(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
17 January 2013 (17.01.2013)

WIPO | PCT

(10) International Publication Number
WO 2013/009420 A1

(51) International Patent Classification:
H04L 9/08 (2006.01)

(21) International Application Number:
PCT/US2012/041971

(22) International Filing Date:
11 June 2012 (11.06.2012)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/495.173 9 June 2011 (09.06.2011) US

(71) Applicant *(for all designated States except US)*: **POWER TAGGING TECHNOLOGIES, INC.** [US/US]; 5425 Airport Boulevard, Boulder, CO 80301 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **BERNHEIM, Henrick, F.** [US/US]; 7777 E. 1st Place, #109, Denver, CO 80230 (US). **MARTIN, Marcia, Reid** [US/US]; 3067 Stevens Circle South, Erie, CO 80516 (US). **BERENS, Steven, J.** [US/US]; 6368 Swallow Lane, Boulder, CO 80303 (US). **LOPORTO, John, J.** [US/US]; 900 South Wiley, Superior, CO 80027 (US). **NIEMANN, Theodore, V.** [US/US]; 3708 Wild View Drive, Fort Collins, CO 80501 (US).

(74) Agent: **HUGHES, Scott, A.**; HOGAN LOVELLS US LLP, 555 Thirteenth Street, NW, Washington, DC 20004 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

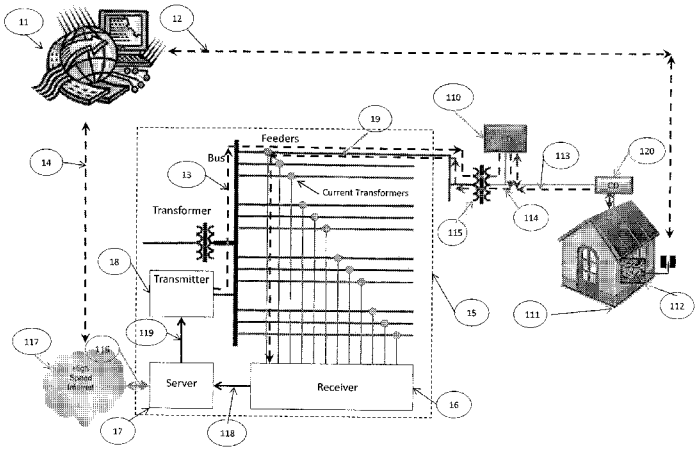
Published:

— *with international search report (Art. 21(3))*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

(54) **Title**: SYSTEM AND METHOD FOR GRID BASED CYBER SECURITY

FIGURE 1
BIDIRECTIONAL ON-GRID LONG-RANGE COMMUNICATIONS



(57) **Abstract**: A method and system for providing a secure communication network using an electrical distribution grid is disclosed. A device connected to the electrical distribution grid initiates a request for a secured key token by signaling an intelligent communicating device residing at or near an edge of the grid. The intelligent communicating device forwards the request to a receiver at a distribution substation on the electrical grid. This receiver enhances the properties of the request such that a grid location for the request can be inferred. The enhanced request is forwarded to a server at the distribution substation, which compares the request grid location to a Grid Map and Policies of known secure grid locations. Any inconsistencies between the grid location inferred from the enhanced request and the Grid Map and Policies locations are considered evidence of tampering, and the server rejects the request.

WO 2013/009420 A1

SYSTEM AND METHOD FOR GRID BASED CYBER SECURITY

CROSS REFERENCE TO RELATED APPLICATIONS

This application claims the benefit of priority of U.S. Provisional Patent Application Serial Number 61/495,173, filed June 9, 2011, the entirety of which is hereby incorporated by references.

BACKGROUND OF THE INVENTION

1. Field of the Invention.

The present invention is directed generally toward the domain of network security, and in particular toward the use of the electrical distribution grid with a system for establishing the schematic location of nodes on the electrical distribution grid, as a key-courier network and as a means for authenticating the key requestor.

2. Background of the Invention

The electrical grid in the United States and most other areas of the world is historically divided into two networks: the transmission grid and the distribution grid. The transmission grid originates at a generation point, such as a coal-burning or atomic power plant, or a hydroelectric generator at a dam. DC power is generated, converted to high-voltage AC, and transmitted to distribution points, called distribution substations, via a highly controlled and regulated, redundant, and thoroughly instrumented high-voltage network. This high-voltage network has at its edge a collection of distribution substations. Over the last century, as the use of electrical power became more ubiquitous and more essential, and as a complex market in the trading and sharing of electrical power emerged, the technology of the transmission grid largely kept pace with the technological requirements of the market.

The second network, the distribution grid, is the portion of the electrical grid which originates at the distribution substations and has at its edge a collection of residential, commercial, and industrial consumers of energy. In contrast to the transmission grid, the technology of the distribution grid has remained relatively static since the mid-1930s until very recent years. Today, as concern grows over the environmental effects of fossil fuel usage and the depletion of non-renewable energy sources, interest has increased in augmenting the electrical distribution grid with communication instruments. The primary goals of this activity are energy-

related - such as energy conservation, resource conservation, cost containment, and continuity of service. However, a side effect of establishing such networks is the ability to transmit information over an existing network, the distribution grid itself, which has special properties that enhance the security and particularly the authenticity and non-repudiability of transmitted messages.

Binary digital encryption has largely superseded all other forms of ciphers as the means of encoding sensitive communications in this digital age. Encryption and decryption algorithms require three components to work: the data itself (in the clear for encryption, or the encrypted string for decryption), a well-known algorithm, and a binary string called a key which must be known in order to drive the algorithm to produce the proper results.

Two major classes of encryption algorithms are in use and well-known in the art. In one class, the same key is used for both encryption and decryption, so that both the data source and the data destination have a copy of the key. These algorithms, typified by the Advanced Encryption Standard (AES), are known as *symmetric key* or *shared secret* methods. Such methods, especially AES itself, are favored for embedded or machine-to-machine applications because the algorithms are relatively low-cost in terms of code space and execution time, and because the keys are relatively short (128 to 256 bits at present). Also, if the data payload is carefully chosen, as little as one bit is added to the message length by the encryption process. This added length is called *overhead.*

Algorithms of the second major class are known as *asymmetric key* or *public key* methods. In these schemes, a different key is used to encrypt the data than is used to decrypt the data. The encryption key is publically known, so that anyone can send an encrypted message. The decryption key must be kept private in order to preserve message security. Public key methods are favored for lower-traffic applications such as client-server or web-service applications, where a broadband network and relatively powerful computers are used at both ends of a secure transaction. The keys are longer, the algorithms are more complex, and the overhead is higher than in symmetric key methods. One well-known method of mitigating the computational and data overhead of public key encryption is to use it only for initially authenticating and establishing a secure session, and exchanging a shared secret. Then longer messages can be exchanged using symmetric-key encryption.

The elements of data security include Privacy, Authentication, Integrity, and Non-repudiation (PAIN). Encryption itself provides only the privacy element, in that it ensures that an agency who is merely intercepting signals on a network cannot extract the information encoded in a signal sequence or message. Authentication is the process of ensuring that an agency initiating or responding to a secure transaction is who it claims to be and not a malicious intruder. Integrity refers to the ability to detect tampering with a message in transit, and either prevent it or make it evident. Non-repudiability means the sender cannot deny having sent the message which was received.

Regardless of the encryption method used, the primary security risks in data communications are not associated with "breaking" the encryption but with other elements of PAIN. Primarily, risks arise from the failure of one of these processes:

- Authenticating the requestor of a key or a secure transaction
- Authenticating the key authority (who may or may not be the agency who receives and decrypts the data)
- Distributing keys in a secure manner
- Establishing that a message actually originated with the purported sender and not some other party who gained access to the encryption key (including the purported receiver, who may self-generate a message and claim to have received it from the purported sender).

