Internet Engineering Task Force (IETF)
Request for Comments: 8052
Category: Standards Track
ISSN: 2070-1721

B. Weis
M. Seewald
Cisco Systems
H. Falk
SISCO

June 2017

Group Domain of Interpretation (GDOI) Protocol Support for IEC 62351 Security Services

Abstract

The IEC 61850 power utility automation family of standards describes 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 is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc8052.

Table of Contents

1. Introduction 2
1.1. Requirements Language 4
1.2. Terminology 4
1.3. Acronyms 4
2. IEC 61850 Protocol Information 5
2.1. ID Payload 5
2.2. SA TEK Payload 6
2.3. KD Payload 11
3. Security Considerations 12
4. IANA Considerations 14
5. References 16
5.1. Normative References 16
5.2. Informative References 16
Appendix A. Example ID, SA TEK, and KD Payloads for IEC 61850 . 19
Appendix B. Implementation Considerations 23
B.1. DER Length Fields 23
B.2. Groups with Multiple Senders 23
Appendix C. Data Attribute Format 23
Acknowledgements 24
Authors' Addresses 25

1. Introduction

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 in 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 Protocol-ID for the particular 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.

This memo extends RFC 6407 in order to define extensions needed by IEC 62351-9. With the current IANA registry rules set up by RFC 6407, this requires "Standards Action" [RFC5226] by the IETF; this document satisfies that requirement. As the relevant IEC specifications are not available to the IETF community, it is not possible for this RFC to fully describe the security considerations that apply. Therefore, implementers need to depend on the security analysis within the IEC specifications. As two different Standards Development Organizations are involved here, and since group key management is inherently complex, it is possible that some security issues have not been identified, so additional analysis of the security of the combined set of specifications may be advisable.

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

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 frames between substation devices.

1.3. Acronyms

The following acronyms are used throughout this document:

AES	Advanced Encryption Standard
GCKS	Group Controller/Key Server
GDOI	Group Domain of Interpretation
GM	Group Member
GOOSE	Generic Object Oriented Substation Events
KD	Key Download
KEK	Key Encryption Key
MAC	Message Authentication Code
SA	Security Association
SPI	Security Parameter Index
TEK	Traffic Encryption Key

2. IEC 61850 Protocol Information

The following subsections 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 the KD payload key types is included.

All multi-octet fields are in network byte order.

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.

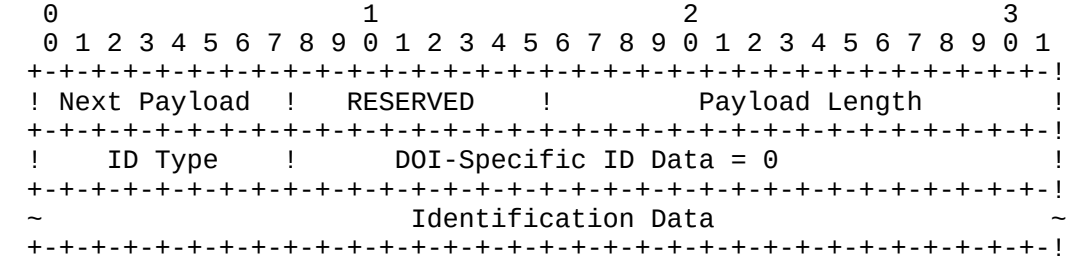

Figure 1: RFC 6407 Identification Payload

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.

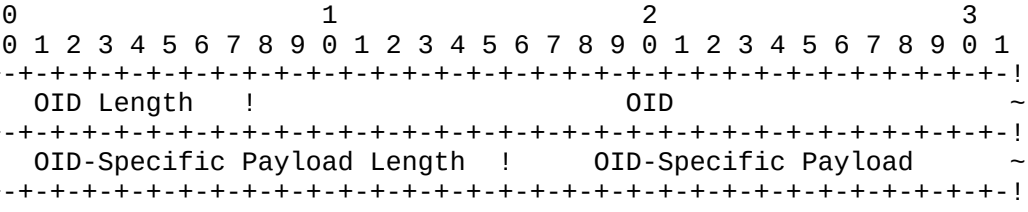

Figure 2: ID_OID Identification Data

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.

