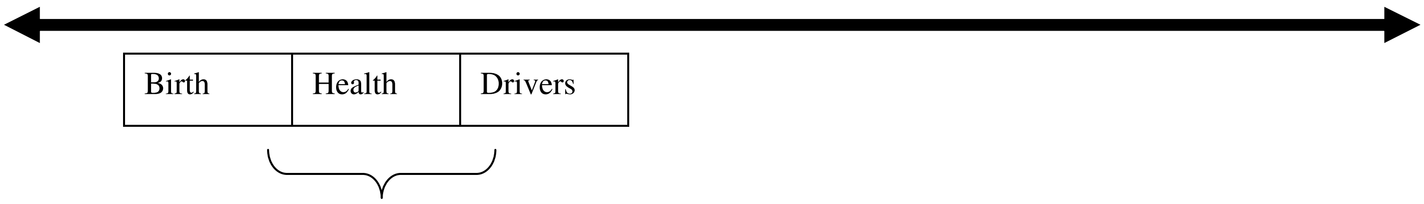
# Government Deployed Identity Management System

## One person–one citizen–one identity management key

This is possible because of the unique characteristics of new generation, deterministic key streams.

### Identity management key

- > $10^{60}$ bytes long key streams
- ~ 240,000 bit strength



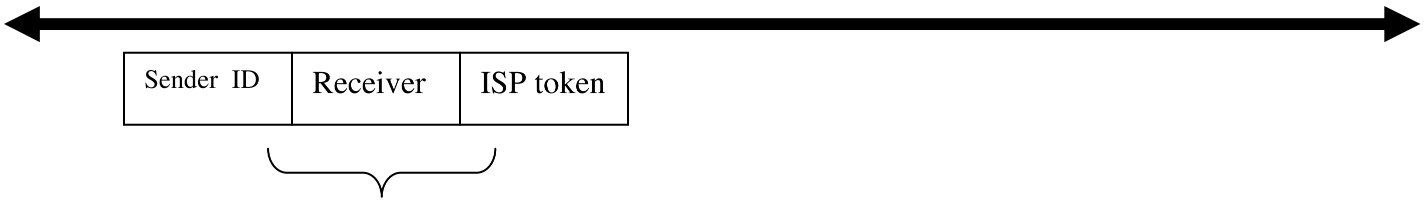
Balance of key used for dynamic authentication.

Birth | Health | Drivers

Fixed service token Unique Identifiers

### Identity management applied to keyMail e.g.

## SPAM Buster – see addendum



Balance of key used for dynamic authentication.

Sender ID | Receiver | ISP token

Fixed service token Unique Identifiers

## The life of a Canadian

A Canadian is born and the government issues an electronic identity management key that is first associated with their birth certification which is represented by a specific range on a key.

The newborn is then issued a health and insurance card which is represented by a different, specific range on the same key.

Throughout their lives different government services are represented by different, unique ranges on the same key for passports, drivers' licenses, tax numbers etc.

The keys are far, far more unique than an individual's DNA. The uniqueness of the keys allow for different, dynamic, distributed topologies.

These topologies overcome the traditional stoppers that have historically been associated with distributed key networks.

## DIVA identity management system

The highly secure Identity Management system called Dynamic Identity Verification and Authentication (DIVA™) utilizes unique features of large, symmetric Identity Management key streams and provide an integrated security system that people will use because it doesn't slow them down.

Identity Management keys provide continuous, state based identity verification and authentication of a user throughout the session and not just at login. Dynamic Identity Verification and Authentication [DIVA] also provides inherent intrusion detection because the offsets must remain in synch. And when intrusion is detected the system automatically denies network access to the hacking and spoofing. This is a technological capability not seen to date.

This identity management system provides multi-layered user access security. Users are issued a unique Identity Management access key that employs user ID and password protection as well as the requirement for the physical presence of a key or device. Any other layers of authentication can be used in conjunction. The key allows access to the system both locally and remotely. Keys can be issued to partner companies as well.

Secured information is exchanged with predefined rules. Information can be sent to one or more recipients, or predefined groups, in one operation.

DIVA Identity Management is simple to implement and is designed to fit within existing security schemes. A very important feature of the system design is the ability for the system administrator to deactivate lost or stolen keys immediately.

## Traditional problems solved

### Key management of these systems explodes into an exponential headache.

Historically the number of keys to manage is the square of the number of secure endpoints on a network. DIVA Identity Management has a one-to-one relationship between the number of keys and endpoints on a secure network.

