


Our goal is to help you shape the future of the telecommunications. Your task is to recognize the complete solution and the almost limitless business opportunities it can create.

We can provide it to you!

This paper presumes that you are familiar with Whitenoise technologies and have easy access to the resources on your portal. A fast look at the core technology that is the foundation of this analytics request is available here: Please see:

http://www.wnlabs.com/papers/Nokia_SV_Open_Innovation_Challenge_WNL.pdf

## Abstract

Novel advanced analytics development approaches and technologies are needed to further support the mission and the full enablement of both the analyst and analytic development communities.

Whitenoise technologies (patented globally), Dynamic Distributed Key Infrastructures (DDKI) and Dynamic Identity Verification and Authentication (DIVA) provide the simple, rational, scalable, interoperable, virtually manufactured, and virtually provisioned framework for secure computing infrastructures and fast, accurate, configurable analytics.

Identity management and data provenance is central to any objective scientific, software or information visualization that your analysts will leverage to satisfy their work mission in analytics. They will provide the highest level of security and utility while streamlining their workflow, increasing their output, buying back time for the analytic developer, reducing costs and risks, simplifying scheduling and maximizing the use of limited resources.

Core Whitenoise, DDKI, and DIVA remain the same in all contexts. They are simple and logically configurable in real time to achieve different goals. In this paper as we examine ways to use Whitenoise technologies with analytics we will get an insight into what your analysts will encounter and consider. We will see how they dial in balancing privacy and security in satisfying their work mission with a standardized design and implementation approach which is a simple and harmonious method to analytic challenges and achieving specific goals.

To do so properly we must first examine the playing field where your analysts are currently huddling.

## Description

There are only two fundamental computing framework choices: public key asymmetric infrastructures (PKI) and Dynamic Distributed Key Infrastructures (DDKI).

DDKI is much simpler than PKI which is losing the cybersecurity war, much cheaper, and far more accurate and secure. And it has the benefit of working seamlessly with PKI and your existing security controls, fixing their fatal flaws and imposing provenance (the one ring/control to rule them all!)

There have been no fundamentally different approaches to network security and communication security frameworks beyond DDKI. The difference in approach is as stark and displays the same fundamental level of impact that Tesla's alternating current electricity approach was (is) when compared to Edison's direct current approaches.

A simple approach is desperately needed to address the exploding universe of security vulnerabilities because of the IoT, sensors, and other low cost components on your networks. Clients need objective information based on perfect provenance to arrive at the best conclusions about whom or what is using their networks and how they are using them. This allows the optimization of everything from physical network infrastructure to workflow, advertising (commercial mining) and to law enforcement oversight (where required.) The solution methodology must be simple and:

