Abstract

The IEC 61850 power utility automation family of standards describe methods using Ethernet and IP for distributing control and data frames within and between substations. The IEC 61850-90-5 and IEC 62351-9 standards specify the use of the Group Domain of Interpretation (GDOI) protocol (RFC 6407) to distribute security transforms for some IEC 61850 security protocols. This memo defines GDOI payloads to support those security protocols.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on March 27, 2017.

Copyright Notice

Copyright (c) 2016 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect
Power substations use Generic Object Oriented Substation Events (GOOSE) protocol [IEC-61850-8-1] to distribute control information to groups of devices using a multicast strategy. Sources within the power substations also distribute IEC 61850-9-2 sampled values data streams [IEC-61850-9-2]. The IEC 62351-9 standard [IEC-62351-9] describes key management methods for the security methods protecting these IEC 61850 messages, including methods of device authentication and authorization, and methods of policy and keying material agreement for IEC 61850 message encryption and data integrity protection. These key management methods include the use of GDOI [RFC6407] to distribute the security policy and session keying material used to protect IEC 61850 messages when the messages are sent to a group of devices.

The protection of the messages is defined within IEC 62351-6 [IEC-62351-6], IEC 61850-8-1 [IEC-61850-8-1], and IEC 61850-9-2 [IEC-61850-9-2]. Protected IEC 61850 messages typically include the output of a Message Authentication Code (MAC) and may also be
encrypted using a symmetric cipher such as the Advanced Encryption
Standard (AES).

Section 5.5.2 of RFC 6407 specifies that the following information
needs to be provided in order to fully define a new Security
Protocol:

- The SPI Size
- The method of SPI generation
- The transforms, attributes, and keys needed by the Security
  Protocol.

This document defines GDOI payloads to distribute policy and keying
material to protect IEC 61850 messages, and defines the necessary
information to ensure interoperability between IEC 61850
implementations.

1.1. Requirements notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",
"SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this
document are to be interpreted as described in [RFC2119].

1.2. Terminology

The following key terms are used throughout this document:

- Generic Object Oriented Substation Events: Power substation control
  model defined as per IEC 61850.
- IEC 61850 message: A message in the IEC 61850 family of protocols
carrying control or data between Substation devices.

1.3. Acronyms and Abbreviations

The following acronyms and abbreviations are used throughout this
document:

- AES: Advanced Encryption Standard
- GCKS: Group Controller/Key Server
- GDOI: Group Domain of Interpretation
2. IEC 61850 Protocol Information

The following sections describe the GDOI payload extensions that are needed in order to distribute security policy and keying material for the IEC 62351 Security Services. The Identification (ID) Payload is used to describe an IEC 62351 GDOI group. The Security Association (SA) Traffic Encryption Key (TEK) payload is used to describe the policy defined by a Group Controller/Key Server (GCKS) for a particular IEC 62351 traffic selector. No changes are required to the Key Download (KD) Payload, but a mapping of IEC 62351 keys to KD Payload key types is included.

2.1. ID Payload

The ID payload in a GDOI GROUPKEY-PULL exchange allows the Group Member (GM) to declare the group it would like to join. A group is defined by an ID payload as defined in GDOI [RFC6407] and reproduced in Figure 1.

```
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-!
|   Next Payload   |   RESERVED    |       Payload Length        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-!
|          ID Type          | DOI-Specific ID Data = 0 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-!
| Identification Data |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-!
```

Figure 1: RFC 6407 Identification Payload
An ID Type name of ID_OID (value 13) is defined in this memo to
specify an Object Identifier (OID) [ITU-T-X.683] encoded using
Distinguished Encoding Rules (DER) [ITU-T-X.690]. Associated with
the OID may be an OID Specific Payload DER encoded as further
defining the group. Several OIDs are specified in [IEC-62351-9] for
use with IEC 61850. Each OID represents a GOOSE or Sampled Value
protocol, and in some cases IEC 61850 also specifies a particular
multicast destination address to be described in the OID Specific
Payload field. The format of the ID_OID Identification Data is
specified as shown in Figure 2.

