



# ENSURING A SECURE SMART GRID

January 2011

## SECURITY: A VITAL ELEMENT OF THE SMART GRID

To build a secure, resilient, mission-critical Smart Grid network, utilities require technology that is secure, reliable, and self-healing. The growth of the Smart Grid and the advance of security technology will necessarily go hand in hand. The electricity grid is the foundational infrastructure on which rests not only economic performance, but also public and personal health, safety and welfare. Without robust security in place, the Smart Grid will not—and should not—be built and deployed.

**Challenge: Ensure a Secure, Resilient, Mission-Critical Network.** The utility industry has seen considerable progress toward ensuring Smart Grid security, but as an industry, we must acknowledge the considerable challenges that remain and build towards a more robust, standards-based approach. Security is unavoidably a dynamic challenge, where systems are built to defend against a raft of threats that evolve as they seek new ways to penetrate even the most formidable defenses. In a world of dynamic threats, there is no place for a static security solution. And the pursuit of interoperability is only feasible with accompanying security standards. The three-volume [National Institute of Standards and Technology \(NIST\) Smart Grid Cyber Security Strategy and Requirements \(NIST IR 7628\)](#), published in August 2010, provides a rational strategy and framework to support the transformation of the nation's aging electric power system into an interoperable Smart Grid.

**Solution: Invest in Secure, Reliable, Self-Healing Technology.** This NIST effort is welcome news, for without the NIST standards, strategy, and framework effort, it would be nearly impossible for utilities to demand (and receive) accountability from vendors of Smart Grid technologies. The challenge before the industry is to ensure that the promotion and advancement of cyber security becomes an integral element of grid transformation. If utility leaders were to lose faith in new solutions that prove to be insecure Smart Grid security shortcomings would become an anchor to drag down efforts to improve grid functionality.

## THE GRID NET MACHINE-TO-MACHINE NETWORK OPERATING SYSTEM FOR THE SMARTER GRID

Grid Net looks forward to a day when there will be a connected broadband network of “smart” devices operating at real-time speeds, with all-IP functionality—from substation infrastructure, to distribution infrastructure, and to meters exchanging information and price signals with buildings and homes equipped with distributed generation (e.g. solar PVs), energy storage, smart devices/appliances, and electric vehicles—to enable utilities and their customers to optimize energy resources and consumption. A real-time, all-IP Smart Grid is proactive toward customers and reduces utility capital and operating costs.

To accomplish this vision, utilities have a challenging path before them. Utilities will need to:

- Leverage the existing transmission and distribution ecosystem
- Reduce carbon footprint and carbon output
- Satisfy regulatory requirements
- Innovate with demand response programs, new services, and renewable energy (solar, wind, etc.) and
- Meet changing, growing customer needs

To make the real-time, all-IP Smart Grid and Smart Home a reality, utilities must also demand full-proof cyber-security and broadband telecommunications technology that is built on open, proven standards.

This devotion to open standards and security defines the core of the Grid Net Machine-to-Machine Network Operating System for the Smarter Grid. Grid Net develops and commercializes this Platform, a real-time, all-IP software platform for *any* device and *any* broadband technology to provide an online, real-time view and control of the Smart Grid.

The Grid Net Platform provides intelligent, reliable, real-time, all-IP, cost-effective, software-based management of millions of Smart Grid devices via any broadband communications technology (Ethernet, Fiber, 3G, WiMAX, LTE, WiFi, HomePlug, and Zigbee). The Platform system server at the utility data center/NOC enables a highly-scalable distributed, intelligent control system while providing centralized management and monitoring of Smart Grid devices using enterprise *policies* (i.e., business rules), to provide unsurpassed security, scalability, and reliability.

The Grid Net Platform also endows Smart Grid devices—smart meters, smart routers, smart inverters—with secure intelligence and capabilities for real-time advanced metering, demand response, and other Smart Grid applications. The design and operations of the Platform are critical to execute the Grid Net security vision. Grid Net’s Machine-to-Machine Network Operating System is architected from the ground up for truly open, highly secure, standards-based Smart Grid and Smart Home applications.