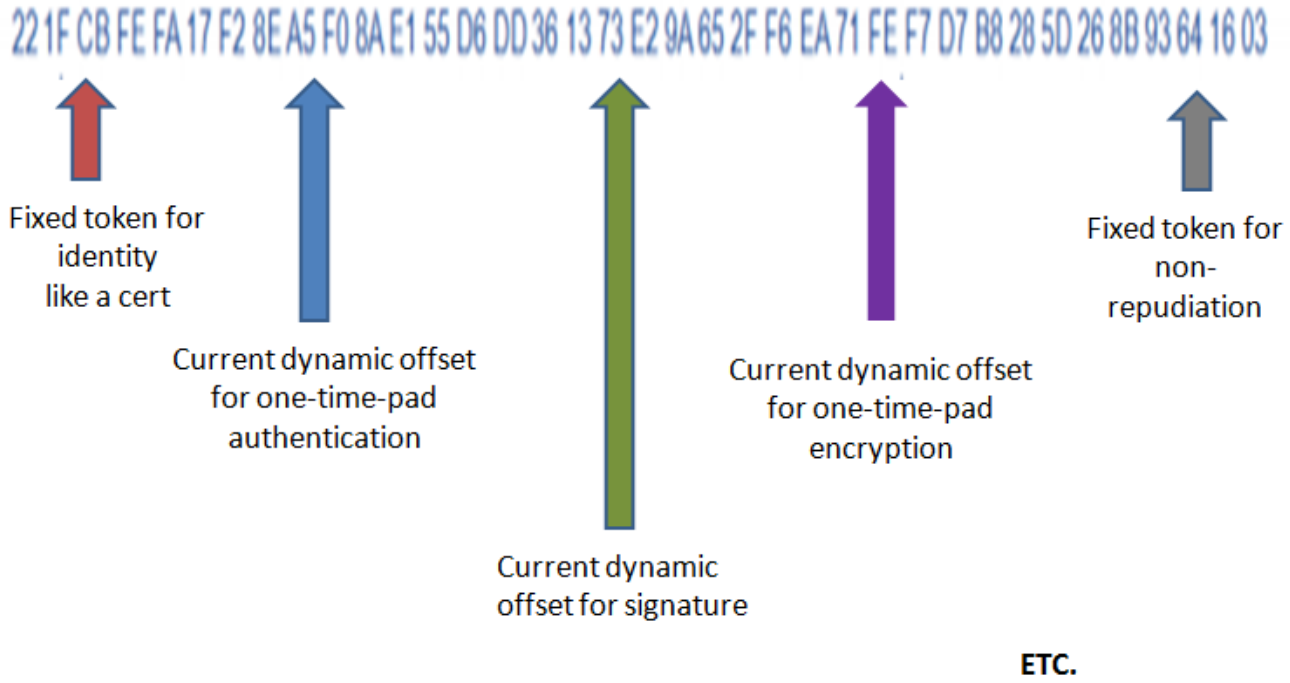
- Easy to teach
- Easy to implement
- Easy to install
- Flexible to dial in degrees of security and privacy
- Virtual manufacturing
- Virtual provisioning
- Extensible on the same framework
- Scalable (virally)
- Interoperable

A previous submission on automatic resiliency and automatic regeneration of enterprise class compute networks showed one technique where data provenance is imposed with one-time-pad accuracy and deterministic tagging or labeling of data. This is central to our approach to analytics. So let's immediately look at the characteristics of Whitenoise keys which are our primary building block for secure computing and meaningful, objective analytics.

## One key

- The key is an exponential deterministic random number generator (RNG) data source.
- The Telco or service provider receives a master key (RNG).
- The Telco can make an unlimited number of client account keys and distributes them to their customers or network endpoints one time.
- The unique, private, account keys create key streams of unlimited length and are deterministic RNG themselves. (Key structure storage requires little space.)
- The unique, endpoint, distributed, private keys create an infinite number of unique one-time-pad tokens (small key subsets) from that one-time-distributed key.
- We know where each key-based cryptographic call or control is being called from in the key stream by tracking current dynamic offsets.
- We track different current dynamic offsets which are pointers or indexes into the key stream for each different, key based, network security control.

## Track all key based security controls from one infinite deterministic random key stream




## Key characteristics

- The keys and tokens can be of ANY bit strength.
- Smaller tokens for authentication can be safely used because DIVA operates as a dynamic, continuous, one-time-pad.
- Because the keys are unique to each endpoint or device they provide authenticated encryption for storage or transmission with provenance and identity.
- Because keys use the fastest function available on computers it is always as fast as the hardware.
- Because the keys are bit independent they can be parsed and cut up and reassembled. This insures secure key storage separating key structure and offsets.
- In hardware (like FPGAs) 2 bytes per clock cycle are processed. Speed is scalable by adding more threads. The fastest RSA algorithm (Spritz 2014) needs 24 clock cycles to process one byte. AES-NI needs 28 clock cycles per byte. Both Spritz and AES-NI are slow and computationally intensive.

  We can use the same key for any use endlessly because the keys are deterministic and of infinite length.

## Analytics

"Analytics is the discovery and communication of meaningful patterns in data. It is especially valuable in areas rich with recorded information, analytics relies on the simultaneous application of statistics, computer programming and operations research to quantify performance." *wiki*

"Firms commonly apply analytics to business data, to describe, predict, and improve business performance. Analytics is a multidimensional discipline. There is extensive use of mathematics and statistics, the use of descriptive techniques and predictive models to gain valuable knowledge from data—data analysis. The insights from data are used to recommend action or to guide decision making rooted in business context. Analytics is not so much concerned with individual analyses or analysis steps, but with the entire methodology." *wiki*

DDKI provides a simple alternative methodology that works. And conceptually DDKI fits because it too is multidimensional.

