Network Working Group
Internet Draft
expires in six months

William A. Nace(NSA)
James E. Zmuda(SPYRUS)
November 21st, 1997

PPP Certificate Exchange Protocol
<draft-ietf-pppext-crtxchg-01.txt>

Status of this Memo

Abstract

The Point-to-Point Protocol (PPP) [1] provides a standard method for transporting multi-protocol datagrams over point-to-point links

PPP also defines an extensible Link Control Protocol, which allows negotiation of an Authentication Protocol for authentication of its peer before allowing Network Layer protocols to transmit over the link.

The Certificate exchange protocol is an extension to PPP that is

in the form of an additional phase, called the certificate exchange phase, that would allow for a PPP entity to request certificates from a peer. If configured, this phase would be negotiated during the LCP exchange. This exchange of certificates is aimed at easing configuration issues by providing for the exchange of certificate path information in a standard manner across different strong, or public-key certificate-based, authentication protocols. The certificate exchange protocol accomodates arbitrary sized certificates.

1. Introduction

In order to establish communications over a point-to- point link, each end of the PPP link must first send LCP packets to configure the data link during Link Establishment phase. After the link has been established, we are suggesting that the PPP provide for an optional Certificate Exchange phase before proceeding to the Authentication phase.

By default, this certificate exchange phase will not be mandatory. If the certificate exchange phase is configured into a PPP entity, and negotiation with the peer has concluded that it can be supported by the peer, then the certificate exchange protocol will be performed after the LCP phase and before the Authentication phase.

If the certificate exchange protocol is desired, an implementation MUST specify the Certificate-Exchange-Protocol Configuration Option during Link Establishment phase.

Of course, if no Authentication Protocol is negotiated during the Link Establishment phase, or one that does not use strong authentication that requires the type of certificate that we have obtained, then the product of the Certificate Exchange protocol will have been wasted. However, this is to be avoided through proper configuration and properly forming certificate exchange requests and responses. This means primarily two things: First, the in the initial certificate exchange request, the requestor shall send the algorithm identifier for the certificate type in which he is interested, as well as his distinguished name. Second, the responder shall include a certificate (if available) in his reply that supports the algorithm identified in the request, and that is within the naming hierarchy indicated by the requestor's distinguished name. These procedures will

insure that the information retrieved by the certificate exchange protocol is relevant.

1.1. Specification of Requirements

In this document, several words are used to signify the requirements of the specification. These words are often capitalized.

MUST	This word, or the adjective required, means that the definition is an absolute requirement of the specification.
MUST NOT	This phrase means that the definition is an absolute prohibition of the specification.
SHOULD	This word, or the adjective recommended, means that there may exist valid reasons in particular circumstances to ignore this item, but the full implications must be understood and carefully weighed before choosing a different course.
MAY	This word, or the adjective optional, means that this item is one of an allowed set of alternatives. An implementation which does not include this option MUST be prepared to interoperate with another implementation which does include the option.

1.2. Terminology

This document frequently uses the following terms:

certificate	A certificate consists of the binding together of one or more public key values and an identity. This binding is effected through a digital signature which is applied to the data containing both the public key and the identity. This signature is applied by a "certification authority" that is recognized as issuing this certificate on behalf of the entity identified in the

certificate. In this manner a recipient of this certificate can determine the recognized public key of the particular entity identified in the certificate. This requires the recipient to, either directly or indirectly, trust the authority that has issued this certificate.

certificate validation
An individual certificate provides the recipient of a certificate the assurance that the subject named in the certificate is the holder of the public key contained in the certificate. However, this assurance

requires that the recipient trust the issuer of the certificate. If the recipient doesn't directly trust the certificate issuer, the recipient will attempt to establish that trust by reviewing and validating the certificate of the issuing authority itself. This process continues until the recipient arrives at an issuer whom it does trust. If this process is successful, the certificate is validated. If this process is unsuccessful within a certain number of steps the certificate is not validated. This process of validation of a chain of certificates is called certificate validation.

certificate pathThe chain of certificates examined during certificate validation.

certification authority (CA)
An authority trusted by one or more users to create and assign certificates. [2].

distinguished name
A unique hierarchical name. Used in the certificate's "subject" field to denote the entity associated with the public key value(s) in the certificate[2]. Also used in the certificate's "issuer" field to denote the entity that issued this certificate.

peer The other end of the point-to-point link.

