



April 10, 2010
Andre Brisson
Stephen Boren



Harmonizing identity management, privacy and security in the cloud and in the grid: dynamic distributed key infrastructures and dynamic identity verification and authentication



International Telecommunications Union Work Group 27 – Cloud Computing
Palais des Nations , United Nations , Geneva Switzerland

The primary technological conclusions of the first **US National Cyber Leap Year Summit in August 2009:**

“Technologies now exist to express **scalable symmetric key authenticated encryption systems** where **no single trusted third party knows the final key.**”

“Robust cryptographic authentication would change the game by employing cryptographic methods which enable **secure authentication without transmitting the raw credentials for validation.**”

National Cyber Leap Year Summit 2009
August 17-19, 2009

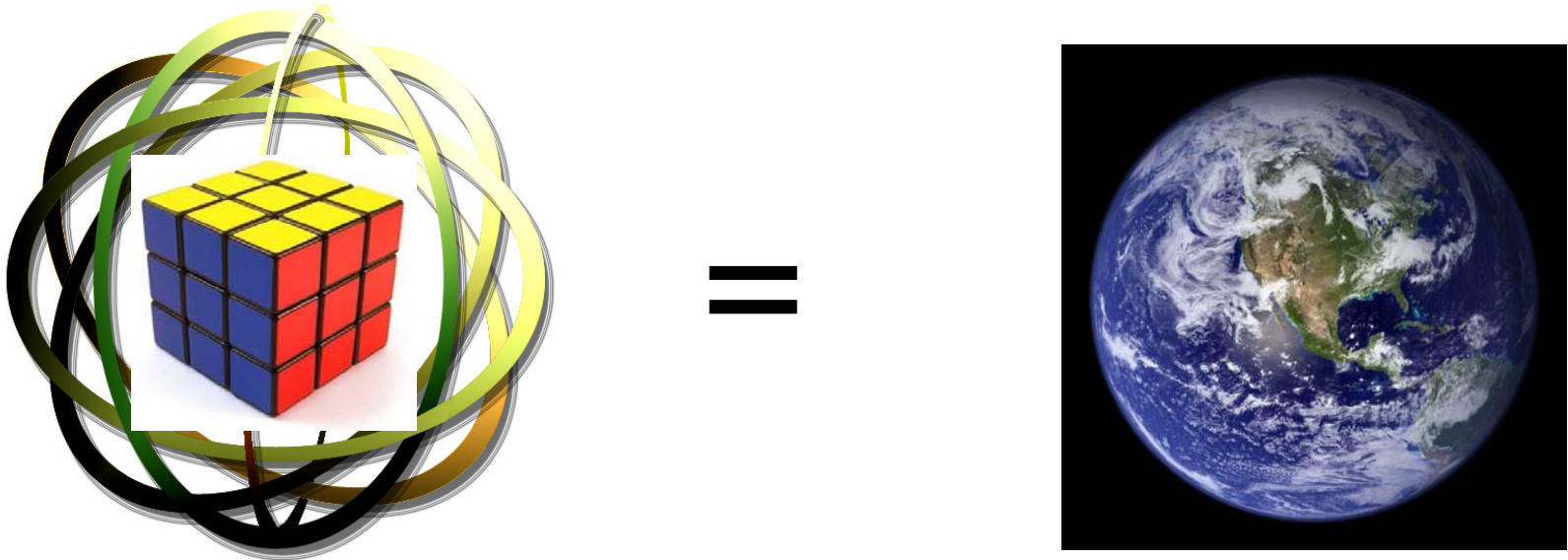


Presentation

Extraordinary science enables extraordinary security.

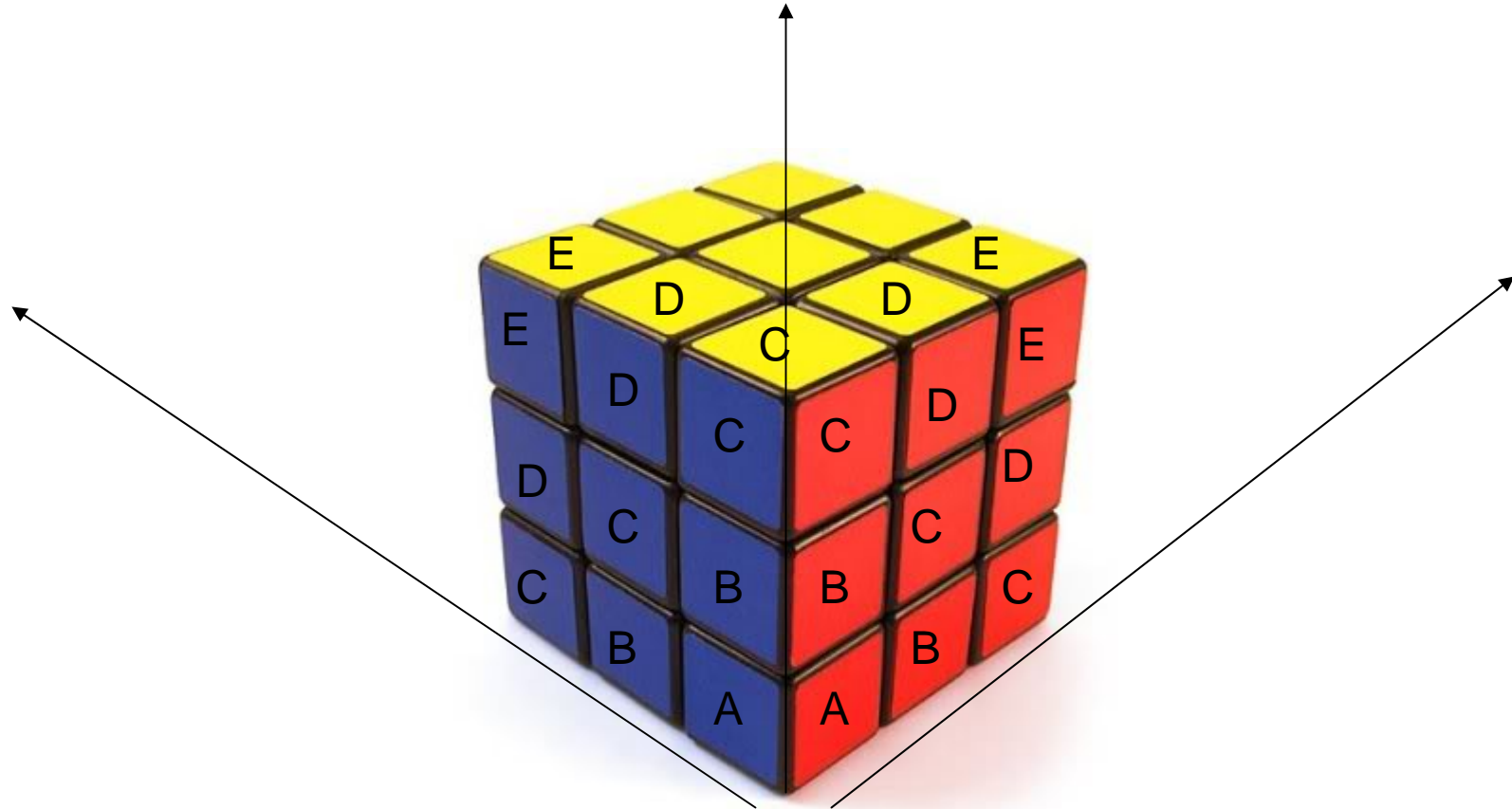
How would we create and express a scalable symmetric key authenticated encryption system? How can we make it act like a one-time pad for perfect security? How will we implement it?

First we need a cipher.



Spin a Rubik cube fast enough and it looks like a sphere. It looks like our world.

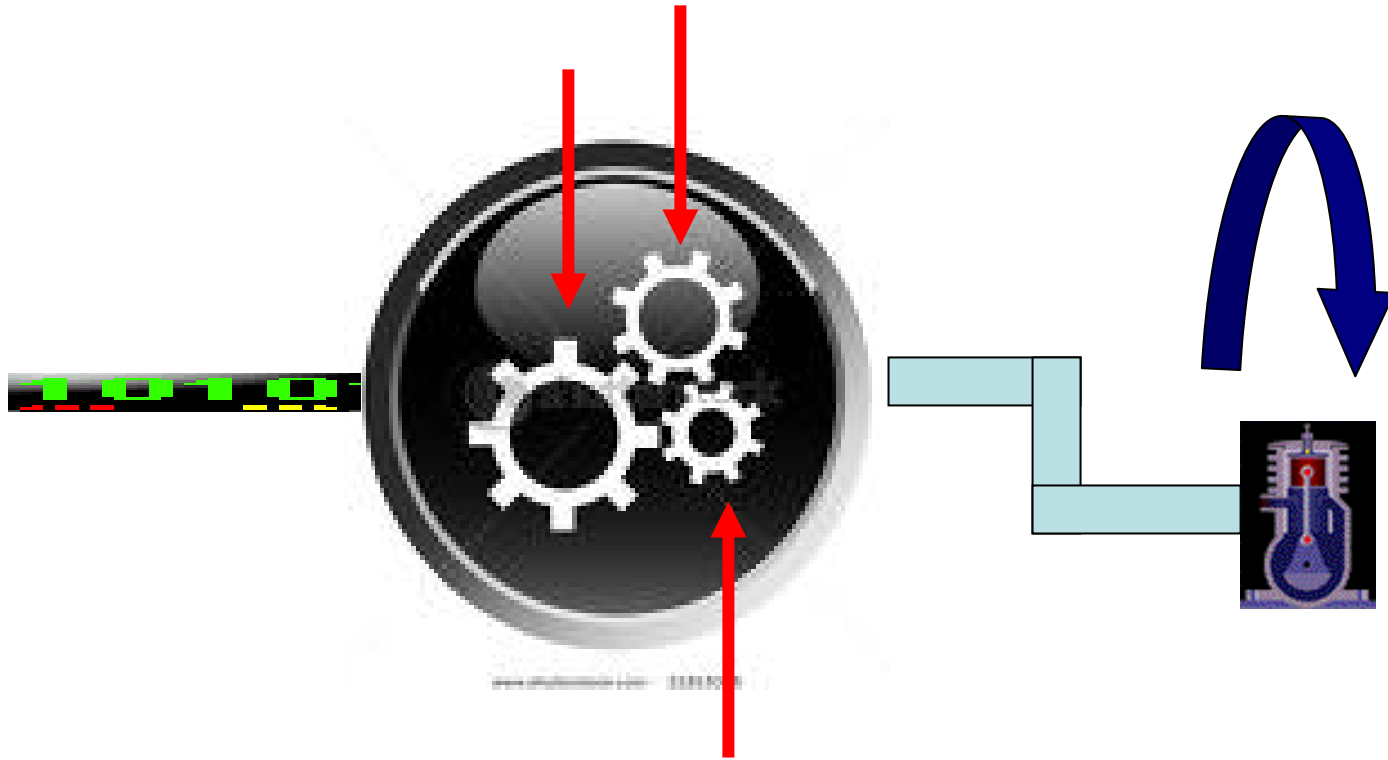
Stop the Rubik cube and we have the construct for a three dimensional cipher.