Well-known means of ensuring full PAIN security involve both the use of a secure encryption algorithm and either a secure "out of band" means of exchanging keys, a trusted third party (TTP) responsible for generating and distributing keys, or both. The simplest example of this is the case of two individuals A and B who wish to exchange private messages over a computer network. They meet face to face and agree on a secret encryption key and an encryption algorithm. They then separate and use their shared secret to exchange private messages. Because the nature of (good) shared secret keys is such that the probability someone else will choose the same secret as A and B is very low, as long as neither party breaks the trust (reveals the secret), the digital conversation between A and B is private and authenticated. A and B could ensure integrity by making further agreements about the organization or contents (such as a hash code) of the messages. This method is never non-repudiable, however, because A

could generate a message and claim that it came from B, and the message would be indistinguishable from one actually generated by B.

The best-known method for establishing a fully secure channel, known as the Diffie-Hellman method, is based on the existence of asymmetric-key encryption algorithms and is described in U.S. Patent No. 4,200,770 to Hellman et al. In this method, A and B each begin with a pair of distinct asymmetric keys. B sends his public key to A, and A sends his public key to B. A and B now each employs his own private key and his correspondent's public key to generate a value called the shared secret, which is in itself a pair of asymmetric keys. The essence of the Diffie-Hellman method is the proof that the two mismatched pairs of public and private keys can, in fact, be used to independently generate the same shared secret. B then generates a symmetric key, using the "public" portion of the shared secret to encrypt it, and sends it to A. A uses the "private" portion of the shared secret to decrypt the symmetric key. Now, A and B can send private communications back and forth efficiently using the symmetric key. The last step is only needed because of the inefficiency of asymmetric keys as a bulk encryption method.

The Diffie-Hellman algorithm is known to be vulnerable to a form of security attack known as man-in-the-middle. In such attacks, the initial exchange of public keys is intercepted by the attacker, who substitutes different public keys for those sent by A and B. If the attacker can intercept both sides of the exchange long enough to learn the symmetric key, then the attacker can pretend to be either member of the secure exchange, and can eavesdrop on the conversation and even alter the information in transit. Public Key Infrastructures (PKIs) have been created to correct this. In a PKI, a trusted third party (TTP) is used by A and B to mediate the generation and exchange of keys. The TTP does this by combining the public keys with information that authenticates the party wishing to exchange information and with the digital signature of the TTP in a tamper-evident manner. Today, many widely used programs such as web browsers are pre-programmed to recognize and honor the format of such certificates and the signatures of widely-known TTPs, more commonly called Certificate Authorities or CAs.

In the year 2011, there were at least 2 documented cases where well-established and trusted CAs were hacked and fraudulent certificates were issued, allowing the fraudulent issuer to steal information. To date, the only remedy for this has been to revoke trust for CAs known to have issued fraudulent certificates. Additionally, some specialized security needs exist where it

is insufficient to authenticate the requesting user or device. For example, a physician may be authorized to use a mobile device to access electronic patient records from her home or office, but not from an internet café or other public place. In this situation, it is necessary to authenticate not only that the user of the device is the physician, but that the device is not in a public place where a patient's privacy could be compromised. In the most extreme examples of highly-secured operations, it is undesirable for the requesting user's interface device to be connected to a conventional network at all.

SUMMARY OF THE INVENTION

The present invention comprises a system of intelligent communicating devices (ICDs) residing at or near the edge of the electrical distribution grid. The electrical distribution grid comprises at least one central collection point. The ICDs transmit messages to at least one of the central collection points on the electrical distribution grid, using the distribution grid as the transmission medium. At the central collection point, a server is connected to a receiver for on-grid transmissions from the ICD to a gateway to a conventional wide-area network such as the Internet. On the wide-area network resides a central server which is the owner of a conventional Public Key Infrastructure (PKI) certificate, so that communications between the central server and the at least one collection point servers are secured by conventional secure protocols such as Transport Layer Security(TLS) or Secure Socket Layer (SSL). The central server runs a software program, the Authority, which is responsible for granting temporary authorizations for remote users to perform certain secured actions. The receiver at any of the at least one central collection points is capable of inferring the schematic location on the electrical distribution grid of any of the distributed ICDs from characteristics of the signal received from the ICD. On each of the ICDs resides a stored program which acts as the agent of the Authority in relaying requests and grants between remote users and the Authority. This system and method incorporates means of authenticating requestors, authorizing grants, ensuring that the receiver of the grant is the same agency as the requestor, and exchanging encryption keys which are more secure and more constrained to a location in time and space than conventional means alone can accomplish. Multiple embodiments of the invention are described, where in some embodiments all communication between the at least one collection point server and the requestor take place over

the electrical distribution grid, and where in other embodiments a conventional network is employed to return the grant to the requestor, but the security benefits of the invention still apply.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 illustrates a bi-directional on-grid long range communications system according to the present invention.

Figure 2 illustrates an on-grid, mixed mode communications system where no on-grid long-range transmitter is available at the central collection points. A conventional network connection is substituted to permit communication from the central collection points to the ICDs.

Figure 3 illustrates the communication system of the present invention where bi-directional on-grid long range communication is available, but where the Device, PC, or Server has no connection to any conventional bi-directional network.

DETAILED DESCRIPTION OF THE INVENTION

The present invention is directed generally toward the domain of network security, and in particular, toward the use of the electrical distribution grid enhanced with a system for establishing the schematic location of nodes on the electrical distribution grid, as a key-courier network and as a means for authenticating the key requestor.

The invention comprises a system for using an electrical distribution grid as a communication medium, wherein the system may be connected at one or more nodes to a conventional data communications network. The invention further includes a method whereby the electrical distribution grid, used as a communication medium, can be used to distribute encryption keys and to authenticate, authorize, and secure a time-and-space limited operation to be performed on a computing Device, PC, or Server or a time-and-space limited communications session to be conducted over a conventional data communications network. Application software resides on the Device, PC or Server, and engages in high-security operations and/or transactions. These high-security operations and/or transactions must be conducted in a secure location, and must be concluded within a limited space of time in order to minimize the probability of a security breach occurring. The present invention allows for secure distribution of limited permissions, or Key Tokens, which the applications require when initiating the secure operations and/or transactions. Client software, which communicates with various other

component nodes of the present invention as described in more detail below, also resides on the Device, PC, or Server. All or part of the client software may be embodied as circuitry or firmware on a specialized networking interface card (NIC) for using the power path (such as from a wall plug) as a communication channel.

In some embodiments, the client software application secures limited permission to engage in the secure operations and/or transaction provided that the Device, PC or Server is not removed from the locale in which the secure operations and/or transactions were initiated, while the operations are in progress. In such embodiments, the software client running on the Device, PC, or Server cancels the secure operations and/or transactions if the Device, PC, or Server is disconnected from the power source or if evidence of a breach of the power path is detected either by the Device, PC, or Server, or the CD, or the ICD or the Server at the substation.

Embodiment 1.

Referring to **Figure 1**, the System may comprise: a Key Distribution Server (KDS) **11**, a Device, PC, or Server **112** operated at a Building, Structure, or Location **111**, where electrical power is provided to Building, Structure, or Location **111** by a distribution grid. The distribution grid may comprise at least one Distribution Substation **15** and at least one Service Transformer **115**, wherein a Phase of a Feeder **19** of the at least one Substation supplies power to the Service Transformer **115**, which in turn supplies power to Building, Structure, or Location **111**. The Phase of a Feeder **19** from the Substation **15** to the Service Transformer **115** is a medium voltage or high voltage line, where medium voltage is defined to be equal to or in excess of 1 kilovolts (KV). The Key Distribution Server **11** is connected to the Internet or private Wide Area Network **117** via network interface **14**, but is not required to be served by the same electrical distribution grid as the Building, Structure, or Location **111**. The Internet or Wide Area Network **117** provides a bidirectional communication path. An intelligent communicating device (ICD) **110** is installed on the low-voltage side of Service Transformer **115**. A Communicating Device (CD) **120**, which is capable of local-only bidirectional on-grid communications with the ICD **110**, is installed at an electrical meter serving Building, Structure, or Location **111**. Said Device, PC, or Server **112** can attach directly to the CD via a direct connection such as serial or Ethernet, or can communicate with the CD via an on-grid home area protocol such as Homeplug. Such protocols

are well-known in the art. The Device, PC, or Server **112** is also capable of using the local-only bidirectional on-grid communications method to communicate directly with the ICD, in which case the CD **120** is not required to be present but is permitted to be present for other purposes. Regardless of how the Device, PC, or Server **112** accesses it, there exists a local-only on-grid bidirectional communication path **113** between the ICD **110** and Building, Structure, or Location **111** which can be accessed only by a Device, PC, or Server **112** either plugged into wall-socket power at the Building, Structure, or Location **111** or connected directly by other physical means to the CD **120**.