<table>
<thead>
<tr>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>+---------------------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>! OID Length ! OID</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>+---------------------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>! OID Specific Payload Length ! OID Specific Payload</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>+---------------------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 2: ID_OID Identification Data

The ID_OID Identification Data fields are defined as follows:

- OID Length (1 octet) -- Length of the OID field.
- OID (variable) -- An ASN.1 ObjectIdentifier encoded using DER [ITU-T-X.690].
- OID Specific Payload Length (2 octets) -- Length of the OID Specific Payload. Set to zero if the OID does not require an OID Specific Payload.
- OID Specific Payload (variable) -- OID specific selector encoded in DER. If OID Specific Payload Length is set to zero this field does not appear in the ID payload.

2.2. SA TEK Payload

The SA TEK payload contains security attributes for a single set of
policy associated with a group TEK. The type of policy to be used
with the TEK is described by a Protocol-ID field included in the SA
TEK. As shown in Figure 3 reproduced from RFC 6407, each Protocol-ID
describes a particular TEK Protocol-Specific Payload definition.
The Protocol-ID name of GDOI_PROTO_IEC_61850 (value TBD1) is defined in this memo for the purposes of distributing IEC 61850 policy. A GDOI_PROTO_IEC_61850 SA TEK includes an OID and (optionally) an OID Specific Payload that together define the selectors for the network traffic. The selector fields are followed by security policy fields indicating how the specified traffic is to be protected. The GDOI_PROTO_IEC_61850 TEK Protocol-Specific Payload is defined as shown in Figure 4.

The GDOI_PROTO_IEC_61850 SA TEK Payload fields are defined as follows:

- OID Length (1 octet) -- Length of the OID field.
- OID (variable) -- An ASN.1 ObjectIdentifier encoded using DER. OIDs defined in IEC 61850 declare the type of IEC 61850 message to be protected, as defined by [IEC-62351-9].
- OID Specific Payload Length (2 octets) -- Length of the OID Specific Payload. This field is set to zero if the policy does not include an OID Specific Payload.

- OID Specific Payload (variable) -- The traffic selector (e.g., multicast address) specific to the OID encoded using DER. Some OID policy settings do not require the use of an OID Specific Payload, in which case this field is not included in the TEK and the OID Specific Payload Length is set to zero.

- SPI (4 octets) -- Identifier for the Current Key. This field represents a SPI.

- Auth Alg (2 octets) -- Authentication Algorithm ID. Valid values are define in Section 2.2.2.

- Enc Alg (2 octets) -- Confidentiality Algorithm ID. Valid values are define in Section 2.2.3.

- Remaining Lifetime value (4 octets) -- The number of seconds remaining before this TEK expires. A value of zero (0) shall indicate that the TEK does not have an expire time.

- SA Data Attributes (variable length) -- Contains zero or more attributes associated with this SA. Section Section 2.2.4 defines attributes.

2.2.1. Selectors

The OID and (optionally) an OID Specific Payload that together define the selectors for the network traffic. While they may match the OID and OID Specific Payload that the GM had previously requested in the ID payload, there is no guarantee that this will be the case. Including selectors in the SA TEK is important for at least the following reasons:

- The KS policy may direct the KS to return multiple TEKs, each representing different traffic selectors and it is important that every GM receiving the set of TEKs explicitly identify the traffic selectors associated with the TEK.

- The KS policy may include the use of a GDOI GROUPKEY-PUSH message, which distributes new or replacement TEKs to group members. Since the GROUPKEY-PUSH message does not contain an ID payload the TEK definition must include the traffic selectors.
2.2.2. Authentication Algorithms

This memo defines the following Authentication Algorithms for use with this TEK. These algorithms are defined in [IEC-TR-61850-90-5], including requirements on one or more algorithms defined as mandatory to implement.