In computers we represent the three axis/dimensions hierarchically as subkeys:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

How would these subkeys interact with one another? What's so special?



If subkeys were gears of just 7, 5 and 3 units (teeth) in length, you would have to rotate the gears 105 times to return to the original position. Gears, like subkeys, dramatically effect the output (force) by orders of magnitude.

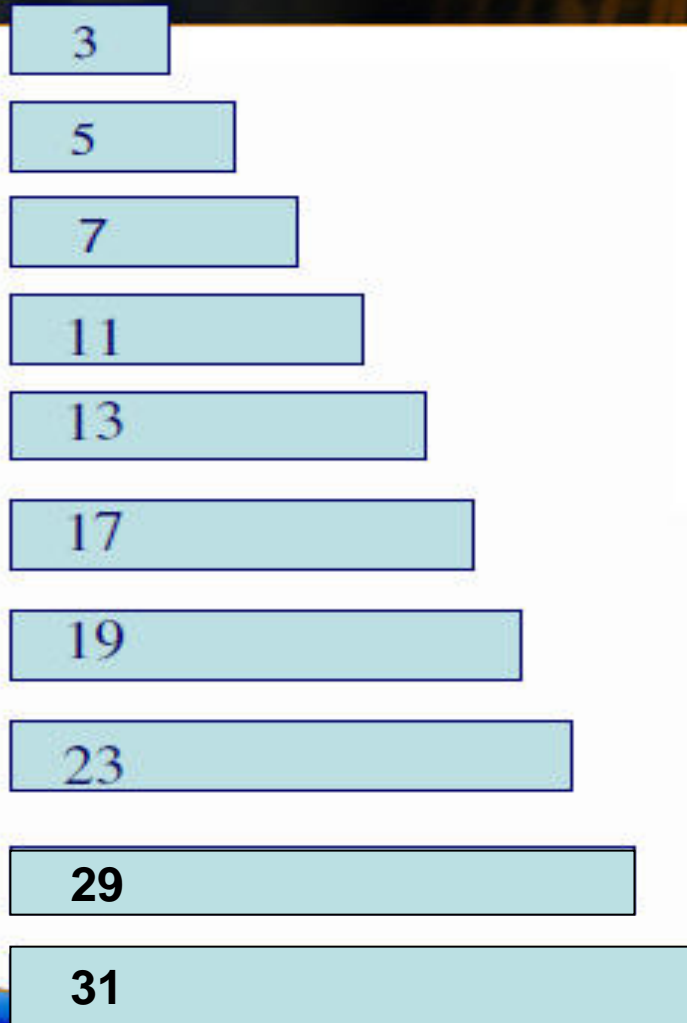
Exponential means that simply adding gears (subkeys/dimensions) increases strength and length of output by orders of magnitude. This construct will always be able to easily scale key strength on the fly. Every time a subkey is added its strength goes up by orders of magnitude with very little impact on key storage space. It is easy to digitally update firmware on network endpoints to fortify a network under threat.

Exploiting this characteristic makes it easy to create key streams larger than the number of atoms in the universe. A single key could easily and uniquely encrypt and log all the electronic communication ever transmitted. It will always stay ahead of the threat curve.

Why stop at three dimensions? Make every “dimension” different prime number byte lengths i.e. 1,2,3,5,7,11.... The smallest ten dimension/hierarchical cipher that can be made this way would look like:

A quick look at the multiplicity

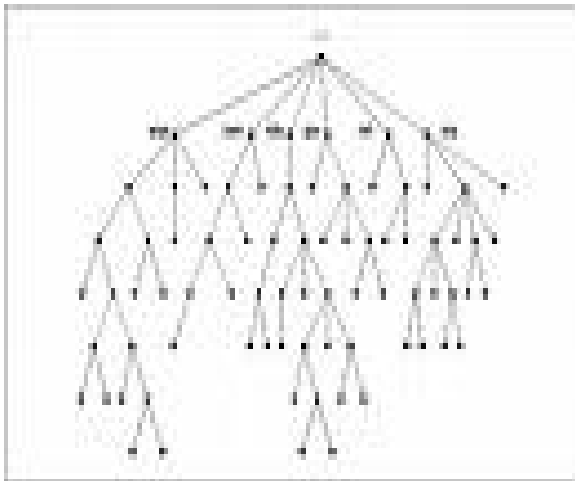
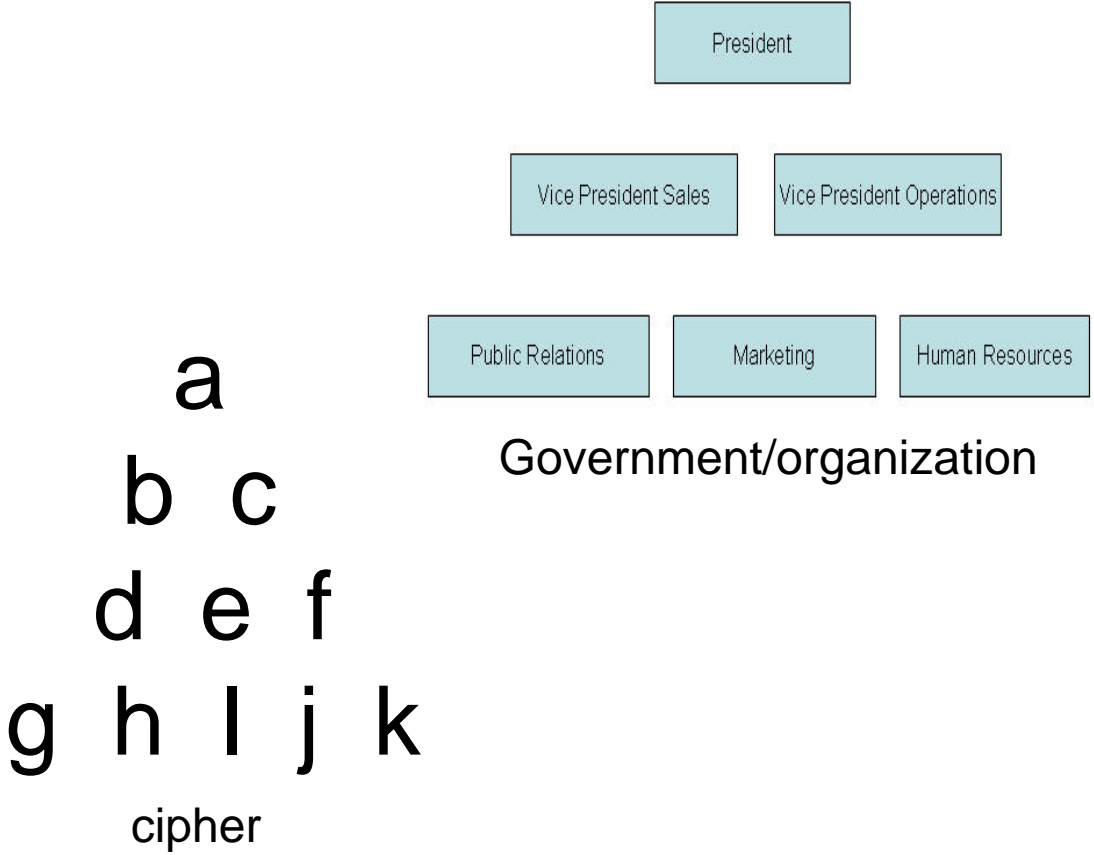
Every “Variable” is variable.



If we multiply the lengths of the subkeys, we see that using 10 subkeys and the smallest primes would result in a key 110,280,245,065 bytes long. We only need to transmit 158 bytes of internal key information (not including offsets) in order to recreate this key.

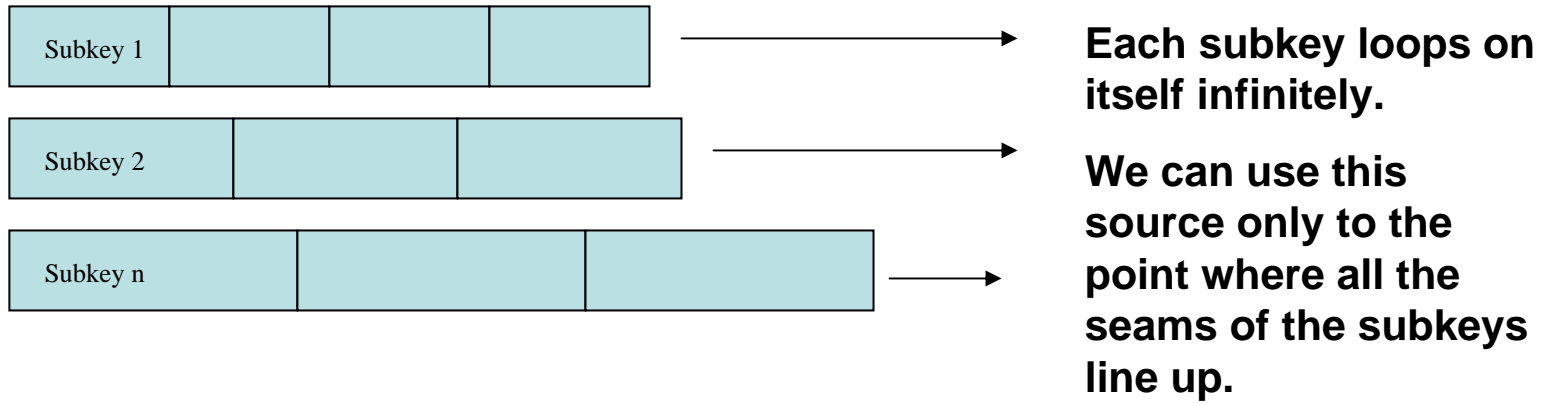
The bit strength of the cipher is calculated by adding the key stream byte lengths and multiplying by 8 bits per byte.

Re-align the subkeys and it is a tiered, hierarchical structure.



The structure of the subkeys looks like the structure of organizations, governments and businesses. It looks like a programming tree structure.