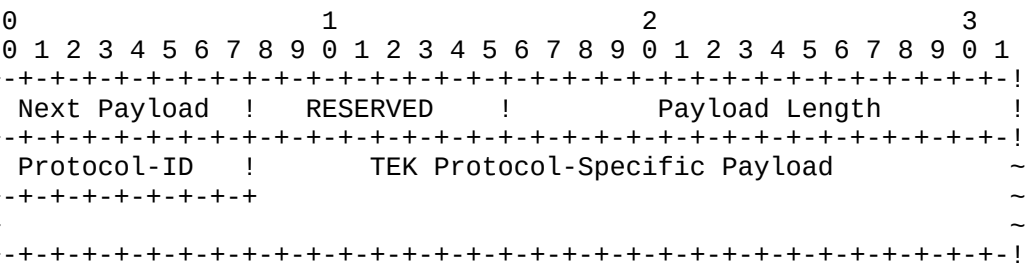

Figure 3: RFC 6407 SA TEK Payload

The Protocol-ID name of GDOI_PROTO_IEC_61850 (value 3) 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.

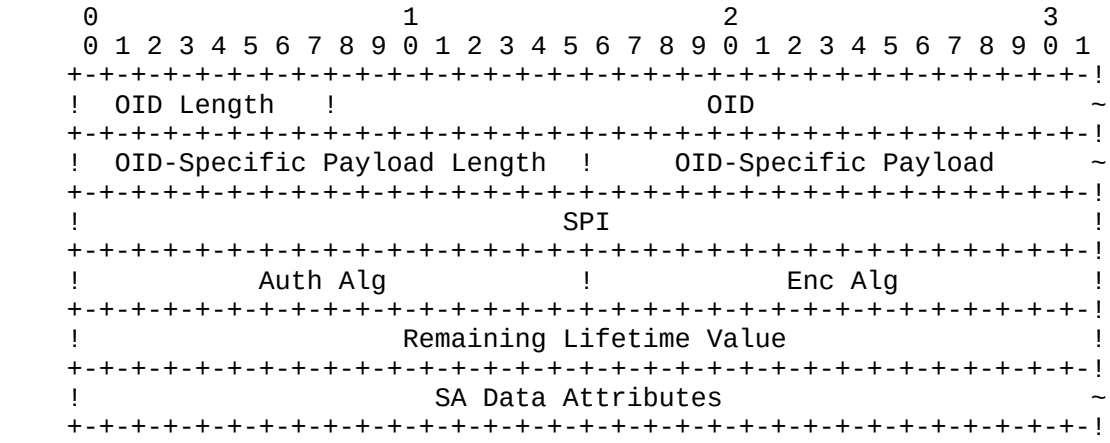

Figure 4: IEC 61850 SA TEK Payload

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 an SPI.

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

- Enc Alg (2 octets) -- Confidentiality Algorithm ID. Valid values are defined 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 2.2.4 defines attributes.

2.2.1. Selectors

The OID and (optionally) an OID-Specific payload 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 Key Server (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.

- NONE. Specifies that an authentication algorithm is not required, or when the accompanying confidentiality algorithm includes authentication (e.g., AES-GCM-128). See Section 3 for cautionary notes regarding using this value without any confidentiality algorithm.

- HMAC-SHA256-128. Specifies the use of SHA-256 [FIPS180-4] 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 [FIPS180-4] combined with HMAC [RFC2104]. The key size is the size of the hash value produced by SHA-256 (256 bits).

- AES-GMAC-128. Specifies the use of AES [FIPS197] in the Galois Message Authentication Code (GMAC) mode [SP.800-38D] with a 128-bit key size.

- AES-GMAC-256. Specifies the use of AES [FIPS197] in the Galois Message Authentication Code (GMAC) mode [SP.800-38D] with a 256-bit key size.

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.

- NONE. Specifies that confidentiality is not required. Note: See Section 3 for guidance on cautionary notes regarding using this value.

- 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. This encryption algorithm does not provide authentication and MUST NOT be used with the NONE authentication algorithm.

- 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. This encryption algorithm does not provide authentication and MUST NOT be used with the NONE authentication algorithm.

- AES-GCM-128. Specifies the use of AES [FIPS197] in the Galois/ Counter Mode (GCM) mode [SP.800-38D] with a 128-bit key size. This encryption algorithm provides authentication and is used with a NONE authentication algorithm.

- 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. This encryption algorithm provides authentication and is used with a NONE authentication algorithm.

