COMMERCIALIZATION - OPERATIONAL REQUIREMENTS DOCUMENT

[Name of System or Needed Capability]

National Cyber Security Framework and Protocol for securing digital information in networked critical infrastructures and communications

Whitenoise Laboratories (Canada) Inc.
abrisson@wnlabs.com

Contents

Whitenoise Laboratories (Canada) Inc.
abrisson@wnlabs.com

1. General Description of Operational Capability

In this section, summarize the capability gap which the product or system[1] is intended to address, describe the overall mission area, describe the proposed system solution, and provide a summary of any supporting analyses. Additionally, briefly describe the operational and support concepts.

[1] In this document, the terms "product" and "system" are synonymous.

The word "system" is used to refer to networked systems/components required to make a secure network-of-networks.

Microprocessor that distributes identity and which is resistant to side channel and man-in-the-middle attack classes

Distributed servers for managing Dynamic Distributed Key Infrastructures [DDKI] frameworks for key creation, key management and key distribution in dynamic, tiered, hierarchical networks in any existing network configuration

Dynamic Identity Verification and Authentication [DIVA] - a single protocol for complete network security

Note: Wiki Leaks type breaches can be mitigated using Secure Session Manager, Secure File Interchange 2 and the Hard Disk Encryptor network solution. DIVA identity management keys can be distributed in several ways. Side Channel attack resistant chips solve a historical problem and are ultimately most efficient in distributing identity to digital devices and appliances.

1.1 Capability Gap

Describe the analysis and rationale for acquiring a new product or system, and identify the DHS Component which contains or represents the end users. Also name the Capstone IPT, if any, which identified the capability gap.

Cyber, Interoperability, and Information Sharing Capstones IPT

The Information Technology communications critical infrastructure and digital provenance fundamentally impact all DHS high priority areas because none can be effective without the secure, real-time sharing of information and the secure storage of data internally (or externally - "the cloud"). The highest order need is safeguarding and securing Cyberspace. In doing so we help facilitate secure communications, information sharing and data storage in all Capstone IPTs since they all rely on computer networks.

Whitenoise Laboratories (Canada) Inc.
abrisson@wnlabs.com

The overarching gap in Homeland Security operations is the limited ability to communicate and collaborate with other departments and personnel, in real-time, securely.

Fundamentally, it is impeded automatically because existing asymmetric communications is always vulnerable to man-in-the-middle attack classes and microprocessors have always been vulnerable to side channel attack classes.

Additionally, most networks often render previous technology investments obsolete or require a need for costly upgrades to legacy networks proving impractical or unaffordable. A system is required that creates an IT/communications framework enabling DHS to allow not only interoperability of disparate networks, but also the ability to interconnect legacy networks and new networks.

Another major DHS capability gap is in providing an affordable solution for the interoperability and interconnection of secure communication networks.

There must be a framework for enabling communications, interoperability and collaboration that is affordable.

1.2 Overall Mission Area Description

Define and describe the overall mission area to which the capability gap pertains, including its users and its scope

The overall mission area is any Homeland Security, government, military or intelligence networks that rely on digital communications which progressively include more broadband and mobile connected networks for efficiencies, cost and economies of scale.

DHS network security is currently comprised of a collection of ad hoc, layered security solutions that fail to effectively provide:

- Identification of all person and non-person network access points
- Continuous, dynamic authentication of all persons, non-persons and backbone components
- Inherent intrusion detection with 100% accuracy
- Automatic, faster-than-human revocation and isolation of incidents
- Complete logging of all network usage
- Authorizations
- DRM
- Repudiation/non-repudiation
- Chain-of-custody of data
- Chain-of-command of data
- Unique, identity-based encryption
- A large, scalable authentication platform where there is only partial disclosure of credentials
- Simple key creation, key management, and key distribution

These are provided with one DDKI framework and one DIVA protocol.

Whitenoise Laboratories (Canada) Inc.
abrisson@wnlabs.com

The mission areas covered by this ORD outline the capabilities needed to enable secure communications and collaboration between all DHS Capstone IPTs so their commands can interoperate with mutual aid, support teams and other responding organizations within moments of any network, smart grid, or critical infrastructure incident.

This ORD also addresses the capabilities needed to provide secure interoperable voice and data networks to command in control of any incidents and increasing collaboration and extending the chain of command across jurisdictions.

Finally, this ORD identifies the requirements of the proposed system capabilities and provides a communications framework for the creation of a dynamic, interoperable system of networks: one microprocessor, one software framework for managing dynamic distributed key infrastructures and key creation, management and distribution, and one software developer kit to rapidly scale integration.

1.3 Description of the Proposed Product or System

Describe the proposed product or system. Describe how the product or system will provide the capabilities and functional improvements needed to address the capability gap. Do not describe a specific technology or system solution. Instead, describe a conceptual solution for illustrative purposes.

The primary set of characteristics that the DDKI/DIVA network solution has that addresses the DHS capability gap and that accomplishes the mission is that DDKI/DIVA networks are dynamic, enabling interoperability between any combinations of different communication device types and converge any type or number of disparate networks on-demand. It is also thwarts all major cyber attack classes.

Dynamic Distributed Key Infrastructures is a key-based framework that works in any topology, on any kind of operating system, and in any digital context. It works alongside any other security topologies or protocols.

Dynamic Identity Verification and Authentication is a key-based protocol that provides complete network security: secure login, continuous dynamic authentication, inherent intrusion detection, faster-than-human automatic revocation, signature, non-repudiation, and unique identity based encryption. It eliminates the fatal flaws of network security and solves the historical problems attendant with distributed key crypto-identity networks.

The three fatal failings of network security have been:

- **Vulnerability to Man-in-the-Middle attack classes**
    - M-i-M-doesn't work against distributed networks because there is no session key exchange. There is only a secure acknowledgement of the current dynamic offset. (Patented.)

- **Vulnerability to Side Channel attack classes**
    - Side Channel attacks don't work against DIVA because after key load all operations are order one operations. This has been confirmed by a 17 month NSERC government funded project at the University of Victoria. (Patented.)