### Key storage – long keys are a better source of identification and security but storing large keys is a nightmare.

Identity Management keys generate unique key streams on the order of $10^{60}$ bytes in length. However, only the internal key structure and the offset are required to recreate any key segment. This is a small amount of data. For example, 158 bytes of this information will generate a random key stream over 1 hundred billion bytes long. You can learn about multiplicity: View a brief description of an Identity Management Key Algorithm (Presentation)

### Key distribution is a major problem for distributed key systems.

This is not true any longer – Dynamic Distributed Key Infrastructure topologies allow distributed keys to in turn securely generate and distribute more encrypted keys. It allows the easy creation of secure tiered networks.

With all the traditional problems solved, DIVA Identity Management provides a secure digital network architecture that is far easier and less expensive to use than asymmetric key systems and there is NO reliance on Trusted Third Parties (outside of the government/law enforcement) for your security.

Distributed symmetric systems have always been the prevalent architecture and are the approach that has the least impact on user behaviour and is the architecture that consumers worldwide are familiar with. This is evidenced by all the important documents that individuals carry daily: drivers' licenses, credit cards, employee ID cards and passports are all examples of distributed keys which people rely on daily.

The flexibility of the DIVA Identity Management architecture allows the systems to be used with existing public key systems to add continuous authentication, 100% accurate inherent intrusion detection, and automatic denial of network access to criminals. Add the DIVA to your security protocols without replacing existing systems and without the need for additional hardware. All you require is an Internet connection.

## Government sets the standard and expectations

The government sets the standard for the key segments that are used for specific identification or services. It is a token, key segment – it is a ***verifiable subset*** of a user's identity that the government/law enforcement can verify.

These kinds of keys are deployed in **Dynamic Distributed Key** tiered architectures. These systems are distinguished by the ability of distributed keys to dynamically create and distribute more keys securely and electronically.

So we can easily issue such keys.

## What do secure networks require?

Only three things:

1. All components of the network are identified by a unique key
2. All persons on the network are identified by a unique key
3. All usage is logged

## Why is such a key secure?

To break keys when they are used for **encryption** there are three pieces:

1. Plain text
2. Cipher text
3. Encryption key

One needs sufficient information from two of the three components in order to break the key.

Identity management keys **are not used** for encryption. There is only one piece – the key itself.

There are only two ways to break a key in this context:

1. One must discover internal linearity characteristics or a mathematical relationship. These keys are structural in nature so mathematical techniques do not work.
   Security Evaluation IdM Keys - David Wagner (PDF)
   UNIVERSITY OF CALIFORNIA Berkeley

2. One can do brute force attacks – super computer attacks and randomness testing

   Brute force to guess the key is the only alternative left if one had the computing power. That is the process of testing every possible key. To apply brute force to a single key is not feasible.

View Dr. Traore's Report

University of Victoria British Columbia • Canada | Electrical & Computer Engineering

*"Exhaustive key search is not a threat.*

*Whitenoise uses keys with at least 1600 bits of randomness. ... Even if we hypothesized the existence of some magic computer that could test a trillion trillion key trials per second (very unlikely!), and even if we could place a trillion trillion such computers somewhere throughout the universe (even more unlikely!), and even if we were willing to wait a trillion trillion years (not a chance!), then the probability that we would discover the correct key would be negligible (about $1/2^{1340}$, which is unimaginably small).*

*In this report, I tried every attack I could think of. All of them failed. This provides evidence for the hypothesis that Whitenoise is cryptographically secure."*

**-Professor David Wagner, University of California, Berkeley, October 2003**

So the keys are secure.

## What is the problem?

It is scary that after three years governments cannot even agree on terminology in terms of addressing identity management. Instead of trying to define the terms, we need to define the outcomes we want to avoid.

- disparate systems, conflicting standards, decades of unorganized implementation, non-interoperability
- theft, crime, etc

## What is the conceptual solution?

Government is the biggest fish and sets the rules (democratically)