Creating an infinite array

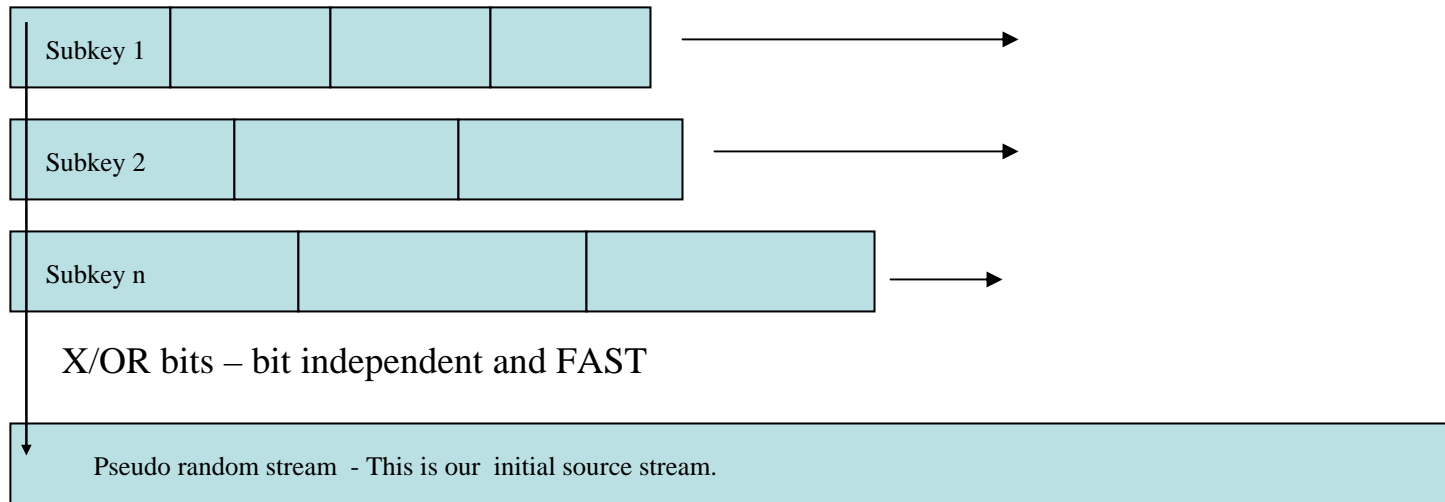


If the subkeys only operated horizontally, then each subkey could be viewed as a Line Feed Shift Register. LFSRs have linearity characteristics that need to be addressed, because “untreated” they can be susceptible to algebraic attacks.

However, this is well known and easily addressed. ATM’s use LFSRs and they are delinearized to protect against attacks by using readily available Invertible Non-Linear Function (INLF) utilities.

Note: the subkey lengths are filled with random data.

source stream – deterministic random number generation



Each bit of each subkey is X OR'd with the corresponding bit of the next subkey in a vertical fashion. Several things occur:

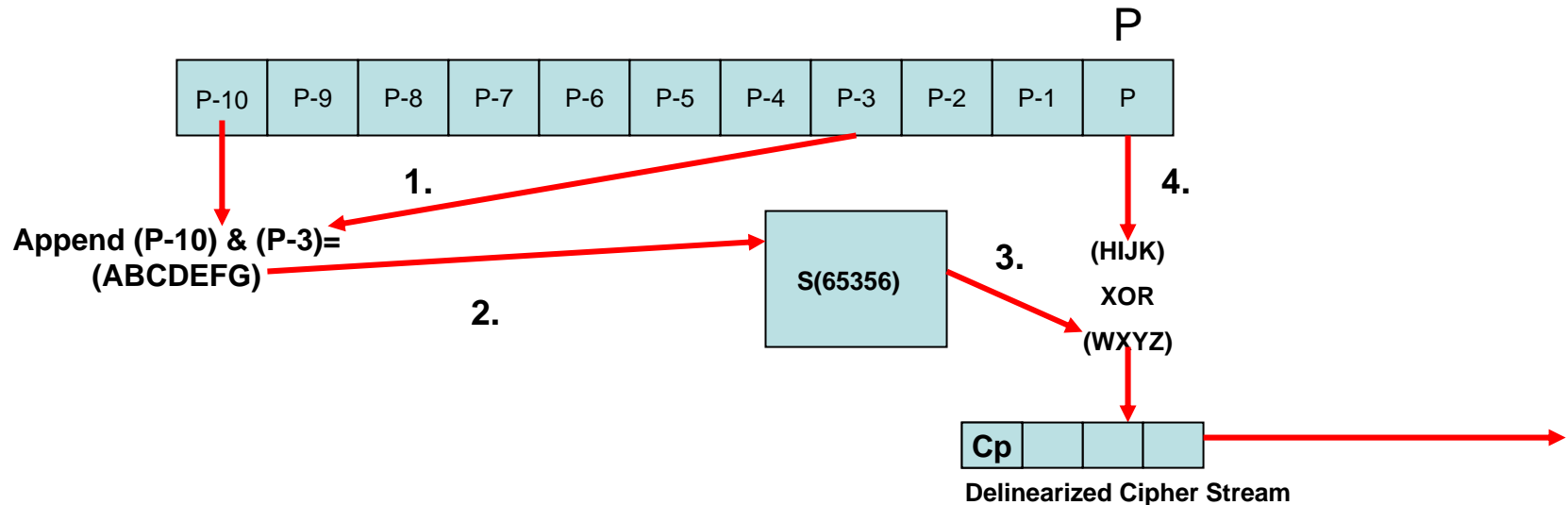
The resulting source stream is bit independent which means that any bits in the stream are not affected by those before them or after them.

We are able to use the XOR function which is the fastest function available on a computer. The entropy, or randomness, increases as you add subkeys.

The resulting source stream is highly random. However, the resulting source stream still retains internal linearity characteristics that we want to remove.

Delinearize source stream using [S65,536] and multi-byte draw one way function

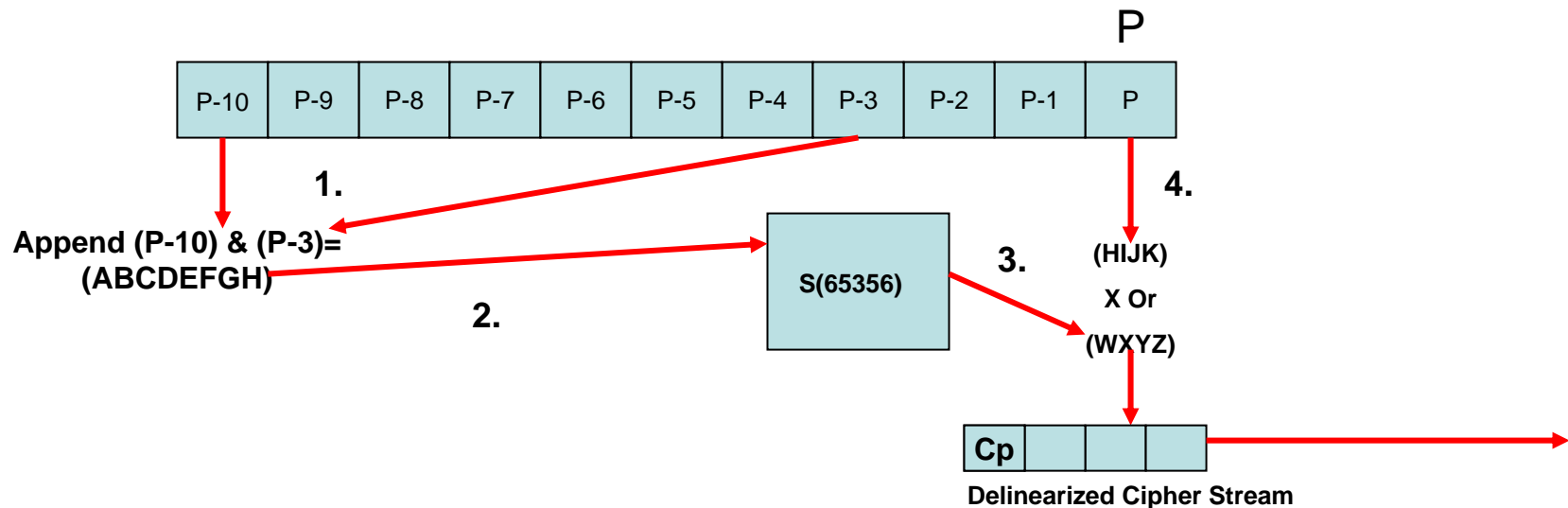
- Each box represents one byte
- P is the byte addressed by our offset point (the first byte in this example)
- The address P-3 is a co-prime distance of three bytes away from P
- The address P-10 is an additional co-prime distance of seven bytes away from P-3



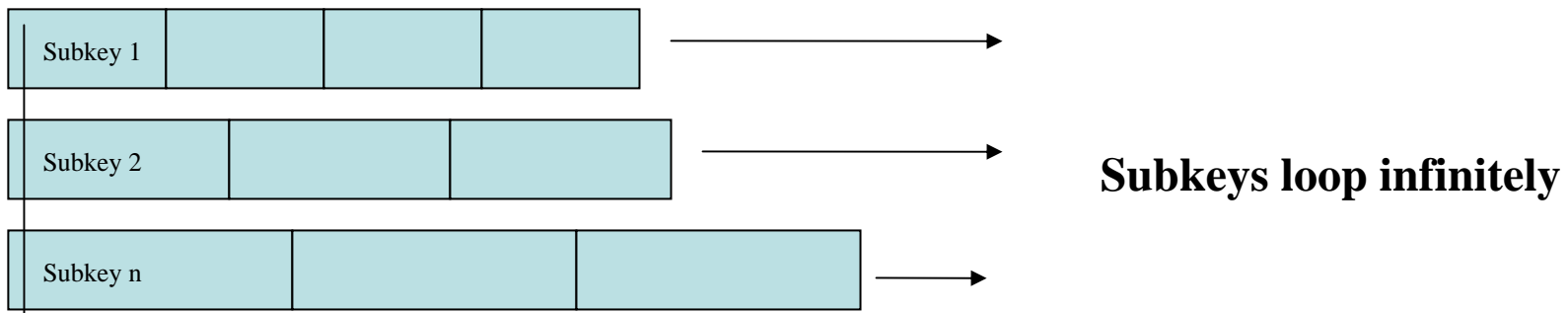
Note: The author of <http://eprint.iacr.org/2003/250> has been recognized on page 8 of the revision <http://eprint.iacr.org/2003/249>.

Delinearization (Cont'd)

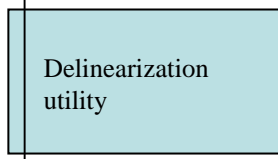
1. Reaching backwards on the pseudo-random stream, grab the addresses for the 2 bytes represented by $P-10$ and $P-3$. Note that both these values are co-prime distances away from P . The value for $P-10$ is ABCD and the value for $P-3$ is EFGH. Append the 2 byte addresses together, with $P-10$ being the higher order bit values, to create a 16 bit value ABCDEFGH.
2. Push this value into the $S(65356)$.
3. One byte emerges from the $S(65356)$. Note: 2 bytes enter-1byte exits-one way function
4. XOR the emerged byte with the bit value of the current byte P .
5. This becomes the first completely delinearized byte of our cipher stream.