A Server **17** controlling a Receiver **16** and a Transmitter **18** is installed at the Distribution Substation **15**. Server **17** has a bidirectional connection **116** to the Internet or private Wide Area Network **117**. The Electrical Distribution Grid provides a unidirectional on-grid communications path **114** from the ICD **110** to the Server **17** via the Receiver **16** and Interface **118** to the Receiver, and a unidirectional on-grid communications path **13** from the Server **17** to the ICD **110** via the Transmitter **18** and Interface to the Transmitter **119**. A conventional network communications path **12** provides an alternate route of connectivity between the Device, PC, or Server **112** and the Key Distribution Server (KDS) **11**. Said bidirectional communication paths **12** and **117** can be any form supporting the TCP/IP protocol and can include, but are not limited to, wireless, leased lines, fiber, and Ethernet. In this and other embodiments, the KDS is the owner of a standard Public Key Infrastructure certificate and a trust relationship with the KDS has already been independently established by the Server **17** and the Device, PC, or Server **112**.

In the method of Embodiment 1, the Device, PC, or Server **112** will initiate a request for a time-and-place secured Key Token by signaling the ICD **110** over local bidirectional on-grid communication path **113**. The Device, PC, or Server's access to the communication path **113** is via the Device, PC, or Server's power cord or charger plugged into a standard wall socket in the Building, Structure, or Location **111**, or by a direct physical connection to the CD **120**. Upon sending the request, a software program stored on the Device, PC, or Server starts a Unique Request Timer for time window verification. Upon receiving the request, a software program stored on the ICD **110** is activated. The activated software program on the ICD **110** records a unique Requestor ID of the requesting Device, PC, or Server **112** and the time the request was received. The ICD **110** then selects a random time within the pre-determined interval of the

Device, PC, or Server's Unique Request Timer at which to forward said request, together with the Requestor ID of the requesting Device, PC, or Server **112** and a unique Local ID of the ICD over the power grid by means of the on-grid unidirectional communications path **114** to Server **17**. Upon transmitting said forwarded request, the ICD **110** starts a different, random Unique ICD Timer for time window verification, again within the pre-determined interval of the Unique Request Timer, associating the Unique ICD Timer with the ID of the requesting Device, PC, or Server **112**.

When the forwarded request is received at the Receiver **16**, the Receiver enhances the request to include at least the electrical phase and feeder(s) upon which the signal was received and the time at which the request was received. The Receiver **16** then passes said enhanced message on to the Server **17**. Software stored and executed on the Server **17** uses the enhanced properties of the signal (known as the Grid Location) together with the time the message was received and the locally unique Local ID of the transmitting ICD **110** to determine the globally unique Physical ID of the ICD by comparing them with a Grid Map and Policies stored at Server **17**. Any inconsistency between the enhanced properties of the message and the Grid Map and Policies shall be considered evidence of tampering, and shall cause the Server to reject the request.

If no evidence of tampering is found, the Server **17** and associated software program posts the request for a time-and-place secured Key Token along with the Requestor ID of the originating Device, PC, or Server **112**, the unique physical ID, and the local ID of the relaying ICD over the conventional wide-area bidirectional data path **117** to the Key Distribution Server. The data path **117** between the Server **17** and the Key Distribution Server **11** is secured by conventional PKI means, a Certified and trusted relationship having previously been established between the Server and the Key Distribution Server.

Upon receiving the request from the Server **17**, the Key Distribution Server **11** generates a Special Decryption Key and a Response ID, and returns the Special Decryption Key with the Response ID appended over the bidirectional data path **117** to the Server **17**. The Server **17** in turn employs Transmitter **18** to send the Special Decryption Key and Response ID over the unidirectional on-grid data path **13** to the ICD **110**. The Special Decryption Key can be either 1) a symmetric key for a well-known encryption scheme such as AES-128, or 2) the decryption half of an asymmetric key pair, where the encryption half of the pair is retained by the KDS **11**. In

either case, the key or key pair is stored on the KDS, associated with an expiration time and date and the unique ID and local ID of the ICD **110** and the Requestor ID of the Device, PC, or Server **112** and the Response ID. Other information may be added to the store as the KDS acquires information about the outcome of said request and said secured session or operation.

When the ICD **110** receives the Special Decryption Key and Response ID, the ICD first checks to ensure that its Unique ICD Timer has not expired. If the ICD timer has expired, then the ICD notifies the client software on the Device, PC, or Server **112** that the request has failed. Otherwise, the ICD notifies the Device, PC, or Server and associated client software that the transaction has succeeded, providing to the client software the ICD-assigned Requestor ID but not the Special Decryption Key. The client software checks to ensure that the Unique Request Timer has not expired. If the Unique Request Timer has expired, then the client application is notified that the request has failed.

Assuming that all success conditions are met, the client component residing on the Device, PC, or Server **112** initiates a separate Request over conventional communication path **12** directly to the KDS **11**, transmitting the ICD-assigned Requestor ID. Identifying the correct stored Key by means of the Requestor ID, the KDS generates the requested permission or Key Token and encrypts it using either the previously stored Special Decryption Key (if the encryption method is symmetric) or the associated Special Encryption Key (if the encryption method is asymmetric). The KDS then responds to the separate Request from the Device, PC, or Server with the encrypted Key Token to which is appended the Response ID.

When the Device, PC, or Server **112** receives the encrypted Key Token and the Response ID, the client software on the Device, PC, or Server uses the Response ID to request the Special Decryption Key from the ICD **110**. The ICD checks its unique ICD Timer again. If said unique ICD Timer has expired, then the ICD notifies the client software that the Request has failed. If the ICD Timer has not expired, the ICD sends the Special Decryption Key to the Device, PC, or Server. Device, PC, or Server **112** can now decrypt the Key Token, but the Special Decryption Key has never travelled over any network session between the KDS **11** and the Device, PC, or Server **112**. This ensures the security of the Key Token even where a PKI-certified trust relationship between the KDS and the Device, PC, or Server has not been established.

The client software on the Device, PC, or Server checks the Unique Request Timer again, and, providing that it has still not expired, decrypts the Key Token and provides it to the

application software. The application software then uses the Key Token as intended to unlock a software function, secure a transaction, or to secure access to media. If at any point in the key exchange process a timer expires, the application software has the option of initiating a new request procedure, provided that connectivity with the ICD **110** is still present.

Embodiment 2.

Figure 2 illustrates a second aspect of the present invention in which a unidirectional on-grid data path from the Server **27** to the ICD **210** is not available. Instead, said ICD **210** contains a cellular wireless modem which it uses to periodically poll on a public IP address of Server **27** over Internet access **23** provided by a commercial cellular service provider. Said polling by said ICD takes place over a secured SSL or TLS connection based on an established PKI trust relationship between the ICD **210** and the Server **27**, with Server **27** being the certificate owner. Additionally, when said Server **27** has an urgent message for said ICD **210**, such that too much time will elapse before said ICD is expected to poll again, the Server may cause the ICD to poll ahead of time by sending an alert to said ICD via the Short Message Service (SMS) protocol, which is well known in the art of cellular communications. Data Path **23** is hence a bi-directional data path between said Server **27** and said ICD **210**. Data path **23** is treated as a limited resource because of the cost constraints on cellular machine-to-machine communications, and is not a substitute for communications between the ICD and the Server along unidirectional data path **214** because only said data path **214** supplies the grid location awareness required to validate the location of said ICD.

In similar embodiments, Data Path **23** may be any other form supporting TCP/IP including, but not limited to, leased line and/or Ethernet. In such embodiments not involving cellular wireless communications, polling by said ICD occurs frequently enough that no signal from said Server **27** to said ICD **210** analogous to said SMS message is required.

In this embodiment, the Server **27** has available to it, either stored locally in a database or accessible via a secure Web Service interface as is well known in the art of internetworking, a Provisioning database which allows the software executing on said Server to derive the SMS address (phone number or short code) of the ICD from its unique Physical ID.