Government IS THE TRUSTED THIRD PARTY IN ALL CASES

## First - encapsulate the problem

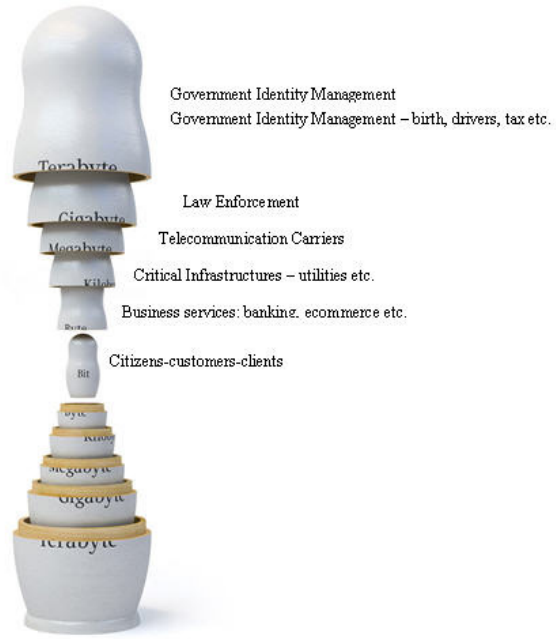
Encapsulate the problem like surrounding an oil slick so it doesn't spread. We are at a critical period of time in regards to security of critical infrastructures etc.

It is a top down solution.

## Top tier

Government issues keys for every telecommunications provider and networks (link keys) and they reside on the government authentication server.

Government issues keys for every citizen. That is about 35 million keys easily stored on a government authentication server.


Government Identity Management
Government Identity Management – birth, drivers, tax etc.
Terabyte
Law Enforcement
Gigabyte
Telecommunication Carriers
Megabyte
Critical Infrastructures – utilities etc.
Business services: banking. ecommerce etc.
Citizens-customers-clients
Bit

## Next tier

The carrier issues keys for every business providing a service. This is a token or subset of their carrier identifying link key, which itself is a subset of a master key which the government issues and regulates.

## Final tier

Citizens/clients have their Government issued electronic identity management key. As they use this key for any possible service, only the token for that particular service is accessed. These can be identified and used for registration or subscription to electronic services as belonging to a specific citizen since **the Government is the ONLY PARTY THAT HAS THE COMPLETE KEY OR KEY STRUCTURE.**

## Law enforcement is the tier linking the government and the public

Law enforcement resolves disputes and prevents cyber crime.

LAW ENFORCEMENT CAN ACCESS BOTH THE TOKEN IN QUESTION THROUGH SERVICE PROVIDERS AND COMPARE AGAINST GOVERNMENT REPOSITORY in court ordered scenarios.

This tiered approach encapsulating the entire ID Management problem and all networks will enable organized, secure co-existence among dysfunctional networks. Over time, of its own volition and evolution, redundant aspects of networks will be removed and disparate networks types will become harmonized as they want the ability to safely communicate with more networks and individuals under the umbrella.

## Implementing the system

Government requires that all telecommunications and network providers to use Dynamic Identity Verification and Authentication on all login and transaction procedures. It can be a redirect to a government run authentication server for this service or the government can mandate that telecommunication companies use it. DIVA can be integrated into existing systems of any kind; it can be used in parallel to any kind of network systems; it can be used in lieu of any other kind of network system.

In encapsulating the entire insecure networks issue, you are mandating that electronic citizens are adding one additional layer in electronic authentication. At the carrier this is the one time addition of three database fields to their client records: unique identifier of person, unique identifier of a device, and current offset. On device firmware/software it is the addition of a small identity application. At today's network speeds the extra step does not impact network performance. Government is simply saying that login protocols will use this system in parallel with any other existing process.

No entity is being asked to change anything in their existing architectures other than this step that ensures continuous authentication, 100% accurate intrusion detection, and automatic denial of network access to criminal behavior.

The government has just become the biggest encapsulating Russian doll and networks and communications are secured and allow accurate identification of everyone and everything on networks. They have simply added one encapsulating protocol at the TOP of the network food chain.

This paradigm allows government to easily and inexpensively address the identity management issues that are part of its legitimate mandate.

The system is simple for everyone involved. The addendum below shows the two ways to configure such a system and the level of “intrusion” or “effort” required.