Requestor	The end of the link initiating the Certificate Exchange. It does this by sending the peer a Certificate Exchange Request packet.

2. PPP Certificate Exchange Protocol

The Certificate Exchange Protocol is a general protocol in support of public-key based PPP authentication protocols.

The gating issue with respect to the deployment of public-key based authentication protocols is the establishment of infrastructure. Two types of infrastructure are needed. The first is the ability to issue certificates. This relies upon the availability of certificate authorities with the means to adequately verify legitimate users before issuing them certificates.

The second type of infrastructure is a method to distribute these certificates to the necessary parties, who are engaged in

certificate-based strong authentication. There are a number of ways that this can be accomplished in practice. The first, and obvious method is to require that all parties who wish to employ certificate/public-key based authentication have a complete database of all the certificates required to authenticate any desired peer. Another alternative would be to utilize one of the many access protocols to retrieve a required certificate from a directory service. Another method would be to require security protocols to transfer certificates during the authentication exchange. None of these options is particularly attractive or even applicable for the case of PPP certificate-based authentication protocols.

The use of a pre-configured database is a possible but limited approach.

The use of a directory service is not feasible due to the point in time at which PPP authentication protocols are run, namely during the authentication phase. At this point in time the connectivity needed to reach a directory service has not yet been achieved.

The current approach used within certificate-based authentication in PPP is to saddle the authentication protocol with the task of

exchanging the certificates required to authenticate a peer. This is problematic. The reason is that more data than can be conveyed in a single PPP packet may be required to be exchanged, and the PPP protocols, running at the level they are and in the simple request response fashion they do, do not immediately lend themselves to conveying large amounts of data.

The authors suggest that a better option is for the PPP authentication protocols to worry about authentication and another protocol to perform the exchanges of certificates required to support certificate validation.

The Certificate Exchange protocol is such a protocol.

The Certificate Exchange Protocol is a challenge- response protocol. The initiator starts the protocol by sending the peer an initial exchange packet. The peer is to respond to this request with an initial exchange response packet containing his own certificate. The initiator then determines if he has the information required to validate this certificate. [See the definition of certificate validation, above.] If the initiator does not possess such information, he issues another certificate exchange request packet. This packet, however is a "DName Specified" request packet. In this packet the initiator puts the Distinguished name of the entity whose certificate he requires to complete the next step in the certificate validation process. The peer is to respond to this request with the certificate

for the entity named in the request. If this certificate itself requires another certificate in order to be validated, the initiator issues yet another Certificate Exchange Request packet with DName of the entity whose certificate is required to validate this certificate. This process continues until the complete certificate path for the peer has been validated.

The protocol also has additional request/response types to handle the case of a certificate that is itself too large for one PPP packet.

3. PPP Certificate Exchange Protocol Packet Format

The Certificate Exchange protocol is accomplished using two different packet formats: a Request packet format and a Response packet format.

Both the Certificate Exchange Request and Response packets have the following common format:

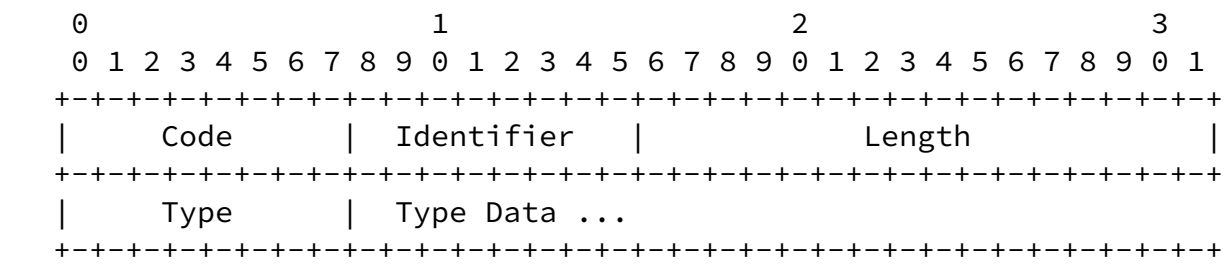

Figure 3.0-1 - The Certificate Exchange protocol packet format

Code

1 (Request)
2 (Response)

Identifier

The identifier field is one octet and aids in matching responses with requests. The identifier field MUST be changed on each Request packet containing a different DName value.