Embodiment 2 is similar to Embodiment 1, except as regards Data Path **13** in Embodiment 1 and Data Path **23** in Embodiment 2. In Embodiment 2, when said Server **27** receives from the KDS **21** a Special Decryption Key with a Response ID appended over

bidirectional data path **217**, over the Internet or a Wide Area Network, to Server **27**, the Server sends an SMS message to the ICD **210** which causes the ICD to immediately send a request for data (a poll) to said Server via a secure SSL or TLS connection over its cellular modem. In contrast, in Embodiment 1 and referring to **Figure 1**, the Server responds to said request with Special Decryption Key and Response ID over data path **13** to said ICD **110**, whereupon the key and token distribution process proceeds as in Embodiment 1.

All other aspects of Embodiment 2 function as described in Embodiment 1. KDS is attached to bidirectional data path **217** via interface **24**. Server **27** is attached to bidirectional data path **217** via interface **216**, and to Receiver **26** via interface **218**. Cellular Modem **28** is attached to Server **27** via interface **219**. A phase of a feeder **29** supplies a long range unidirectional data path **214** from the ICD **210** to the Server **27**. The low-voltage electrical grid supplies bidirectional on-grid communication path **213** between ICD **210** and CD **220**. Service Transformer **215** is supplied with power by substation **25** and supplies Building, Structure, or Location **211** with power. Device, PC, or Server **212** is powered by conventional means such as a wall-socket to a power source said Building, Structure, or Location **211** and may also have a non-power-line direct physical connection to CD **220**. Conventional bi-directional data path **22** provides an alternative non-grid data path from Device, PC, or Server **212** to KDS **21**.

Embodiment 3.

Figure 3 illustrates aspects of where the Device, PC, or Server performing the secured operation lacks a direct connection to a conventional network. As shown in **Figure 3**, the System comprises a Key Distribution Server (KDS) **31**, and a Device, PC, or Server **312** operated at a Building, Structure, or Location **311**. Attached to the Device, PC, or Server is a storage device **32** capable of writing data originating on said Device, PC, or Server to removable media. Electrical power is provided to Building, Structure, or Location **311** by a distribution grid. The distribution grid comprises at least one Distribution Substation **35** and at least one Service Transformer **315**, wherein a Phase of a Feeder **39** of the at least one Substation supplies power to the Service Transformer **315**, which in turn supplies power to Building, Structure, or Location **311**. The Key Distribution Server **31** is connected to the Internet or private Wide Area Network **317** via interface **34**, but is not required to be served by the same electrical distribution grid as the Building, Structure, or Location **311**. The Internet or Wide Area Network **317** provides a bidirectional communication path between Server **37** and KDS **31**. An ICD **310** is installed on

the low-voltage side of Service Transformer **315**. A CD **320**, which is capable of local-only bidirectional on-grid communications with said ICD **310** via data path **313**, is installed at an electrical meter serving Building, Structure, or Location **311**. Said Device, PC, or Server **312** can attach directly to said CD via a direct connection, such as serial or Ethernet, or can communicate with said CD via an on-grid home area protocol such as Homeplug. Such protocols are well-known in the art. The Device, PC, or Server **312** is also capable of using said local-only bidirectional on-grid communications method to communicate directly with said ICD, in which case said CD **320** is not required to be present but is permitted to be present for other purposes. Regardless of how said Device, PC, or Server **312** accesses it, there exists a local-only on-grid bidirectional communication path **313** between said ICD **310** and Building, Structure, or Location **311** which can only be accessed by a Device, PC, or Server **312** plugged into wall-socket power at said Building, Structure, or Location **311** or connected directly by other physical means to said CD **320**.

A Server **37** controlling a Receiver **36** and a Transmitter **38** is installed at the Distribution Substation **35**. Said Server is connected to Receiver **36** via interface **318** and to Transformer **38** via interface **319**. Server **37** has a connection **316** to the Internet or private Wide Area Network **317**. The Electrical Distribution Grid provides a unidirectional on-grid communications path **314** from said ICD **310** to said Server **37** via said Receiver **36**, and a unidirectional on-grid communications path **33** from said Server **37** to said ICD **310** via said Transmitter **38**. In this embodiment, no conventional network communications path provides any alternate route of connectivity between said Device, PC, or Server **312** and said Key Distribution Server **31** or any other node on any local-area, wide-area network, or the Internet. The bidirectional communication path **317** can be any form supporting the TCP/IP protocol and can include, but is not limited to, wireless, leased lines, fiber, and Ethernet. In this and other embodiments, said KDS is the owner of a standard Public Key Infrastructure certificate and a trust relationship with the KDS has already been established by said Server **27**. Further, in this embodiment said Server **37** and said ICD **310** have previously established a shared secret symmetric key by means of which communications along unidirectional data paths **33** and **314** are encrypted and decrypted. Said shared secret symmetric key may be used in any embodiment of the present invention, but is required in this embodiment.

In the method of Embodiment 3, said Device, PC, or Server **312** will initiate a request for a time-and-place secured Media Encryption Key by signaling said ICD **310** over local bidirectional on-grid communication path **313**. The Device, PC, or Server's access to said communication path **313** is via said Device, PC, or Server's power cord or charger plugged into a standard wall socket in said Building, Structure, or Location **311**, or by a direct physical connection to said CD **320**. Upon sending said request, a software program stored on said Device, PC, or Server starts a Unique Request Timer for time window verification. Upon receiving said request, a software program stored on said ICD **310** is activated. The activated software program on the ICD **310** records a unique Requestor ID of said requesting Device, PC, or Server **312** and the time said request was received. As in Embodiment 1, said ICD **310** forwards said request, together with said Requestor ID of said requesting Device, PC, or Server **312** and a unique Local ID of said ICD over the power grid by means of said on-grid unidirectional communications path **314**. Upon transmitting said forwarded request, the ICD **310** starts a different Unique ICD Timer for time window verification, associating said Unique ICD Timer with the ID of said requesting Device, PC, or Server **312**.

When said forwarded request is received at said Receiver **36**, the Receiver enhances the request to include at least the electrical phase and feeder(s) upon which the signal was received and the time at which said request was received before passing said enhanced message on to said Server **37**. Software stored and executed on said Server **37** uses the enhanced properties of said signal (known as the Grid Location) together with the time the message was received and the unique Local ID of said transmitting ICD **310** to determine the unique Physical ID of said ICD by comparing them with a Grid Map and Policies stored at Server **37**. Any inconsistency between the enhanced properties of said message and the Grid Map and Policies shall be considered evidence of tampering, and shall cause the Server to reject the request.

If no evidence of tampering is found, said Server **37** and associated software program posts the request for a time-and-place secured Media Encryption Key along with the Requestor ID of the originating Device, PC, or Server **312** and the unique physical ID and the local ID of the relaying ICD over the conventional wide-area bidirectional data path **317** to the Key Distribution Server. The bidirectional data path **317** from said Server **37** to and from said Key Distribution Server **31** is secured by conventional PKI means, a Certified and trusted relationship having previously been established between said Server and said Key Distribution Server.

Upon receiving said request from said Server **37** the Key Distribution Server **31** generates a Media Encryption Key and a Response ID, and returns the Media Encryption Key with the Response ID appended over bidirectional data path **317** to said Server **37**. Said Server **37** in turn encrypts said Media Encryption Key and associated Requestor ID using said shared secret, encrypts said Response ID using the secret shared by said Server **37** and said KDS **31**, concatenates the two encrypted messages, and employs Transmitter **38** to send said resulting message over the unidirectional on-grid data path **33** to said ICD **310**. Said Media Encryption Key can be either 1) a symmetric key for a well-known encryption scheme such as AES-128, or 2) the encryption half of an asymmetric key pair, where the decryption half of the pair is retained by said KDS **31**. In either case, said symmetric key or decryption half is stored on said KDS, associated with an expiration time and date, the unique ID and local ID of said ICD **310**, the Requestor ID of said Device, PC, or Server **312**, and said Response ID.