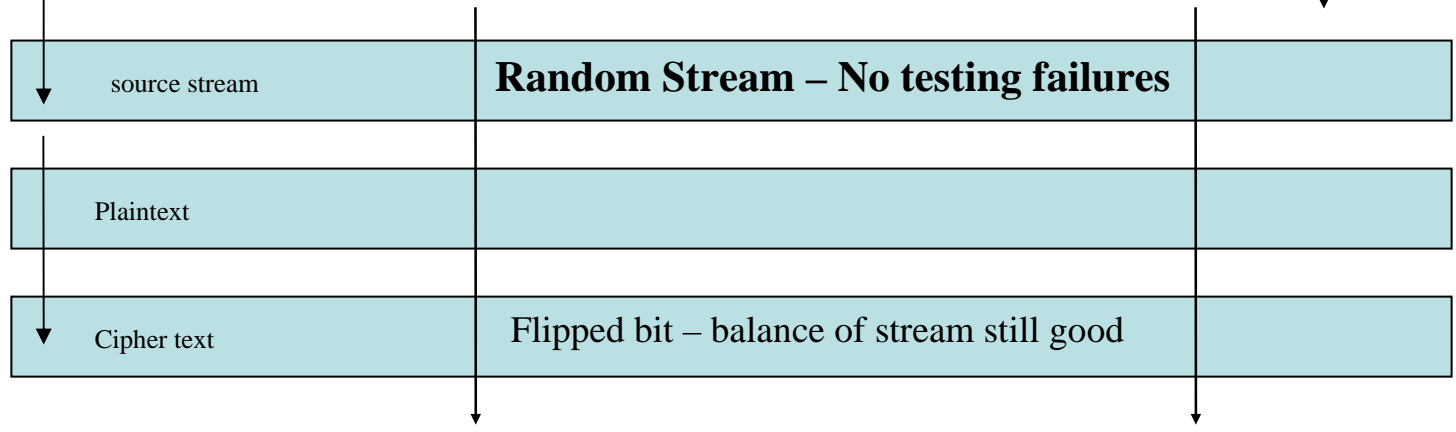
key construct for scalable symmetric key authenticated encryption



X/OR bits – bit independent and FAST



SuperKey is larger than the data.



Bit independent “deterministic random number generator” Carlisle Adams. Ph.D., P.Eng

- Run keystream in channels to increase speed
- Bit-for-bit encryption and order one processing keeps the data from bloating
- Jump anywhere in keystream - no re-framing or starting over because of flipped bits
- Real-time decryption (first responders)
- Allows keys to be parsed so that it possible that no single party has a complete IdM key
- Since all operations after key load are order 1 operations, it is Side Channel Attack resistant because it is not possible to correlate data from the physical manifestations of computer processes and digital output in an effort to learn anything discernable.

Order 1 operations can never lag in efficiency to increasing processing speeds because it exploits top hardware speeds. It will always be **quantum computing secure** because speed increases allow these key sizes and strengths to increase by the same order of magnitude.

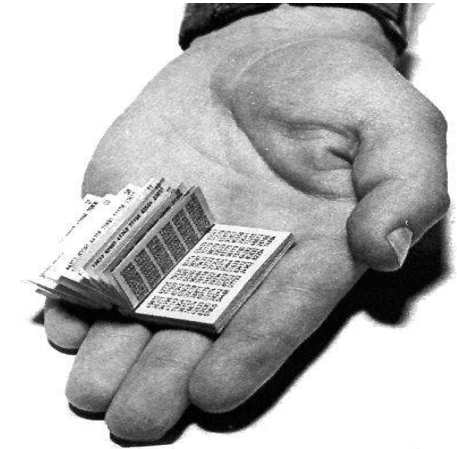
Note: It is the only example of a source [testing as perfectly random](#) and not pseudo-random against the NIST test suite. It is orders of magnitude more random than radioactive decay.

Bio reference: [Carlisle Adams](#) is the inventor of CAST and he coined the phrase.

These *scalable, authenticated symmetric keys* lead to dynamic identity verification and authentication which acts like a one-time pad.

They are also “useful to encrypt never-ending streams of communications traffic.”

Dr. Issa Traore, Michael Yanguo Liu, University of Victoria, February 2003



A one-time pad is the only mathematically proven unbreakable key or encryption technology. There are only three characteristics:

- **key is longer than the data encrypted or logged**
- **key segment or token is only used once**
- **key is random**

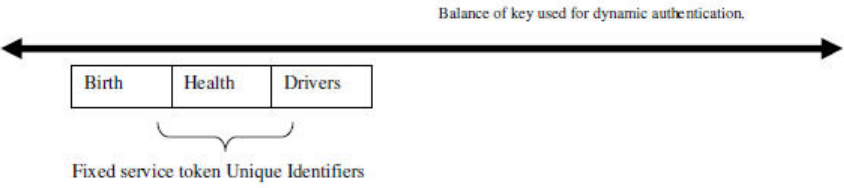
These scalable, authenticated symmetric keys allow us to embed identity into encryption in order to bind any credential to a person and to bind identity to the credential. Significantly it allows the binding to be accomplished in a manner that insures that no one party has the complete key.

One person-one citizen-one identity management key

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

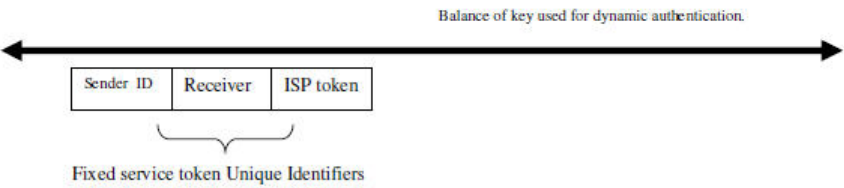
Identity management key

- > 10⁶⁰ bytes long key streams
- ~ 240,000 bit strength



Identity management applied to keyMail e.g.

SPAM Buster – see addendum



Bind credential to person

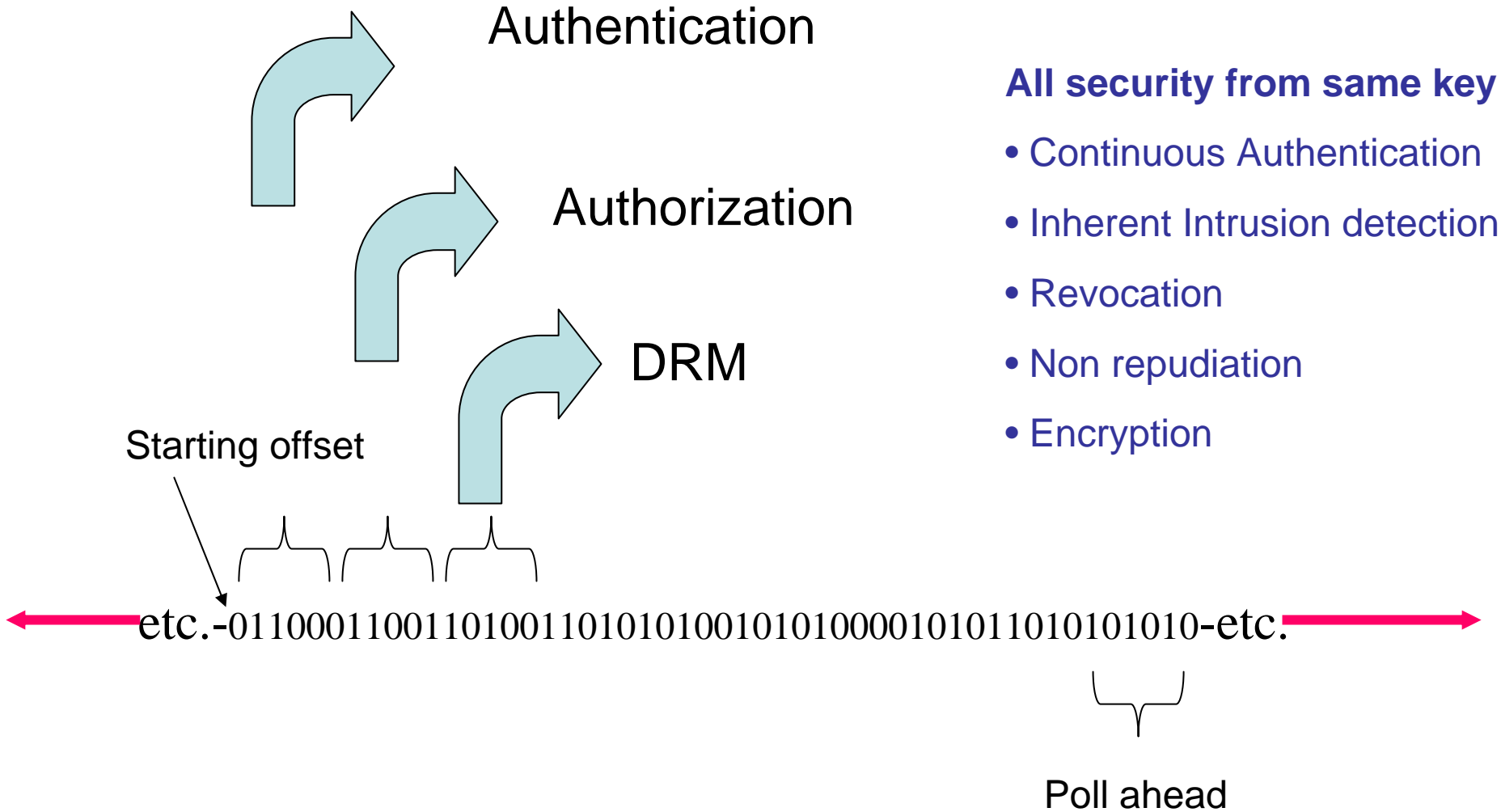
Technological magic

- Small data = enormous random key streams
- Secure electronic handshake delivers a user/device specific key
- Each end creates any identical random stream segments
- Use and compare sections of key stream which have never yet been created or transmitted




Bind the identity to credential

Different key segments also have different security uses



The keys can be configured to address need-to-know and chain-of-command authentication/authorization.

dynamic identity verification and authentication

Identity theft prevention, detection, and immediate revocation protocol

- Server continuously queries devices to ensure no invalid, stolen, or pirated keys are present.
 - This querying can be periodic, transactional or done at the packet level of communications.
 - DIVA can be integrated into PKI; DIVA can run in parallel or instead of PKI.
-

Process uses

- Key structures generated by the algorithm
- Initial offsets randomly generated by the system

It is 100% foolproof. Any unauthorized actions will be detected.