Length

The Length field is two octets and indicates the length of the Certificate Exchange Request and Response packets including the Code, Identifier, Length, Type, and Type Data fields. Octets in the packet outside the range of the Length field should be treated as Data Link Layer padding and should be ignored on reception.

Type

1 (Initial Exchange)
2 (DName Specified Exchange)
3 (Certificate unavailable)
4 (Partial Certificate Request/Response)

Type Data

Depending upon the setting of the type field, the Request packet will either use this field to carry the algorithm ID and DName from its own certificate (in the case of an Initial Exchange), or will use this field to specify the DName of the certificate being requested (in the case of a "DName Specified" Exchange). The Response packet uses this field to hold the certificate value. The length of this field is inferred from the length field for this packet as a whole.

In the event the responder must reply to a request (either Initial, or DName-specified) with a certificate that is too big to fit within the current PPP MTU, the certificate exchange protocol will respond with a "Partial Certificate" response type packet. This format allows the responder to return a partial certificate and indicate the amount remaining. Subsequent "Partial Certificate" Requests and Responses will be used to transfer the complete certificate.

The following sections define the format of the various request and response packets used in the certificate exchange protocol. The first to be dealt with are the PDUs exchanged during the retrieval of complete certificates. Following this are the PDUs required to support retrieval of certificates too large to fit within the current PPP MTU.

3.1. Certificate Exchange Protocol Request Packet

The Certificate Exchange Protocol Request Packet is formatted as follows:

Figure 3.0-2 - Certificate Exchange Protocol Request Packet format

Code

1 (Request)

Identifier

The identifier field is one octet and aids in matching responses with requests. The identifier field MUST be changed on each Request packet containing a different DName value.

Length

The Length field is two octets and indicates the length of the Certificate Exchange Request packet including the Code, Identifier, Length, and Type, Algorithm ID, and DName fields. Octets in the packet outside the range of the Length field should be treated as Data Link Layer padding and should be ignored on reception.

Type

1 (Initial Exchange)
2 (DName Specified Exchange)

AlgIDLen

Indicates the length of the AlgorithmID field.

AlgorithmID

If the type field is set to a 1, indicating an "Initial Exchange" then this field will contain the Algorithm Identifier from the Certificate that the requestor will

use during the authentication phase. This field is carried in its raw ASN.1 form, right out of the certificate. On the other hand, if the type field is set to a 2, indicting this is a subsequent request, then this field will not be present. This is indicating by a value of 0 in the AlgIDLen field.

DName

If the type field is set to a 1, indicating an "Initial Exchange" then this field contains the DName from the certificate that the requestor will use during the authentication phase. On the other hand, if the type field is set to a 2, indicting this is a subsequent request, then this field will contain the DName of the entity whose certificate is being requested.

3.2. Certificate Exchange Protocol Response Packet

The Certificate Exchange response packet is formatted as follows.

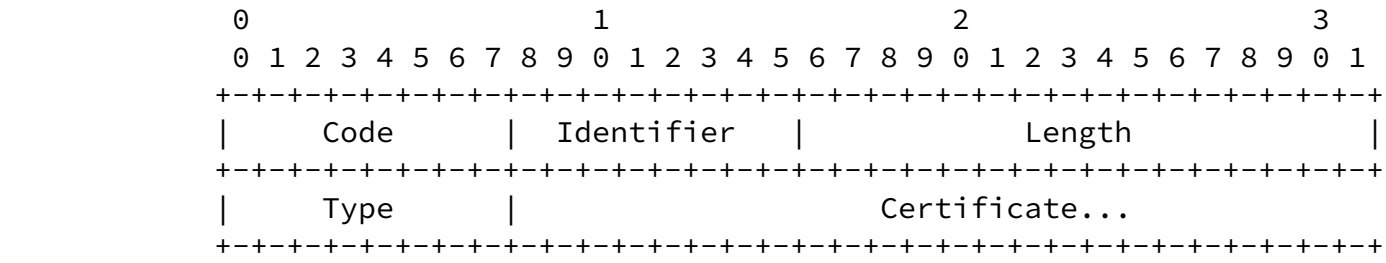

Figure 3.0-3 - Certificate Exchange Protocol Response Packet format

Code

2 (Response)

Identifier

The identifier field is one octet and MUST match the Identifier field from the corresponding request.