Analytics is usually coupled with scientific, software, image, and information visualization which are representative techniques to better understand the data (usually massive volumes) to make better predictions and decisions. See Addendum for Visualizations.

# Maximizing the use of limited resources

Communications, analytics and security need a simple, repetitive way of configuring networks to solve various problems.

Limited resources are maximized by building/providing solutions that have just a few simple building blocks that remain the same and a simple configuration dashboard.

## First core key characteristics

Above we saw that Whitenoise is a deterministic random number generator. Go to this page and you can easily create a key stream that is quadrillions of bytes long.

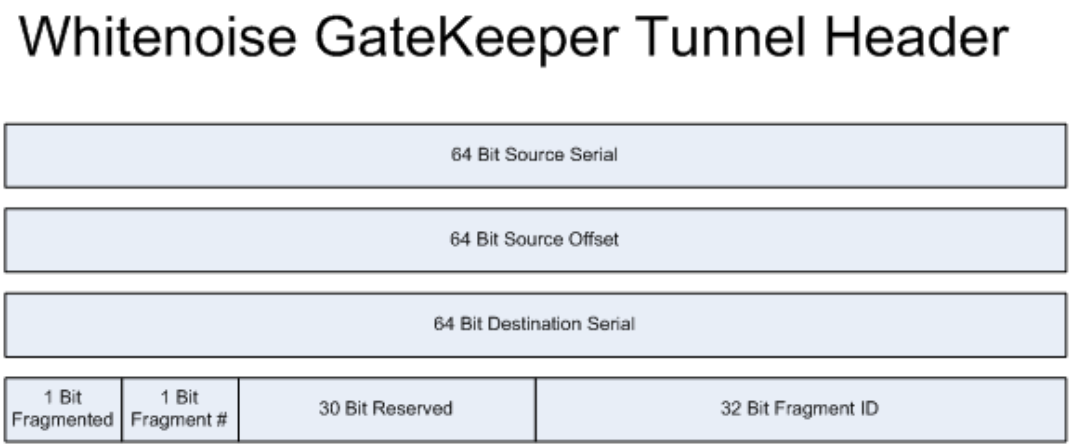
Because this key stream is so long we can use different specific tokens identified by length and a current offset to represent anything we would like such as permissions, identity of users or endpoints, different web sites that have been visited, different products that have been used etc. (literally anything can be represented by a trackable token.)