- HMAC-SHA256-128. Specifies the use of SHA-256 [FIPS180-3.2008] combined with HMAC [RFC2104]. The output is truncated to 128 bits, as per [RFC2104]. The key size is the size of the hash value produced by SHA-256 (256 bits).
- HMAC-SHA256. Specifies the use of SHA-256 [FIPS180-3.2008] combined with HMAC [RFC2104]. The key size is the size of the hash value produced by SHA-256 (256 bits).

2.2.3. Confidentiality Algorithms

This memo defines the following Confidentiality Algorithms for use with this TEK. These algorithms are defined in [IEC-TR-61850-90-5], including requirements on one or more algorithms defined as mandatory to implement.

- AES-CBC-128. Specifies the use of AES [FIPS197] in the Cipher Block Chaining (CBC) mode [SP.800-38A] with a 128 bit key size.
- AES-CBC-256. Specifies the use of AES [FIPS197] in the Cipher Block Chaining (CBC) mode [SP.800-38A] with a 256 bit key size.
- AES-GCM-256. Specifies the use of AES [FIPS197] in the Galois/Counter Mode (GCM) mode [SP.800-38D] with a 256 bit key size.

2.2.4. SA Attributes

The following attributes may be present in an SA TEK. The attributes must follow the format described in Appendix C).
2.2.4.1. SA Time Activation Delay (SA_ATD)

A GCKS will sometimes distribute an SA TEK in advance of when it is expected to be used. This is communicated to group members using the SA Activation Time Delay (SA_ATD) attribute. When a GM receives an SA_TEK with this attribute, it waits for the number of seconds contained within the attribute before installing it for either transmission or receiving.

This Activation Time Delay attribute applies only this SA, and MAY be used in either a GROUPKEY-PULL or GROUPKEY-PUSH exchange. RFC 6407 also describe an ACTIVATION_TIME_DELAY attribute for the Group Associated Policy (GAP) payload, which is applied to all Security Associations and restricted to use in a GROUPKEY-PUSH message. If both attributes are included in a GROUPKEY-PUSH payload, the value contained in SA_ATD will be used.

2.2.4.2. Key Delivery Assurance (SA_KDA)

Group policy can include notifying a multicast source ("Publisher") of an indication of whether multicast receivers ("Subscribers") have previously received the SA TEK. This notification allows a Publisher to set a policy as to whether to activate the new SA TEK or not based on the percentage of Subscribers that are able to receive packets protected by the SA TEK. The attribute value is a number between 0 and 100 (inclusive).

2.2.5. SPI Discussion

As noted in Section 1, RFC 6407 requires that characteristics of a SPI must be defined. A SPI in a GDOI_PROTO_IEC_61850 SA TEK is represented as a Key Identifier (KeyID). The SPI size is 4 octets. The SPI is unilaterally chosen by the GCKS using any method chosen by the implementation. However, an implementation needs to take care not to duplicate a SPI value that is currently in use for a particular group.

2.3. KD Payload

The KD Payload contains group keys for the policy specified in the SA Payload. It is comprised of a set of Key Packets, each of which hold the keying material associated with a SPI (i.e., an IEC 61850 Key Identifier). The RFC 6407 KD payload format is reproduced in Figure 5.
Each Key Packet holds the keying material associated with a particular IEC 61850 Key Identifier, although GDOI refers to it as a SPI. The keying material is described in a set of attributes indicating an encryption key, integrity key, etc., in accordance with the security policy of the group as defined by the associated SA Payload. Each Key Packet has the following format, reproduced in Figure 6.

No changes are needed to GDOI in order to distribute IEC 61850 keying material, but the keys MUST be distributed as defined in Section 5.6 of RFC 6407. The KD Type MUST be TEK (1).