- Dynamic continuous authentication throughout network session
- Inherent intrusion detection
 - It is the time between a breach and a well defined response that determines the efficiency and integrity of any system and the amount of harm endured
- Authorizations and permissions
- Revocation or denial of network access
- DRM, third party non-repudiation, signatures

“Robust cryptographic authentication would change the game by employing cryptographic methods which enable **secure authentication without transmitting the raw credentials for validation.**”

How does dynamic identity verification and authentication work?

Both server and endpoint have a copy of the account identity management key. The server sends a request to the endpoint for an identification token of a specific length, in this case twenty-five bytes. It is not sending across either an offset or a key with this request.

Device state 1a

Last valid offset



22 1F CB FE FA 17 F2 8E A5 F0 8A E1 55 D6 DD 36 13 73 E2 9A 65 2F F6 EA 71 FE F7 D7 B8 28 5D 26 8B 93 64 16 03

Keystream is a minimum of 10^{60} bytes in length. We are continuously and dynamically comparing tokens to insure the correct identity of the network user. A token is an unused segment of key stream of an arbitrary length. It is random and has the equivalency of being encrypted – it cannot be guessed or broken and it is only used once.

The endpoint replies by sending a 25-byte token beginning at its last valid offset.

Device state 1b

Last valid offset plus token



22 1F CB FE FA 17 F2 8E A5 F0 8A E1 55 D6 DD 36 13 73 E2 9A 65 2F F6 EA 71 FE F7 D7 B8 28 5D 26 8B 93 64 16 03

length = 25 bytes This is arbitrary and scalable depending on security requirements.

Server authenticates user/device by comparing the received token to the token generated at the server for this account/person/device.

- **Server acknowledges the successful authentication by sending authorization**
- **Both server and endpoint update dynamic offset independently**

Device state 2

Last offset



22 1F CB FE FA 17 F2 8E A5 F0 8A E1 55 D6 DD 36 13 73 E2 9A 65 2F F6 EA 71 FE F7 D7 B8 28 5D 26 8B 93 64 16 03

length = 25 bytes

This is arbitrary and scalable depending on security requirements.

New offset = last offset + token + 1



The system is synchronized for the next continuous authentication query.

The account is automatically locked if the comparison of tokens fails. This would happen if someone has copied a key and the offsets are not synchronous.

100% Accuracy - Only two DIVA outcomes

Someone tries to steal a key.

1. The legitimate user logs back onto the network first.

DIVA - Secure Air Card Verification

home	options	feedback	logout
users	classes	keys	logs

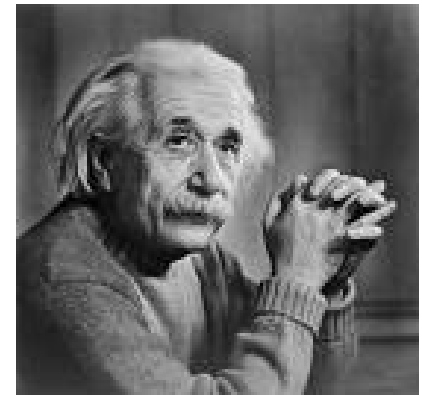
Edit User

User Information

Username:	<input type="text" value="Andre Brisson"/>
First Name:	<input type="text" value="Andre"/>
Last Name:	<input type="text" value="Brisson"/>
e-Mail:	<input type="text" value="abrisson@wnlabs.com"/>
Description:	<input type="text" value="Aircard User"/>
State:	<input type="button" value="Active"/> ▾

- The legitimate key and server offset dynamically updates with this use independently.
- The pirated or spoofed key (if possible) is no longer synchronized with the server and the legitimate key.
- The pirate will be detected if he makes a login attempt.
- The pirate can't access network. Stolen copy is useless.
- No theft has occurred.

This is the likely scenario the vast majority of the time.




2. The pirate logs onto the network first.

- The offset at the server and pirated key updates with this use.
- The legitimate key is no longer synchronized with the server.
- The next time the legitimate owner logs onto the secure network, the server recognizes that the offset is no longer synchronized because of the pirated key.
- The account is automatically locked.
- System Administrator and client know that their account has been accessed.
- *The logs know the exact duration of the event and the exact transactions within that time beginning at the last time the server and client were synchronized and ending at the point in time when the account was locked. The pirate IP address is known for law enforcement use.*

Simple customer service
Reactivate the account
Re-issue a new device

Gotcha Hacker!

DIVA - Secure Air Card Verification 

home options feedback logout
users classes keys logs tools e-mail

Manage Logs

From: 2008-9-26 To: 2008-9-26
Log Type: All None None Current
Username:

date & time	user	type	description
2008-9-26 16:43	Admin	Login	Source: 68.51.130.137 Platform: WinXP IE 7.0
2008-9-26 16:41	Admin	UserEnabled	Enabled user: (2) Andre Brisson
2008-9-26 16:41	Admin	UserDisabled	Disabled user: (2) Andre Brisson
2008-9-26 16:39	Admin	UserCreated	user: Andre Brisson name: Andre Brisson email: abrisson@wnlabs.com id: 2

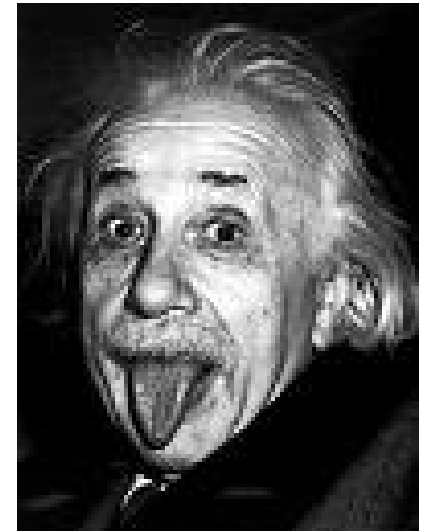
DIVA - Secure Air Card Verification

home options feedback logout
users classes keys logs

Edit User

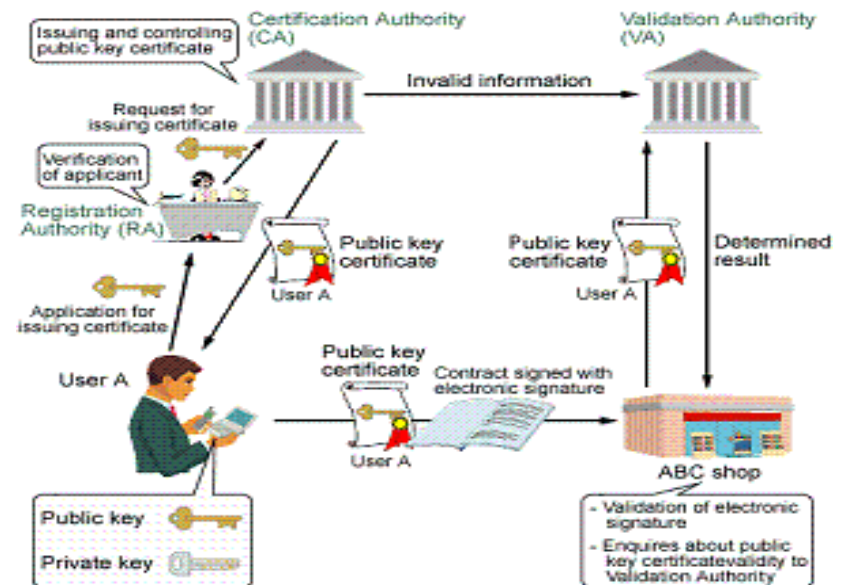
User Information

Username: Andre Brisson
First Name: Andre
Last Name: Brisson
e-Mail: abrisson@wnlabs.com
Description: Aircard User
State: Disabled



So what architecture or topology should be used to exploit these advancements?

Dynamic distributed key topologies is the logical approach because it addresses all the weaknesses of existing topologies, particularly public key infrastructures, without having to eliminate the investments in them made to date. Add a simple identity management protocol that can be called from any application at the point of network access. It is HIGH security and LOW cost.



- Public key systems are **always** vulnerable to man-in-the-middle attacks
- Public key systems are difficult to implement and are too expensive.

Man-in-the-Middle [MiM] Thwarted

The Man-in-the-Middle is the guy trying to steal your data or listen to your conversation.

Man-in-the-Middle Z wants X to think he is Y and wants Y to think he is X.

Man-in-the-Middle is free to capture encrypted traffic.

- **Distributed Key Infrastructure**

- **The private key is never transmitted (mfg) unsecured**
- **There is NO public key**
- **There is no available key material to create a break**

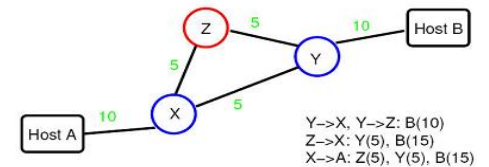
Routing Security

Steven M. Bellovin

<http://www.research.att.com/~smb>

Routing Security

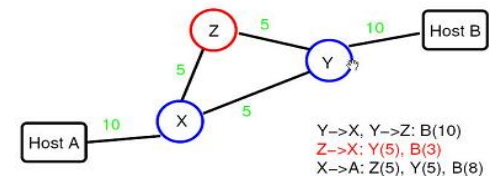
Normal Behavior



AT&T Steven M. Bellovin— June 13, 2003 ... 8

Routing Security

But Z Can Lie



Note that X is telling the truth as it knows it.

AT&T Steven M. Bellovin— June 13, 2003 ... 9

DDKI versus PKI for Securing Critical Infrastructures

- Grids for Systems Control and Data Acquisition (SCADA) do not want PKI
- The reality is that the asymmetric processes exasperate traffic and computational effort and are difficult to scale
- This overhead becomes an exponential problem affecting
 - Implementation overhead, complexity and cost
 - Scalability is dramatically simpler with DDKI



PKI COSTS



DDKI Costs

0

Outrageous Costs

Pain

Public key systems (asymmetric) by definition are ALWAYS vulnerable to Man-in-the-Middle attacks. Distributed, symmetric authentication can be used with PKI, integrated into PKI, or used in lieu of PKI to prevent this. An expert who sold his credentialing company to RSA wrote the following:

“Even if the [REDACTED] key was stolen, or were the corresponding key structure compromised along with knowledge of the [REDACTED] algorithm, on-going use of the key to gain unauthorized access to protected data would not be possible without the index value corresponding to the authorized history of use between legitimate correspondents.”

Critical Insights and Differentiators of [REDACTED]

Authenticated cryptosystem components

- key generation
- key distribution
- key security

Historic problems attendant with distributed crypto systems have been solved:

Key management of these systems explodes into an exponential head ache.

Historically the number of keys to manage is the square of the number of secure endpoints on a network. Now there is 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.

158 bytes will generate a random key stream over 100 billion bytes long.

Key distribution is a major problem for distributed key systems.

