Dynamic Distributed Key Infrastructures (DDKI)

Dynamic Identity Verification and Authentication (DIVA)

(Interoperable, scalable software frameworks)

ETSI

DIVA
Dynamic Identity
Verification & Authentication

IFSEC
FUTURE OF SECURITY
COMPETITION

GLOBAL SECURITY
CHALLENGE

Certified Solutions
at&t

First let’s look at how dynamic identity verification and authentication [DIVA] key technologies work.

Then we will examine how DIVA naturally leads to fixing existing flaws in network security by extending its range through Dynamic Distributed Key Infrastructure frameworks.

How does DIVA 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.

Last valid offset

Device state 1a

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.

Last valid offset plus token

Device state 1b

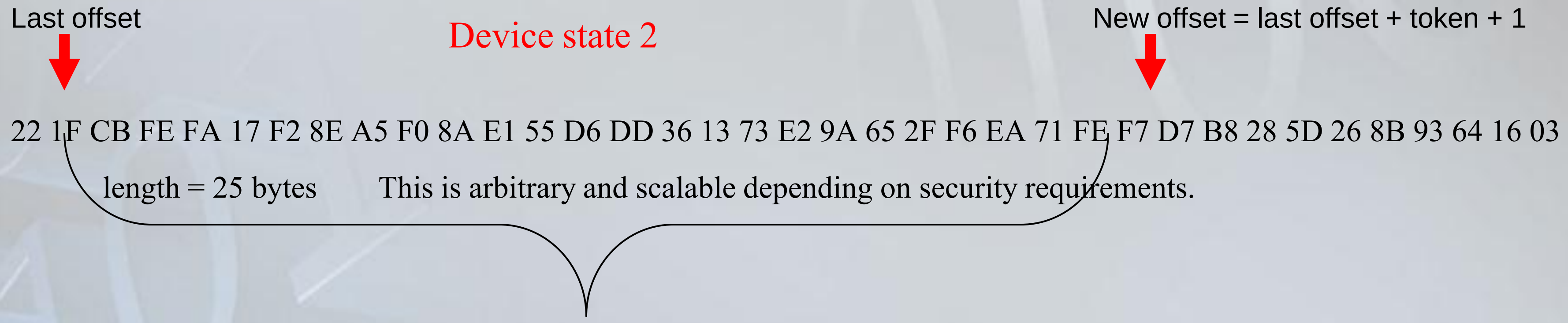
22 1F CB FE FA 17 F2 8E A5 F0 8A E1 55 D6 DD 36 13 73 E2 9A 65 2F F6 EA 71 FE F7 D7 B8 28 5D 26 8B 93 64 16 03

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

DIVA dynamic update of offset

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

- □ Server acknowledges by sending authorization
- □ Both server and endpoint update dynamic offset independently



Last offset

Device state 2

New offset = last offset + token + 1

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.

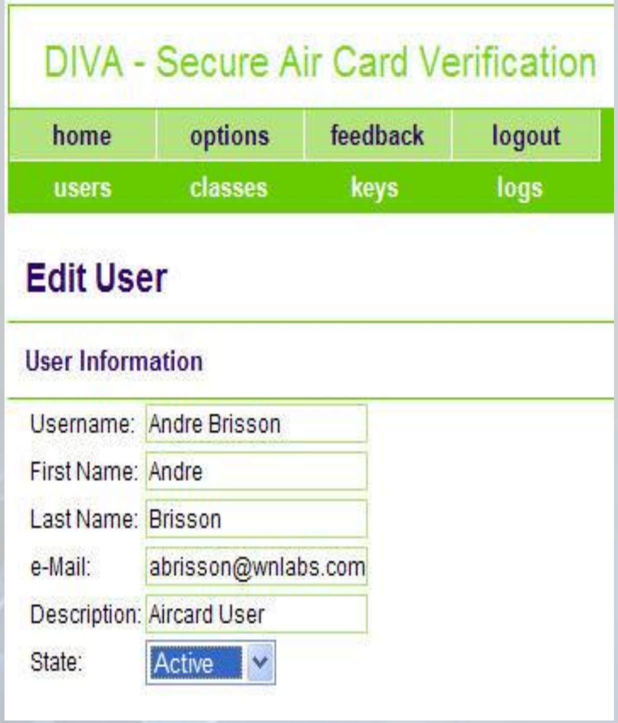
The system is synchronized for the next continuous authentication query.