The Platform seamlessly integrates with utilities’ back-end software applications (including OMS, DMS, CIS, billing, etc.) via a real-time Web Services Bus that is compliant with IEC CIM 61970, 61850, and 61968. The key integration services offered include IEC CIM WSDL APIs; an IEC CIM-based data model; a Transactional Queue Manager; OASIS WS-Notification based event-driven inter-object communication patterns with full brokering and topic publish/subscribe support providing seamless and incremental Enterprise Service Bus integration; role-based access control with multi-layered authorization and session management; local and/or centralized (i.e., OASIS XACML) authorization support; single sign-on (SSO) authentication against enterprise directories (e.g., LDAP, ActiveDirectory); powerful and scalable group policy object inheritance for individual, group, and system-wide policies, devices, users and roles, which combine to provide ultimate control and management capabilities while reducing complexity, cost, and time to deployment.

The Platform’s core policy engine is based upon the IETF Common Open Policy Service (COPS) and leading utility and advanced networking standards. The COPS Protocol, part of the IETF’s [Internet protocol suite](#) (TCP/IP), specifies a simple distributed model for supporting policy control for advanced networking services, such as Quality of Service and Security; and now, Smart Grid network and application services. COPS Policy Information Bases (PIB) provide an open standard method for describing a technology and platform-independent repository of policies. Smart Grid PIBs are published as open standard IETF RFC’s, enabling any software vendor to build interoperable Policy Clients and Policy Servers, eliminating lock-in to proprietary and closed Smart Grid software applications and services.

Grid Net leverages proven investments in advanced network security from the telecommunications industry to deliver “industrial-strength/government-grade” security to Smart Grid devices. In addition, the Platform is based on policy-based networking technology and protocols currently used in real-world internet operations that scale reliably and consistently to millions of networked devices. Grid Net-enabled devices serve as fully functional and secure network access points and/or routers, and provide full Quality of Service (QoS), Security, Virtual Private Network (VPN), Intrusion Detection and Firewall

capabilities, providing the strongest security protocols and standards available today, including PKMv2, CCM-Mode AES key-wrap with 128-bit key, EAP/TLS (with x.509 Certificates), and IKE/IPSec.

As all Security is based upon trust and identity, the Grid Net Platform provides secure and automated Identity Management and In-field Provisioning services beginning in the device supply-chain and securely managed throughout the entire device life cycle by leveraging the commercial-grade Grid Net Public Key Infrastructure in conjunction with Trusted Platform Module (TPM) hardware architectures. Field-deployed Certificate Authorities (CA) and Registration Authorities (RA) provide secure, scalable and highly-available IETF RFC 4210 PKI Certificate Management Protocol (CMP) compliant services for identity verification, certificate signing, certificate issuance, certificate revocation, and proof of private key possession (POP). IETF RFC 2560 PKIX Online Certificate Status Protocol (OCSP) compliant OCSP Responders provide scalable and highly-available light-weight real-time certificate verification services. For domains requiring certificate verification during the unlikely event of a loss of WAN communications, Grid Net distributes Certificate Revocation Lists (CRL) to those domains. In addition to public key cryptography, Grid Net also provides secure, scalable, highly-available and automated identity management services for a variety of Pre-Shared Keys (PSK) such as meter passwords, device operating system credentials, and application user credentials.

In addition to Grid Net software capabilities, Grid Net also develops and commercializes broadband communications reference designs for integration with Smart Grid devices, an expanding category that will ultimately include not only *smart meters* at the ends of the lines, but also *smart routers* which network with other devices such as transformer monitoring systems in distribution substations, capacitor banks and reclosers along distribution feeders; *smart inverters* connected to such distributed energy resources as distributed solar PV systems, electric vehicles and charging systems, and distributed storage systems; and *smart consumer devices*, including home energy management systems and building energy management systems. Grid Net's communications products are architected using open standards, government-grade security and leading broadband communications protocols to facilitate easy, standards-based integration with other Smart Grid devices.

## OPEN COLLABORATION

Industries innovate rapidly with open standards, which not only enable vendors to collaborate and compete for the benefit of utilities and their customers, but also drive greater choice and lower costs for utilities. Open standards-based products incorporate ongoing, adaptive innovations, in essence, providing “future-proofing” assurance for utilities.