When ICD **310** receives said message containing said Media Encryption Key, the ICD first checks to ensure that its Unique ICD Timer has not expired. If said ICD timer has expired, then said ICD notifies said client software on said Device, PC, or Server **312** that the request has failed. Otherwise, the ICD notifies the Device, PC, or Server and associated client software that the transaction has succeeded, providing to the client software said ICD-assigned Requestor ID but not said Media Encryption Key. The client software checks to ensure that its Unique Request Timer has not expired. If said Timer has expired, then the client application is notified that the request has failed.

Assuming that all success conditions are met, the client component residing on Device, PC, or Server **312** requests the Media Encryption Key from said ICD **310**. The ICD again checks the Unique ICD timer, and fails the request if the Unique ICD Timer has now expired. If it has not, the ICD returns to the Device, PC, or Server, over the bi-directional communication path **313**, the Media Encryption Key and Requestor ID, and the still-encrypted Response ID. Note that neither the ICD **310** nor the Device, PC, or Server **311** alone has sufficient information to decrypt the Response ID.

Device, PC, or Server **311** now writes data to removable media via Storage Device **32** as follows: 1) said encrypted Response ID, 2) said Requestor ID in the clear, and 3) the data payload for which the Media Encryption Key was requested, encrypted by means of said Media Encryption Key.

The resulting Encrypted Media can now be securely removed from Building, Structure, or Location **311**. To decrypt said Encrypted Media at another site, a Reader must recognize the media type, know the URL of said KDS **31**, and have established a PKI-certified trust relationship with said KDS **31**. The Reader then, using a secure and certified TLS or SSL session with said KDS, makes a Key Request of the KDS containing said Requestor ID and encrypted Response ID. The KDS uses the Requestor ID to determine the correct decryption key for the Response ID, decrypts said Response ID, and, provided that the decrypted Response ID matches said Requestor ID, returns the proper Media Decryption Key to the Reader, allowing the Encrypted Media to be deciphered. It will be apparent to one skilled in the art that the Grid Location information described in the present invention can be used to further restrict the use of the data on said Encrypted Media by ensuring that the Media Decryption Key is returned only to Readers at approved sites, whether the approved site is the same as or different from the Building, Structure, or Location **311** where the media was created. It will further be apparent that the method of Embodiment 3 is operable, though less secure, even if said Device, PC, or Server used to create said Encrypted Media has a conventional network connection.

Secure Session Embodiment.

In Embodiments 1, 2, and 3 one ordinarily skilled in the art will observe that the methods of the present invention are used to authenticate the site at which a secured session or operation, including the writing of encrypted media, takes place, and the time at which said session or operation begins.

The present invention ensures that a secured session or operation is completed within a prescribed time interval, and that the completion is at the site.

Referring again to **Figure 1**, after providing said Device, PC, or Server **112** with the necessary Key or Key Token, said ICD **110** may start a new Unique Session Timer defining the time within which the secured session or operation must be completed. Said Unique Session Timer is not randomized, but reflects the actual expected time for completing the secured session or operation. The Key Token may encode the expected time, although other methods of determining the expected time may be used.

The client component software of the present invention provides the application software running on said Device, PC, or Server **112** which will carry out the secured session or operation

with the Key and or Key Token required to initiate said secured session or operation. The client software component of the present invention then polls said ICD **110** at regular intervals until said application software notifies said client software that the secured session or operation is complete. If, prior to the completion of the secured session or operation, an attempt to poll said ICD should fail, the client software notifies the application software that the secured session or operation is compromised and must be aborted. A polling failure indicates that the host Device, PC, or Server **112** has been disconnected from the power source and hence potentially removed from said secured Building, Structure, or Location **111**.

If the application software notifies the client software that the secured session or operation has completed successfully, then the client software notifies the ICD **110** of the completion event. If the Unique Session Timer has not expired, then the ICD cancels the Timer and sends a notification via secure unidirectional data path **114** to the Server **17** that the transaction associated with the Requestor ID has completed its work. Server **17** forwards the notification to the KDS **11**, which marks the stored keys and other data associated with said Requestor ID as valid and complete.

If the Unique Session Timer expires on the ICD **110** and the client software running on the Device, PC, or Server **112** has not notified the ICD that the secured session or operation has been completed, the ICD sends a notification via secure unidirectional data path **114** to Server **17** that the secure session or operation associated with the Requestor ID has failed or been compromised. The Server **17** forwards the notification via the bi-directional data path **117** over the Internet or a Private Wide-Area Network to the KDS **11**, which marks the stored keys and other data associated with the Requestor ID as invalid and untrustworthy.

If the ICD **11** experiences a power outage, then upon recovery software residing on the ICD checks the non-volatile storage associated with the ICD to determine whether any Unique Session Timers or Unique ICD (request) Timers were unexpired at the time of the power loss. If any such Timers are discovered, then the ICD again notifies the Server **17** and the KDS **11** that the associated keys, media, and requests are invalid and untrustworthy.

Designated Secure Sites Embodiment.

Referring again to **Figure 1**, it may be that in some Buildings, Structures, or Locations **111** which are served by a single ICD **110**, such as hotels, convention centers, and the like, some rooms or sites within the Building, Structure, or Location are secure (e.g. a hotel room) and other

rooms or sites within the same Building, Structure, or Location (e.g. a restaurant) are not secure. It is well known in the art that a power outlet installed in a Building, Structure, or Location can be enhanced with electronics such that said outlet is addressable by means of a local on-grid communication protocol such as Homeplug. To ensure that said secure sessions or operations with said Device, PC, or Server **112** are initiated only from secure sites within said Building, Structure, or Location, the software residing on said ICD can be configured such that any Request for a secure session or operation must reach said ICD by way of such an addressable outlet, and the client software on said Device, PC, or Server can be configured to obtain from the ICD information as to whether the address of such an enhanced outlet must accompany any Request for such a secure session or operation.

Means by which such enhanced outlets are authenticated by the local or home area network are well-known in the art. Use of such well-known authentication methods prevents users of mobile Devices or PCs from carrying an addressable plug-in outlet enhancer in order to subvert this requirement. This method may also be used in the case where one ICD serves a plurality of Buildings, Structures, or Locations which do not have attached CDs. When CDs are present, said CDs serve to differentiate one Building, Structure, or Location from another.

Other Embodiments.

This description of the preferred embodiments of the invention is for illustration as a reference model and is not exhaustive or limited to the disclosed forms, many modifications and variations being apparent to one of ordinary skill in the art.

It should be recognized that the use of High Speed Internet to provide a bidirectional communication path, depicted in **Figures 1, 2, and 3** as **117, 217 and 317** respectively, is only one method of providing the bi-directional communications path between the Server and the KDS, and that the invention may use alternate form of communications.

It should further be recognized that this invention may be enhanced in certain installations wherein the Service Transformer, depicted as element **115, 215** and, **315** in the Figures may be located in a physically secure site, such as within the building housing a Device, PC, and/or Server. As such, attack vectors attempting to directly attach equipment to the Grid would have to deal with Feeder voltage. Given the voltage range of Feeders in the USA, 4.1 KV to 34.5 KV (and higher elsewhere in the world) this physical/electrical impediment further strengthens the protective nature of this invention. Attachment and grid-related introduction of

detection/communications equipment creates disturbances on the Grid, and therefore devices implementing this invention (e.g. said Receiver and said ICD) can be made to detect and protect against an attack vector.

We hereby claim:

CLAIMS:

1. A method for the establishment and maintenance of secure communications paths, comprising the steps of:
   providing an intelligent communicating device at or near the edge of an electrical distribution grid, wherein the intelligent communicating device uses the electrical distribution grid as a transmission medium;
   providing, at a substation, a receiver capable of inferring a grid location of a device associated with the intelligent communicating device;
   requesting, by the device, a secure communications path, session, or permission to perform a secured operation; and
   granting Keys and Key Tokens based upon the grid location of the device .
2. The method of claim 1, wherein the device granted one or more Keys and Key Tokens is at a fixed location.
3. The method of claim 1, wherein the device granted one or more Keys and Key Tokens is mobile and may be at a different location each time a Key and Key Token is granted.
4. The method of claim 1, wherein the device is required to remain at the location where the Key and Key Token were granted for the duration of the secured communications path, session, or secured operation.
5. The method of claim 4, wherein the secured communications path, session, or secured operation is cancelled, deleted, erased, or otherwise destroyed if the device is detected to have been removed from the location where the Key and Key Token were granted.
6. The method of claim 4, where the continued presence of the device at the required location is established by means of a software program on the device that communicates over the power grid with the intelligent communicating device, wherein the intelligent communicating device is at the location's service transformer or electrical meter.
7. The method of claim 1, wherein some sites within a building, structure, or location are authorized locations for the granting of a Key and/or Key Token, and other sites are not authorized.
8. The method of claim 7, wherein a single intelligent communicating device communicates with both authorized and unauthorized sites within a Building, Structure, or Location, or

with a plurality of Buildings, Structures, or Locations, wherein some of the plurality of buildings, structures, or locations are authorized and some are not.