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.



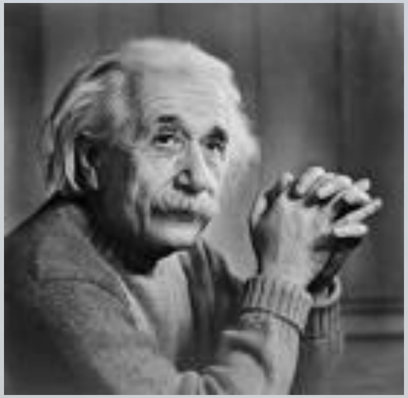
DIVA - Secure Air Card Verification

Edit User

User Information

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

- The legitimate key and server offset dynamically update 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.

Simple customer service

Reactivate the account

Re-issue a new device

- The offset at the server and pirated key update with this use.

- The legitimate key is no longer synchronized with the server.

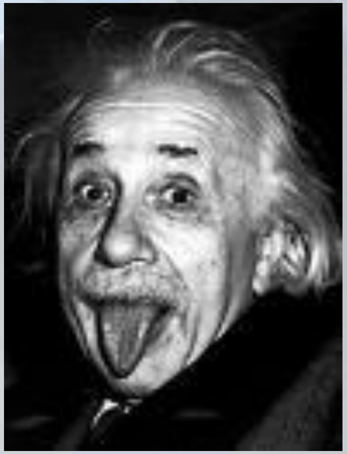
- The next time the legitimate owner logs onto the secure network, the server recognizes that the offset is no longer synchronized because of the pirated key.

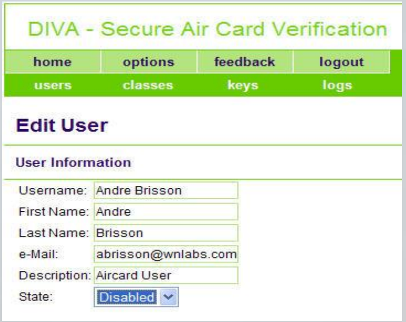
- The account is automatically locked.

- 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 I P address is known for law enforcement use.

Gotcha Hacker!