Grid Net has architected its products based on leading utility standards; internet, web services and telecommunications standards and protocols; and leading government-certified security standards. Grid Net supports, participates in, or belongs to the following standards organizations:

- [The WiMAX Forum](#)
- [OASIS](#)
- [IEC TC57 WG14 \(61968 part 9\)](#)
- [IEC CIM 61968](#)
- [Utility Communications Alliance \(OpenSG\)](#)

- [ZigBee-HomePlug Joint Working Group](#)
- [IEEE 802.16 Working Group](#)
- [IEEE P1901 Working Group](#)
- [IETF Working Groups](#)

Standards drive rapid innovation and accountability. The Smart Grid should leverage proven, open-standards and best-of-breed technologies, including utility industry standards and telecommunications standards that support the internet and software industries. For greater choice in solutions and more rapid innovation at lower cost, utilities should demand standards-based solutions. Grid Net promotes an open, networked Smart Grid with the following features:

- **Built on open standards and protocols** to enable utilities to choose the most innovative and cost-effective solutions, and avoid “single vendor, proprietary product” lock-in
- **High performing and scalable** to manage millions of customer service points effectively
- **Integrated, interoperable and optimized** to leverage technology innovations
- **Resilient and adaptive** to enable utilities to identify, isolate, and resolve specific points of failure, and/or provision new services rapidly and cost effectively and
- **Secure and reliable** to protect Smart Grid devices, networks, and services from attacks

**Grid Net has architected this dynamic set of standards into its products.**

<p><b>Utility Industry Standards</b></p> <p>ANSI C12.1 ANSI C12.10 ANSI C12.18 ANSI C12.19 ANSI C12.20 ANSI C12.21 IEC 61000-4-4 IEC 61000-4-2 IEC 61968</p> <p><b>IEEE, IETF, HAN Standards</b></p> <p>IEEE 802.1X IEEE 802.3 (Ethernet) IEEE 802.1Q (VLAN) IEEE 802.1Q (QoS) HomePlug v1/HomePlug AV IPv4/IPv6 Networking Protocols (DHCP, DNS, ICMP, IGMP, IP, IPSec, NTP, OSPF, SLAAC, TCP, UDP) IETF RFC 2474 – Differentiated Services Field IETF RFC 2560 – PKIX OCSP IETF RFC 2616 – HTTP v1.1 IETF RFC 2702 – Requirements for Traffic Engineering Over MPLS IETF RFC 2784 – COPS IETF RFC 2865 – RADIUS IETF RFC 2866 – RADIUS Accounting</p>	<p>IETF RFC 3031 – Multi Switching Arch IETF RFC 3060 – PCIM IETF RFC 3084 – COPS-PR IETF RFC 3159 – Structure of Policy Provisioning Information IETF RFC 3280 – PKI CRL Profile IETF RFC 3460 – Policy CIM Extensions IETF RFC 3579 – RADIUS Support for EAP IETF RFC 3748 – EAP IETF RFC 4210 – PKI Certificate Mgmt Protocol IETF RFC 4261 – COPS/TLS IETF RFC 4346 – TLS v1.1 IETF RFC 4493 – AES-CMAC IETF RFC 4523 – LDAPv3 / PKI IETF RFC 4557 – Online Certificate Status Protocol IETF RFC 5777 – Traffic Classification QoS Attributes</p> <p><b>W3C/OASIS Standards</b></p> <p>SOAP 1.1/1.2 SOAP RPC, document/literal SOAP request-response, one-way SwA MTOM (streaming) WS-I Basic Profile 1.0a WS-Addressing (2003/03, 2004/03, 2004/08, 2005/03) WS-Discovery WS-Enumeration WS-Security (2004/01) WS-Notification</p>
---	---

## A UNIQUE SECURITY ARCHITECTURE, PROCESS AND RESPONSE

Grid Net's approach to Smart Grid security is "multi-level and multi-layer." The core architecture delivers an end-to-end secure solution, which begins with Grid Net-enabled devices (smart meters, routers, inverters, and consumer devices), proceeds to data encryption for both data storage and data transport on the network, and concludes with Platform at the Utility NOC. The Grid Net Machine-to-Machine Network Operating System is based on three foundations—Architecture, Process, and Response—that take a "defense-in-depth" approach to security to provide robust end-to-end security.