Distributed keys can securely generate and distribute more encrypted keys.

Technology must reflect society values and structure

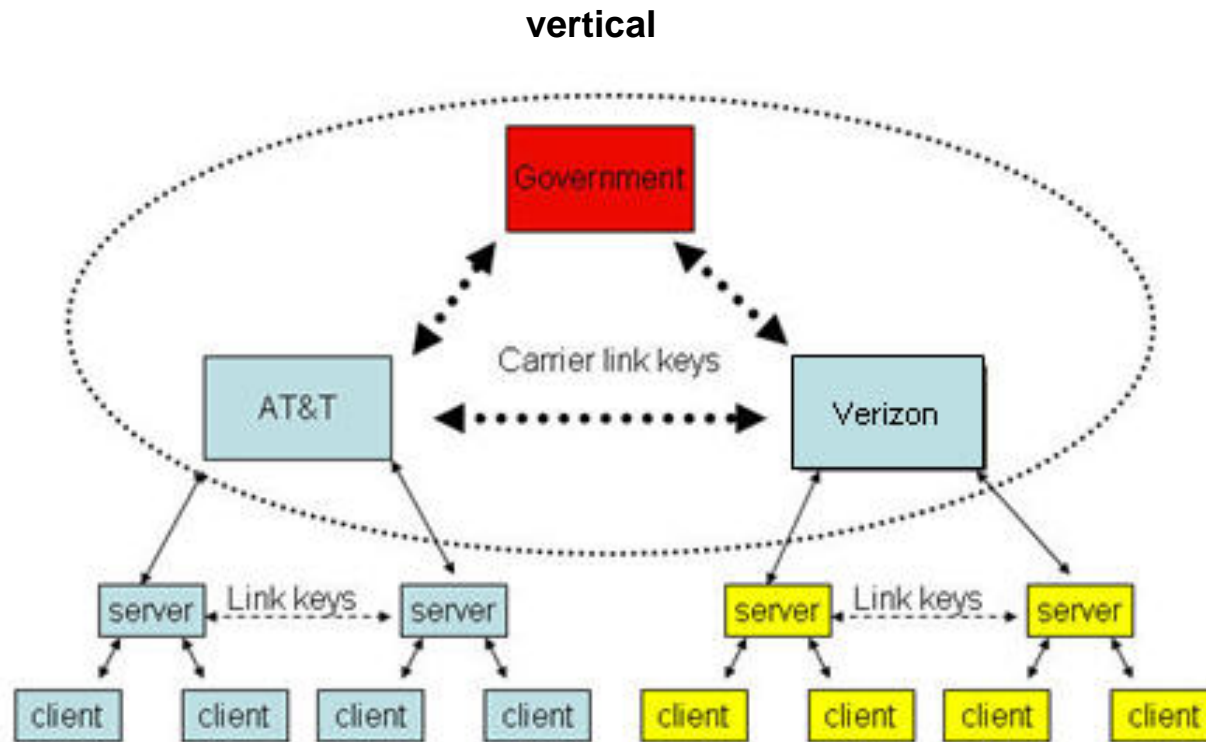


Dynamic distributed key infrastructures and dynamic identity verification and authentication should be a common choice of protocols because of its ability to augment the functional requirements at minimal cost for any kind of architecture.

Complete identity can be aggregated at a central location like a non-governmental organization trusted third party that brings together the stakeholders from public-private partnerships i.e. government, law enforcement, industry, and watch groups such as an international or national body comprised of privacy and security experts from all articulated stakeholders.

Complete identity can be parsed and federated horizontally between different stakeholders within government to create checks and balances that reflect particular societies. No one entity/department would have the complete identity of an individual/entity/device and act on a complete identity without transparency to other sectors of the government, i.e.

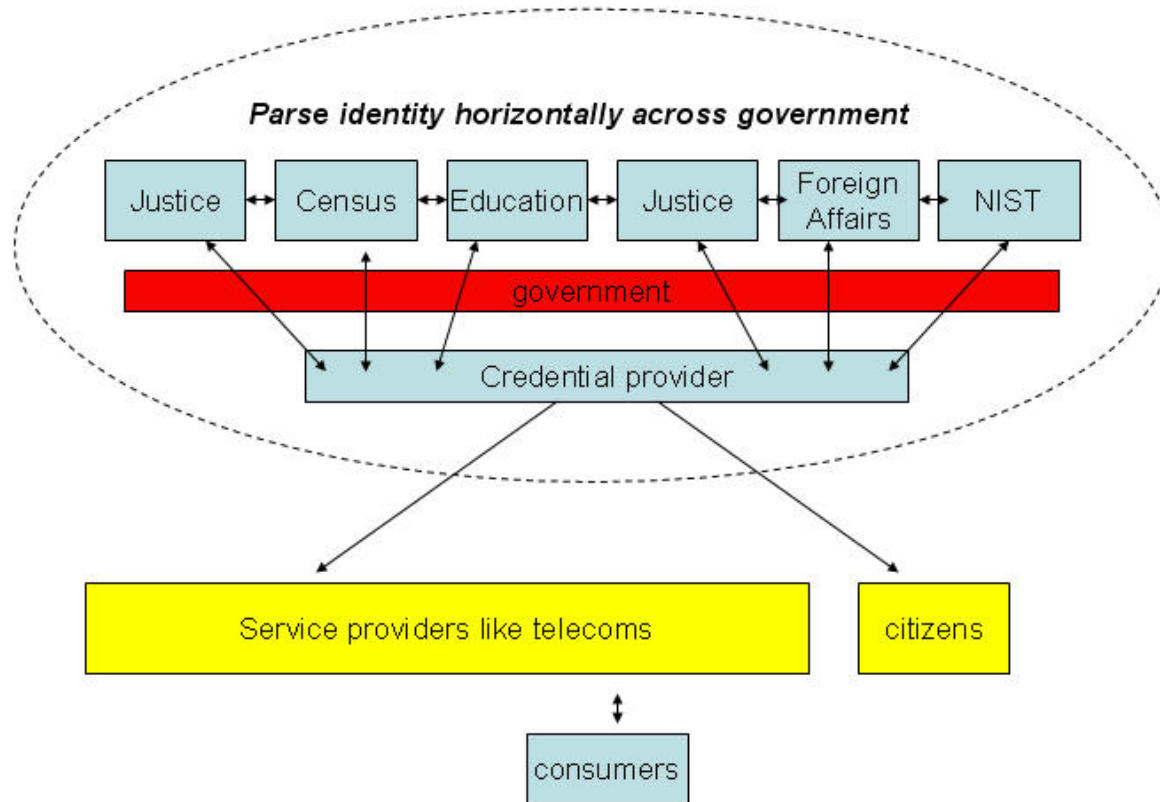
Deploy it in dynamic, distributed, tiered topologies that support public-private partnerships.



The government issues all citizens a unique identity management key. A single identity would allow consumer/citizens to access all services with unique key segments without ever exhausting the key.

The government also issues master keys to Tier 1 communication providers. These master keys in turn can be used by the carriers and communications providers to issue an unlimited number of keys/identities to access non-government business services.

horizontal

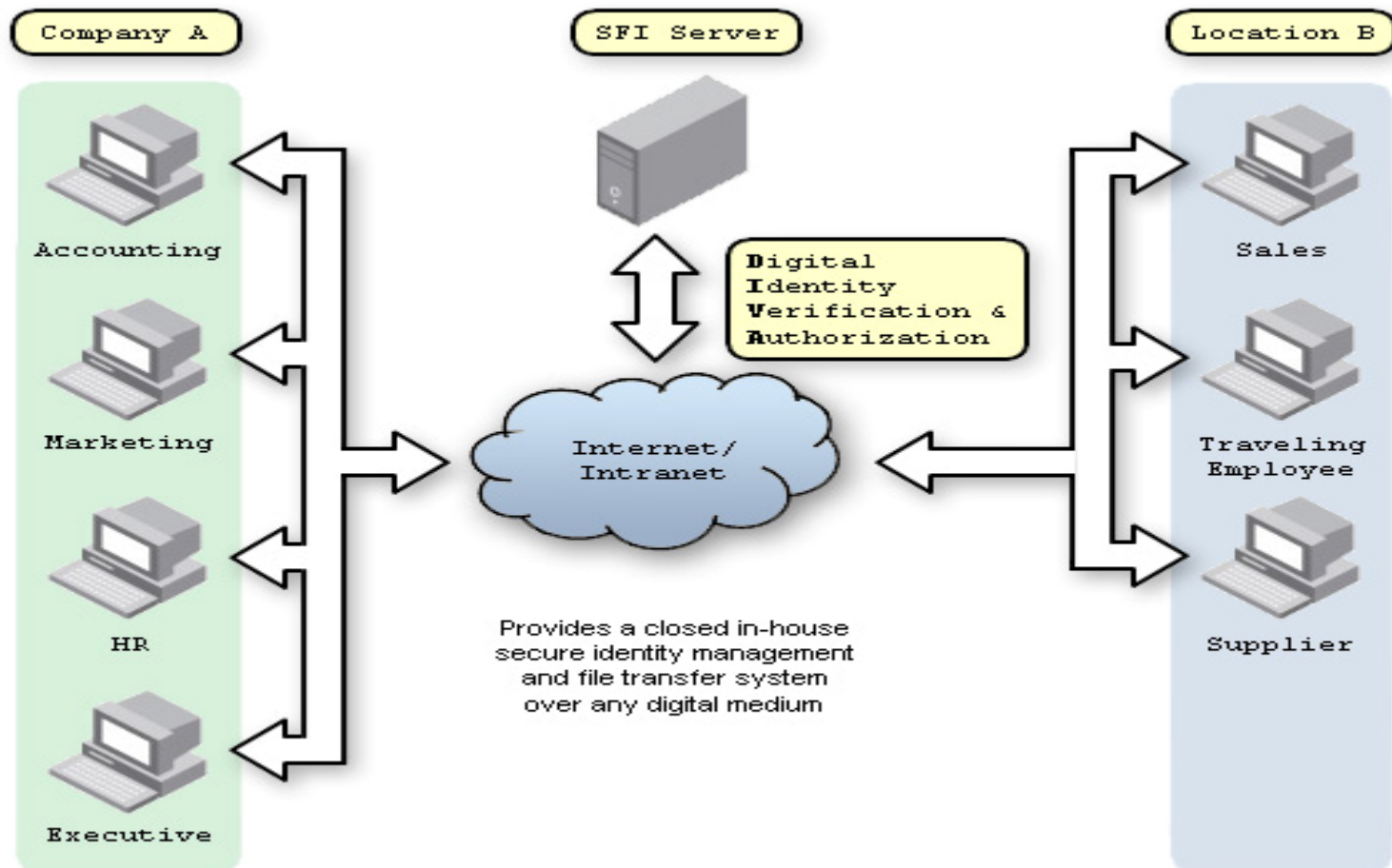


Legend

- **Department of Census:** responsible for issuing identity
- **Department of Homeland Security:** integrates law enforcement and military
- **Privacy Commissioner:** creates transparency
- **Department of Justice:** legally responsible for enforcing legislation
- **Department of Education:** building the capacity for a digital nation
- **Department of Foreign Affairs:** bring likeminded nations together
- **Standards and Technology:** build the architect of the future and provide technical oversight