Whitenoise Laboratories (Canada) Inc.
abrisson@wnlabs.com

- **Uncontrolled life of data**
    - Life of data can be controlled by enterprises, governments or consumers who can now prevent access to their own data uploaded into the cloud with unique identity based encryption and control of a single dynamic offset. *(Provisional filed - patent pending.)*

The system is based on software (whether implemented as firmware into microprocessors or not) that converges network protocol types and provides network presence awareness. The system enables data interoperability among any combinations of ad hoc, terrestrial data, telephony or satellite networks that are available or will be introduced in the future.

The second set of characteristics that DDKI/DIVA network characteristics have that address the DHS mission is that these networks easily create a network-of-networks and provide connectivity to the interoperable DDKI tiered, hierarchical framework. Everything that is needed will be provided and are simple to install anywhere with the kit (physical components) or to install anywhere electronically to devices which have connectivity, write-back and storage. These network-of-networks can handle all voice, video, and data communications peer-to-peer.

These systems are human portable resilient communication networks that can provide connectivity to the interoperability framework. These networks, whether chip-based or software based, require only that devices have a minimal amount of storage, write-back capacity and connectivity.

The communication security capabilities required that DDKI and DIVA provide are:

- Perfect identity of persons and non-persons components using ISO/ITU level 4 identity proofing
- A micro-processor or firmware that distributes identity and identity keys.
- Secure network access
- Continuous dynamic authentication (moving target defense)
- Inherent intrusion detection (self defending networks)
- Automatic, faster-than-human revocation
- DRM
- Repudiation/non-repudiation
- Signature
- Unique, identity based encryption
- Resistance to man-in-the-middle attack classes
- Resistance to side-channel attack classes
- Ability to control data life cycle
- One-to-one relationship between endpoints and the server
- One-to-many communications capability
- It works in any topology or configuration
- It works on any operating system
- It works in conjunction with any other security technologies
- It works in any medium - wireless, wired, RF, storage etc.
- It provides secure, two-way, peer-to-peer communications
- Simple network management software
- Simple operation and use without experience
- Simple to add IP-based devices and peripherals allowing on-the-fly scaling

The third critical set of characteristics that DDKI/DIVA network-of-networks have which satisfy the DHS mission is that it is an affordable, interoperable and scalable cyber network. DHS can afford to distribute enough network servers to create a National Communication Cyber Secure Network-of-networks to provide the infrastructure for the DDKI framework.

1.4 Supporting Analysis

Describe the analysis that supports the proposed system. If a formal study was performed, identify the study and briefly provide a summary of results.

- Canada funded an NSERC Side Channel Attack project at the University of Victoria ECE Labs. Whitenoise is side channel attack resistant.
- Global Patenting of DDKI and DIVA has been successful.
- Communications Security Establishment (references)
- Presented to the US National Cyber Leap Year Summit
- Presented to the United Nations International Telecommunications Union
- Members of every pertinent national and international standards group
- ATT Certification (SFI2)
- It is being presented to the European Telecommunication Standards Institute workshop in January 2012.

1.5 Mission the Proposed System Will Accomplish

Define the missions that the proposed system will be tasked to accomplish.

US National Leap Year Summit 2009

"... defend our information and communications infrastructure, strengthen public/private partnerships, invest in cutting edge research and development and to begin a national campaign to promote cyber-security awareness and digital literacy." President Barrack Obama

"...it is imperative that we achieve a "leap forward" in cyber-security through development of "game changing" technologies." Aneesh Chopra, U.S. Chief Technology Officer

- US National Leap Year Summit
- The Whitenoise Vision
- The National Leap Year Summit Top 100 Cybersecurity Experts
- Whitenoise Laboratories (Canada) Inc. Digital Provenance Vision

Whitenoise Laboratories (Canada) Inc.
abrisson@wnlabs.com

Specifically the proposed system will ***defend our information and communications infrastructure*** *and* accomplish this mission because it:

- Provides a dynamic distributed key framework that can operate in any existing environment and alongside any existing technologies or with any legacy system and create a simple means of securing data at rest or in motion in our network and telecommunications networks

- Provides an identity based protocol that provides secure network access, continuous dynamic authentication, inherent intrusion detection, automatic revocation, DRM, signature, non-repudiation, logs and identity-based encryption.

- Provides a system that manages identity and allows secure, dynamic, interoperable communications and data sharing with anyone tasked by the Department of Homeland Security and who has data or telephony capability anywhere in the country. There is no need for additional equipment.

- Enables a secure network server and system to be implemented in under 4 hours (including system administration training).

- Enables the training of employees to use a secure network in minutes. There is no training for components that comprise our critical infrastructures and smart grids.

- Creates a system for voice, data and video interoperability.

- Provides the ability to log all network usage and identify all persons and non-person entities accessing the network

- Provides peer-to-peer communications that enable instant alerts, warnings and advisories that can be viewed and responded from anywhere in the country.

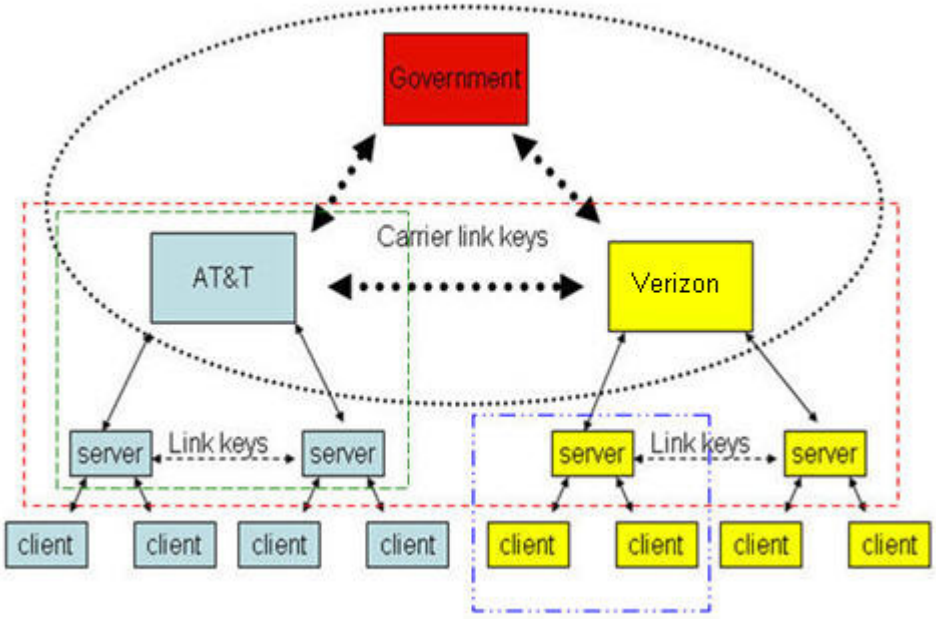
1.6 Operational and Support Concept

1.6.1 Concept of Operations

Briefly describe the concept of operations for the system. How will the system be used, and what is its organizational setting? It's appropriate to include a graphic which depicts the system and its operation. Also describe the system's interoperability requirements with other networks.