A key associated with an IEC 61850 Authentication Algorithm (distributed in the Auth Alg field) MUST be distributed as a TEK_INTEGRITY_KEY attribute. The value of the attribute is interpreted according to the type of key distributed in the SA TEK:

- HMAC-SHA256-128, HMAC-SHA256. The value is 32 octets.
- AES-GMAC-128. The value is 20 octets. The first 16 octets are the 128-bit AES key, and the remaining four octets are used as the salt value in the nonce.
o AES-GMAC-256. The value is 36 octets. The first 32 octets are the 256-bit AES key, and the remaining four octets are used as the salt value in the nonce.

A key associated with an IEC 61850 Confidentiality Algorithm (distributed in the Enc Alg SA TEK field) MUST be distributed as a TEK_ALGORITHM_KEY attribute. The value of the attribute is interpreted according to the type of key distributed in the SA TEK:

o AES-CBC-128. The value is 16 octets.

o AES-CBC-256. The value is 32 octets.

o AES-GCM-128. The value is 20 octets. The first 16 octets are the 128-bit AES key, and the remaining four octets are used as the salt value in the nonce.

o AES-GCM-256. The value is 36 octets. The first 32 octets are the 256-bit AES key, and the remaining four octets are used as the salt value in the nonce.

3. Security Considerations

GDOI is a security association (SA) management protocol for groups of senders and receivers. This protocol performs authentication of communicating protocol participants (Group Member, Group Controller/Key Server). GDOI provides confidentiality of key management messages, and it provides source authentication of those messages. GDOI includes defenses against man-in-middle, connection hijacking, replay, reflection, and denial-of-service (DOS) attacks on unsecured networks. GDOI assumes the network is not secure and may be under the complete control of an attacker. The Security Considerations described in RFC 6407 are relevant to the distribution of GOOSE and sampled values policy as defined in this memo.

Message Authentication is a mandatory property for IEC 62351 Security Services. A common practice is to truncate the output of a MAC and include part of the bits in the integrity protection field of the data security transform. Current guidance in [RFC2104] is to truncate no less than half of the length of the hash output. The authentication algorithm HMAC-SHA256-128 defined in this memo truncates the output to exactly half of the output, which follows this guidance.

Confidentiality is an optional security property for IEC 62351 Security Services. Confidentiality Algorithm IDs SHOULD be included in the IEC-61850 SA TEK Payload if the IEC 61850 messages are expected to traverse public network links and not protected by
another level of encryption (e.g., an encrypted Virtual Private Network). Current cryptographic advice indicates that the use of AES-CBC-128 for confidentiality is sufficient for the foreseeable future [SP.800-131], but some security policies may require the use of AES-CBC-256.

4. IANA Considerations

The following additions are made to the GDOI payloads registry [GDOI-REG].

A new SA TEK Payload Values - Protocol-ID value is defined. Its type is GDOIPROTO_IEC_61850, with a value of TBD1.

A new registry is added defining Auth Alg values. The Attribute Class is called "IEC62351-9 Authentication Values". The terms Reserved, Expert Review and Private Use are to be applied as defined in [RFC5226].

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reserved</td>
<td>0</td>
</tr>
<tr>
<td>Reserved</td>
<td>1</td>
</tr>
<tr>
<td>HMAC-SHA256-128</td>
<td>2</td>
</tr>
<tr>
<td>HMAC-SHA256</td>
<td>3</td>
</tr>
<tr>
<td>AES-GMAC-128</td>
<td>4</td>
</tr>
<tr>
<td>AES-GMAC-256</td>
<td>5</td>
</tr>
<tr>
<td>Expert Review</td>
<td>6-61439</td>
</tr>
<tr>
<td>Private Use</td>
<td>61440-65535</td>
</tr>
</tbody>
</table>

A new registry is added defining Enc Alg values. The Attribute Class is called "IEC62351-9 Confidentiality Values". The terms Expert Review and Private Use are to be applied as defined in [RFC5226].