# Configuring/tagging information you are interested in (or all data)

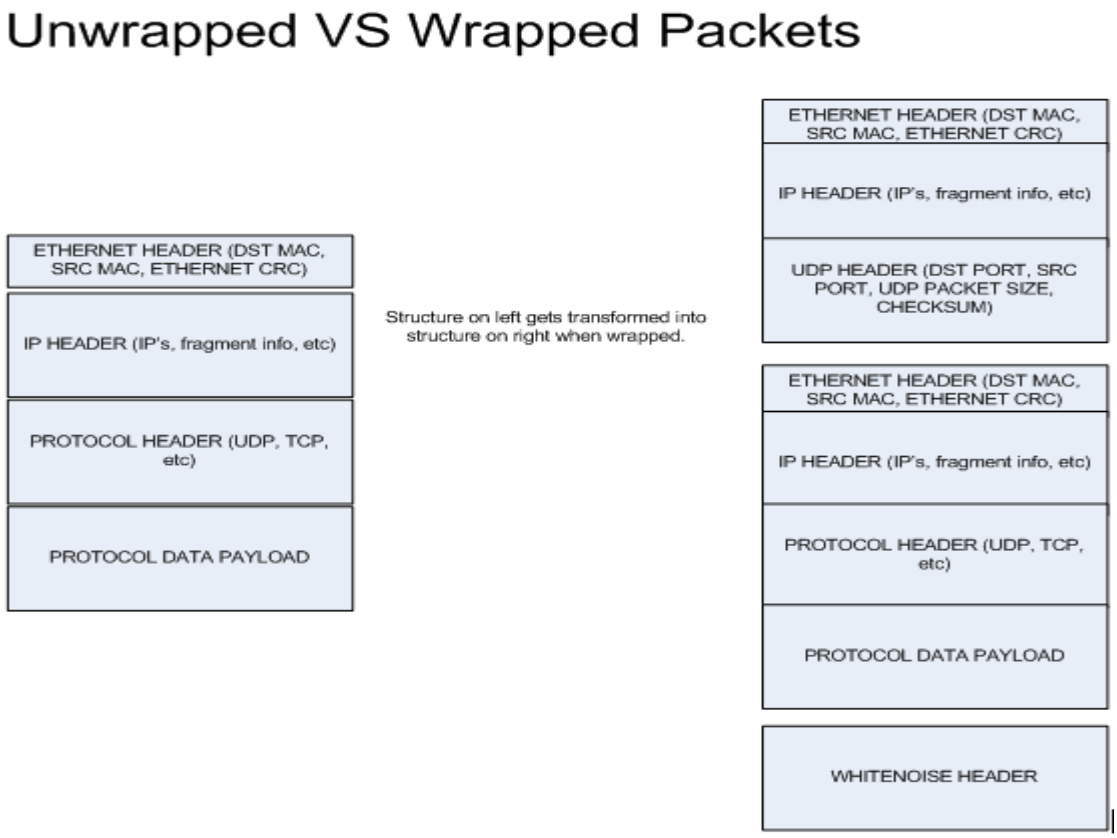
Because of the length of the keys we impose data identity by using different static tokens from the unique, private, and authenticated key streams to represent any demographic or characteristic or use data. The place and technique that is selected to "brand" or label specific data for analytics can be done a few different ways. The prime concern the analyst makes is in regards to a choice of labeling so that the information pathway has proper

routing and identity in context so that communications are not likely to be interrupted. Here are a couple of points where labeling can be applied.

## Secure point-to-point tunnel header




## Wrapped and unwrapped encrypted payloads



The first serial is the serial of the originating system, the second serial is the destination system serial, and the offset is the offset into the Whitenoise stream that was used to encrypt this particular packet.

The fragmented bit indicates if this is a fragmented tunnel packet, the 1 bit fragment number indicates if it's the first or second fragment, 30 bits have been reserved for an authentication pad (see the future enhancements section) and 32 bits are used for the fragment id used to distinguish these fragments to other fragments. There is a 1 in 2^32 chance that fragments may have overlapping fragment ids and this would corrupt the re-assembly.

This header, consisting of 256 Bits, plus the additional Ethernet, IP, and protocol headers, in the encapsulated packet, make up the overhead in the overall tunnel system. This overhead is per packet, so if many small packets are sent out, then the percentage overhead is relatively large, however if large packets from file transfers are used then the overhead is very low.

- Meta data (i.e. XML, Predictive Model Markup Language - PMML)

## Balancing Privacy and Security

The responsibility in making these choices is significant and fairly represents one of the gate keeping points of balancing privacy and security in the ultimate mission of protecting our democracy. Techniques easily implement varying degrees of privileges and rights in confidential communications.

- Level of anonymity (commercial) ranging from complete to partial
- Authorizations and permissions and configurable scrutiny levels
    - Clearance levels (military)
    - Alert levels (Homeland Security)
    - Tag and send back (intelligence and law enforcement)

### Analytic Business Codes – (ABCs or AB Code) example

This technique can be effectively used in supply chain management, customs etc. identifying particular goods, countries of manufacture, etc.

- Vehicle identification
- Universal Product codes
- Production code numbers
- ISBN
- Bar codes
- Etc.

Here is an example on how to manage goods moving between the 350 ports globally and tracking goods for customs and preventing dirty bombs. The process secures the movement of goods and is also pertinent to the "streaming" discussion we will have.

http://www.wnlabs.com/Papers/SierraWirelessStopsMediaTheftandSecuresCargo.pdf

Obviously, any existing commercial and government coding systems can be used and available for analysis. Privacy can be ensured just by embedding those numbers in encrypted payload.