Length

The Length field is two octets and indicates the length of the Certificate Exchange Response packet including the Code, Identifier, Length, and Type, and Certificate

fields. Octets in the packet outside the range of the Length field should be treated as Data Link Layer padding

and should be ignored on reception.

Type

The Type field in the Response can carry either the value 1 (signifying an initial certificate exchange request) or the value 2 (signifying a subsequent certificate exchange request), or the value 3 (signifying a retrieval failure).

Certificate

The Certificate field contains the complete ASN.1 encoded X.509 certificate for the entity named in the Certificate Exchange request that this response corresponds to. In the case there was no entity named in the Certificate Exchange request (e.g. an Initial Certificate Exchange Request) the responder will choose a certificate to use to send to the requestor. The type of certificate returned should correspond to the type of algorithm indicated by the Requestor in the Initial Exchange Request. The public key in this certificate should correspond to the private key that will be used in any subsequent EAP authentication operations.

A type value of 4 indicates a "Partial Certificate" response. This format is described in section 3.3.

3.3. Certificate Exchange Protocol "Partial Certificate" Response Packet

The Certificate Exchange "Partial Certificate" response packet is formatted as follows.

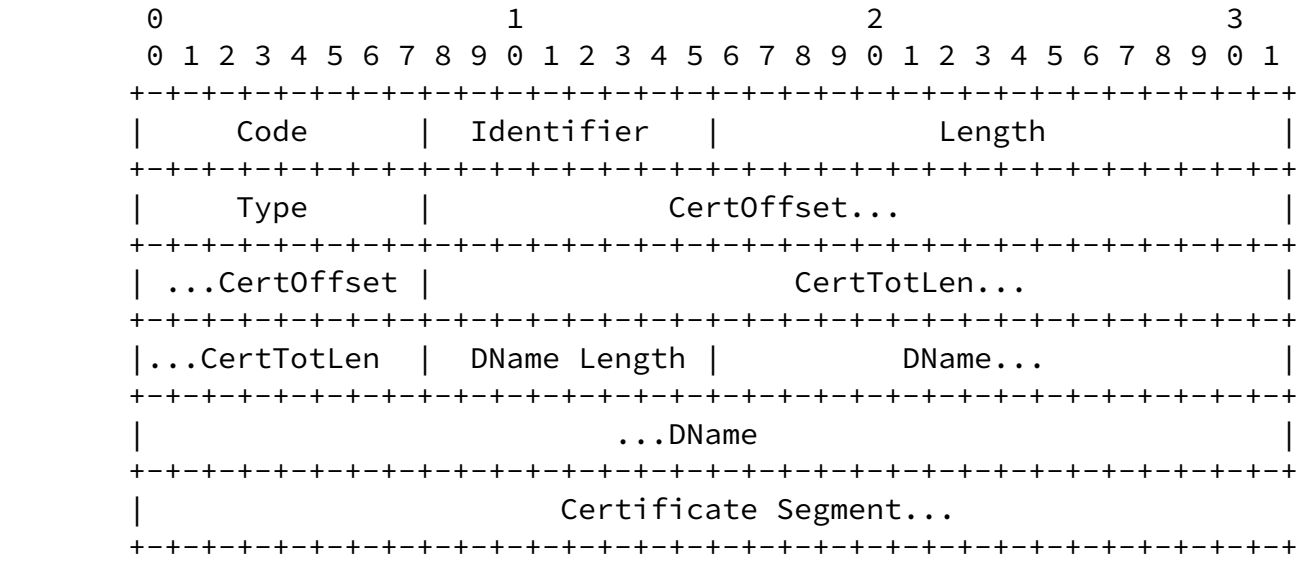

Figure 3.0-4 - Certificate Exchange Protocol "Partial Certificate" Response Packet format

Code

2 (Response)

Identifier

The identifier field is one octet and MUST match the Identifier field from the corresponding request.