9. The method of claim 8, wherein the intelligent communicating device distinguishes between authorized and unauthorized sites by means of a grid-location-aware addressing mechanism associated with individual electrical outlets or jacks with the Building, Structure, or Location.
10. The method of claim 1, further comprising establishing and supporting multiple simultaneous secure communications paths, sessions, or permissions for secured operations.
11. The method of claim 10, wherein the multiple secure communications paths, sessions, or permissions for secured operations are established for a multiplicity of different devices communicating via a single intelligent communicating device.
12. The method of claim 10, wherein the multiple secure communications paths, sessions, or permissions for secured operations are established for a multiplicity of different devices communicating via a multiplicity of intelligent communicating devices.
13. The method of claim 10, wherein the multiple secure communications paths, sessions, or permissions for secured operations are established for a multiplicity of different devices communicating via a multiplicity of Servers and Receivers at a multiplicity of substations.
14. The method of claim 1, wherein the Key and the Key Token are distributed to the requesting devices over distinct communication paths.
15. The method of claim 14, wherein the Key required to decrypt the Key Token reaches the requesting device by means of a combined communications path comprising multiple segments, wherein at least one segment of said path is the electrical distribution grid.
16. The method of claim 14, wherein the Key required to decrypt the Key Token reaches the requesting device by means of a combined communications path comprising multiple segments, wherein at least one segment of said path is a medium-voltage (> 1KV) or high-voltage segment of the electrical distribution grid.
17. The method of claim 1 wherein the request by the device for a Key Token travels over a combined communication path comprising multiple segments, wherein at least one segment is a medium-voltage (>1KV) or high voltage segment of the electrical distribution grid.

18. The method of claim 1 wherein, if the Key Token authorizes the creation of a secure communications path or session, said secure communications path or session uses a distinct communication path from the path over which the request for the Key Token traveled from the device to the Key Distribution Server.
19. The method of claim 1 wherein, if the Key Token authorizes the creation of a secure communications path or session, said secure communications path or session uses a distinct communication path from the path over which the decryption Key reached the device.
20. The method of claim 1 wherein the Key Token contains an encryption key, authorizes the encryption of data residing on the server, and authorizes the writing of the encrypted data onto a removable storage medium attached to the device.
21. The method of claim 13 where the multiplicity of Servers and Receivers process requests from devices located in buildings serviced by a multiplicity of utilities.
22. The method of claim 20, where the resulting encrypted medium can only be read at the encryption site.
23. The method of claim 20, where the device reading the encrypted medium can be a device other than the device that wrote the encrypted medium.
24. The method of claim 20, wherein the resulting encrypted media can be read at other locations than the encryption site.
25. The method of claim 20, wherein the resulting encrypted media can be read at locations other than the encryption site, provided that the other locations contain an intelligent communicating device capable of forwarding a request to the key distribution server which holds the secret to decrypting the media, and where said key distribution server grants said request and provides the decryption secret to the requesting device based on grid location.
26. The method of claim 20, wherein the device that writes the encrypted medium is not attached to any conventional network, but is attached to the electrical distribution grid.
27. The method of claim 1, further comprising requiring the device carrying out a secured session or operation to remain connected to a power source for the duration of said session or operation.
28. The method of claim 1, further comprising requiring the device carrying out a secured session or operation to remain in communication with its authorizing intelligent communicating device for the duration of said session or operation.

29. The method of claim 1, further comprising invalidating the outcome of the secured session or operation and declaring the secured session or operation to be untrustworthy if a device carrying out a secured session or operation is disconnected from its power source and/or loses communication with its authorizing intelligent communicating device.
30. The method of claim 1, further comprising, if the intelligent communicating device loses electrical power while authorization requests or timed secured sessions or operations which it has authorized are incomplete, invalidating and declaring to be untrustworthy all incomplete requests, sessions, or operations upon recovery.
31. The method of claim 1 further comprising, if an inferred Grid Location of a requesting intelligent communicating device is inconsistent with a Grid Map, refusing the request as invalid or untrustworthy.
32. The method of claim 8, further comprising the intelligent communicating device distinguishing between authorized and unauthorized sites by means of a grid-location addressing mechanism associated with a communicating device attached to an electrical meter at each site.
33. A system for the establishment and maintenance of secure communications paths, comprising:

an electrical distribution grid comprising at least one distribution substation;

an intelligent communicating device located at or near the edge of an electrical distribution grid, wherein the intelligent communicating device uses the electrical distribution grid as a transmission medium;

a server located at the distribution substation;

a receiver connected to the server at the substation;

a Key distribution server in bidirectional communication with the server located at the distribution substation; and

a device associated with the intelligent communicating device, wherein a location of the device on the electrical distribution grid is determined by a receiver at the distribution substation, and wherein the requesting device requests a secure communications path, session, or permission to perform a secured operation; and

wherein the Key distribution server grants Keys and Key Tokens to the device based upon the grid location of the device.

34. The system of claim 33, wherein the device granted one or more Keys and Key Tokens is at a fixed location.
35. The system of claim 33, wherein the device granted one or more Keys and Key Tokens is mobile and is at a different location each time a Key and Key Token is granted.
36. The system of claim 33, wherein the device is required to remain at the location where the Key and Key Token were granted for the duration of the secured communications path, session, or secured operation.
37. The system of claim 36, wherein the secured communications path, session, or secured operation is cancelled, deleted, erased, or otherwise destroyed if the device is detected to have been removed from the location where the Key and Key Token were granted.
38. The system of claim 36, further comprising a software program residing on a computer readable medium of the device and a communications interface at the device, wherein the software program communicates with the intelligent communicating device over the power grid through the communication interface to establish the continued presence of the device at the required location.
39. The system of claim 33, wherein the device is present at a building, structure, or location, and wherein some sites within the building, structure, or location are authorized locations for the granting of a Key and/or Key Token, and other sites are not authorized.
40. The system of claim 39, wherein a single intelligent communicating device communicates with both authorized and unauthorized sites within a Building, Structure, or Location, or with a plurality of Buildings, Structures, or Locations, wherein some of the plurality of buildings, structures, or locations are authorized and some are not.
41. The system of claim 40, wherein the intelligent communicating device distinguishes between authorized and unauthorized sites by means of a grid-location-aware addressing mechanism associated with individual electrical outlets or jacks with the Building, Structure, or Location.
42. The system of claim 33, further comprising multiple secure communications paths, sessions, or permissions for secured operations.
43. The system of claim 42, wherein the multiple secure communications paths, sessions, or permissions for secured operations are established for a multiplicity of different devices communicating via a single intelligent communicating device.