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 transmitting 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 describes an ACTIVATION_TIME_DELAY attribute for the Group Associated Policy (GAP) payload, which is applied to all Security Associations and is 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 an SPI must be defined. An 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 an 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 an SPI (i.e., an IEC 61850 Key Identifier). The RFC 6407 KD payload format is reproduced in Figure 5.

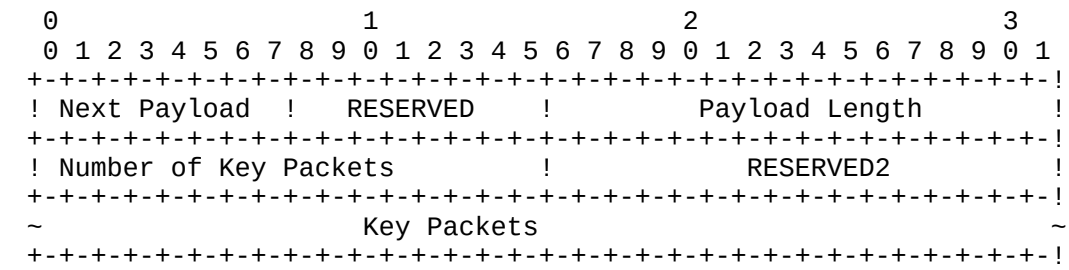

Figure 5: KD Payload

Each Key Packet holds the keying material associated with a particular IEC 61850 Key Identifier, although GDOI refers to it as an 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.

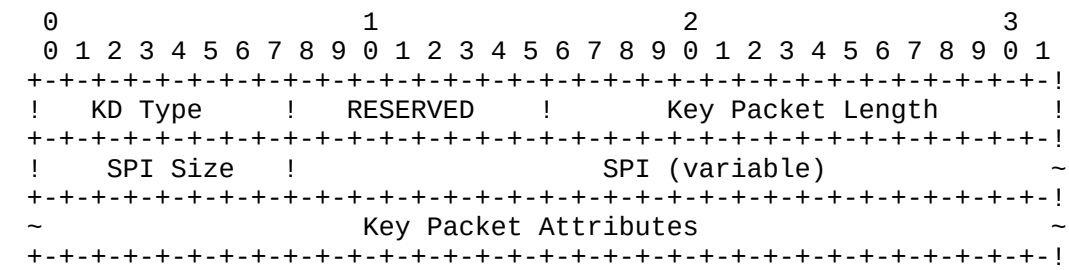

Figure 6: Key Packet

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.

- 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:

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

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

- 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.

- 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 that 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 an optional property for IEC 62351 Security Services; however, when encryption is used, authentication MUST also be provided by using an authenticated encryption algorithm such as AES-GCM-128 or by using a specific authentication algorithm such as HMAC-SHA-256. Setting the authentication algorithm to NONE but setting the confidentiality algorithm to an algorithm that does not

include authentication (i.e., is marked with an N in the "Authenticated Encryption" column of the "IEC 62351-9 Confidentiality Values" registry) is not safe and MUST NOT be done.

When Message Authentication is used, a common practice is to truncate the output of a MAC and include some 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 are 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.800-131A], but some security policies may require the use of AES-CBC-256.

IEC 62351 Security Services describe a variety of policy choices for protecting network traffic, including the option of specifying no protection at all. This is enabled with the use of NONE as an authentication algorithm and/or confidentiality algorithm. The following guidance is given regarding the use of NONE.

- Setting both the authentication algorithm and confidentiality algorithm to NONE is possible but NOT RECOMMENDED. Setting such a policy is sometimes necessary during a migration period, when traffic is being protected incrementally and some traffic has not yet been scheduled for protection. Alternatively, site security policy for some packet flows requires inspection of packet data on the private network followed by network-layer encryption before delivery to a public network.

- Setting the confidentiality algorithm to NONE but setting the authentication algorithm to a MAC can be an acceptable policy in the following conditions: the disclosed information in the data packets is comprised of raw data values and the disclosure of the data files is believed to be of no more value to an observer than traffic analysis on the frequency and size of packets protected for confidentiality. Alternatively, site security policy for some packet flows requires inspection of packet data on the private network followed by network-layer encryption before delivery to a public network.

- Setting the authentication algorithm to NONE but setting the confidentiality algorithm to an algorithm that does not include authentication is not safe and MUST NOT be done.