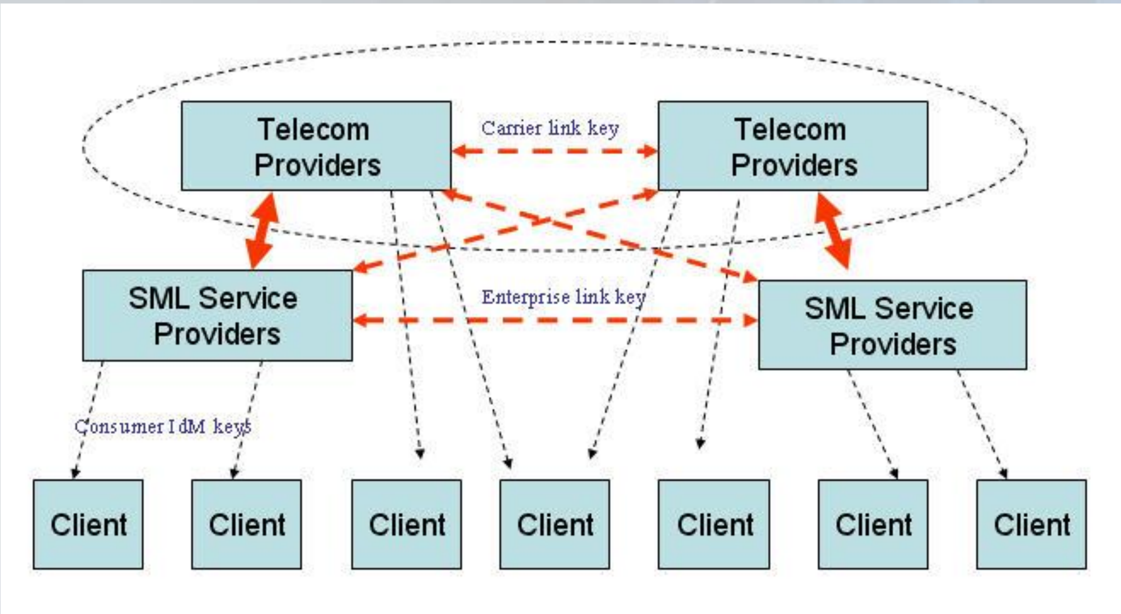
DIVA - Secure Air Card Verification

Edit User

User Information

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

Scenario for a secure communication framework topology



DDKI frameworks are tiered, hierarchical, secure, network-of- networks. Master Keys (which create an infinite number of unique Identity Management keys) can be distributed to telecommunication and service providers.

Master Keys can be distributed directly to telecommunication providers following regulatory protocols. Carriers create their own keys internally.

Carriers in turn can provide keys to service providers, enterprises and consumers (subkeys of the master key). Enterprises create keys internally for their own employees or clients. Link keys between carriers and between enterprises create a secure network-of-networks necessary for vast area communication architectures.

This tiered distribution approach facilitates secure networks while balancing privacy and legitimate law enforcement needs.

Problem defined by all international standards bodies

ETSI

There is an urgent need for large, dynamic, on-line authentication systems where there is only partial disclosure of credentials for distributed platforms and services (DAPS)

These are cyber security requirements necessary for all cyber contexts.

- □ identity management
- □ securing the internet and enterprise networks
- □ secure cloud computing/endpoint authenticated encryption
- □ secure critical infrastructures
- □ secure identity based telecommunications
- □ secure smart grids
- □ prevention of malwares and spam

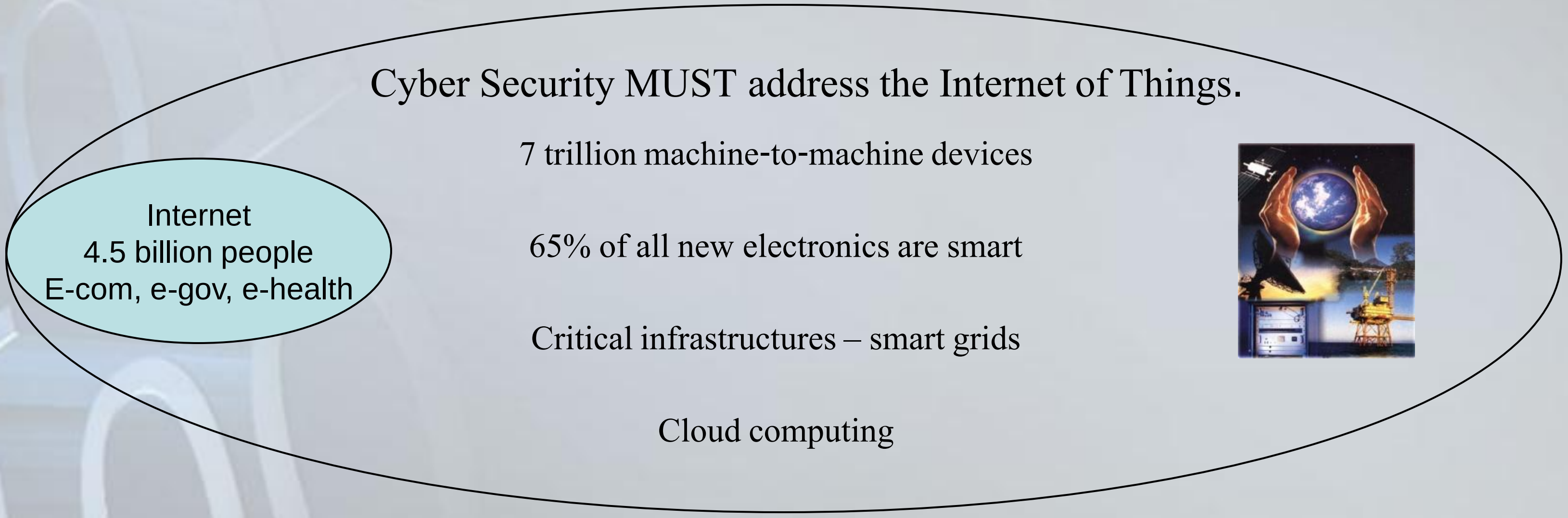
Market Universe for DIVA Cyber Security

The United Nations speaks of our growing reliance on the Internet of Things.

