Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: February 3, 2014

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

August 2, 2013

IEC 62351 Security Protocol support for GDOI
draft-weis-gdoi-iec62351-9-02

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

Copyright Notice

Table of Contents

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] has specified the use of GDOI [RFC6407] to distribute security policy and session keying material protecting these frames.

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 for IEC 61850, 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.

1.3. Acronyms and Abbreviations

The following acronyms and abbreviations are used throughout this document

GCKS	Group Controller/Key Server
GDOI	Group Domain of Interpretation
GM	Group Member
GOOSE	Generic Object Oriented Substation Events
KD	Key Download Payload
KEK	Key Encryption Key
SA	Security Association
SPI	Security Parameter Index
TEK	Traffic Encryption Key

2. IEC 61850 Protocol Information

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
    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 ASN.1 Object Identifier (OID) [ITU-T-X.683]. Associated with the OID may be an OID Specific Payload 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.

```
    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
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-!
   !  OID Length   !                     OID                       ~
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-!
   !  OID Specific Payload Length  !     OID Specific Payload      ~
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-!
```

Figure 2: ID_OID Identification Data

The ID_OID Identification Data fields are defined as follows:

- OID Length (1 octet) -- Total length of the ASN.1 encoded OID.

- OID (variable) -- An ASN.1 encoded ObjectIdentifier using Distinguished Encoding Rules (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. 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.

```
     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        !
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-!
    ! Protocol-ID   !       TEK Protocol-Specific Payload           ~
    +-+-+-+-+-+-+-+-+                                               ~
    ~                                                               ~
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-!
```

Figure 3: RFC 6407 SA TEK Payload

The Protocol-ID name of GDOI_PROTO_IEC_61850 (value TBD1) is defined in this memo for the purposes of distributing IEC 61850 policy. An 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.

```
      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
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-!
     !  OID Length   !                       OID                     ~
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-!
     !  OID Specific Payload Length  !     OID Specific Payload      ~
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-!
     ! Current KeyID !   RESERVED    ! CK Remaining Lifetime Value   !
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-!
     !          CK Auth Alg          !           CK Key Alg          !
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-!
     !  Next KeyID   !   RESERVED    ! NK Remaining Lifetime Value   !
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-!
     !          NK Auth Alg          !           NK Key Alg          !
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-!
```

Figure 4: IEC-61850 SA TEK Payload

The GDOI_PROTO_IEC_61850 SA TEK Payload fields are defined as follows:

- OID Length (1 octet) -- Total length of the ASN.1 encoded OID.

- OID (variable) -- An ASN.1 encoded using Distinguished Encoding Rules (DER) ObjectIdentifier. OIDs defined in IEC 61850 declare the type of traffic to be encrypted.

- 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. 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.

- Current KeyID (1 octet) -- Identifier for the Current Key. This field represents a SPI.

- RESERVED (1 octet) -- MUST be zero, and MUST be ignored on receipt.

- CK Remaining Lifetime value (2 octets) -- The number of minutes prior to the next scheduled Current Key change. A value of zero (0) shall indicate that no key change has been scheduled.

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

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

- Next KeyID (1 octet) -- Identifier for the Next Key. This field represents a SPI.

- RESERVED (1 octet) -- MUST be zero, and MUST be ignored on receipt.

- NK Remaining Lifetime value (2 octets) -- The number of minutes prior to the next scheduled Next Key change. A value of zero (0) shall indicate that no key change has been scheduled.

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

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

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].

- HMAC-SHA256-80. Specifies the use of SHA-256 [FIPS180-3.2008] combined with HMAC [RFC2104]. The output is truncated to 80 bits, as per [RFC2104]. The key size is the size of the hash value produced by SHA-256 (256 bits).

- 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].

- NONE. Specifies that no Confidentiality Algorithm is to used.

- 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.

2.2.4. 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). It's size is 1 octet. The KeyID is unilaterally chosen by the GCKS using any method chosen by the implementation. However, an implementation needs to take care not to duplicate a KeyID value that is currently in use for a particular group.

2.3. Key Download Payload

The Key Download 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.

```
     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        !
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+!
    ! Number of Key Packets         !            RESERVED2          !
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+!
    ~                    Key Packets                                ~
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+!
```