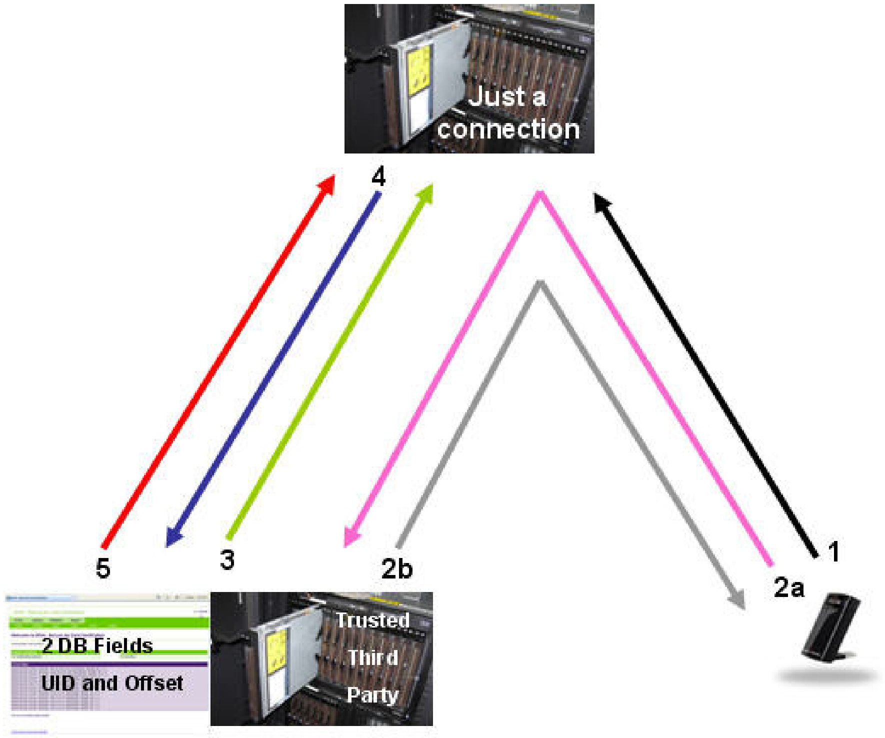
The system is simple for citizens because they only have one key, just like they only have one identity, and this simplifies or eliminates all problems associated with compliance and password and key fatigue. This system when applied to keymail (secured email) would eliminate spam as a nice bonus.

## ADDENDUMS

Each endpoint Aircard or cell phone has the DIVA protocol, a small amount of code, inserted into the device executable (i.e. Watcher.exe) and recompiled one time. This simple one time effort your mobile handset devices to be included as endpoint options in secure enterprise networks.

There are two ways to configure a Dynamic Identity Management system for secure systems. This represents the entire technological implementation requirements.

## TRUSTED THIRD PARTY SERVICE CONFIGURATION



1 - The Aircard or cell phone must connect to the network.

2a – Card sends authentication token through Telco to server

2b – Server sends pass/fail to the Aircard

3 – TTP and TELCO share last login time stamp (prevents bypassing DIVA)

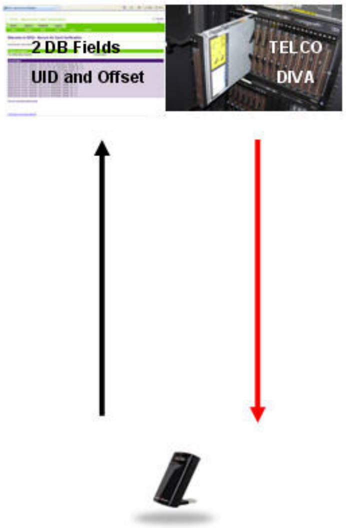
4 – TTP receives timestamp info and makes comparison

5 – On fail, TPP request Telco to terminate connection/deactivate.

With each "Pass" both the endpoint and the server automatically update their current dynamic offset, INDEPENDENTLY BY INCREMENTING THE OFFSET BY THE LENGTH OF THE TOKEN, so that an authentication token is NEVER re-used.

This Third Party authentication configuration can plug the security hole if the carrier shares with the Third Party provider information about when the last time a card using our service was connected. This information is the unique identifier and last login timestamp, neither which is a security risk for the TELCO. This would stop the ability to bypass step 2 and 3 in this authentication process protocol.

## CARRIER CENTRIC IDENTITY MANAGEMENT SERVICES



1. The Aircard begins connection routine to the carrier including an authentication token.

2. The carrier server verifies the authentication token and gives a pass/fail.

- The carrier needs to add only two fields to the data base managing logins for specific accounts: unique key identifier and last current offset. 64 bit offset for current offset.

- The carrier would add a DIVA authenticating code segment to the firmware or service application manager to thus embed it into the network protocol.

- The carrier would embed the DIVA service into the network access system on their server.

Note: With each “Pass” both the endpoint and the server automatically update their current dynamic offset, INDEPENDENTLY BY INCREMENTING THE OFFSET BY THE LENGTH OF THE TOKEN, so that an authentication token is NEVER re-used.

All of this can be done with software and electronically with existing systems and so it is the lowest cost approach.