44. The system of claim 42, wherein the multiple secure communications paths, sessions, or permissions for secured operations are established for a multiplicity of different devices communicating via a multiplicity of intelligent communicating devices.
45. The system of claim 42, wherein the multiple secure communications paths, sessions, or permissions for secured operations are established for a multiplicity of different devices communicating via a multiplicity of Servers and Receivers at a multiplicity of substations.
46. The system of claim 33, further comprising distinct communication paths over which the Key and the Key Token are distributed to the requesting devices.
47. The system of claim 46, wherein the distinct communication paths comprise a combined communication path of multiple segments, and wherein at least one segment of said combined communication path is the electrical distribution grid.
48. The system of claim 46, wherein the distinct communication paths comprise a combined communication path of multiple segments, and wherein at least one segment of said combined communication path is a medium-voltage (> 1KV) or high-voltage segment of the electrical distribution grid.
49. The system of claim 33, further comprising a combined communication path comprising multiple segments over which the request from the device travels, wherein at least one segment is a medium-voltage (>1KV) or high voltage segment of the electrical distribution grid.
50. The system of claim 33, wherein, if the Key Token authorizes the creation of a secure communications path or session, said secure communications path or session uses a distinct communication path from the path over which the request for the Key Token traveled from the device to the Key Distribution Server.
51. The system of claim 33, wherein, if the Key Token authorizes the creation of a secure communications path or session, said secure communications path or session uses a distinct communication path from the path over which the decryption Key reached the device.
52. The system of claim 33, wherein the Key Token contains an encryption key, authorizes the encryption of data residing on the server, and authorizes the writing of the encrypted data onto a removable storage medium attached to the device.
53. The system of claim 45, wherein the multiplicity of Servers and Receivers process requests from devices located in buildings serviced by a multiplicity of utilities.

54. The system of claim 52, wherein the resulting encrypted medium can only be read at the encryption site.
55. The system of claim 52, wherein the device reading the encrypted medium can be a device other than the device that wrote the encrypted medium.
56. The system of claim 52, wherein the resulting encrypted media can be read at other locations than the encryption site.
57. The system of claim 52, wherein the resulting encrypted media can be read at locations other than the encryption site, provided that the other locations contain an intelligent communicating device capable of forwarding a request to the key distribution server which holds the secret to decrypting the media, and where said key distribution server grants said request and provides the decryption secret to the requesting device based on grid location.
58. The system of claim 52, wherein the device that writes the encrypted medium is not attached to any conventional network, but is attached to the electrical distribution grid.
59. The system of claim 33, wherein the device carrying out a secured session or operation remains connected to a power source for the duration of said session or operation.
60. The system of claim 33, wherein the device carrying out a secured session or operation remains in communication with its authorizing intelligent communicating device for the duration of said session or operation.
61. The system of claim 33, wherein the outcome of the secured session or operation and is invalidated and declared untrustworthy if a device carrying out a secured session or operation is disconnected from its power source and/or loses communication with its authorizing intelligent communicating device.
62. The system of claim 33, wherein, if the intelligent communicating device loses electrical power while authorization requests or timed secured sessions or operations which it has authorized are incomplete, invalidating and declaring to be untrustworthy all incomplete requests, sessions, or operations upon recovery.
63. The system of claim 33, further comprising a Grid Map, and wherein, if an inferred Grid Location of a requesting intelligent communicating device is inconsistent with the Grid Map, refusing the request as invalid or untrustworthy.
64. The system of claim 33, further comprising the intelligent communicating device distinguishing between authorized and unauthorized sites through a grid-location

addressing mechanism associated with a communicating device attached to an electrical meter at each site.