### Multi-level, Multi-layer Security: Key Network Features

#### 1. Meter energizes, self-authenticates

- Hardware-enforced boot-loader, operating system and application software digital signature verification at power on
- Secure device identity via X.509 and ECC Certificates
- Code signing Chain-of-Trust via Grid Net PKI

#### 2. Meter authenticated, authorized by 4G broadband network

- 802.1X three-party Authentication model
- EAP-TLS Authentication and Authorization over RADIUS
- PKMv2 AES-CCM-based data encryption and data authentication over air interfaceCMAC and HMAC based control message protection schemes
- Devices quarantined upon initial network entry
  - a. Initial State: Authorized
    - i. Supply-chain issued credentials provide limited network access
    - ii. Layer 2 (VLAN) and Layer 3 (IP subnet) segregation
    - iii. Device identity verification required to receive domain-specific security credentials
    - iv. Only identity management services available to device
  - b. Operational State: Authorized
    - i. Device provisioned with domain-specific security credentials
    - ii. Full network services available as authorized per device

#### 3. Meter authenticated, authorized by the Grid Net Platform

- Authentication, Authorization and Accounting Services (RADIUS, EAP-TLS)
- Identity Management Services (CA, RA, OCSP, RADIUS)
- Device Authorization Policies and Profiles (RADIUS, Policy Server, VMPS)

#### 4. Secure Smart Grid system connections established

- IPSec
- TLS
- Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP)
- Policy-based Layer 2 (VLAN) and Layer 3 (IP subnet) segregation

#### 5. Risk Profile Reduction

- TPM and Identity Management limit device compromise to one device per attack
- TPM and Identity Management negates individual device compromise cost/benefit
  - a. Extremely sophisticated multi-month acid/laser-based micro-controller destruction required
  - b. Time/Expense of attack not worth benefit of energy theft or single service switch operation
  - c. Device monitoring detects tamper/unplanned outage prior to device compromise

- Secure micro-controller voltage glitch and temperature attack monitors erase sensitive on-chip RAM
- Private keys stored in NAND Flash memory are always encrypted
- Private key decryption facilities are restricted to each individual micro-controller
- Decryption and private key operations conducted in secure on-chip RAM

#### 6. End-to-end Quality of Service Policy Enforcement

- IETF RFC 5777 Traffic Classification attributes
- Traffic Engineering:
  - DiffServ Code Points map to MPLS Flow Labels
  - DSCP and MPLS map to WiMAX QoS Schedule Types
- Online Change of Authorization (RADIUS CoA, RADIUS Disconnect)

### Multi-level, Multi-layer Security: Key Server Feature

#### 1. Role Based Access Control (RBAC)

- Role and Group inheritance plus direct assignment permission model
- Rule of Least Privilege enforced when calculating Effective Permissions

#### 2. Single Sign-On (SSO) Authentication

- Enterprise Directory integration (LDAP, AD)
- User Interface and Web Service (SOAP) support

#### 3. Multi-layered Authorization

- User Interface (UI) Security Context controls content display and web service invocations
- Web Service (SOAP) Security Context controls direct web service invocations
- Web Service (SOAP) Security Context double-checks UI web service invocations
- Database Security Context triple-checks permission authorization on every service invocation
- Local and/or centralized (XACML) authorization stores
- PKI Certificate Policy Extensions used for distributed run-time presentation of device authorizations

#### 4. Input and Output Validation

- User Interface employs client-side and server-side data type and range Input Validation
- Web Services employ data type and range Input and Output Validation
- Policy Servers employ data type and range Input and Output Validation on device communications
- Database employs data type and range Input Validation

#### 5. Session Management

- Reduces the threat of session hi-jacking
- Facilitates Security Context access and authorization verification
- Real-time enforcement of Change of Authorization: real-time message queues signal context holder to destroy context, requiring new login and context/permissions loading

#### 6. Data Privacy and Integrity

- TLS and IPSec protects data and control messages in transit
- Symmetric encryption protects data at rest