Dynamic distributed key infrastructures are tiered, hierarchical, peer-to-peer(s) frameworks that allow scaling and interoperability. The following graphic shows one way the government could issue master keys to telecommunication providers and link keys for those providers to interoperate securely between that tier. The telecommunication providers in turn distribute keys to their clients in that tier. Any configuration is simple either vertically, horizontally or in a mesh.

Government-carrier-consumer tiered, hierarchical network of secure networks



Each person or non-person entity on a network has a predistributed and pre-authenticated identity management key that is distributed either by the inclusion of a DIVA identity management chip in a device or an electronically distributed key to any device accessing a network that requires only write-back, storage, and connectivity.

Key creation, key management, and key distribution are managed by an authentication server. This can be provided as a third-party service. This server capacity can be installed as software on existing servers. A physical server can be cloned and provided to any department or enterprise that wants to manage these capacities. It is received, put behind the existing firewall, and the system administrator simply configures a DNS address.

Each person, non-person entity, and network component is assigned a unique DIVA Identity Management Key. Because dynamic distributed key infrastructures create tiered, hierarchical topologies, servers themselves can be provided “link” keys to allow interoperability with other authorized IP based networks through their servers.

The DDKI framework and DIVA protocol communication framework are data and operating system agnostic.

Billions of dollars has been spent on interoperability but today there is no capability for secure interoperability of voice, video and data that can be used on a local, state, regional and national basis immediately.

The proposed DDKI framework and DIVA protocol will provide that capability for far less money, effort and training than the cost of alternative networks that do not have the capability of meeting the mandate. Implementation of a program that would use the system is called for. Meeting this requirement saves hundreds of millions of taxpayer dollars while also being rolled out nationally within three short years.

Whitenoise Laboratories (Canada) Inc.
abrisson@wnlabs.com

1.6.2 Support Concept

Briefly describe the support concept for the system. How will the system (hardware and software) be maintained? Who will maintain it? How, where, and by whom will spare parts be provisioned? How, where, and by whom will operators be trained?

Managing identity and network access and use can be provided as a third party service.

System administration can also be done internally with minimum staff since the system is self protecting and so simple.

Software updates will be pushed to all networks in a planned and coordinated manner. Because the DDKI network is a peer-to-peer framework, updates will automatically be logged to the support database with an acknowledgement of a successful update.

If updates are required, the support will have the ability to remotely update the system. Key replacement and account activation/reactivation can be performed remotely.

Live interactive teleconferencing will be held as needed to provide training and customer support.

2 Threat

If the system is intended as a countermeasure to a threat, summarize the threat to be countered and the projected threat environment. 4

Ret. Admiral McConnell recently stated that in the event of cyber warfare we would lose.

The CIA has listed cyber security as the most serious threat that is faced.

We have seen the recent failure of the power grid through the American Southwest.

We have experienced the negative effects of Wiki Leaks.

The threats we face are multiplying exponentially as electronic devices become more pervasive and as economics and international relations sour.

It was recently uncovered that systems have been hacked into over the last six years in one of the greatest intellectual property thefts in history. Departments at the United Nations, Canada, the United States and countries all over Europe and the world, as well as major corporations, were victimized. This is unacceptable.

3 Existing System Shortfalls

Describe why existing networks cannot meet current or projected requirements. Describe what new capabilities are needed to address the gap between current capabilities and required capabilities.

The current list of high priority Homeland Security needs in cyber security, interoperability and information sharing articulate known existing short-comings of our current information and communication infrastructures. DDKI and DIVA fixes these shortcomings.

Cyber Security

Representative technology needs

• Secure Internet protocols, including standard security methods (Command, Control and Interoperability Division)

> Dynamic Distributed Key Infrastructures (DDKI) is a key-based framework that creates tiered, hierarchical topologies where each network user (either person or non-person entity) and each network component is provided a unique, secure identity.
>
> Dynamic Identity Verification and Authentication (DIVA) is a single key-based protocol that provides all network security functionality: secure access, dynamic-continuous authentication, inherent intrusion detection, automatic revocation, non-repudiation, signature, DRM and unique, identity-based encryption.
>
> Current systems are vulnerable to Man-in-the-Middle and Side Channel attack classes as well as generally being blinded to internal malfeasance.

• Improved capability to model the effects of cyber attacks—in particular, measuring security and risk in IT infrastructure components and understanding of Internet topography (Command, Control and Interoperability Division)

> This capacity is facilitated with DDKI and DIVA because each component of the infrastructure as well as each user is identified by a unique key. Current systems do not do this.

• Software Testing and Vulnerability Analysis Technologies—*in particular, services and capabilities to rigorously and routinely build, test, and analyze source and binary forms of software in realistic conditions representative of operational environments* (Command, Control and Interoperability Division)

• Usable Security—*in particular, focused technologies that demonstrate new ways to address the confluence of usability and security* (Command, Control and Interoperability Division)

> Identities are distributed to end-users and endpoints either with a microprocessor (the subject of this application) or by secure firmware upgrades to devices with storage, write-back capacity and connectivity.

• Information-system insider-threat detection models and mitigation technologies—in particular, technology aids that increase the accuracy, reduce the time, and reduce the cost of detecting and discovering unauthorized insiders (Command, Control and Interoperability Division)

> DIVA provides inherent intrusion detection and automatic revocation without human action with 100% accuracy.