FIGURE 1
BIDIRECTIONAL ON-GRID LONG-RANGE COMMUNICATIONS

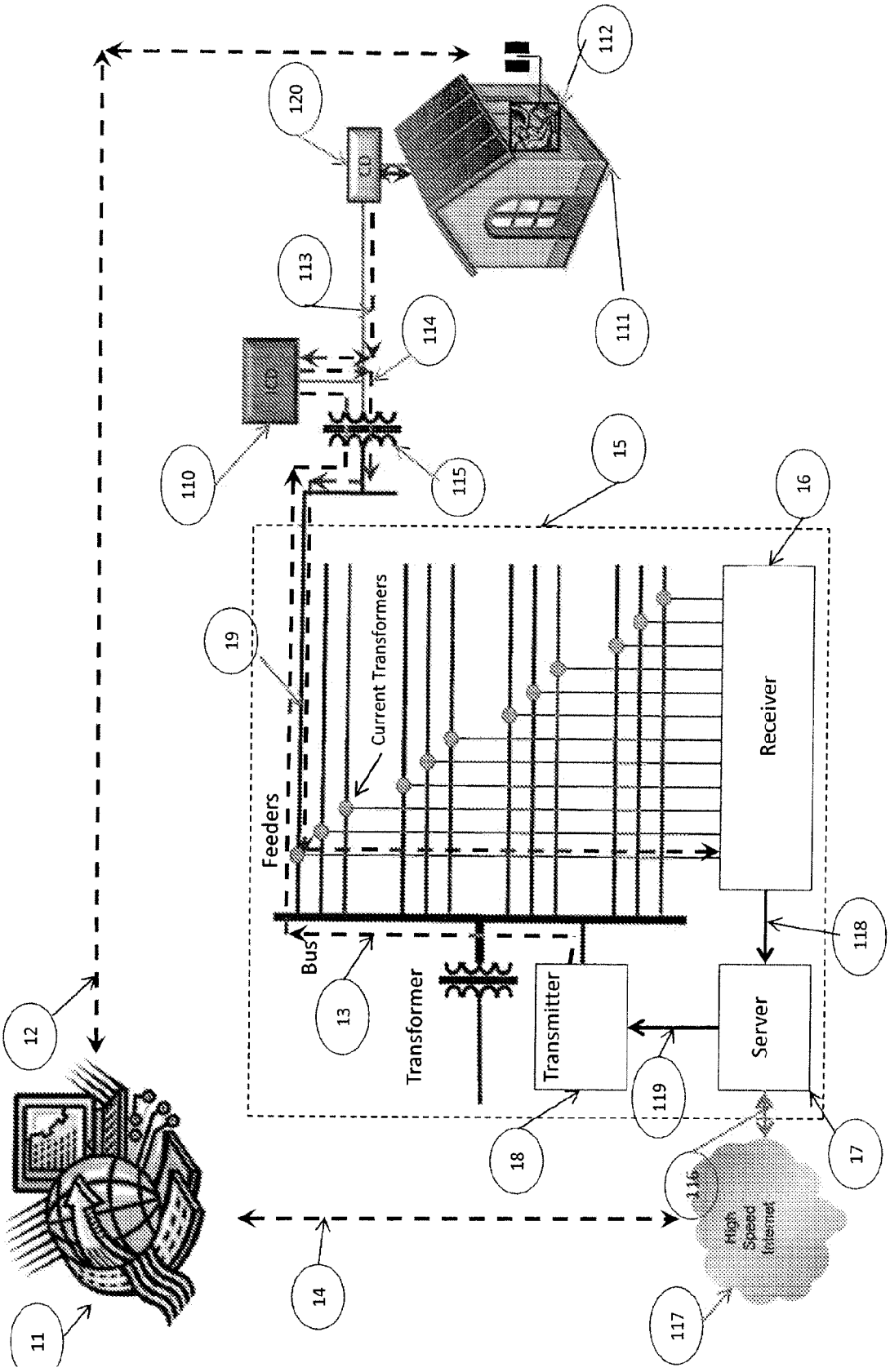


FIGURE 2
MIXED MODE COMMUNICATIONS

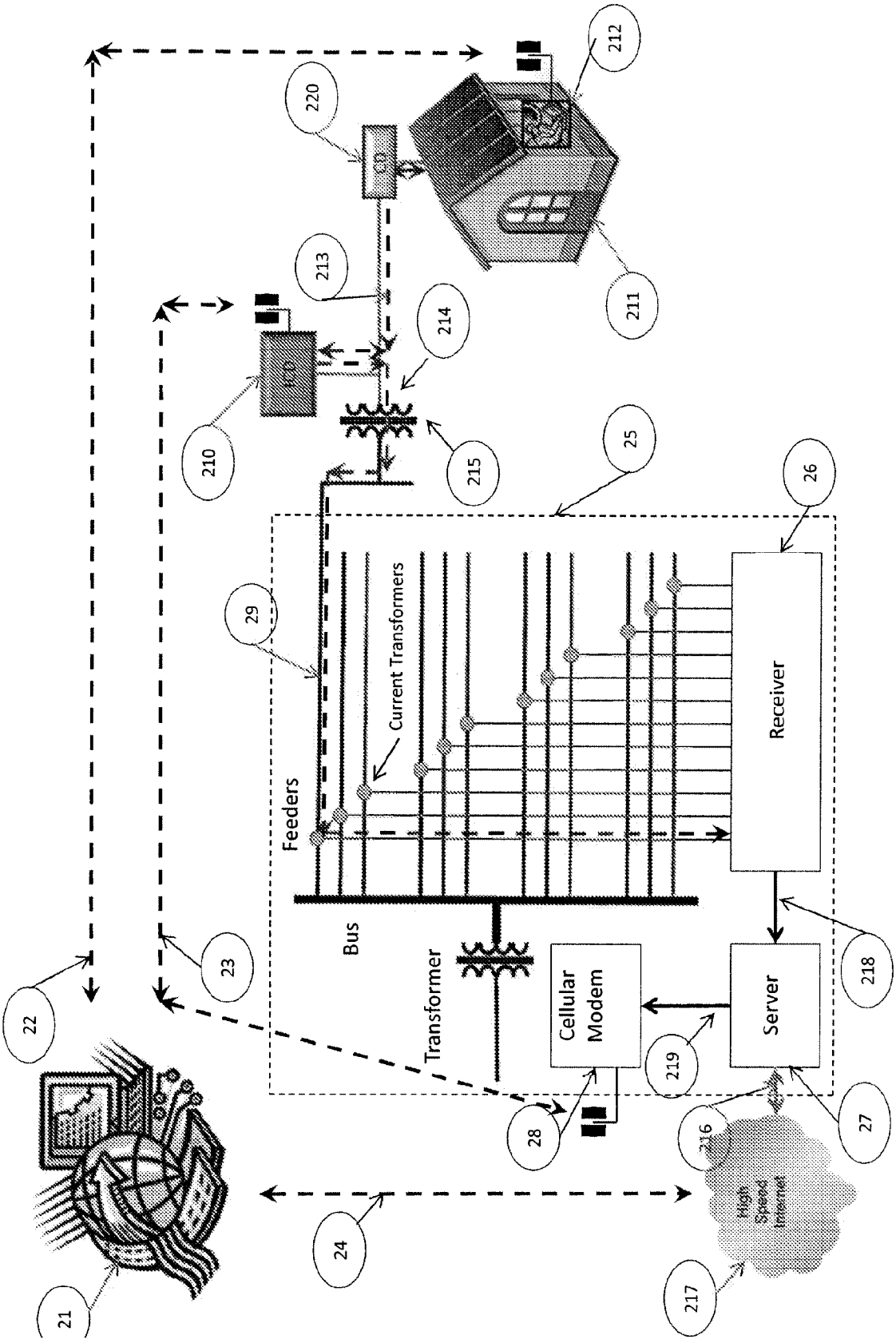
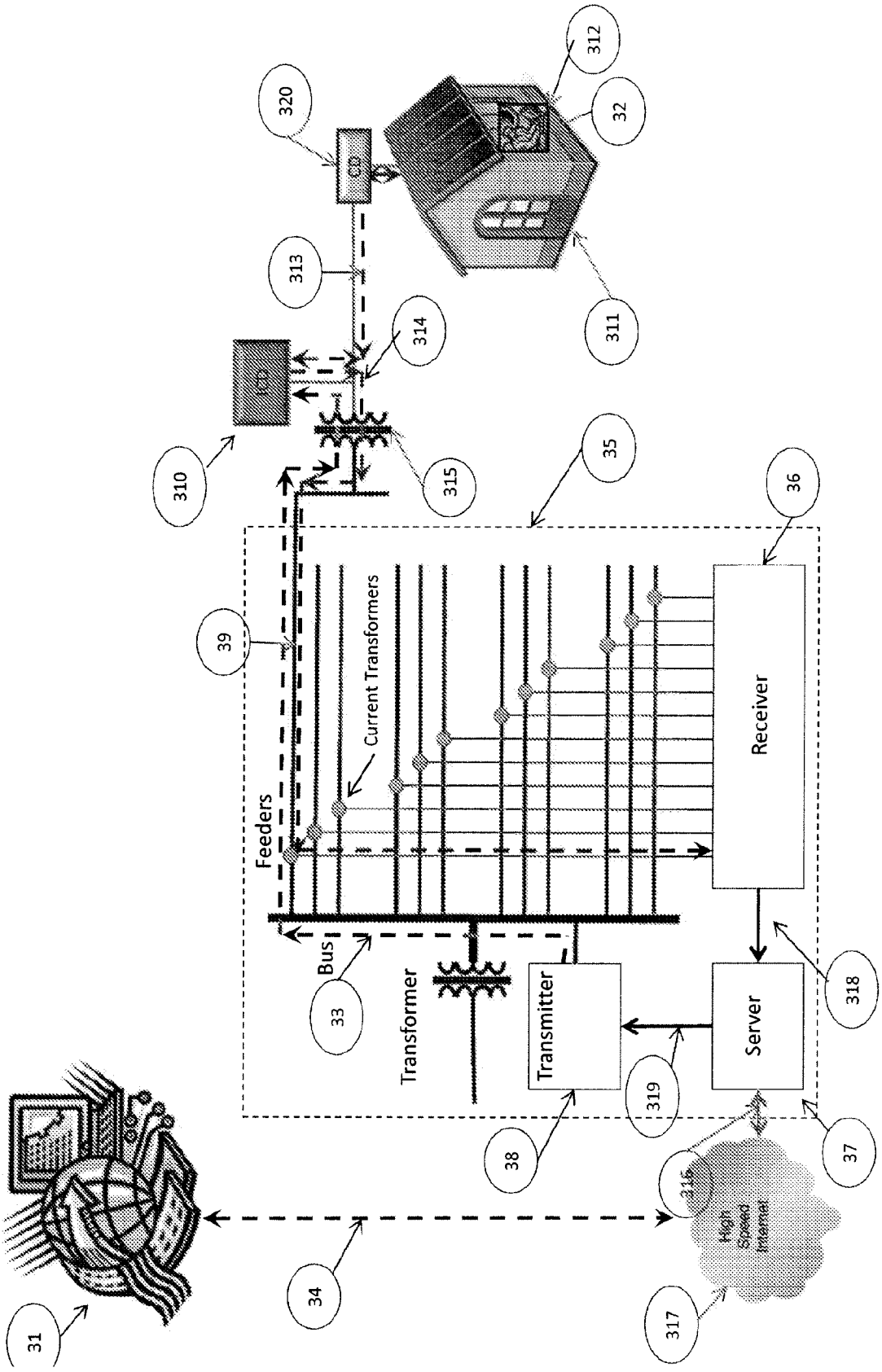


FIGURE 3
ISOLATED ENDPOINT



INTERNATIONAL SEARCH REPORT

International application No
PCT/US2012/041971

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L9/08
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2005/005150 A1 (BALLARD THOMAS VANCE [US]) 6 January 2005 (2005-01-06) abstract; claims 1,4-6,12,23-25,26-28; figures 9,10 paragraphs [0004], [0008] - [0011], [0025], [0029] - [0034], [0037] - [0039], [0041], [0042] paragraphs [0046], [0047], [0068], [0069], [0076], [0080] - [0082], [0088], [0090], [0091], [0094] ----- -/--	1-64

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
3 December 2012	07/12/2012

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Wolters, Robert

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2012/041971

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2010/306533 A1 (PHATAK DHANANJAY S [US]) 2 December 2010 (2010-12-02) abstract; claims 1-6,14-16,18,27-29,31-34; figures 2-10 paragraphs [0035] - [0038], [0040] - [0042], [0050], [0051], [0064], [0082], [0083], [0087] - [0091] paragraphs [0094] - [0101], [0104] - [0108], [0110], [0112], [0115] - [0120], [0123] - [0137]	1-64
A	US 2007/101438 A1 (GOVINDARAJAN GUNASEKARAN [US]) 3 May 2007 (2007-05-03) abstract; claims 1,9,11,19,20; figures 3-6 paragraphs [0002], [0003], [0009], [0013] - [0015], [0027] - [0031], [0033] paragraphs [0035] - [0038], [0040] - [0048], [0052] - [0057]	1-64

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2012/041971

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2005005150 A1	06-01-2005	NONE	
US 2010306533 A1	02-12-2010	US 2010306533 A1	02-12-2010
		WO 2010141375 A2	09-12-2010
US 2007101438 A1	03-05-2007	NONE	