#### 7. Monitoring and Mitigation Strategies

- Full Audit Trail of every database operation on every object
- Database Audit Trail logs rogue database client access attempts
- Full-featured Service logging capabilities
- Configurable Service Log Levels for key service operations
- Configurable Policy-based Network Monitors and Alerts
- Configurable Policy-based Service Monitors and Alerts

## ARCHITECTURE

Grid Net's security framework architecture is based on an N-Tiered architecture, with security built into all architectural layers. The security framework incorporates Federal Information Processing Standard (FIPS) and NIST-approved crypto standards, algorithms, and processes, and open standards-based network protocols (ITU, IEEE, and IETF), as described below. The key goal for this architecture is to build a security framework that is relevant throughout the multiple areas of the emerging Smart Grid. Key features of the Grid Net Platform security framework architecture include:

- **Standards-based Identity Management**, the back bone of Grid Net's security framework
- **Measures to address the lack of physical security**, where Smart Grid devices distributed out in the field benefit from a trusted computing hardware and firmware platform
- **Network Security non-specific to architecture or access technologies**, which incorporates proven Transport Layer Security (TLS) for the application level and Internet Protocol Security (IPSec) for the network link level to enable flexible Smart Grid network architectures and deployments; and finally
- **Measures extending security to incumbent devices**, such as Intelligent Electronic Devices (IEDs) and American National Standards Institute (ANSI) C12.19/.21-based meters

## PROCESS

Grid Net's security framework focuses on both technologies and processes in order to provide the protection required to ensure the confidentiality, authentication, integrity, non-repudiation, access control, and availability of the Smart Grid cyber infrastructure. The objective of the security framework is to address deliberate attacks, as well as inadvertent compromises of the information infra-structure due to user errors, equipment failures, and natural disasters.

Grid Net incorporates secure processes across all phases of Smart Grid device development, manufacturing, and deployment lifecycles, such as:

- A secure **Development** process that eliminates vulnerability classes

### Security Protocols, Standards, and Methodologies

Grid Net architected its solutions using the leading security protocols, standards, and methodologies. Grid Net's Smart Grid technology contains robust, sophisticated device security, secure data encryption, and secure data transport via secure broadband communications networks. Moreover, Grid Net is committed to continuous standards-based innovation to ensure that succeeding generations of its solutions contain the latest security enhancements and improvements.

A brief review of the industry discussion on security protocols, standards, and methodologies begins with FIPS and NIST, which has responsibility to approve crypto standards, algorithms, and processes. The discussion continues with proven open standards-based network protocols (e.g., ITU, IEEE, and IETF).

**Access Network Interface.** IEEE 802.16e-2005 (WiMAX)

**WiMAX Government-Licensed Spectrum Frequency Band(s).** 2300-2400 MHz 2496-2690 MHz

**Secure Device Authentication.** EAP-TLS, RADIUS, PKMv2

**Digital Identity.** X.509 Public Key Certificates

**Secure Device Authenticity Check.** Secure micro-controller Hardware-Enforced Code Signing and process monitors

**Cryptographic Key Exchange.** TLS: RSA, ECDH; IPSec: IKE/ISAKMP

**Encryption Algorithms.** CCM-Mode AES

**Secure Communications Channel.** PKM, TLS, IPSec

- A secure **Manufacturing** process, where multiple hardware component vendors customize their components with embedded unique digital IDs and public keys issued by the Grid Net PKI for firmware code signing and secure boot process per individual customer orders to enable secure deployment and automated plug-and-play in-field provisioning and identity management, and
- Secure **Operational Efficiency, Enterprise Policies, and Automation** to enable the customer to set security controls through enterprise policies appropriate to specific organizational needs

By incorporating manufacturing supply-chain processes with Trusted Platform Modules, commercial-grade security infrastructure and telco-grade provisioning infrastructure into its solution, Grid Net simplifies the operational aspects of the Smart Grid, while providing the best security possible.