### SDK or Security as a Service (SecAAS) online configuration

- Choose services and features that the client wants
- Choose what you want to track or query or mine
- Choose what kind of handshake
- Dial in security and privacy to fit context

## Client side components

- Virtual (and viral) provisioning online

    - Pilot – IPSec/IPv6, LDAP/CAS, SIMs
    - Web page
    - Utility upgrade

- Standard endpoint requires communication ability, a little storage and write back
- 20k endpoint utility provides identity and provenance, answers authentication calls and performs selected security controls.

    - Phones
    - Tablets
    - Computers
    - Printers etc.

- And we can be implemented in places that pki cannot go because PKI has excessive overhead needs. Whitenoise technologies give fractional cost components identity and one-time-pad strength.

    - IoT inexpensive components
    - RFID
    - Sensors
    - Peripheral interface controllers
    - Circular shift registers
    - Line feed shift registers
    - Counters
    - Biometrics

## Server side

Server is provisioned one time physically so that the system master key is never transmitted electronically and is unknowable for any cyber criminals. This is Level 4 identity proofing.

- Key generation utility
- Make unlimited client/account/end point keys
- Make session keys when desired for some configurations

(This handshake paper shows the simple basic handshake process and alternative session key creation process. Using session keys would mean there is no encrypted traffic travelling through the server and available for internal capture.)
- Make the one-time-pad authentication call comparisons
- Dashboard for system analysts and remote authorized access
- Making infinite number of one-time-pad tokens for configurations leveraging the master key

### Databases

- Track accounts, keys, current dynamic offsets, offsets, analytics tokens
- Separate databases for keys and offsets for key security
  - Separate servers for keys and offsets
- Encrypted key and offset and database storage

### Computing Infrastructure

Currently wiki lists only PKI and Converged Infrastructure as the only computing infrastructures. PKI has fatal flaws and converged infrastructures are groups of various components and layers cobbled together to hide those flaws and improve resiliency.

The goals of these infrastructures is to provide a secure computing environment for critical processes like automation of machinery, predictive workflows etc. but they have severe physical and security challenges in trying to accomplish those goals.

DDKI and DIVA does not have these challenges and therefore offer a revolutionary alternative that works, works with existing frameworks and security controls, and fixes their flaws.

This paper was presented to the First US National Cyber Leap Year Summit at the invitation of NIST/OSTP at the White House.

http://www.wnlabs.com/Papers/generic_idm_policies-for-international-harmonization_whitenoise.pdf

## Streaming

Whitenoise technologies were presented as a Fail Safe for Quantum Cryptography and transmission to the European Telecommunications Standards Institute.

Quantum cryptography requires a data source to make keys which are then used to orient quantum for encryption and transmission. Quantum computing requires the most random data source available for not problems.

It is recognized that it is unlikely that quantum computing will ever be able to prevent denial of service attacks in unshielded transmission because of the inherent instability of quantum (just looking at a quantum particle will change its position.) Whitenoise technologies were

recognized as being the fastest semi-traditional key technologies that could take over those communications and still move at the speed of the hardware involved.

Because Whitenoise technologies create exponential length keys that are bit independent and corruption resistant, and which use the fastest function available on any computing device/component it is ideally suited for streaming. Examples of high volume streaming contexts would be surveillance, live media, etc.

http://www.wnlabs.com/technology/Self_Demo.php

http://www.wnlabs.com/downloads/WNspeedUtilitydemonstrator.zip

http://www.wnlabs.com/papers/WNL_HDD_and_Streaming_Demos.zip


# Addendum

## TCSV/Nokia document

This document is taken in total and was the application for the Telecom Council of Silicon Valley Nokia Global Innovation Challenge for Cloud and Colossal Data (analytics). Because the overall methodology of the framework is consistent across verticals, contexts etc. this is being included because it highlights an area of great overlap. A massive amount of data will be collected from the cloud for analytics.

Whitenoise Technologies are revolutionary. www.wnlabs.com . We are pleased that this has been recognized by our selection for the International Trade Canada Boston Cyber Accelerator at Harvard/MIT commencing June 1, 2014. http://www.thecene.org/#!cta-boston/c1v1m.

One Whitenoise distributed key will create an infinite number of one-time-pads, the only provable, unbreakable key technology.

http://www.wnlabs.com/papers/Executive_Overview.pdf

Once distributed key is all a person or endpoint will ever need for their entire lives.