Length

The Length field is two octets and indicates the length of the Certificate Exchange Response packet including the

Code, Identifier, Length, and Type, and CertOffset, CertTotLen, DName Length, DName, and Certificate fields. Octets in the packet outside the range of the Length field should be treated as Data Link Layer padding and should be ignored on reception.

Type

The Type field in the "Partial Certificate" Response will carry a value of 4, or the value 3 (signifying a retrieval failure).

CertOffset

The CertOffset, or "Certificate Offset" field contains the offset within the entire certificate of the segment

carried within this partial response.

CertTotLen

The CertTotLen, or "Certificate Total Length" field contains the length of the entire certificate, of which only a portion is carried in this partial response.

DName Length

The Length of the DName field in bytes.

DName

This field contains the DName field from the Certificate, whose segment is being carried in the Certificate Segment field. This is present to facilitate the Requestors formation of the subsequent "Partial Certificate" Requests required to retrieve the complete Certificate.

Certificate Segment

The Certificate Segment field contains as much of the complete ASN.1 encoded X.509 certificate that can be carried within the current PPP MTU-sized packet.

3.4. Certificate Exchange Protocol "Partial Certificate" Request Packet

The Certificate Exchange "Partial Certificate" request packet is formatted as follows.

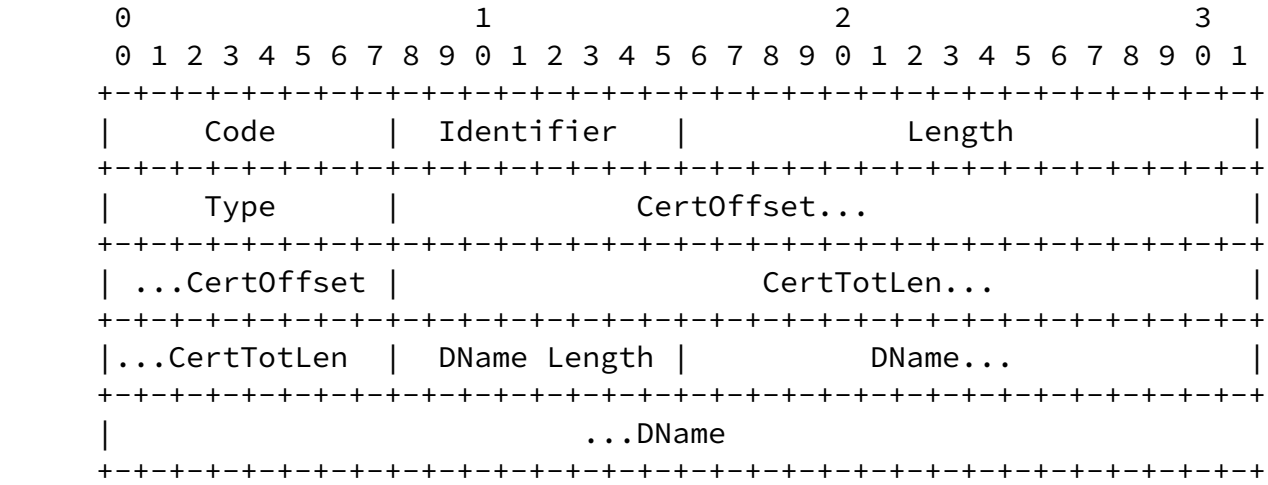

Figure 3.0-5 - Certificate Exchange Protocol "Partial Certificate" Request Packet format

Code

1 (Request)

Identifier

The identifier field is one octet and aids in matching responses with requests. The identifier field MUST be changed on each Request packet containing a different DName value.

Length

The Length field is two octets and indicates the length of the Certificate Exchange Response packet including the Code, Identifier, Length, and Type, and CertOffset, CertTotLen, DName Length, and DName fields. Octets in the packet outside the range of the Length field should be

treated as Data Link Layer padding and should be ignored on reception.

Type

The Type field in the "Partial Certificate" Request will carry a value of 4.

CertOffset

The CertOffset, or "Certificate Offset" field contains the offset within the entire certificate of the certificate segment being requested.