“Internet security is a branch of computer security specifically related to the Internet. Its objective is to establish rules and measures to use against attacks over the Internet.[1]” Wikipedia

□ Everything is integrated now.

□ Critical infrastructures rely on broadband and Internet because of cost and scalability.



Cyber Security MUST address the Internet of Things.

Internet
4.5 billion people
E-com, e-gov, e-health

7 trillion machine-to-machine devices

65% of all new electronics are smart

Critical infrastructures – smart grids

Cloud computing

Secure networks require only three things

It is not daunting to either fix or harmonize all network communications.

1. **All components of the network are identified by a unique key**
2. **All persons/devices are identified dynamically and continuously**
3. **All usage is logged**

Devices only require three things

For perfect identity management and security a device only needs

1. A little bit of storage space for keys

   158 bytes of key DNA creates a 100 billion byte keystream because of exponentialism

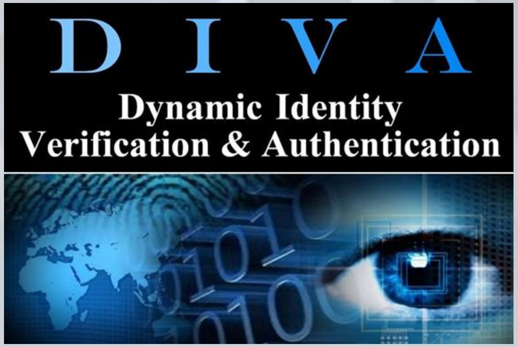
2. Write-back capacity to update dynamic offsets

3. An internet connection or connectivity

Complimentary technology

Dynamic identity verification and authentication [DIVA] is an identity-based, software protocol that can be used in any digital context and with any existing security processes and addresses all security requirements:

- □ dynamic and continuous authentication
- □ authorization
- □ revocation
- □ repudiation
- □ inherent intrusion detection
- □ DRM
- □ digital signature
- □ secure network access



Users are pre-authenticated and keys are pre-distributed (distributed keys eliminate man-in-the middle attacks)

- ➢ end-to-end authentication
- ➢ operates as a one-time pad
- ➢ perfect identity for persons and devices
  - ✓ pseudo-identity
  - ✓ anonymity.

We need disruptive technology without the disruption so DDKI lets existing security work together.

Note: there will not be a single, secure asymmetric network on earth within five years when quantum computing arrives because of the fixed keys sizes.

Integrate DIVA into a Single Sign-On login protocol for network or application access. This mitigates the asymmetric vulnerability to man-in-the-middle attacks. Integrate into microprocessors and mitigate side channel attacks.

Asymmetric systems are safely transitioned

First add DIVA to protect the network and augment existing security.

Create two channel authentication – distributed and asymmetric.

Over time any redundant, expensive, or ineffective existing security components can be phased out.

- Asymmetric key exchange was an ad hoc approach implemented after the fact
- Asymmetric networks were never designed to be a ubiquitous framework
- Asymmetric communications are ALWAYS vulnerable to man-in-the-middle attacks
- Existing key constructs are ALWAYS vulnerable to side channel attack classes in micro-processors
- After 40 years < 10% of North American enterprises use secure asymmetric networks
- Security demands the fundamental, safe, addition of DDKI and DIVA
- Existing security protocols will become additional authentication factors which can be phased out in the future.

Whitenoise is recognized internationally:

Aug 2009 - White House OSTP invitation to the US National Cyber Leap Year Summit.