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reserved</td>
<td>0</td>
</tr>
<tr>
<td>Reserved</td>
<td>1</td>
</tr>
<tr>
<td>AES-CBC-128</td>
<td>2</td>
</tr>
<tr>
<td>AES-CBC-256</td>
<td>3</td>
</tr>
<tr>
<td>AES-GCM-128</td>
<td>4</td>
</tr>
<tr>
<td>AES-GCM-256</td>
<td>5</td>
</tr>
<tr>
<td>Expert Review</td>
<td>6-61439</td>
</tr>
<tr>
<td>Private Use</td>
<td>61440-65535</td>
</tr>
</tbody>
</table>

A new registry for SA TEK attributes is defined. The Attribute Class is called "GDOI SA TEK Attributes". The terms Expert Review and Expert Review are to be applied as defined in [RFC5226]. In the
table, attributes that are defined as TV are marked as Basic (B); attributes that are defined as TLV are marked as Variable (V).

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reserved</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>SA_ATD</td>
<td>1</td>
<td>V</td>
</tr>
<tr>
<td>SA_KDA</td>
<td>2</td>
<td>B</td>
</tr>
<tr>
<td>Expert Review</td>
<td>3-28671</td>
<td></td>
</tr>
<tr>
<td>Private Use</td>
<td>28672-32767</td>
<td></td>
</tr>
</tbody>
</table>

A new registry for ID Types is defined for the Identification Payload when the DOI is GDOI. The registry is taken from the ID Types registry for the IPsec DOI, which were previously assumed. Values 1-12 are defined identically to the equivalent values in the IPsec DOI. Value 13 is defined in this memo. The terms Expert Review and Private Use are to be applied as defined in [RFC5226].

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reserved</td>
<td>0</td>
</tr>
<tr>
<td>ID_IPV4_ADDR</td>
<td>1</td>
</tr>
<tr>
<td>ID_FQDN</td>
<td>2</td>
</tr>
<tr>
<td>ID_USER_FQDN</td>
<td>3</td>
</tr>
<tr>
<td>ID_IPV4_ADDR_SUBNET</td>
<td>4</td>
</tr>
<tr>
<td>ID_IPV6_ADDR</td>
<td>5</td>
</tr>
<tr>
<td>ID_IPV6_ADDR_SUBNET</td>
<td>6</td>
</tr>
<tr>
<td>ID_IPV4_ADDR_RANGE</td>
<td>7</td>
</tr>
<tr>
<td>ID_IPV6_ADDR_RANGE</td>
<td>8</td>
</tr>
<tr>
<td>ID_DER_ASN1_DN</td>
<td>9</td>
</tr>
<tr>
<td>ID_DER_ASN1_GN</td>
<td>10</td>
</tr>
<tr>
<td>ID_KEY_ID</td>
<td>11</td>
</tr>
<tr>
<td>ID_LIST</td>
<td>12</td>
</tr>
<tr>
<td>ID_OID</td>
<td>13</td>
</tr>
<tr>
<td>Expert Review</td>
<td>14-61439</td>
</tr>
<tr>
<td>Private Use</td>
<td>61440-65535</td>
</tr>
</tbody>
</table>

5. Acknowledgements

The authors thanks Sean Turner, Steffen Fries, Yoav Nir, Vincent Roca, Dennis Bourget, and David Boose for their thoughtful reviews, each of which resulted in substantial improvements to the memo.

6. References
6.1. Normative References


6.2. Informative References


Appendix A. Example ID, SA TEK, and KD payloads for IEC 61850

An IED begins a GROUPKEY-PULL exchange and requests keys and security policy for 61850_UDP_ADDR_GOOSE (OID = 1.2.840.10070.61850.8.1.2 as defined in [IEC-61850-9-2]) and IP multicast address 233.252.0.1 encoded as specified in [IEC-61850-9-2].

OID and OID Specific Payload protocol fields are variable length fields. To improve readability, their representations in Figure 7 and Figure 8 are "compressed" in the figure, as indicated by a trailing "~" for these fields. Implementations should be aware that because these fields are variably sized, some payload fields may not be conveniently aligned on an even octet.

Note 2: The actual DER for the OID Specific Payload field is defined in [IEC-62351-6].