4. IANA Considerations

The "Group Domain of Interpretation (GDOI) Payloads" registry [GDOI-REG] has been updated as described below. The terms "Expert Review", "Reserved", and "Private Use" are used as defined in [RFC5226].

- GDOI_PROTO_IEC_61850 (value 3) has been added to the "SA TEK Payload Values - Protocol-ID" registry.

- A new "IEC 62351-9 Authentication Values" registry has been created. This registry defines Auth Alg values. Initial values for the registry are given below; future assignments are to be made through "Expert Review" [RFC5226].

Name	Value
Reserved	0
NONE	1
HMAC-SHA256-128	2
HMAC-SHA256	3
AES-GMAC-128	4
AES-GMAC-256	5
Unassigned	6-61439
Reserved for Private Use	61440-65535

- A new "IEC 62351-9 Confidentiality Values" registry has been created. This registry defines Enc Alg values. Initial values for the registry are given below; future assignments are to be made through "Expert Review" [RFC5226].

Name	Value	Authenticated Encryption
Reserved	0	
NONE	1	
AES-CBC-128	2	N
AES-CBC-256	3	N
AES-GCM-128	4	Y
AES-GCM-256	5	Y
Unassigned	6-61439	
Reserved for Private Use	61440-65535	

- A new "GDOI SA TEK Attributes" registry has been created. This registry defines SA TEK attributes. Initial values for the registry are given below; future assignments are to be made through "Expert Review" [RFC5226]. In the table, attributes that are defined as Type/Value (TV) are marked as Basic (B); attributes that are defined as Type/Length/Value (TLV) are marked as Variable (V).

Attribute	Value	Type
Reserved	0	
SA_ATD	1	V
SA_KDA	2	B
Unassigned	3-28671	
Reserved for Private Use	28672-32767	

- A new "ID Types" registry has been created for the Identification Payload when the DOI is GDOI. This registry is taken from the "IPSEC Identification Type" registry for the IPsec DOI [IPSEC-DOI-REG]. Values 1-12 are defined identically to the equivalent values in the "IPSEC Identification Type" registry. Value 13 (ID_OID) is defined in this memo. Initial values for the registry are given below; future assignments are to be made through "Expert Review" [RFC5226].

Name	Value
Reserved	0
ID_IPV4_ADDR	1
ID_FQDN	2
ID_USER_FQDN	3
ID_IPV4_ADDR_SUBNET	4
ID_IPV6_ADDR	5
ID_IPV6_ADDR_SUBNET	6
ID_IPV4_ADDR_RANGE	7
ID_IPV6_ADDR_RANGE	8
ID_DER_ASN1_DN	9
ID_DER_ASN1_GN	10
ID_KEY_ID	11
ID_LIST	12
ID_OID	13
Unassigned	14-61439
Reserved for Private Use	61440-65535

5. References

5.1. Normative References

[IEC-62351-9]
International Electrotechnical Commission, "Power systems management and associated information exchange - Data and communications security - Part 9: Cyber security key management for power system equipment", IEC 62351-9:2017, May 2017.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, DOI 10.17487/RFC5226, May 2008, <http://www.rfc-editor.org/info/rfc5226>.

[RFC6407] Weis, B., Rowles, S., and T. Hardjono, "The Group Domain of Interpretation", RFC 6407, DOI 10.17487/RFC6407, October 2011, <http://www.rfc-editor.org/info/rfc6407>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <http://www.rfc-editor.org/info/rfc8174>.

5.2. Informative References

[FIPS180-4]
National Institute of Standards and Technology, "Secure Hash Standard", FIPS PUB 180-4, DOI 10.6028/NIST.FIPS.180-4, August 2015, <http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf>.

[FIPS197] National Institute of Standards and Technology, "Advanced Encryption Standard (AES)", FIPS PUB 197, November 2001, <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>.

[GDOI-REG]
IANA, "Group Domain of Interpretation (GDOI) Payloads", <http://www.iana.org/assignments/gdoi-payloads>.

[IEC-61850-8-1]
International Electrotechnical Commission, "Communication networks and systems for power utility automation - Part 8-1: Specific communication service mapping (SCSM) - Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3", IEC 61850-8-1, June 2011.

[IEC-61850-9-2]
International Electrotechnical Commission, "Communication networks and systems for power utility automation - Part 9-2: Specific communication service mapping (SCSM) - Sampled values over ISO/IEC 8802-3", IEC 61850-2, September 2011.