Apr 2010 - United Nations International Telecommunications Union - UN-ITU – for identity management and identity systems

Jun 2010 - Invited to Commonwealth Telecommunications Organization on cyber security

Jun 2010 - International Standards Advisory Council of Canada for the Global Standards Collaboration plenary working groups

July 2010 - Named by Industry Canada as a delegate to UN-ITU

Aug 2010 – Release of the book In Denial:Code Red

Nov 2010 – Grand Finalist of the Global Security Challenge Cyber contest

Memberships

International and national standards organizations

Canadian Advisory Council CAC/JTC1/SC27 WG2 and WG5 for contributions to ISO/ITU 2010/2011

Canadian National Organization for the International Telecommunications Union/Industry Canada

Standards Council of Canada - International Standards Advisory Council of Canada

Information Technology Association of Canada Cyber Security Committee

Information Technology Association of Canada National Identity Management Committee

Information Technology Association of Canada Radio Frequency Committee

Computer Systems Training Advisory Committee at the British Columbia Institute of Technology

Information Technology Association of Canada Cryptography Committee

Information Technology Association of Canada Cyber Security Forum, Electronic Commerce Protection (Anti-Spam)

Information Technology Association of Canada Cyber Security Forum, Privacy Subcommittee

These technologies impact a broad spectrum of telecommunication security.

How are they related to existing work, if any?

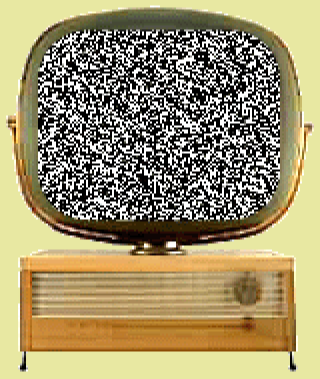
Who would be interested in collaboration or to be involved?

Thank you

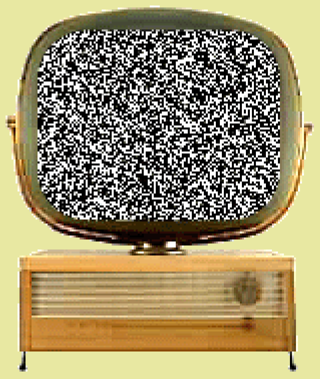
Presentation by André Brisson

Whitenoise Laboratories (Canada) Inc.

www.wnlabs.com



Whitenoise is controlled static



DIVA Dynamic Identity Verification & Authentication

IFSEC FUTURE OF SECURITY COMPETITION

GLOBAL SECURITY CHALLENGE

Certified Solutions at&t

ETSI

Addendum

DIVA and DDKI are naturally flexible, extensible, scalable and interoperable. They lend themselves to be easily configurable in any context or environment. The following addendum will examine:

1. The historical fatal flaws of network security that have been addressed.
2. Binding organic identity from iris biometrics to digital DIVA keys to create Level 3 & 4 Identity Proofing for persons and non-person entities.
3. We will look at example tunneling and application paradigms that are configured to exploit DIVA.

Addendum 1

Public key, asymmetric networks have always been vulnerable to Man-in-the-Middle attack classes – a scientific reality.

HISTORICAL PROBLEMS SOLVED

Micro-processors have always been vulnerable to Side Channel attack classes.

The three fatal failings of network security have been:

- Vulnerability to Man-in-the-Middle [M-i-M] attack classes
  - M-i-M-doesn’t work against dynamic distributed key systems [DDKI] because there is no key exchange.

- Vulnerability to Side Channel attack classes
  - This doesn’t work against DIVA because after key load all operations are order one operations. This has been validated by a 17 month NSERC funded research project at the University of Victoria, British Columbia, Canada that tested Whitenoise enabled microprocessors against this attack class.
    - Please contact the Electrical Computing Engineering Department at the University of Victoria directly: Dr. Mihai Sima - msima@ece.uvic.ca; Dr. Stephen Neville – Founder Aspire Labs – University of Victoria - Stephen.Neville@ieee.org; Paul Thiel Founder –Canadian Microelectronics Consortium career. paul_thiel@telus.net

- Uncontrolled life of data
  - This can be controlled by enterprise, 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.