0                   1                   2                   3  
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+++
 ! Next Payload ! RESERVED ! Payload Length !
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+++
 ! ID Type=13 ! DOI-Specific ID Data = 0 !
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+++
 ! OID Len=13 ! OID=<06 0B 2A 86 48 CE 56 83 E3 1A 08 01 02> ~
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+++
 ! OID Specific Payload Len ! OID SP=<DER for 233.252.0.1> ~
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+++

Figure 7: Sample Identification Payload

The Key Server responds with the following SA TEK payload including two GDOI_PROTO_IEC_61850 Protocol-Specific TEK payloads in the second GROUPKEY-PULL message. The first one is to be activated immediately, and has a lifetime of 3600 seconds (0x0E10) remaining. The second
have a lifetime of 12 hours (0xA8C0) and should be activated in 3300 seconds (0x0CE4), which gives a 5 minute (300 seconds) overlap of the two SAs.
Figure 8: Sample IEC-61850 SA Payload
The IED acknowledges that it is capable and willing to use this policy in the third GROUPKEY-PULL message. In response the KS sends a KD payload to the requesting IED. This concludes the GROUPKEY-PULL exchange.
Appendix B. Implementation Considerations

Several topics have been suggested as useful for implementors.

B.1. DER Length Fields

The ID and SA TEK payloads defined in this memo include explicit lengths for fields formatted as DER. This includes the OID Length and OID Specific Payload Length fields shown in Figure 2 and Figure 4. Strictly speaking, these lengths are redundant since the length of the DER value is also encoded within the DER fields. It would be possible to determine the lengths of the fields from those encoded values. However, many implementations will find the explicit length fields convenient when constructing and sanity checking the GDOI messages including these payloads. Implementations will thus be spared from manipulating the DER itself when performing activities that do not otherwise require parsing in order to obtain values therein.

B.2. Groups with Multiple Senders

GCKS policy may specify more than one protected type of IEC 61850 message within a GDOI group. This is represented within a GDOI SA Payload by the presence of an SA TEK Payload for each multicast group that is protected as part of group policy. The OID contained in each of the SA TEK Payloads may be identical, but the value of each OID Specific Payload would be unique. Typically, the OID Specific Payload defines a destination address, and typically there is a single sender to that destination address. XXX what else to say here?
Appendix C. Data Attribute Format

Data attributes attached to an SA TEK following the Data Attribute format described in this section. Data attributes can be in Type/Value (TV) format (useful when a value is defined to be less than two octets in size) or in Type/Length/Value (TLV) form.

The Data Attributes fields are defined as follows:

- **Attribute Type (2 octets)** - Unique identifier for each type of attribute. These attributes are defined as part of the DOI-specific information. The most significant bit, or Attribute Format (AF), indicates whether the data attributes follow the Type/Length/Value (TLV) format or a shortened Type/Value (TV) format. If the AF bit is a zero (0), then the Data Attributes are of the Type/Length/Value (TLV) form. If the AF bit is a one (1), then the Data Attributes are of the Type/Value form.

- **Attribute Length (2 octets)** - Length in octets of the Attribute Value. When the AF bit is a one (1), the Attribute Value is only 2 octets and the Attribute Length field is not present.

- **Attribute Value (variable length)** - Value of the attribute associated with the DOI-specific Attribute Type. If the AF bit is a zero (0), this field has a variable length defined by the Attribute Length field. If the AF bit is a one (1), the Attribute Value has a length of 2 octets.
Brian Weis
Cisco Systems
170 W. Tasman Drive
San Jose, California 95134-1706
USA

Phone: +1 408 526 4796
Email: bew@cisco.com

Maik Seewald
Cisco Systems
Am Soeldnemoos 17
D-85399 Hallbergmoos
Germany

Phone: +49 619 6773 9655
Email: maseewal@cisco.com

Herb Falk
SISCO
6605 19-1/2 Mile Road
Sterling Heights, MI 48314
USA

Phone: +1 586 254 0020 x105
Email: herb@sisconet.com