One distributed key enables Dynamic Identity Verification and Authentication which is a single protocol that provides all network security controls including perfect identity; secure network access, dynamic-continuous authentication, authorization, signature, non-repudiation, national security level encryption (when desired), inherent intrusion detection and automatic account revocation without human intervention.

Dynamic Distributed Key Infrastructures (DDKI) is a virtual framework that creates a secure network of networks of devices, endpoints, and servers that deploy DIVA. It is completely interoperable and forever scalable (both the keys themselves and the virtual network.)
This single protocol and single framework eliminates all known attack classes:

- Man-in-the-Middle attacks are prevented because there is no key or offset exchange Side
- Channel attacks are prevented because all operations are order 1 after key load and because there is no access to the key
- Botnet attacks are prevented by configuration with server so the botnet never has access to the entire key and offset information.
- Quantum computing attacks are impossible because every variable is variable.
- Brute force attacks are prevented because the keys can’t be factored.
- Denial of service attacks can be prevented by exploiting unbreakable identity and secure network access so that hackers could never get on a network.

Although DIVA and DDKI can completely replace asymmetric systems, they are designed to work seamlessly with Public Key Infrastructures without direct integration into any of your existing security controls or frameworks.

DIVA and DDKI in conjunction with PKI (the predominantly implemented network security scheme) raises the bar by creating a two channel (both asymmetric and symmetric frameworks) multi-factor authentication protocol that also provides ALL network security controls.

The attacker then needs to break keys from two unrelated frameworks, one of them dynamic (DIVA), for each and every breach. You can see in the DEFCON – Black Hat Challenge the key in this example is set to dynamically change every 15 seconds. Currently the dynamic offset has changed almost 1,600,000 times. And of course, no one at either of the globally prominent hacker groups has been able to break it.

--

Whitenoise Technologies provide fabulous business opportunities which are virtually manufactured and virtually provisioned.

**Optimal network resource utilization is ensured.**

Whitenoise Technologies operate with X-OR after key load. X-Or is the fastest function available on a computer. We will always only be limited in speed and efficiencies by the physical speed limits of your hardware even in quantum computing and quantum cryptographic contexts.

- We don't add overhead.
- We don't bloat data – DRM 1 gig = 1 gig.
- Whitenoise does not chew up bandwidth with mathematically intensive asymmetric authentication protocols and inefficient encryption that generally need additional hardware to operate in big data contexts.

This ensures that we will always remain ahead of the leading threat curve.

**Whitenoise Technologies enhance user experience in many ways.**

Two of the primary enhancements are:

1. Your clients will finally get secure communications (and piece of mind from identity and cyber theft) that they expect but don't believe in when they purchase your services. (You in turn get massive technological competitive advantages.)
2. Clients will no longer have to remember user names and passwords.

**Unlock revenues**

Telecoms can completely eliminate the middle layer service and network providers by provisioning secure networks and services directly at a fraction of the cost and with no difficulty. This will build greater perpetual revenue streams. These middle level providers can never compete price-wise.

Here are three examples out of a host of products and services:

Verisign charges approximately $1500/year to enterprises for their certificate services. It takes days just to order and set this up. Whitenoise and DIVA can provide certificateless authentication in just moments. And we can charge any price and be profitable – a dollar a year, a dollar a month, a dime a transaction etc.

VeriSign whitepapers indicate that for even a mid-sized enterprise that a PKI system can cost hundreds of thousands of dollars, takes months to install, and that they still can't insure that it has been implemented properly.

**Marketing materials and links**

(bottom of presentation page)
http://www.wnlabs.com/technology/presentations.php


Whitenoise usually provisions virtual networks. However, we can provision fully loaded servers by overnight delivery for about $2,000 per server and $1000 per seat (employee). Upon receipt of the server, the system administrator places it behind their existing firewall, configures and single DNS, and distributes keys.

50 years after the advent of public key networks only about 10% of enterprises deploy them and they are not secure. Now companies of any size can afford perfectly secure networks.