[IEC-62351-6]
International Electrotechnical Commission, "Power systems management and associated information exchange - Data and communications security - Part 6: Security for IEC 61850", IEC 62351-6, June 2007.

[IEC-TR-61850-90-5]
International Electrotechnical Commission, "Communication networks and systems for power utility automation - Part 90-5: Use of IEC 61850 to transmit synchrophasor information according to IEEE C37.118", IEC TR 62351-90-5, May 2012.

[IPSEC-DOI-REG]
IANA, "'Magic Numbers' for ISAKMP Protocol", <http://www.iana.org/assignments/isakmp-registry>.

[ITU-T-X.683]
International Telecommunications Union, "Information technology - Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 specifications", ITU-T Recommendation X.683, August 2015, <https://www.itu.int/rec/T-REC-X.683-201508-I/en>.

[ITU-T-X.690]
International Telecommunications Union, "Information technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)", ITU-T Recommendation X.690, August 2015, <https://www.itu.int/rec/T-REC-X.690-201508-I/en>.

[RFC2104] Krawczyk, H., Bellare, M., and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, DOI 10.17487/RFC2104, February 1997, <http://www.rfc-editor.org/info/rfc2104>.

[SP.800-131A] Barker, E. and A. Roginsky, "Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths", NIST Special Publication 800-131A, DOI 10.6028/NIST.SP.800-131Ar1, November 2015, <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar1.pdf>.

[SP.800-38A] Dworkin, M., "Recommendation for Block Cipher Modes of Operation: Methods and Techniques", NIST Special Publication 800-38A, DOI 10.6028/NIST.SP.800-38A, December 2001, <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a.pdf>.

[SP.800-38D] Dworkin, M., "Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC", NIST Special Publication 800-38D, DOI 10.6028/NIST.SP.800-38D, November 2007, <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38d.pdf>.

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

An Intelligent Electronic Device (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 Figures 7 and 8 are "compressed", 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: The actual DER for the OID-Specific Payload field is defined in [IEC-62351-6].

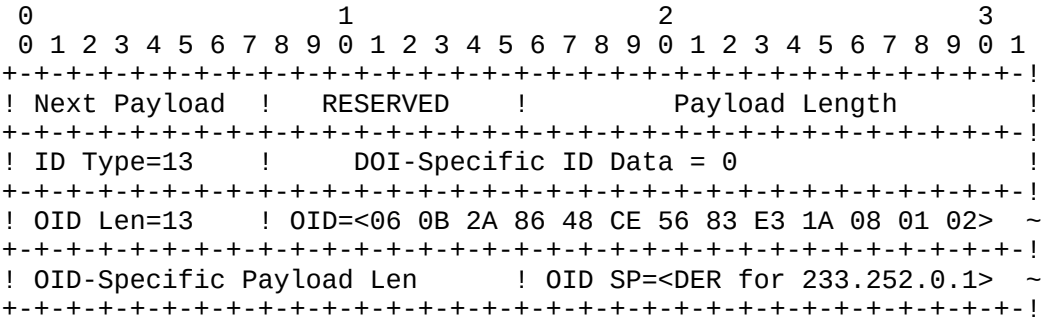

Figure 7: Sample Identification Payload

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 has a lifetime of 12 hours (0xA8C0) and should be activated in 3300 seconds (0x0CE4), which gives a 5-minute (300-second) overlap of the two SAs.