Pursuit of large distributed platforms where there is only partial disclosure of credentials stalled because of three historical problems that have been solved:

Key storage was a problem

Because of the exponentialism of DIVA Identity Management and network security keys a small key structure generates a massive, random, deterministic key stream. Just 158 bytes of stored key structure information creates a key stream greater than 100 billion bytes long. The weakest strength of DIVA used is >250,000 bits and it generates key streams greater than 10 to the 60th power in length.

Key management was a problem

Historically the number of keys to manage is the square of the number of secure endpoints on a network. A ten endpoint secure distributed network would require managing 100 keys. Secure File Interchange has a one-to-one relationship between the number of keys and endpoints on a secure network.

Key distribution is a major problem for distributed key systems.

This is not true any longer – Whitenoise topologies allow distributed keys to in turn securely generate and distribute more encrypted keys. Keys are distributed using ISO/ITU Level 4 identity proofing for person and non-person entities. Keys cannot be stolen at enrollment without being identified.

Addendum 2

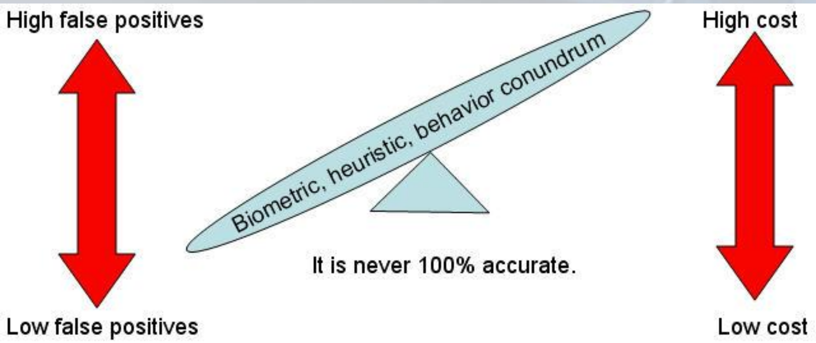
Binding organic identity to digital identity.

DIVA and Iris Scanning biometrics for Level 3 & 4

Identity Proofing for persons.

ETSI

DIVA makes biometrics - 100% accurate


High false positives
High cost
Biometric, heuristic, behavior conundrum
It is never 100% accurate.
Low false positives
Low cost

The biometric (biological), behavioral (person or code) and heuristic (experience based) conundrum when used without DIVA

❑ A person distributes a scan of a biometric (fingerprint, face scan etc.) to the server one time.

❑ A scanner takes a "snapshot" and compares specific co-ordinates against the stored copy.

The more points compared, the greater the accuracy and fewer false positives – but the greater the cost.

Mass market biometrics compare fewer points but have more false positives. This defeats the purpose.

Note: DIVA and Whitenoise can be used to randomize the coordinates that are compared between an end-point scanner and minimize the number of coordinates that need to be compared (because it is now operating like a one-time-pad) in order to get an acceptable level of assurance while minimizing the attendant costs of utilizing biometric information. DIVA can be used to secure video feeds and securely share the mined information.

An iris biometric binds identity to a DIVA account

This is 100% accurate with digital keys using Level 3 & 4 Identity Proofing:

- Identity proofing must be local (same as biometrics)
- Dynamic verification of reputation material

- Biometrics/behavior/heuristics - one additional authentication factor.
- Biometrics - market universe is human (disregards machine-to-machine)
- Safeguarding biometric information is not addressed.
- An iris biometric binds identity to a DIVA key which in turn can be used for complete network security and identity management. The DIVA key can also be used to secure and store the biometric ‘key’ as well.

ALL cyber security is dependent on secure communications (internally + externally).

DDKI, DIVA and iris biometrics are distributed key systems (each endpoint has a copy of the key) and together they provide authentication for assured identity and network access (iris identification). DDKI lays down a dynamic distributed framework; DIVA provides complete network and transactional security; and, iris authentication binds a biometric key to a digital key.

Together they provide perfect identity proofing and DDKI and DIVA provide continuous, dynamic authentication; inherent intrusion detection; automatic revocation; non-repudiation, signature, and authorization to secure the network and all transactions.