Whitenoise Laboratories (Canada) Inc.
abrisson@wnlabs.com

• Analytical techniques for security across the IT system-engineering lifecycle—in particular, analytical techniques to facilitate detecting, quantifying, measuring, visualizing, and understanding system security (Command, Control and Interoperability Division)

These technologies can be deployed to provide chain-of-command, chain-of-custody and identity and aid in creating usable analytical techniques since everything is logged.

• Process Control Networks (PCS) security—in particular capabilities for metrics, wireless communications, and system vulnerability assessment. (Command, Control and Interoperability Division)

DDKI and DIVA satisfy all these needs.

• Cyber Forensics—*in particular, cyber-related tools and investigative techniques that support law enforcement to address the full range of investigating and solving cyber related crimes* (Command, Control and Interoperability Division)

The inherent intrusion detection and automatic revocation, coupled with all network usage being logged creates an immediate response system for a network and an easy trail for forensics to be conducted since all access is identified. If a breach were ever to occur, the forensic personnel simply need to go to the flagged, locked account. Any malfeasance is quickly located by the locked account and the area for investigation is any transaction that occurred between the time the legitimate key was synchronized with the server and the time where the account was locked.

Information Sharing

Representative technology needs

• Data fusion from law enforcement, intelligence partners, and other sensors to support a user-defined operating picture (UDOP)—in particular, technologies to correlate and fuse sensor data into a comprehensive representation (Command, Control and Interoperability Division)

Data can be shared in real-time, simultaneously between all partners. Data will be sent to all authorized and authenticated parties encrypted in their own unique key. Asymmetric networks require a session key for each party to be notified. All parties in a DDKI group will share information in a single operation.

• Management of user identities, rights, and authorities—In particular, technologies and standards to enable external identity adjudication (Command, Control and Interoperability Division—shared between Information Sharing and Cyber Security)

DIVA and unique identity-based encryption satisfy all authentication, authorizations and data security.

• Distribution of intelligence products—in particular, technologies and techniques to automate the distribution of unclassified or lower classification portions of intelligence information to DHS mission partners (Command, Control and Interoperability Division)

DDKI/DIVA networks satisfy this requirement.

• Information sharing within and across sectors on terrorist threats—in particular, analytic capabilities for structured, unstructured, and streaming data (Command, Control and Interoperability Division)

DDKI/DIVA networks satisfy this requirement.

Whitenoise Laboratories (Canada) Inc.
abrisson@wnlabs.com

• Improvement of situational awareness and decision support horizontally across Federal Law Enforcement and Intelligence partners as well as vertically through Federal, state, local and tribal partners —*in particular, technologies that provide automated, dynamic, real-time data processing and visualization capability and the information sharing protocols that enable them* (Command, Control and Interoperability Division)

DDKI/DIVA networks satisfy this requirement.

• Protection of U.S. citizen personal data—in particular, advanced data integrity techniques to automatically purge or anonymizing personal identifiable information (Command, Control and Interoperability Division) • Improved cross-agency reporting of suspicious activity—in particular, technologies that would improve real-time awareness through alerting others to and sharing information about suspicious activities and persons (Command, Control and Interoperability Division)

DDKI/DIVA networks satisfy this requirement.

Interoperability

Representative technology needs

• Accelerate the development of voluntary consensus standards for interoperable communications, including Project 25 and Voice over Internet Protocol. (Command, Control and Interoperability Division)

DDKI/DIVA networks satisfy this requirement.

• Develop message interface standards and architectures that enable emergency-information sharing, data exchange, and public alerts and notifications. (Command, Control and Interoperability Division)

DDKI/DIVA networks satisfy this requirement.

• Develop standards, applications, and technologies to enable seamless access to voice, data, and imagery via a single, unified communications device. (Command, Control and Interoperability Division)

DDKI/DIVA networks satisfy this requirement.

• Develop ad-hoc and mesh networks to link local, state, and Federal personnel in emergency situations and other security events. (Command, Control and Interoperability Division)

DDKI/DIVA networks satisfy this requirement.

4 Capabilities Required

4.1 Operational Performance Parameters

Identify operational performance parameters (capabilities and characteristics) required for the proposed system. Articulate the requirements in output-oriented and measurable terms. Use Threshold/Objective[2] format and provide criteria and rationale for each requirement.

[2] The threshold value for a requirement is the minimum acceptable performance. The objective value is the desired performance.

DDKI and DIVA enabled networks satisfy all operation, performance and mission critical parameters.

DDKI/DIVA networks (and network-of-networks):

• converge multiple protocols and networks to provide interconnectivity to any IPv4 or IPv6 network or optimally a system that will interconnect to IPv4 and IPv6 networks wired or wireless, and terrestrial or satellite.

• support IPv6 connectivity and be capable of routing to an IPv4 LAN. (O/T)

• support interoperable secure data sharing

• set up at a client in less than ten minutes.

• require no more than three steps to setup.

• provide secure network communications anywhere in the United States (T) or anywhere in the world.

• provide a framework that supports unlimited number of users and usage at the same time.

• interconnect with any available network providing Internet connectivity or the ability to connect to multiple networks and rollover to a backup network for redundancy.

• support interoperable peer-to-peer networking and support peer-to-peer data sharing and connectivity.

• support up any number of users on the network at one time

• support any IP-over-satellite network access (T) or have the ability to provide satellite service for the system without having to increase the size of the system.

• provide complete instructions for setup and trouble shooting (T) or complete color-coded instructions with pictures so that any person with an elementary education has secure network access.

• are affordable enough to purchase and maintain

The DDKI/DIVA network of networks:

• create a network-of-networks simple enough for a department to setup in 10 to 20 minutes or optimally extend the network of networks to any system in the country, if the system has access to the Internet or mutually accessible dedicated network.

• create a dynamic distributed key framework for interconnecting disparate local area data networks, video networks and radio networks and enable automatic interoperability between all interconnected networks or optimally securely interconnect disparate networks anywhere in the country creating a WAN on-demand.

• support the interoperability of peer-to-peer communications for secure data sharing and optimally support peer-to-peer and one-to-many and many-to-many connectivity of all users within the network of networks.