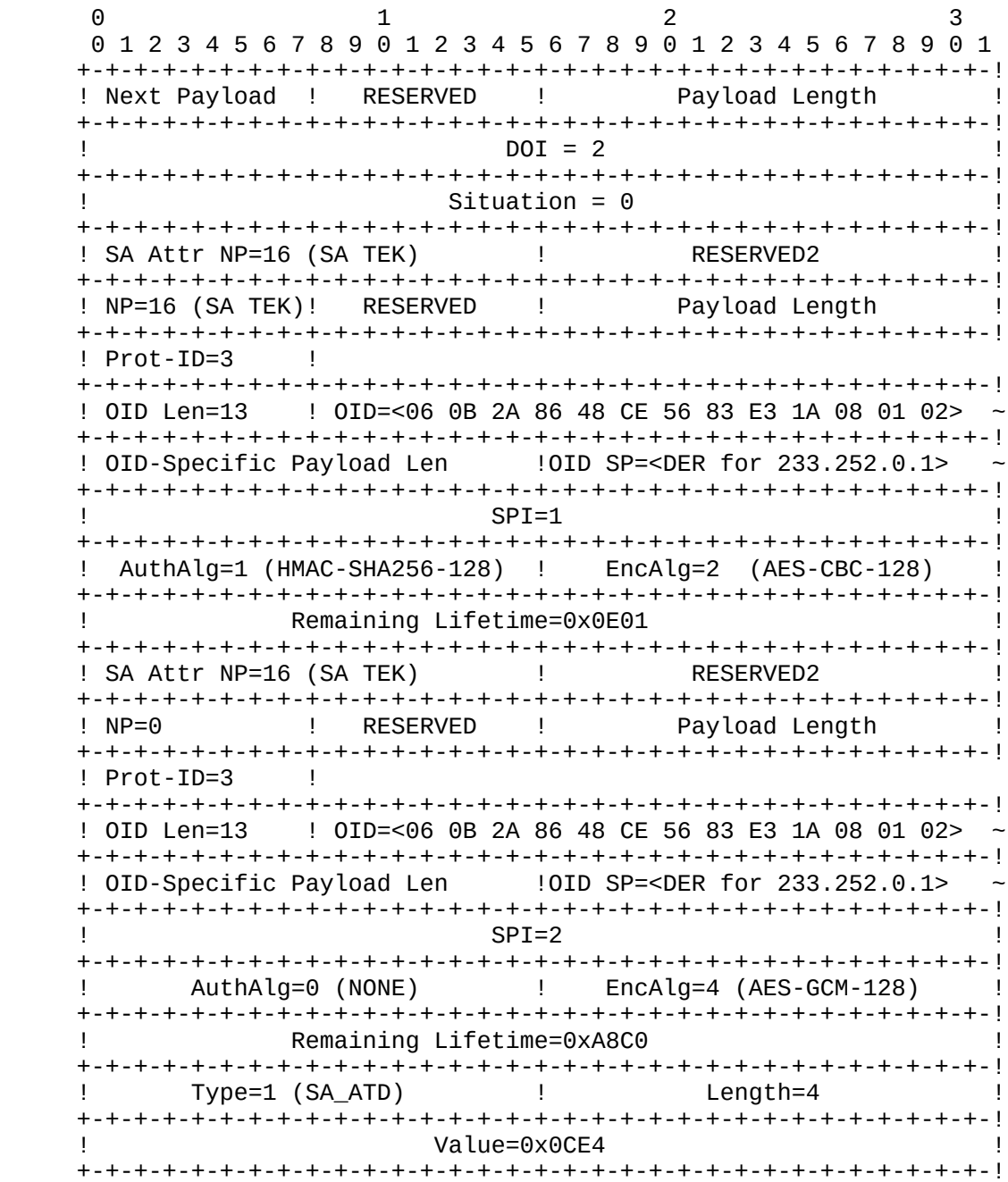

Figure 8: Sample IEC 61850 SA Payload

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.