## Critical Note on Electronic Provisioning and Scaling:

*There are two perspectives in deploying and configuring Dynamic Identity Verification and Authentication.*

*If the call for the DIVA protocol **IS NOT** included in the network login and access protocol of the network provider, then this security is configured to the specific handset and the third party authentication provider. This means the call for DIVA needs to be implemented into the firmware of the endpoint device so that it cannot be bypassed by a hacker.*

*If the call for the DIVA protocol **is required** by the network provider for secure access and login, then the DIVA routine on the handheld device **does NOT** need to be included on the firmware of the device. This absolutely simplifies the distribution process of this IdM functionality. The DIVA protocol can be downloaded through the Internet to ANY handheld device that has memory and the IdM capability is added. This eliminates having to deal with vendors of hand held devices who do not in general provide access to their firmware.*

*When the DIVA protocol is required at the server, the  hacker gains nothing by bypassing the DIVA routine on the handheld, mobile device. The server (Telco/ISP) is expecting a response token from the device. If none is given, there can be no network access.*

*This simplified provisioning capability is critical when considering how to update and secure components of critical communications infrastructures, SCADA, and machine-to-machine networks.*

## UBIQUITOUS END POINT CONFIGURATION

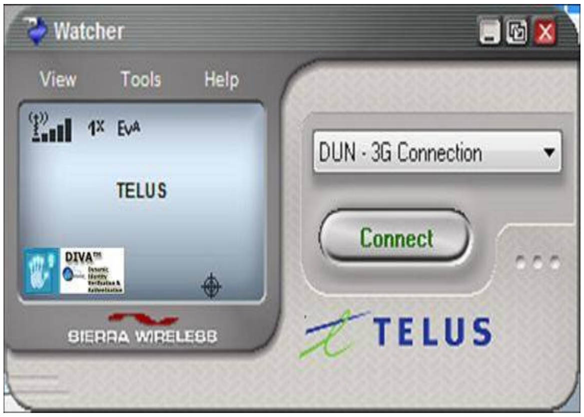
**This is a one time, minimal effort with partners.**

This configuration allows any handheld device to exploit the security of Dynamic Identity Verification and Authentication and move in and out of any network the device is allowed to access.

The issues this paradigm addresses are:

- It prevents a hacker from bypassing our protocol to connect to a cellular network

- It makes the secure mobile device mobile: Aircards and cell phones can move in and out of participating networks as the device travels



This configuration requires the **ONE-TIME** integration of DIVA into the device executable.

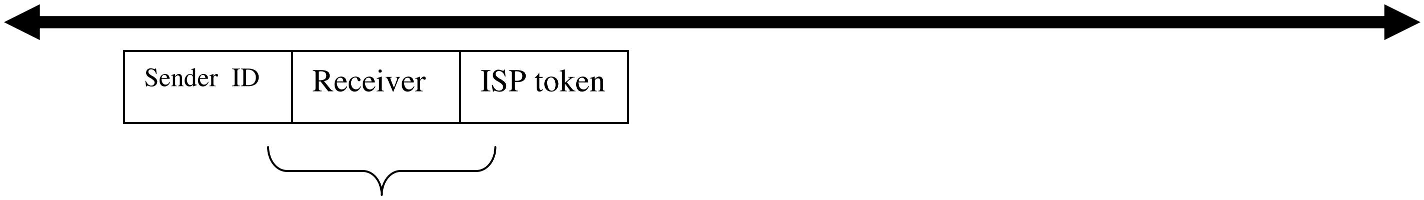
A software development engineer would **spend a small amount of time:**

1. They identify the point in the device executable (i.e. Watcher.exe) where to insert DIVA in the login procedure.
2. The engineer tests the DIVA code for viruses, integrity etc.
3. The engineer drops DIVA into this source code, compiles this executable, and we are done!
4. When this Identity Management and authentication service is performed by entities, this executable is integrated into firmware devices providing securen network access and IdM. This is a third party authentication service that can be provided companies or the government for national identity management systems.
5. This separate executable could be included in the burn list during manufacturing at NO EXTRA COST and is available for clients to activate in order to subscribe to secure services.
6. Third party authentication over cellular networks does not appreciably increase the system overhead when used to encapsulate secure network access and use. It is very low overhead.

# 7. ADDENDUM 4 – SPAM BUSTING KEYMAIL

## Identity management applied to keyMail e.g.

Balance of key used for dynamic authentication.



Fixed service token Unique Identifiers

In a dynamic tiered network, each level can continuously request authentication. In implementation, secure keyMail services request continuous authentication for access. This authentication can be implemented at each of the ISP, service, and consumer layers transparently.

The tiered, static addressing would include the unique identifier of the sender, the unique identifier of the receiver, the token identifying the ISP service provider, and the token identifying the keyMail service.

Each level demands dynamic identification. This would require a spammer to capture and store and use the keys and dynamic offsets for each and every email. This is infeasible.