Dynamic, distributed application example:

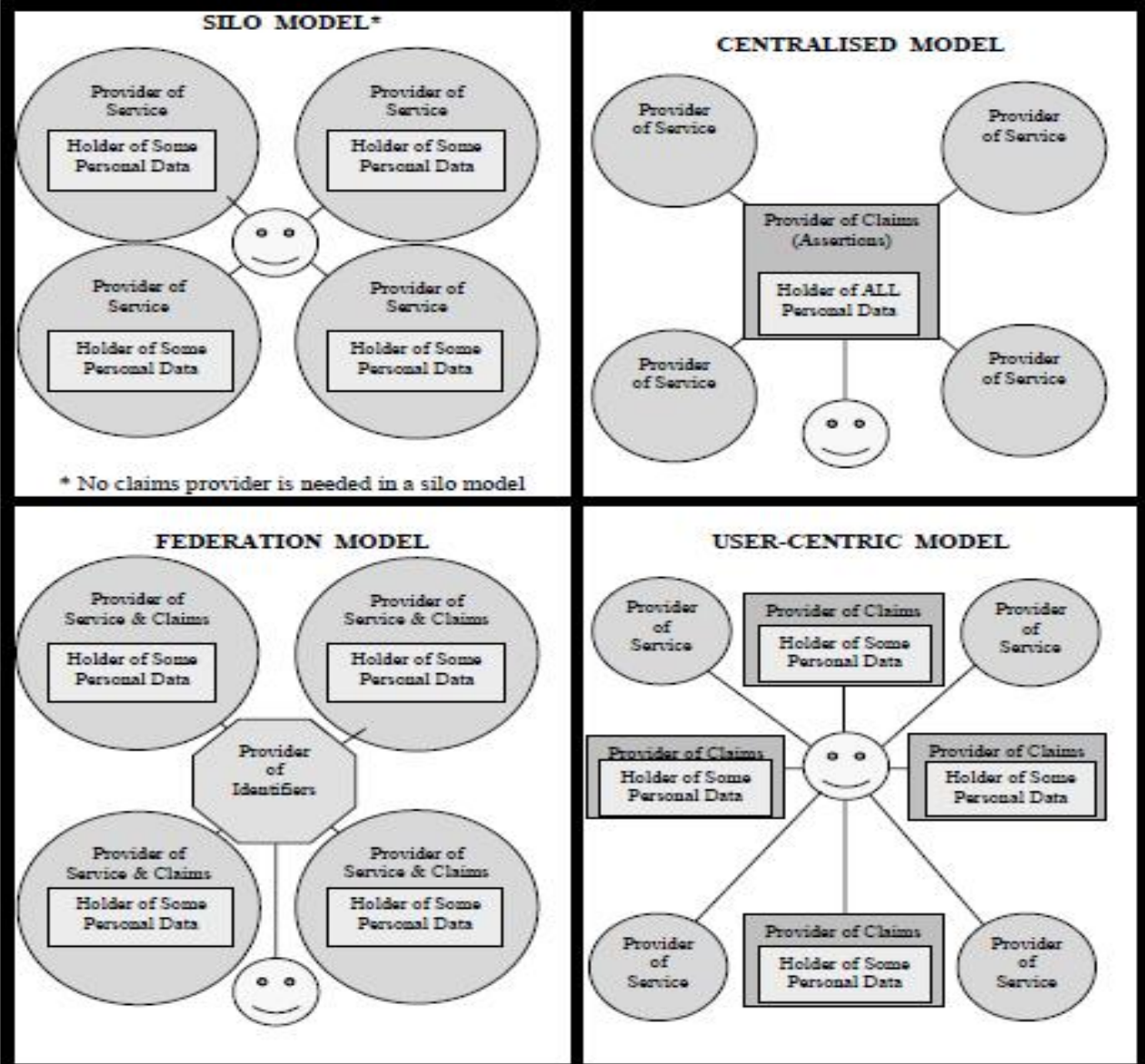
- point-to-point continuous authentication
- safe data flow and identity exchange is seamless
- any device or service that has access to the Internet can implement effective IdM protocols and mandates
- a person's private identity information is encrypted by them in their own unique key
- need-to-know and chain-of-command



dynamic distributed tiered architectures

- minimize the damage caused by disruption or corruption of data
- secure redundant systems
- compatible with data recovery schemes (RAID)
- automatically quarantines itself from breach, denial of service attacks, etc.
- prevent spam because of key based addressing
- consumer's/citizen's unique IdM keys log and index all activity
- automatic implementation and enforcement of rules and roles
- auditing is automatic and technologically self-monitoring.
- revocation is automatic because the inherent intrusion detection
- no single party has the entire identity management key
- information of potentially unlimited lifespan are secured with user specific encryption
- logging and automatic notification of illegal access
- single sign on because there is continuous authentication throughout network use
- facilitate anonymity and pseudonymity
- shared responsibility in public-private partnerships
- simplifies or eliminates key exchange

No single model is likely to fit all situations: dynamic identity verification and authentication's end-to-end authentication allows the protocol to be used between any numbers of endpoints in any combination of models or frameworks for interoperability.



Harmonizing Identity Management, Privacy and Security in the cloud and in the grid

Problem statement

There is a need for a new, flexible, cost-effective online authentication solution that meets a wide range of requirements.



- **dynamic identity verification and authentication allows choice of credential providers**
- **dynamic identity verification and authentication can easily be used with any model or framework: federated, silo, user-centric, centralized, public key or biometric systems**
- **dynamic identity verification and authentication easily scales to facilitate international commerce with international partners**

A common identity management framework can help nations achieve:

- **safe online transactions**
- **better use of resources**
- **growth overcoming barriers**
- **fostering innovation**
- **fostering secure collaboration**
- **fostering fair competition**
- **enhanced user convenience**
- **enhanced security and privacy**

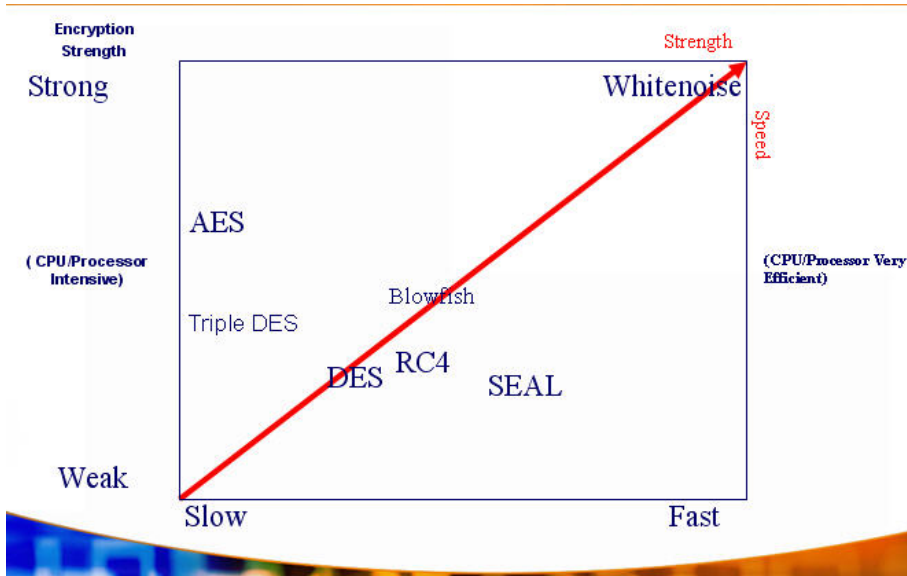


We must scale as populations and commerce reach compound growth rates.

goals

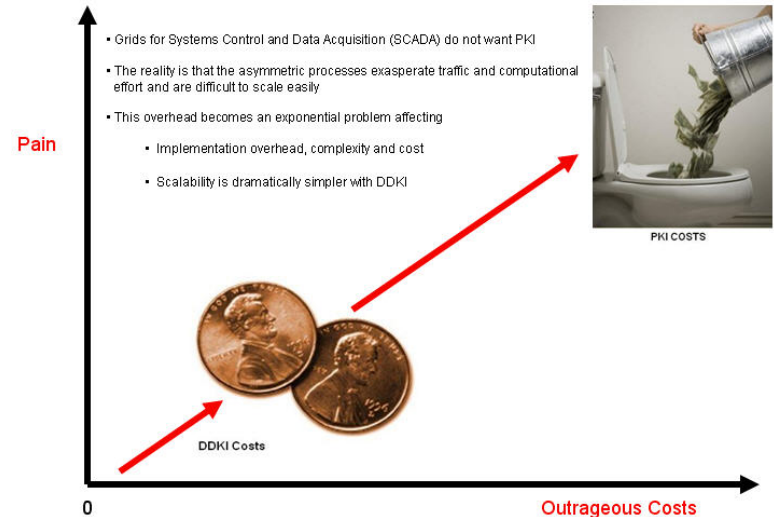
- minimize costs
- minimize business dislocation
- all stakeholders need to benefit
- eliminate vulnerabilities
- make it reflect societies
- enhanced secure IdM is more convenient and financially smart

Increase security



Minimize costs

DDKI versus PKI for Securing Critical Infrastructures



How

Add a simple new protocol as opposed to eliminating old technology



Security providers add the identity management protocol to create interoperability.

Dynamic distributed identity management technologies can run alongside existing systems, or be integrated into existing systems, or be used in lieu of them i.e. public key systems, biometric systems etc.