## RESPONSE

Event response and mitigation assumes that no solution is perfectly secure. An essential part of the Grid Net Platform architecture is the monitoring and reporting of security events. Grid Net-enabled devices monitor for configurable policy-based conditions such as tamper or unauthorized activity, and take configurable policy-based actions in response to such conditions such as: report detailed records and/or time-stamped event logs for analysis and correlation, asynchronously publish alerts on a variety of media, or automatically change access to network services.

Grid Net provides the necessary tools and mechanisms to enable corrective actions when necessary. Key response features include:

- Asynchronous **Event Reporting** via web services, email, and SMS, where published events can be consumed by Security Operations Center (SOC) applications or support personnel
- **Event Filtering**, which allows administrators to set global policies so that Grid Net-enabled devices can locally monitor, filter, and prioritize events, and
- **Incident Response** and **Firmware Upgrades** that enable patches to be rolled out quickly through the remote firmware upgrade mechanism

## CONCLUSION

The solution to the challenges outlined in this whitepaper are found in the secure, reliable, self-healing technology Grid Net has designed into its Machine-to-Machine Network Operating System. The four themes summarized below provide a set of requirements for a sound Smart Grid security approach:

- **Security starts at the “edge” device.** While attacks on Smart Grid devices with or without physical security are inevitable, a utility can protect its Smart Grid from a massive and pervasive attack by implementing ubiquitous security architectures which (a) limit compromise to individual nodes or domains, (b) make the cost and sophistication of attacks much greater than the benefit, and (c) effectively respond to attacks in accordance with business requirements. Embedding unique, standards-based hardware and software security into every network device prevents penetration attacks (e.g., worms and viruses) from spreading throughout the Smart Grid network. Granular, device-level security quickly identifies and isolates a compromised device, limiting damage. ATM networks, which connect ubiquitous ATM machines and are often the

target of malicious hackers, provide a useful analogy. ATM networks remain well-protected and reliable despite such persistent threats because of the highly sophisticated, standards-based, device-level security that resides in each ATM machine, rendering it inoperable upon threat detection before any connection to the ATM network, thereby avoiding virus or worm proliferation. Similarly, Grid Net's sophisticated, device-level security incorporated in its embedded device communications reference designs ensures protection when licensed partners place that software in their devices.

- **Use only standards-based security.** Incorporating security standards throughout the Smart Grid lets utilities leverage the collective best efforts of tens of thousands of engineers, universities, government agencies, white hat hackers, and hundreds of millions of dollars of investments in the latest security technologies. Moreover, standards-based security ensures faster, simpler upgrades and "future-proofing" that is essential for utilities to stay ahead in the never-ending "attack/patch" cycle of cyber security. The security open standards community uses its advanced research and development activities to actively expose security vulnerabilities in the leading standards, providing for continuous improvement on a global scale.
- **Make security pervasive and granular.** Data encryption and IP security schemes are necessary conditions, but insufficient by themselves. Utility industry and regulatory leaders must insist that vendors incorporate pervasive and granular security architecture in their solution offerings. The solutions must architect government-grade security into not only the Smart Grid devices in the distribution network, but also into their embedded applications, the Smart Grid communications network infrastructure, Smart Grid network operating systems, the data being stored and transmitted, and utility enterprise systems. The utility is thus afforded multiple safeguards against security threats (security experts usually characterize such a multi-level and multi-layer approach as "defense-in-depth," analogous to peeling the layers of an onion).
- **Remember that security is a marathon, not a 50-yard dash.** Maintaining a safe, secure Smart Grid requires continuous vigilance and a commitment to ongoing investments in security oversight, critical software patches, software upgrades and process improvements. Just as personal computers receive automatic security updates from anti-virus software companies, so should the Smart Grid receive automatic security updates and adjustments to the latest threats. When standards-based security is deployed throughout a Smart Grid network—especially when it is deployed via a modular system architecture—device identity management, remote firmware upgrades, and system level improvements will become routine aspects of the Smart Grid.

In conclusion, the Smart Grid should not be built without the provisions outlined and described in this brief. To meet the challenge of a secure, resilient mission-critical Smart Grid that will transform utility operations, the Grid Net Machine-to-Machine Network Operating System provides a secure, reliable, self-healing technology solution that ensures sustainable, pervasive, and granular end-to-end protection to secure devices, software, network, and utility NOC.