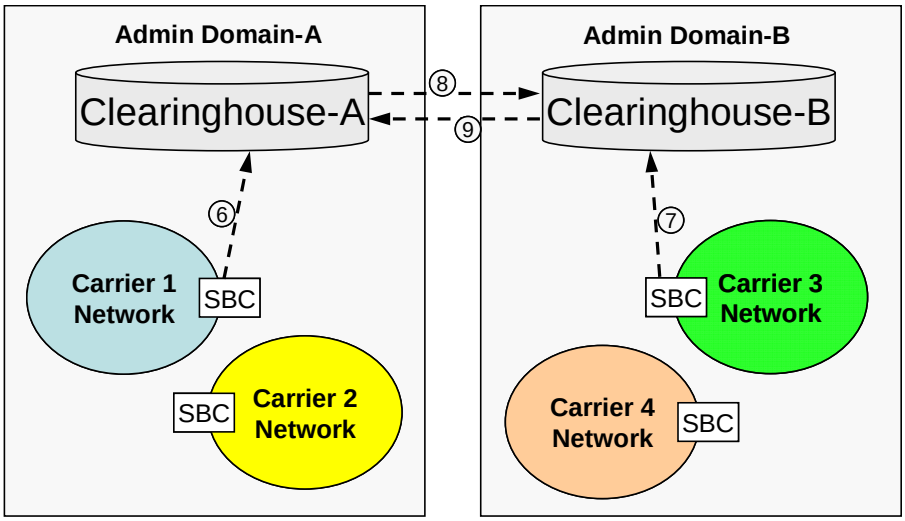
The OSP model provides secure authorization of the call and collection of accounting records from both the source and destination without requiring the clearinghouse in the signaling path between NGN peers. This feature makes the OSP model unique because it is the only standard which facilitates secure settlement for direct peer to peer communications

5 Clearing and Settlement between NGN Clearinghouses

As with certificate authorities, a vertical hierarchy of OSP clearinghouse is possible. However, one of the unique features of the OSP model is how its clearinghouse architecture can be extended *horizontally* to support a mesh of trusted administrative domains for cascading clearing and settlement. The diagrams below illustrate how OSP is used for clearing and settlement of interconnect transactions between NGNs which are served by different clearinghouses. In this example, Carrier1 uses the settlement services of Clearinghouse-A and Carrier3 uses the settlement services of Clearinghouse-B. The two clearinghouses, A and B, have a bilateral relationship for clearing and settlement between their administrative domains.



0. The preliminary step in this call scenario is route discovery as described in section 4.2.
1. Carrier1 sends an OSP AuthorizationRequest to Clearinghouse-A. The request includes the IP address of Carrier3 as the session destination.
2. Clearinghouse-A recognizes that Carrier3 is a peer in the Clearinghouse-B administrative domain and sends the OSP AuthorizationRequest to Clearinghouse-B. Clearinghouse-B authenticates the OSP AuthorizationRequest from Clearinghouse-A.
3. Clearinghouse-B authorizes the interconnect transaction with Carrier3 and returns an OSP AuthorizationResponse to Clearinghouse-A with a digitally signed authorization token.
4. Clearinghouse-A sends the OSP AuthorizationResponse to Carrier1.
5. Carrier1 includes the OSP Authorization Token in its session setup request to Carrier3. Carrier3 validates the digital signature of OSP Authorization Token using the public key of Clearinghouse-B. Since the token is a valid token from Clearinghouse-B (Carrier3's trusted clearinghouse), Carrier3 accepts the call.



6. When the call ends, Carrier1 sends an OSP UsageIndication to Clearinghouse-A.
7. Carrier3 sends an OSP UsageIndication to Clearinhouse-B.
8. To complete the transaction, Clearinghouse-A sends an OSP UsageIndication to Clearinghouse-B.
9. Clearinghouse-B sends and OSP UsageIndication to Clearinghouse-A.

With this transaction model, both clearinghouses have all the transaction data needed for anonymous NGN peer to peer settlement between different administrative domains. This simple bilateral example of the OSP model can be extended to include intermediate clearinghouses between the source and destination clearinghouses. OSP enables cascading settlement among an unlimited chain of networks.

6 More Information on the OSP Protocol

The OSP protocol has two important design factors that make it well suited for wide adoption – flexibility and simplicity.

6.1 Flexibility

First, the OSP protocol standard offers a broad range of flexibility for managing a wide variety of IP transactions. This paper provides an example of a simple OSP transaction for intercarrier settlement. But the OSP protocol defines many XML data elements not described here that may be used in the following transaction messages.

OSP Messages	**Description**
PricingIndication	Used to identify the price for a particular service. Prices may be sent individually or in bulk.
AuthorizationRequest	Described in section 4.
AuthorizationIndication	If a destination device cannot validate an authorization token, the device can forward the token in an AuthorizationIndication message to a device that can validate the token.
UsageIndication	Described in section 4.

ReauthorizationRequest	The OSP protocol can be used to authorize an IP transaction for a specific amount of usage, such as a one hour phone call. If a session in progress is nearing its authorized usage limit, a peer may send a ReauthorizationRequest to the Clearinghouse to authorize additional session usage.
SubscriberAuthenticationRequest	Asks for authentication of a subscriber's credentials.
CapabilitiesIndication	This message can be used to indicate what services or features are available.

6.2 Simplicity

The second factor which is important to OSP relevance as a useful protocol for NGN networks is its simplicity. OSP is a simple XML message set designed for transmission over HTTP. Any web server that can parse XML message can be an OSP server. Software developers familiar with the Apache or Tomcat open source web servers can easily develop an OSP server.

7 Commercial Implementations of the OSP Protocol

The OSP protocol has been implemented in the following commercial products and open source projects.

Vendor / Project	**Product**
Cisco	VoIP gateways and session border controllers running of 2000, 3000 and 5000 series routers. www.cisco.com
Digium	Asterisk PBX (open source) www.asterisk.org
iptel.org	SIP Express Router (open source SIP proxy) www.iptel.org
Kamailio	Open source SIP server. http://www.kamailio.org
NexTransit	Open source H.323 gatekeeper http://sourceforge.net/projects/nextransit
OpenOSP	Open source OSP server written in C for Solaris http://sourceforge.net/projects/openosp
OpenSIPS	Open source SIP server. www.opensips.com
OSP Toolkit	Open source OSP client http://sourceforge.net/projects/osp-toolkit
RAMS	Open source OSP server written in Java sourceforge.net/projects/rams
Stratus	Entice softswitch www.stratus.com
TransNexus	NexSRS OSP server www.transnexus.com
Veraz	Veraz Softswitch www.veraznetworks.com
Voice System	OpenSER (open source SIP proxy) www.openser.org
Vox Gratia	Open source H.323 proxy www.voxgratia.com

8 Requirements Compared to OSP Capabilities

This section provides an assessment of OSP capabilities for fulfilling NGN peering settlement requirements defined in section 2.

Requirement	**OSP Capabilities**
Standards Based	ETSI TS 101 321 V.4.1.1 is a mature standard.
Proven Technology	Carrier networks have been using the OSP protocol since 2000.
Flexibility	OSP is not limited to telephony and can be used to clear and settle any IP communication transaction.
Competitive Solutions	The architecture enabled by the OSP model facilitates the operation of multiple clearinghouses competing to offer settlement services.
Security	Standard implementations of PKI services with OSP ensure strong security for NGN clearing and settlement.