The first authentication happens with iris authentication to 'enter' the network and access services.

Successful authentication with an iris biometric will allow access to the account and the secure, unique DIVA key within the database. This marries ISO/ITU Identity Proofing Level 4 for human endpoints with a unique, digital DIVA IdM key which provides distributed identity and ensures all digital network and transactional security (as well as logs of all use) for that authenticated person throughout the life of the session.

IRIS > DIVA > secure, tamper-proof network use

Problems with security

No one buys a home alarm until their house has been robbed. Security should be inherent in any service we use. Public security measures for persons often require some kind of invasive touching or something that many consider offensive or intrusive. Most identification requires that a physical key be carried with the person.

Advantages of iris biometrics

EVERYONE, everywhere, understands the uniqueness of their own biometrics. A user cannot forget or give away his key. It is always with them. It can't be tampered with.

A user does not require any other physical key for identity based network access – no USB drive, no credit card, no health card, etc.

Two completely unique keys for network security (a person's iris and DIVA) bind organic identity to digital identity using ITU/ISO Level 4 identity proofing.

A person does not need to be touched. It is not intrusive. It is legal in all cultures and societies (developed, underdeveloped, literate, and non-literate.)

This legal approach works in any culture or society.

The iris biometric is a totally unique distributed key. Successful authentication by iris scan authorizes the person to use an account with a unique, identity-based, dynamic, distributed digital DIVA key (organic to digital).

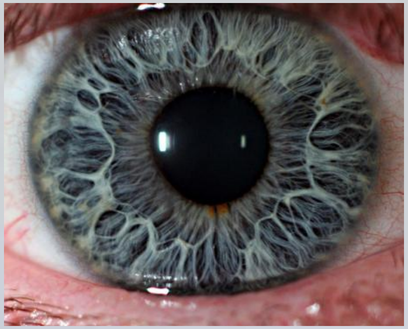
The DIVA key is secure within the application and can’t be accessed and tampered with.

Authorized use of the DIVA key then provides complete internal and external network security.

This approach acknowledges cultural contexts while providing complete security.

In conservative cultures that require a dress code, an iris scan is a reasonable requirement that can be demanded legally.

No touching. Nothing invasive. Discreet. In satisfying these criteria, it guarantees iris scans can be used in any context.



An iris scan is a reasonable security identifier globally. Many countries are experiencing rapidly growing, diverse ethnic populations.

Global travel, tourism, business, migrations etc. create larger, more diverse, flowing populations that need to be identifiable to access public and commercial services in digital contexts. This approach is functional in the most trying of contexts i.e. identifying persons for distribution of humanitarian aid after disasters.

Any digital service is simple and secure: securing banking, moving through an airport, or traveling through a foreign country etc.