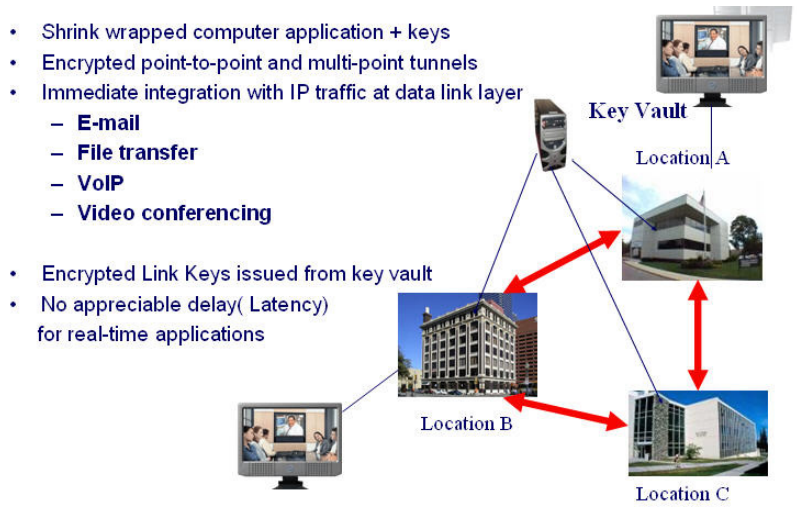
• provide a framework for collaboration or optimally a framework for collaboration that can provide application functionality by writing an XML document.

• support presence management and optimally will include a self aware application that several times a minute updates the authorized user list enabling dynamic collaboration and peer-to-peer communication.

• support multiple applications or optimally multiple applications and services, including multiple security services.

• operate at level 4 of the IP communication layer and optimally as much functionality as possible should operate at layer 5, 6 and 7.

Tunneling topology at IP data link layer



Whitenoise Laboratories (Canada) Inc.
abrisson@wnlabs.com

• Support the Federal efforts to provide extended alerting:
  o inherent intrusion detection
  o automatic revocation and system administration notification
  o provide a mechanism for Trusted Identity Management:

DDKI/DIVA:

- National Incident Management System (NIMS) requirements (SP 800-73, SP 800-78, SP 800-79, IR 6887)

- Homeland Security Presidential Directive 12 (HSPD-12) and Federal Information Processing Standard (FIPS) 201 compliance and support

Note: Dynamic Distributed Key Infrastructure framework exploit characteristics of next generation symmetric key technologies that run in parallel with other network processes to provide identity and log activity and to provide: dynamic continuous authentication, inherent intrusion detection, automatic revocation etc. While use of these keys would provide much stronger, more flexible identity based encryption this is not a requirement. Other encryption algorithms can be used. DIVA provides the oversight of identifying whether the other encryption algorithms and their keys are broken or stolen.

4.2 Key Performance Parameters (KPPs)

The KPPs are those attributes or characteristics of a system which are considered critical or essential. Failure to meet a KPP threshold value could be the basis to reject a system solution.

The only requirements to set up a secure DDKI/DIVA network, or network of networks, is a server for key creation, key management and key distribution (system administration) and devices or endpoints (terminals, computers, mobile devices, critical infrastructure components etc.) that have a little bit of storage or memory to hold a secure distributed key, write-back capacity to manage dynamic offsets, and connectivity.

DDKI network of networks also have the following key performance parameters:

• **Resiliency** - Interoperable communications establish secure data communications. Redundant communication is provided with the networks.

• **Accessibility** - Communications is established without the need for technical support. No configuration of the software is required to setup a client.

• **Portability** – the system allows secure access from anywhere with any device.

• **Interoperability** - The network provides full interoperable data communications among all supporting agencies regardless of communication device types. The interoperability is dynamic. Dynamic interoperability is the ability to connect any user across any network and have the ability to connect any IP communication device with any other IP communication device. The interoperability is at level 4 or 5 of the communication layer enabling the network to connect any network and run on any IP device.

• **Expandability** - The network does not have any limitation on the number of users it can support.

• **Visibility** - The network is able to allow span of control and mutual assessment and collaboration. The software interface supports a span of control over the users allowing for grouping users into manageable groups and subgroups without compromising security. The ability to group is simple. System administration and command sees all resources. Peer-to-peer voice, video and data communication gives the ability on demand to have private one-on-one communication or private group conversations.

• **Transparency** - The DDKI network enables the interoperability of voice, video and data communications, but it must also interconnect and support other networks and networks providing alert, warnings and advisories. The software enables alerts and advisories between any parties without needing anything but the software. The alerts and advisory capability will expand to provide public advisories.

• **Flexibility** - The system provides full featured software that is configurable from an easy-to-use system administration GUI interface.

• **Usability** - the network works in any digital context.

• **Adaptability** - The communication framework allows for the rapid implementation of services and development or integration of applications used for collaboration. It creates a network of networks, enabling scalability, interconnectivity and rapid data convergence among all parties in minutes. This capability does not require dedicated technical resources to maintain. The networks function in any environment without need of other networks and seamlessly interconnect to those networks without requiring the user to do anything.

• **Affordability** - The system is affordable. The networks must be COTS compliant and provide volume-pricing incentives.

4.3 System Performance.

Secure identity based network communications work in any Homeland Security context.

4.3.1 Mission Scenarios

Describe mission scenarios in terms of mission profiles, employment tactics, and environmental conditions.

Secure identity based network communications work in any Homeland Security context.

4.3.2 System Performance Parameters

Identify system performance parameters. Identify KPPs by placing an asterisk in front of the parameter description.

• Resilient communication established in minutes.

• No technical support is required to set up system.

• Same functionality is available in any context.

• Works in low power and small footprint devices.

Whitenoise Laboratories (Canada) Inc.
abrisson@wnlabs.com

• Provide an easy-to-use administration control GUI or HMI.

• Allow for computing devices to be networked together using 10BaseT or 100BaseTX LAN connections.

• Allow any combination of LAN ports to be connected together in subnets for use in small or large secure networks.

• Equipped with system status, warning, error indicators.

• Encryption standard must compile with 802.11i with AES-CCM & TKIP Encryption, 802.1x, 64/128/152bit WEP.

• Wireless data transfer speed is only restricted by hardware.

• Wireless nodes peer-to-peer

• Port forwarding / tunneling allowing an external user to reach a port on a private IP address (inside the LAN) from the outside WAN connection.