Figure 5: Key Download Payload

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. based upon the security policy of the group as defined by the associated SA Payload. Each Key Packet has the following format, reproduced in Figure 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
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+!
    !   KD Type     !   RESERVED    !            KD Length          !
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+!
    !    SPI Size   !                   SPI (variable)              ~
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+!
    ~                    Key Packet Attributes                      ~
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+!
```

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 CK Auth Alg and NK Auth Alg SA TEK fields) MUST be distributed as a TEK_INTEGRITY_KEY attribute, and a key associated with an IEC 61850 Confidentiality Algorithm (distributed in the CK Key Alg and NK Key Alg SA TEK fields) MUST be distributed as a TEK_ALGORITHM_KEY attribute.

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.

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 GDOI_PROTO_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 Specification Required and Private Use are to be applied as defined in [RFC5226].

Name	Value
Reserved	0
HMAC-SHA256-80	1
HMAC-SHA256-128	2
HMAC-SHA256	3
Specification Required	4-61439
Private Use	61440-65535

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

Name	Value
Reserved	0
NONE	1
AES-CBC-128	2
AES-CBC-256	3
Specification Required	4-61439
Private Use	61440-65535

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 Specification Required and Private Use are to be applied as defined in [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
Specification Required	14-61439
Private Use	61440-65535

5. Acknowledgements

The authors thanks Sean Turner for his careful review, which resulted in several improvements to the memo.

6. References

6.1. Normative References

[IEC-62351-9]
International Electrotechnical Commission, "IEC 62351 Part 9 - Key Management", IEC 62351-9 , January 2013.

[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 62351-9 , May 2012.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, May 2008.

[RFC6407] Weis, B., Rowles, S., and T. Hardjono, "The Group Domain of Interpretation", RFC 6407, October 2011.

6.2. Informative References

[FIPS180-3.2008]
National Institute of Standards and Technology, "Secure Hash Standard", FIPS PUB 180-3, October 2008, <http://csrc.nist.gov/publications/fips/fips180-3/fips180-3_final.pdf>.

[FIPS197] "Advanced Encryption Standard (AES)", United States of America, National Institute of Science and Technology, Federal Information Processing Standard (FIPS) 197, November 2001.

[GDOI-REG]
Internet Assigned Numbers Authority, "Group Domain of Interpretation (GDOI) Payload Type Values", IANA Registry, December 2004, <http://www.iana.org/assignments/gdoi-payloads/gdoi-payloads.xml>.

[IEC-61850-8-1]
International Electrotechnical Commission, "Specific 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.

[ITU-T-X.683]
"Information technology - Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 specifications", SERIES X: DATA NETWORKS AND OPEN SYSTEM COMMUNICATIONS OSI networking and system aspects - Abstract Syntax Notation One (ASN.1) , July 2002, <http://www.itu.int/ITU-T/studygroups/com17/languages/X.683-0207.pdf>.

[ITU-T-X.690]
"Information technology-ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)", SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY OSI networking and system aspects - Abstract Syntax Notation One (ASN.1) , 2008, <https://www.itu.int/rec/T-REC-X.690-200811-I>.

[RFC2104] Krawczyk, H., Bellare, M., and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, February 1997.

[SP.800-38A]
Dworkin, M., "Recommendation for Block Cipher Modes of Operation", United States of America, National Institute of Science and Technology, NIST Special Publication 800-38A 2001 Edition, December 2001.

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 (an OID defined in [IEC-61850-9-2]) and IP multicast address 233.252.0.1.

```
      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       ! OID=<ASN.1 for 1.2.840.10070.61850.8.1.2>     ~
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-!
     ! OID Specific Payload Len      !OID SP=<ASN.1 for 233.252.0.1> ~
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-!
```

Sample Identification Payload

The Key Server responds with the following SA TEK payload including a single GDOI_PROTO_IEC_61850 Protocol-Specific TEK payload in the second GROUPKEY-PULL message.

```
      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        !
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-!
     !                             DOI = 2                           !
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-!
     !                         Situation = 0                         !
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-!
     ! SA Attr NP=16 (SA TEK)        !          RESERVED2            !
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-!
     ! Prot-ID=TBD1  !
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-!
     ! OID Len       ! OID=<ASN.1 for k>     ~
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-!
     ! OID Specific Payload Len      !OID SP=<ASN.1 for 233.252.0.1> ~
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-!
     ! Cur KeyID=1   !   RESERVED    ! CK Remaining Lifetime=0x3600  !
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-!
     ! CK AuthAlg=1 (HMAC-SHA256-80) !  CK Key Alg=2  (AES-CBC-128)  !
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-!
     !  Next KeyID=2 !   RESERVED    ! NK Remaining Lifetime=0xffff  !
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-!
     ! CK AuthAlg=2 (HMAC-SHA256-128)!  CK Key Alg=1  (NONE)         !
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-!
```

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.

```
      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        !
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-!
     ! Number of Key Packets=2       !            RESERVED2          !
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-!
     !   KD Type=1   !   RESERVED    !            KD Length=30       !
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-!
     !    SPI Size=1 !      SPI=1    !
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-!
     ! TYPE=TEK_INTEGRITY_KEY (2)    ! LENGTH=32 (256-bit key)       !
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-!
     !                                                               !
     !                                                               !
     !                                                               !
     !                        HMAC-SHA256 Key                        !
     !                                                               !
     !                                                               !
     !                                                               !
     !                                                               !
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-!
     ! TYPE=TEK_ALGORITHM_KEY (1)    ! LENGTH=16                     !
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-!
     !                                                               !
     !                        AES-CBC-128 Key                        !
     !                                                               !
     !                                                               !
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-!
     !   KD Type=1   !   RESERVED    !            KD Length=42       !
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-!
     !    SPI Size=1 !      SPI=2    !
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-!
     ! TYPE=TEK_INTEGRITY_KEY (2)    ! LENGTH=32 (256-bit key)       !
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-!
     !                                                               !
     !                                                               !
     !                                                               !
     !                        HMAC-SHA256 Key                        !
     !                                                               !
     !                                                               !
     !                                                               !
     !                                                               !
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-!
```

Sample Key Download Payload

Authors' Addresses

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 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
USA

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