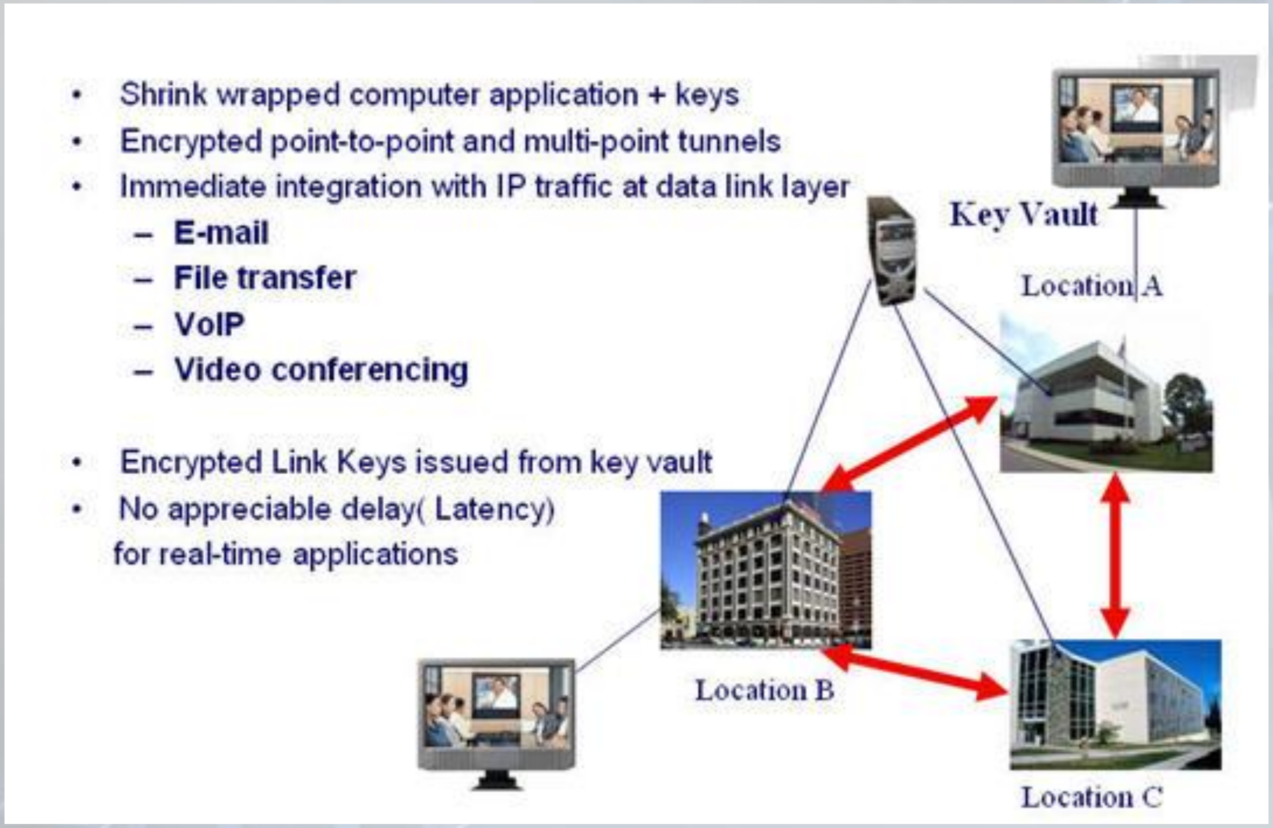
Dynamic Distributed Key Infrastructures (DDKI) and Dynamic Identity Verification and Authentication (DIVA) follow the iris scan which binds organic identity to a digital key and they probably satisfy all the ETSI and ITU/ISO criteria for securing data, communications and networks.

Addendum 3

Example topologies:

Tunneling and applications

Example enterprise topology



- Shrink wrapped computer application + keys
- Encrypted point-to-point and multi-point tunnels
- Immediate integration with IP traffic at data link layer
  - E-mail
  - File transfer
  - VoIP
  - Video conferencing

- Encrypted Link Keys issued from key vault
- No appreciable delay(Latency) for real-time applications

This graphic shows one topology for creating a secure network using tunneling and a key-vault authentication server.

Application topologies

DIVA is implemented at single sign-on network access (login) and DIVA is implemented at application and account access.

Addendum 4

Next Generation Networks

Testimonial

80 Next Generation Networks (NGN) requirements are met

DDKI/DIVA satisfy all international standard bodies requirements for Identity Management (IdM) and Privacy by Design protocols.

They operate on any operating system like Windows and in any kind of network model:

- federated
- silo
- centralized
- user-centric

It can be used with asymmetric systems for two channel authentication.

Testimonial

DIVA and DDKI provide a completely interoperable and scalable software framework that isn’t hardware dependent.

“… has developed a leading edge technology that is ripe and ready for large scaled distributed dynamic authentication and enablement of secure on-line transactions.”

Dr. Abbie Barbir

- Chair of International Telecommunications Union Technology Identity Management Question
- Steering Committee for the OASIS IDtrust Member Section
- Chair for the Kantara Initiative Privacy, OASIS, W3C, WS-I, OMA, ITU-T, Canadian Advisory Committee (CAC) JTC1 SC6, Standards Council of Canada
- IETF, Parlay and IPSphere
- System administration Bank of America