• Usage Details - all network access and use is logged.

• Remote Office Support - yes

• Satellite services when they are needed.

DDKI / DIVA Frameworks and Software:

• Provide for modular system development and composition.
• Provide a method for brokering transactions amongst the composed subnetworks.
• Provide a method for definition of composition of services.
• Provide for communications among any clients.
• Are able to render audio and video supplied in various formats.
• Are able to capture audio and video in some number of oft-supported formats.
• Provide a method for publishing availability/capabilities to other possible clients.
• Provide for authentication of credentials and access to identity information.
• Provide for ad hoc network creation where indicated.
• Provide for store and forward of data where required
• Provide a method of finding clients with known characteristics.
• Provide a method for decoupling content from the method for transporting said content to other clients.
• Provide for data transport.
• Provide for control/throttling of data transfer (particularly streamed data transfer)
• Support the Federal efforts to provide extended alerting.
• Provide a mechanism for Trusted Identity Management.

4.3.3 Interoperability

Identify all requirements for the system to provide data, information, materiel, and services to and accept the same from other networks, and to use the data, information, materiel, and services so exchanged to enable them to operate effectively together.

Interoperability provided by software create a dynamic distributed key infrastructure communication framework that enables any IP device or system to create a network-of-networks which provide interconnectivity between any IPv4 or IPv6 user device and multiple IPv4 or IPv6 networks.

Any authorized person or non-person entity can communicate using voice, video or share data with any other endpoint or server; limited only by the capability of their device (i.e. a LMR would be limited to voice communications).

There is secure interagency communications and collaboration.

The only requirement for interoperability is that the terminal or device have a Unique Universal Identifier, storage, write-back capability and connectivity.

4.3.4 Human Interface Requirements

Discuss broad cognitive, physical, and sensory requirements for the operators, maintainers, or support personnel that contribute to, or constrain, total system performance. Provide broad staffing constraints for operators, maintainers, and support personnel.

Based on a communications framework presented in this ORD, the strength of a network-of-networks is software that will run on any operating system and which will run on an IPv4 or IPv6 networks.

There are no special human interface requirements other than logging on with a user name and password when accessing a network. A physical key can be required (like an access key or ID badge) or a key can be associated with the networkable device or component itself.

It is easier than sending email. Existing components, mobile devices, static devices and terminals can be used.

Around-the-clock telephone and online support shall be available from the provider.

The human interface requirement for this system requires the person to enter a user name and password and optionally to carry a physical key like an id badge. It is also possible to issue a key to a device (like a phone) and distribute the device to an authorized person in which case their device is their key which is distributed using ISO/ITU identity proofing level 4.

It is also possible to simply associate network access authentication with an additional biometric like an iris scan and thereby eliminate the need to carry a physical key.

4.3.5 Logistics and Readiness

Describe the requirements for the system to be supportable and available for operations. Provide performance parameters for availability, reliability, system maintainability, and software maintainability.

The number of servers required for key creation, key management and key distribution will vary according to how many departments wish to internally control their own security. For instance, the CIA and NSA could each have their own servers to create, issue and manage their own keys for their own personnel and connected devices and appliances. (This can also be provided by a managed third party or centralized service.)

In instances where the CIA then would want to communicate with the NSA, the servers for each of those departments in turn would have unique keys identifying themselves to one another and communicating rules, roles and permissions for interoperability and inter-agency secure communications.

Self contained servers with these capacities can be cloned, a physical box sent overnight, received by a system administrator, and installed behind their own perimeters and firewalls with complete system administration training in under two hours by just configuring a DNS address.

Key distribution occurs in three ways:

1. The device accessing the network has an enabled chip
2. A device accessing the network can have a key securely distributed as long as the device or chip has connectivity, minimal storage and write-back capacity.
3. A key can be provisioned by a system administrator (or supplier) onto a USB, Identity Badge or any other kind of portable digital device and that device is then distributed directly by the system administrator to the pre-authenticated and pre-authorized personnel or appliance.

Key distribution utilizes ITO/ITU Level 3 and 4 Identity Proofing for person and non-person entities.

Installation of the software is quick, simple and intuitive. No training is necessary to install the software and configure DNS for server software. No training is needed to install client side software.

No training is needed to securely log onto a network. No training is required to use the Hard Disk Drive Encryptor. No training is required to use a device enabled with a DIVA chip.

If the device is only able to run on an IPv4 network, free VPN tunneling software shall be available for installation. Installing and using the VPN requires no configuration. If a VPN is needed it should be as simple as clicking on ‘install VPN” and the VPN must automatically install, configure and connect to the network.

If software updates are released for the network, a release method of upgrading the software for free will be implemented.

Logistics must be handled by an organization, which specializes in delivering network technology efficiently to the public/private sector.

Efficient distribution of keys and software occurs on-line with virtual manufacturing of keys and provisioning.

Inventory is not required since new keys can be created and distributed as needed.

4.3.6 Other System Characteristics

Characteristics that tend to be design, cost, and risk drivers.

The system is simple to use and affordable. Services are provided with a flat rate annual license based on the number of human users or enabled endpoints for unlimited use. Pricing is simple to understand.

5 System Support

Establish support objectives for initial and full operational capability. Discuss interfacing networks, transportation and facilities, and standardization and interoperability. Describe the support approach including configuration management, repair, scheduled maintenance, support operations, software support, and user support (such as training and help desk).

Support is provided online 7 X 24 X 365, remotely either over text or voice (i.e. Skype) for both managed and self contained services. License costs including support and maintenance and upgrades for year 2 forward is 15% of yr 1 licensing and installation costs.

5.1 Maintenance

Identify the types of maintenance to be performed and who will perform the maintenance. Describe methods for upgrades and technology insertions. Also address post-development software support requirements.

A maintenance agreement shall be in place on every system. The networks will run around the clock, and if issues arise, users should contact the support desk. The support will be available unceasingly. If updates to the system software are needed, the update will be sent directly to the user by the support desk and will be downloadable from a support website.

The day-and-night support center shall have the ability to run remote diagnostics on any kit and if possible repair the system remotely.

5.2 Supply

Describe the approach to supplying field operators and maintenance technicians with necessary tools, spares, diagnostic equipment, and manuals.