For example, a company of 10 employees can get a secure network for about $12,000. A company of 20 employees can get a secure network for about $22,000, etc. For the Telcos, the majority of that cost is still profit and subsequently they will generate perpetual annuity licensing and maintenance fees. This can be sent overnight by FedEx and then a system administrator needs only configure a DNS and issue keys.

Mobiles are all provisioned with cameras. It is easy to use Whitenoise technologies to turn biometrics into a one-time-pad. Currently if a biometric is stolen or compromised a person's identity is jeopardized for their entire life because they can't change their biometrics. We prevent that and also facilitate the binding of organic identity to digital keys using ISO-IEC Level 3 and 4 Identity Proofing.

Please see the Gartner Vendor Briefing given on May 1, 2014 in relation to turning biometrics into one-time-pads, managed mobile services and secure adaptive networks:

http://www.wnlabs.com/downloads/Gartner_Video.mp4

**The Telco Cloud Challenge**

Cloud computing has revolutionized IT datacenters.

The only way to secure cloud computing is to provide the endpoint, client or enterprise the control of encrypting their own data before sending it into the “Cloud.”

Because of the extraordinary speed as well as the strength of the Whitenoise DIVA keys, endpoints can rapidly and with absolute minimal overhead encrypt any volume of data moving at any speed. This eliminates any risk to clients and enterprises that their data can be breached at the data centers or in the cloud.

DIVA and DDKI create an absolutely secure virtual, programmable infrastructure that can have open interfaces. This leverages the Telco Cloud opportunity in a holistic way and simply evolves current communications into a new Cloud Optimized Network Architecture – one that the Gartner Group calls a secure, adaptive network for mobile as well as static communications frameworks.

Build new cloud oriented business

**Delivery**

Virtually manufactured, virtually provisioned with online enrollment, authentication, collection of fees and activation of accounts and services.

**Operating models**

- marketing via social media
- top down models
- self running third party services
- secure the cloud/internet
- run any kind of business service in any kind of network, delivery topology

**How do we ensure security?**

**How is a key made?** - https://www.youtube.com/watch?v=9Ebgya6lxS4

DIVA and DDKI are the foundation

**What problem do we solve and how it does it work**
https://www.youtube.com/watch?v=GwkwgR_78dQ&feature=youtu.be

**Carrier grade reliability**
Carrier grade reliability is assured because of the characteristics of the technology and the absolute simplicity of implementation.

**Zero latency?**
To verify what you are being told you need to invest a few minutes.

First, here is a YouTube video showing Whitenoise key creation and speed testing. https://www.youtube.com/watch?v=9Ebgya6lxS4

Now, you should test it yourself. Download and install this simple utility that you just watched on the video. http://www.wnlabs.com/downloads/WNspeedUtilitydemonstrator.zip
When you create a key use it by encrypting and decrypting a file many thousands of times, you will see that after key load that the key can encrypt and decrypt easily as speeds near a gigabit/sec.

You can also test it with a simple streaming utility that only will play encrypted and authenticated media. http://www.wnlabs.com/papers/WNL_HDD_and_Streaming_Demos.zip

**Cloud Optimized Network Architecture**

One of your stated goals is to build new Cloud Optimized Network Architectures in a holistic way that simply evolves current communications into a new Cloud Optimized Network Architecture.

That is not stated so much differently by the Gartner Group who have targeted major needs in managed, mobile-centric services and scalable, secure adaptive networks.

To attain this goal, one of the examples you describe is Evolved Packet Core that have become virtual applications running on top of off the shelf IT hardware. WNL Technologies fit that description as well.

When you look for optimization, NOTHING is more optimal than our secure-cloud secure-internet topology described in the following paper on how in Dynamic Distributed Key Infrastructures that single, distributed keys can in turn distribute more secure, distributed keys. This is the mechanism that allows seamless scalability and interoperability.

In this topology, DIVA is deployed at data link layer with a GateKeeper and KeyVault. By definition it is unseen by applications running above it on the internet stack and therefore invoking security of the network only occurs one time and does not need to be repeated application by application. Where you mention packets, you will see that in this topology that Whitenoise headers are appended to routing packets.

www.wnlabs.com/Tunnel_Distributed_Keys_distributing_more_keys.pdf

abrisson@wnlabs.com