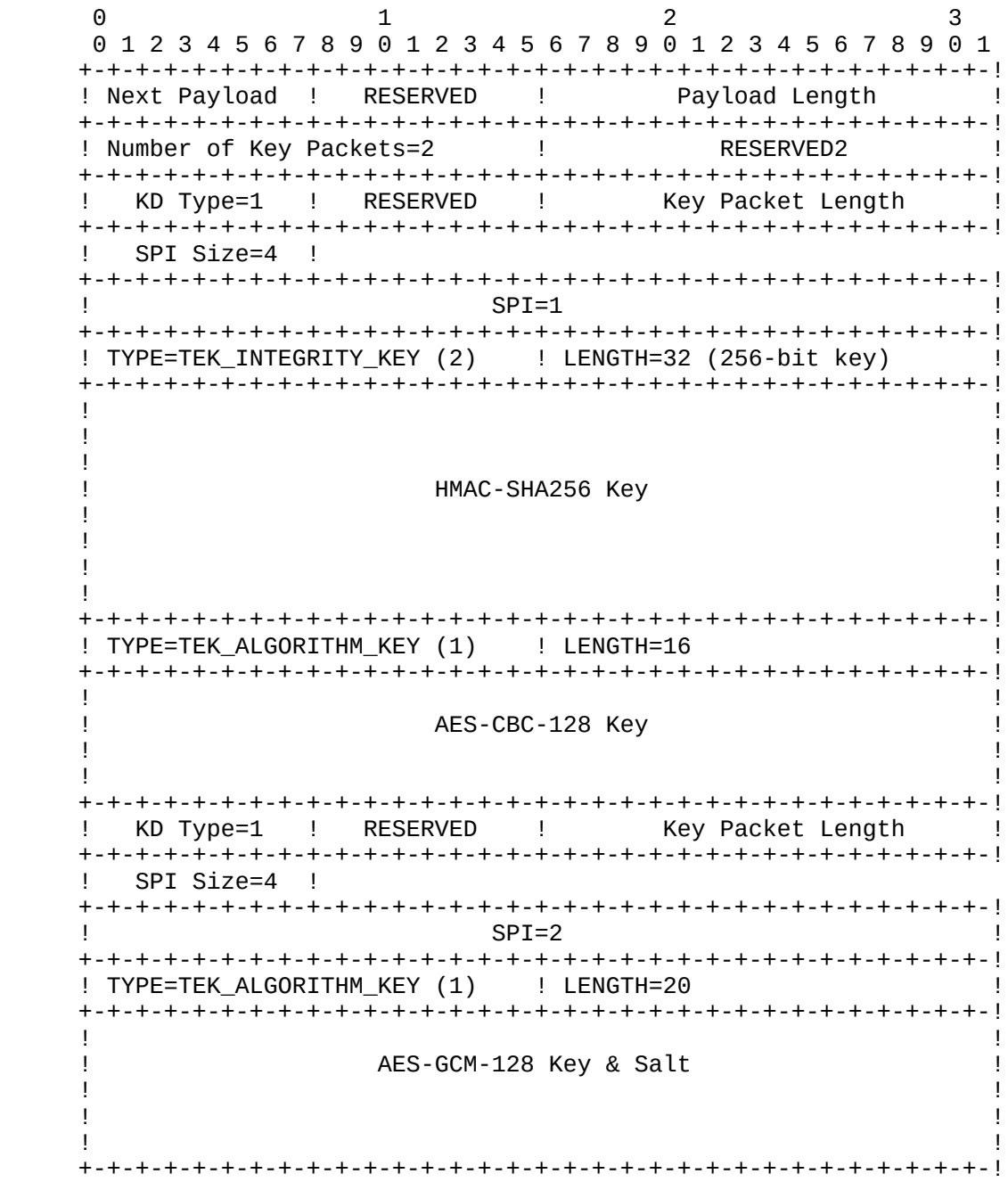

Figure 9: Sample KD Payload

Appendix B. Implementation Considerations

Several topics have been suggested as useful for implementers.

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 Figures 2 and 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 there is typically a single sender to that destination address.

Appendix C. Data Attribute Format

Data attributes attached to an SA TEK following the data attribute format are 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.

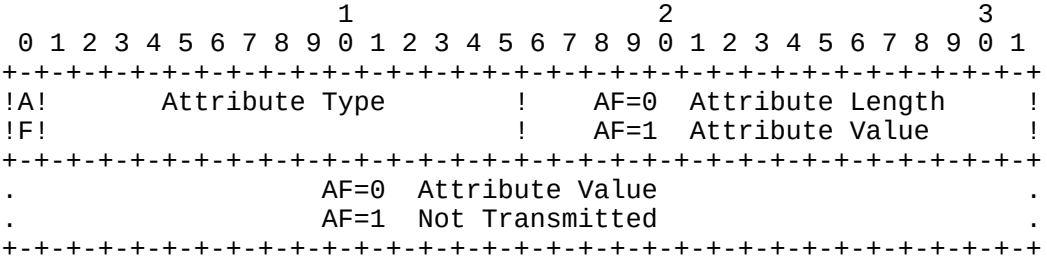

Figure 10: Data Attributes

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.

Acknowledgements

The authors thank 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 this memo. Joe Salowey provided valuable guidance as document shepherd during the publication process. The authors are indebted to Kathleen Moriarty for her agreement to sponsor the publication of the document.

Authors' Addresses

Brian Weis
Cisco Systems
170 W. Tasman Drive
San Jose, California 95134-1706
United States of America

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

Maik Seewald
Cisco Systems
Am Soeldnermoos 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
United States of America

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