The installation software will also be available on servers so that the software can be downloaded if necessary. The software shall also be downloadable from approved, secure websites with proper authorization. Installation of the software is quick, simple and intuitive. No training is necessary for any pre-authorized and authenticated person/device to install the software and securely connect to the network.

5.3 Support Equipment

Define the standard support equipment to be used by the system. Discuss any need for special test equipment or software development environment

The system will include any equipment necessary for testing and the system shall be available to be tested remotely by customer support if needed. The remote diagnostics will require nothing more than the customer's approval.

5.4 Training

Describe how the training will ensure that users are certified as capable of operating and using the proposed system.

The system is simple enough that user training is not required. System administration training and installation requires only about two hours.

However, in order to maximize the power of the secure networks and to fully understand what secure services are available and how they work, webinars will be held as needed on demand on a regional basis covering topics that will improve the effective use of the DIVA enabled secure networks.

An online group forum will be available for users to share ideas and ask questions. It will also be a point where users can request additional specific service capabilities or functionality on an ongoing basis.

5.5 Transportation and Facilities

Describe how the system will be transported to the field, identifying any lift constraints. Identify facilities needed for staging and training.

The software does not require transportation or storage. It can be securely downloaded on your own servers and your own endpoint devices. A cloned physical server can be prepared and delivered overnight.

6 Force Structure

Estimate the number of networks or subnetworks needed, including spares and training units. Identify organizations and units that will employ the networks being developed and procured, estimating the number of users in each organization or unit.

Many homeland security applications rely on resilient communications. The must be a communications system (ISP) to connect to.

Because Dynamic Distributed Key Infrastructures create tiered, hierarchical network topologies, enough servers must be distributed across the country to provide resilient communication in enough locations to guarantee a national emergency communication network can be created from a network or identity based authentication servers (or managed services.) It would take 200,000 servers to provide at least one system to each of the following:

Potential system users Approximate Number

- Law enforcement agencies in the United States 17,000
- Fire departments in the United States 30,000
- Incorporated cities in the United States 80,000
- Counties and or Parish Governments in the United States 3,000
- School Districts and Colleges in the United States 20,000
- Emergency Operation Centers in the United States 15,000
- Ports of entry in the United States 240
- Critical Infrastructure and Key Assets in the United States 33,000
- Hospitals in the United States 5,500

These numbers do not reflect the number of court houses whether Federal, State, District or Local, the number of jails and or prisons, total number of Federal Government agencies buildings or personnel in the United States, the number High Schools, Middle Schools or Elementary Schools in the United States. The numbers also do not reflect the number of substations and offices within a particular category. If a system was distributed to each of the 53,000 fire stations alone, the infrastructure for a national resilient communications network would be in place.

The system can be distributed to every department in the country as needed online.

A secure communication infrastructure is created and scaled at a local, regional, state and national level creating interoperability and enabling collaboration and cooperation on an as-needed basis or a basis scaled by budgets, priorities etc.

7 Schedule

To the degree that schedule is a requirement, define target dates for system availability. If a distinction is made between Initial Capability and Full Operational Capability, clarify the difference between the two in terms of system capability and/or numbers of fielded networks.

- Secure File Interchange 2 - available
- Secure Session Manager - available
- Hard Disk Encryptor - Available
- Chip - 6 months to commercial ready
- Firmware upgrades available now. Server is currently available to create, manage and distribute keys.

Because almost all provisioning uses virtual manufacturing and secure electronic distribution, these technologies can implement quickly and easily at your demand.

Whitenoise Laboratories (Canada) Inc.
abrisson@wnlabs.com

Testing should not only include the natural crypto-analytics but also measure basic network efficiencies that we are really interested in like:

- have the number of attacks against the system gone down
- have there been any successful breaches
- has the system self protected
- has the system isolated intrusion attempts and prevented any cascading of events
- has the cost of maintaining the networks gone down
- how have end users responded

The system should be rolled out in phases. Year one should establish secure servers in the most vital areas creating a national framework of priority departments and supporting agencies with a nationwide roll-out completed in less than four years.

8 System Affordability

Identify a threshold/objective target price to the user at full-rate production. If price is a KPP, include it in the section on KPPs above.

Because almost all provisioning uses virtual manufacturing and secure electronic distribution, these technologies can always be integrated into existing networks at a small fraction of the cost of competing networks. Because of the different ways in which a network is used, and who or what is accessing these networks, pricing/licensing/maintenance cost models vary among contexts. However, all pricing models are designed and intended to be consistent with the pricing model that enterprise or government units already use. They are also negotiable.

Example 1:

The government already buys devices from approved manufacturers that have microprocessors in these components. A manufacturer has already priced in the cost of the chip sets used in their devices. Should a government request that certain devices they already have and or are purchasing come equipped with a microprocessor that distributes identity, and is man-in-the-middle and side channel attack resistant, then there is little or no change in costs to manufacture those devices because they are simply exchanging types of chip sets (and not adding a component that wasn't required before.)

Enterprises using networks employing asymmetric PKI security technologies are charged licensing and setup and installation fees and ongoing maintenance/licensing fees.

For example: The Verisign white paper on installing self managed secure networks estimate that ANY size unit will spend hundreds of thousands to millions of dollars to install and setup such a network. This will take up to three or four months. It will require the overhead of full time employees to maintain these more complicated networks.

- Cost for Verisign self managed secure networks
- Rainbow Technologies, Price List

Additionally, the above competitive pricing and licensing is presented in a way that is not intuitive and simple to understand.

Additionally, the pricing of the above competitive approaches does not scale linearly. For example, it will cost an enterprise with 10 employees and an enterprise with 100 employees the same amount of money for the installation and setup costs to get going. This reality has precluded small and middle sized enterprises from being able to afford secure networks in the first place. We see this in the fact that outside of government, less than 10% of all businesses in the US use secure network technology forty years after public key networks were invented and available.

Conversely our pricing model for "enterprise network-of-networks" is:

$1000 per seat (person) installation and setup and provisioning and training costs

Thereafter, there is a 15% annual license and maintenance fee for use, support, maintenance, and upgrading of these networks.