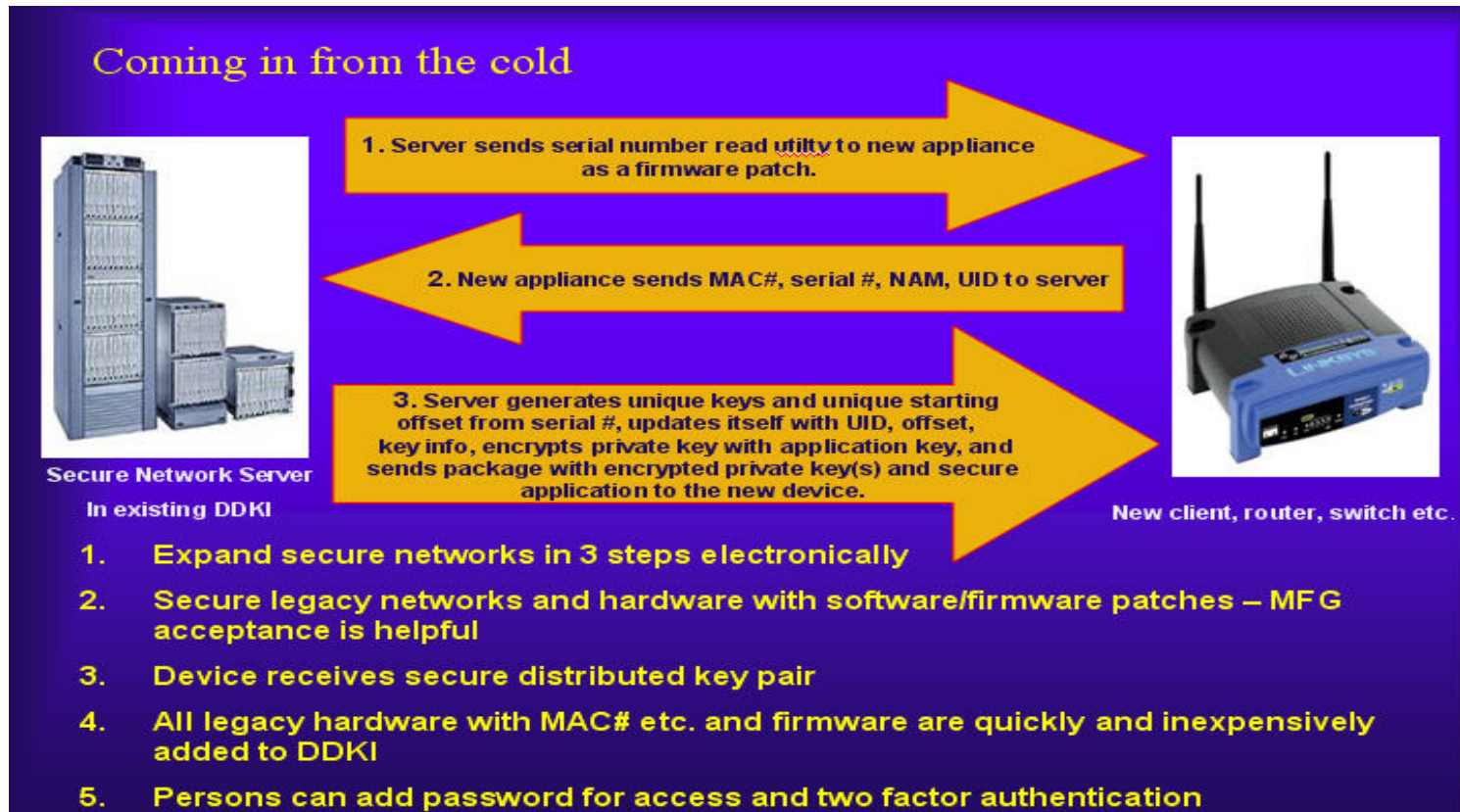
If an identity management solution is a required protocol that is **operating system specific and not application specific then it can easily be used in all contexts.**

Drive down cost

Deployment of ASIC chips for distributed identity credentials will create economies of scale and embed the capacity for identity management and key distribution at the point of manufacturing.



Devices and applications can download and install the IdM service onto their firmware. Devices can be upgraded securely, electronically and at minimum cost.



Why?

- decrease in breaches and cyber crime vulnerability
- fewer costs
- greater security with less effort
- lower security management and maintenance costs
- happy clients
- lower bandwidth and overhead
- easily monetize privacy and identity management
- allow any construct
- facilitate anonymity and pseudonymity
- shared responsibility between the public/private partnership
- policies can be implemented at any level



harmonized dynamic distributed systems will allow:

- excellent interoperability across organizations and borders
- users are empowered
- end-to-end authentication
- sufficient-for-the-task information stored in a secure manner
- consumer/citizens participate in securing their own identities
- consumer/citizens provide additional monitoring of their identity

As additional technical benefits it addresses current network weaknesses:



- **outdated and weak encryption algorithms**
- **no secure, two-way broadband communication protocol**
- **vulnerability to man-in-the-middle attacks**
- **vulnerability to side channel attacks**
- **vulnerability to spoofing and other kinds of illegal network access**
- **poor scalability of network topology**
- **no one-to-many communication capability**
- **no inherent intrusion detection**
- **no integrated identity management**
- **no continuous authentication**
- **no automatic revocation**
- **no simple key distribution and management**
- **poor interoperability with other network protocols**
- **high overhead and bandwidth**
- **no authentication of documents**
- **no device or domain-level authentication**
- **no authorization**
- **no electronic signatures**

Privacy is a right of citizens in democratic societies and a privilege in others. Privacy is determined by its rules and policies. Rules and policies balance security and privacy and reflect society specific values.

Education

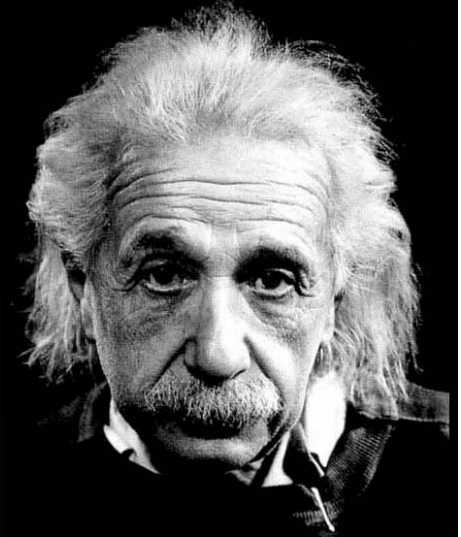


- **people can easily be taught about dynamic distributed key systems**
- **dynamic identity verification and authentication protocol is a simple either-or construct**
- **system administration training can be accomplished online in under two hours**
- **training for users takes minutes**

Consumers/Citizens

“Everything should be made as simple as possible, but not simpler.”

Albert Einstein



- A trustworthy and familiar interface
- Consumers assist with the management and oversight of their own information
- Consumers are unwilling to pay for IdM services at this time:

The onus for change then lies with service providers and governments to better educate citizens and provide secure services as a matter of best practices.

One simplifier is to create a dynamic identity verification and authentication tier that all different identity management systems can access and exploit. This will create one look for users and yet accommodate the architectural flexibility that the markets demand.

“...is an efficient and cost-effective algorithm for securing direct communications from point-to-point over different media. It is also ideal to be utilized to create a secure network layer for the Internet.”

Dr. Issa Traore, Michael Yanguo Liu, University of Victoria, February 2003

Identity and encryption cryptosystems



- greater than 250,000 bits in scalable strength
- embedded identity
- quantum computing secure
- exponential – can be fortified on the fly
- data can only be accessed by persons who have legitimate authority and purpose in the cloud or storage



The tipping point between peril and promise of the Internet is now in delicate balance.

The outcome has yet to be determined. Countries will either be properly positioned and leveraged or overwhelmed when compound growth and quantum computing takes over.

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**

Cryptanalysis

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

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

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



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

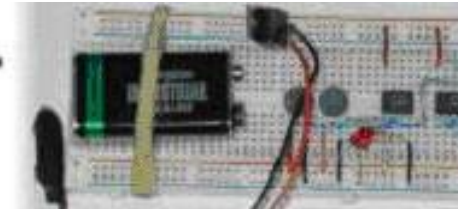
- Mathematical and correlation attacks
- Brute force attacks
- Side Channel attacks

brute force attacks

In [cryptography](#), a brute force attack is a [strategy](#) used to break the encryption of data. It involves traversing the [search space](#) of possible [keys](#) until the correct key is found.



**Electrical & Computer
Engineering**



[The key stream could not be broken by supercomputers at the University of Victoria](#). It didn't even have anticipated statistical randomness failures. It tested perfectly random against the NIST test suite. It could not be broken in a [security analysis by the University of California, Berkeley](#). It could not be broken in the [\\$100,000 Challenge](#). It is [patented as an OTP](#).

Since all operations after key load are order 1 operations, it is Side Channel Attack resistant because it is not possible to correlate data from the physical manifestations of computer processes and digital output in an effort to learn anything discernable.

Mathematical and correlation attacks

The keys are structural in nature so mathematical and correlation attacks do not work.

[Security Evaluation of Whitenoise™ - David Wagner \(PDF\)](#)

"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



Bio for reference

[David Wagner is co inventor with Bruce Schneier of Twofish in addressing the security issues of Blowfish.](#)

scalable symmetric key authenticated encryption attributes

Extremely Secure –

Keystream length exceeds the size of data to be sent, stored or logged; keys are built from a small amount of stored data; key segments are never re-used; key stream data is never transmitted in an unsecured state

Fast – 5 Clock Cycles per Byte (S/W) ; >2 Bytes / CC (H/W) done in FPGA – speed and strength are scalable

Error Tolerant - only damaged bits are affected - no reliance on preceding or following data – bit and data independent

Efficient - low processor requirements – Lower cost devices

Data type independent - multimedia support – voice data video – real time streaming, video surveillance

Manages linear offsets - strong identity & digital rights management dynamic identity verification and authentication

Receiver & sender synchronized keystream

Scaleable - small Footprint $\leq 300k$ – will run on 8 bit cpu

Why should we care about the critical infrastructures?

1 / 2 the people
who have lived
are alive!!!

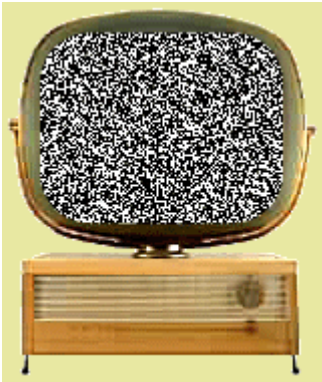
- Technical information doubles every 2 years.
- Communication explosion follows population explosions.
- Fiber optic strand carries 10 trillion bits/sec of data.

= 1900 CDs per second

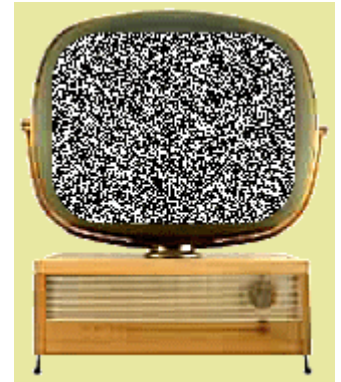
= 150 million phones calls per second simultaneously

- Volumes will double every 6 months for next 20 years.

Thank you



white noise is controlled static



[The Best of British Columbia Olympic 2010 Outreach](#)

Presentation by Andre Brisson and Stephen Boren, co founders of
Whitenoise Laboratories (Canada) Inc.
www.wnlabs.com