CertTotLen

The CertTotLen, or "Certificate Total Length" field contains the length of the entire certificate.

DName Length

The Length of the DName field in bytes.

DName

This field contains the DName field from the Certificate, whose segment is being requested.

4. Certificate Exchange Protocol Processing

During the certificate exchange phase, a PPP entity that is configured to use the certificate exchange protocol will initiate the Certificate Exchange protocol. The Certificate Exchange protocol is a series of REQUEST/RESPONSE exchanges. The PPP entity configured to perform the Certificate Exchange protocol, or "initiator", will send REQUEST packets requesting the peer send it a certificate. In the initial exchange the initiator will send a initial Certificate Exchange request asking the peer for its current certificate. The Requestor will place its own certificate in this outgoing Initial

Exchange Request. The reason for this is so that the Responder will know which, compatible type of certificate of the many it may have available to send back in the Response. Next, the peer will reply with a response packet containing its certificate of the appropriate type, it available. If not, it will return a Response packet with a type field indicating a retrieval failure. The initiator will then determine if this certificate can be validated with the information it currently has. (If it has the complete path to a common trust point that this certificate requires.) If the initiator decides it has sufficient information to validate this certificate, it finishes the certificate exchange protocol phase and continues to the authentication phase. If, on the other hand, the initiator does not have enough information to validate this certificate, it sends another Certificate Exchange protocol request packet to the peer requesting the certificate (or the first certificate of a number of certificates) which it is missing in order to complete validation. This process continues until the complete path has been obtained. The Certificate Exchange protocol is unilateral in that the requests are in one direction only. If the peer PPP entity requires certificates to accomplish authentication then that peer should also be configured to perform the certificate exchange protocol.

In the event that the type field of a certificate response contains a 4 - indicating that the data field contains a partial response, the requestor will use a partial certificate request type packet to request the next segment in the certificate. The segment requested is indicated in the partial certificate request by indicating the byte offset within the total certificate of the next segment of the certificate. The exchange of these request-response pairs continues until the requestor is satisfied that it has retrieved the entire certificate. Then processing continues, if necessary, to retrieve the complete certificate path as in the normal case, above.

Figure 4.0-1 depicts the operation of the Certificate Exchange protocol. (For the purposes of this example, it is assumed that the certificates fit within a single PPP packet) In this figure depicting protocol exchanges, the curly braces ({, }) denote items in ASN.1

representation.

Side: B A

```
Authenticator           Authenticatee

CRTXCHG Request (ID1, Initial Exchange, {certB}) =>

            <= CRTXCHG Response(ID1, Initial Exchange, {certA})

CRTXCHG Request (ID2, DName Specified, {DName}) =>

            <= CRTXCHG Response(ID2, DName Specified, {Cert(DName)})
```

Figure 4.0-1 Certificate Exchange protocol processing

Security Considerations

This memo defines a method for exchanging certificates to be used to support public-key based authentication protocols, which rely upon the validity of the public key used to verify signatures from the peer. The validity of these public keys is vouched for by having the certificates that bind them to an identity signed for by either a directly or indirectly trusted third party. Obviously, the security of such a system depends upon there being some common trust point between the parties.

References:

[1] Simpson, W. A., 'The Point to Point Protocol (PPP)', July 1994, RFC 1661.

[2] CCITT Recommendation X.509, 'The Directory - Authentication Framework', 1988.

Acknowledgements:

Thanks to Peter Yee and Russ Housley who provided helpful comments on earlier versions of this Memo. And thanks to Bill Simpson for the standard PPP spec boilerplate from which I have borrowed heavily.

Chair's Address:

The working group can be contacted via the current chair:

Karl Fox
Ascend Communications, Inc.

Email: karl@ascend.com

Author's Address:

Questions about this memo can also be directed to:

DIRNSA
Attn: X22 (W. Nace)
9800 Savage Road
Fort Meade, MD 20755-6000
USA

Phone: +1 410 859-4464
Email: WANace@missi.ncsc.mil

James E. Zmuda
SPYRUS
2460 N. First Street
Suite 100
San Jose, CA 95131-1023
USA

Phone: +1 408 432-8180
Email: jzmuda@spyrus.com