Example 2

Smart grids and critical infrastructures are generally comprised of MANY non-person entity components that communicate critical information to control. These devices (as well as legacy devices) generally have adequate storage, write-back capacity, and connectivity. This is all that is required to harden the security of these devices and integrate them into large, rapidly scalable secure networks with an electronic/online upgrade or firmware.

This virtual manufacturing and electronic provisioning structure creates economies of scale and speed that cannot be replicated by competitive technologies. As such, on a negotiated basis, critical infrastructure components can be provisioned at pennies (to dollars) for endpoints.

http://www.wnlabs.com/marketing.html

Secure digital networks and networks

- Secure File Interchange Total Cost of Ownership
- Total Cost of Ownership Comparison
- The Value Chain for the Telecom Industry

10 Appendixes

Homeland Security High Priorities

When the United States held the first National Cyber Leap Year Summit, the highest prioritized group was Digital Provenance since the communication/IT critical infrastructure impacts ALL the other Capstone groups. Whitenoise Laboratories (Canada) Inc. was the only Canadian company invited to this summit and our technology was placed into the Digital Provenance group.

http://www.wnlabs.com/leapforward.html

Likewise, Dynamic Distributed Key Infrastructures (DDKI) and Dynamic Identity Verification and Authentication (DIVA) affect ALL Homeland Security High Priority areas:

5. Cyber Security
6. Information Sharing
7. Interoperability
1. First Responder
2. Border Security
3. Cargo Security
4. Maritime Security
8. Transportation Security
9. Counter-IED
10. Chemical/Biological Defense
11. People Screening
12. Infrastructure Protection
13. Incident Management

Whitenoise Laboratories (Canada) Inc.
abrisson@wnlabs.com

11 Glossary

DDKI - dynamic distributed key infrastructures
DIVA - dynamic identity verification and authentication
IPv4 or IPv6 networks - internet addressing protocol (32 bits and 64 bits IP address lengths)

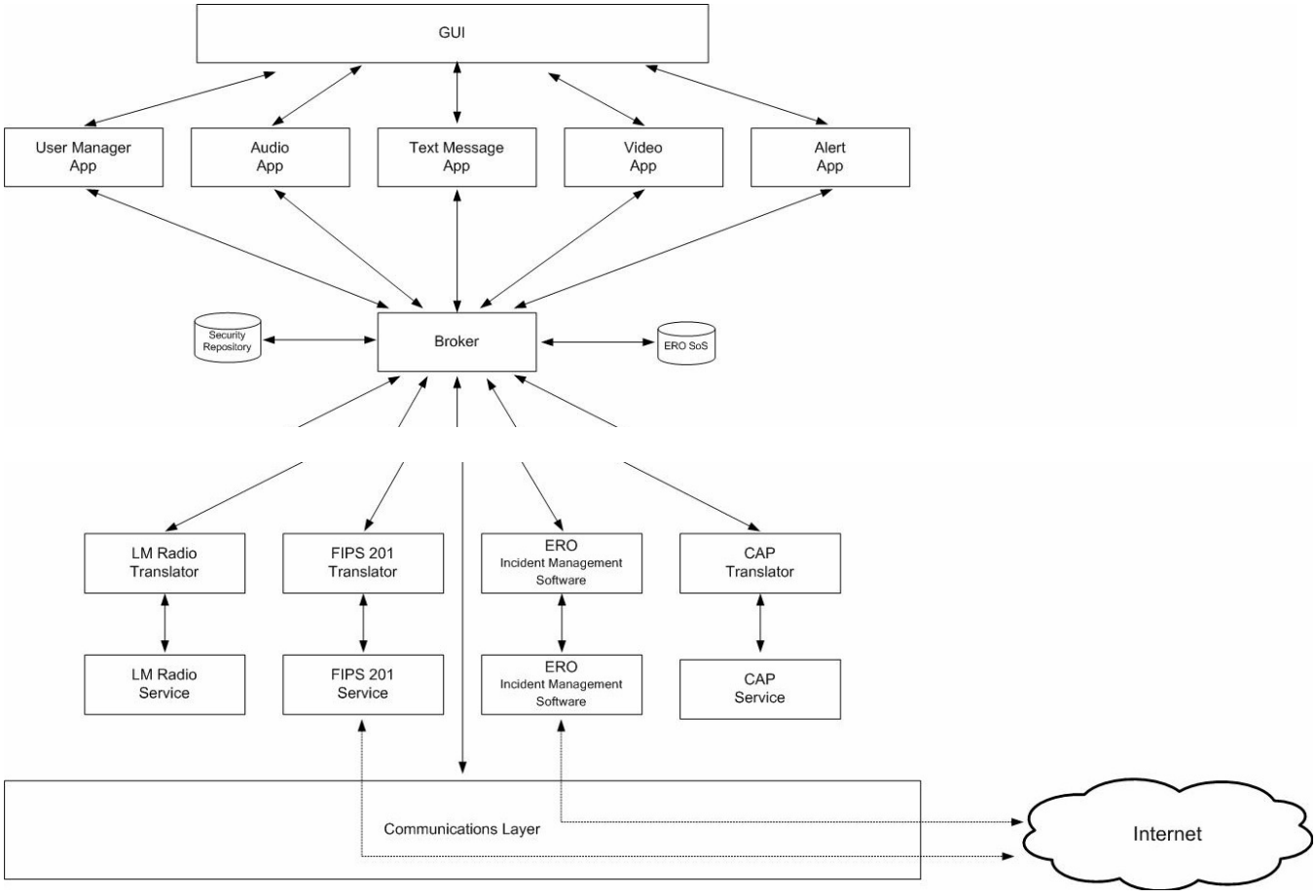
In this document, the terms "system" refers to any combination of components and servers and applications that are utilized to create a dynamic distributed key infrastructure invoking dynamic identity verification and authentication to create secure, identity based network frameworks.

The components as presented could include:

- Secure enabled microprocessors
- Secure enabled firmware upgrades
- Secure authentication and identity management servers
- Secure data storage with the Hard Disk Drive Encryptor
- Secure communications and file exchange with Secure File Interchange 2
- Secure network access with Secure Session Manager

Whitenoise Laboratories (Canada) Inc.
abrisson@wnlabs.com

Example Application topology



Whitenoise Laboratories (Canada) Inc.
abrisson@wnlabs.com