

## DDKI a virtual framework

Dynamic Distributed Key Infrastructures are secure, tiered, hierarchical virtual frameworks of devices and components deploying DIVA.

They are easily scalable and interoperable and have solved the traditional problems that have stopped large scale distributed networks of key storage and distribution. There is a one to one relationship between the keys at a server and endpoint. There is easy key storage and transfer because of multiplicity.

It is ideal for most things including Managed Mobile Networks and services and Scalable Adaptive Secure Networks.

NOKIA

### How does Dynamic Identity Verification and Authentication protocol 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

The key stream 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.

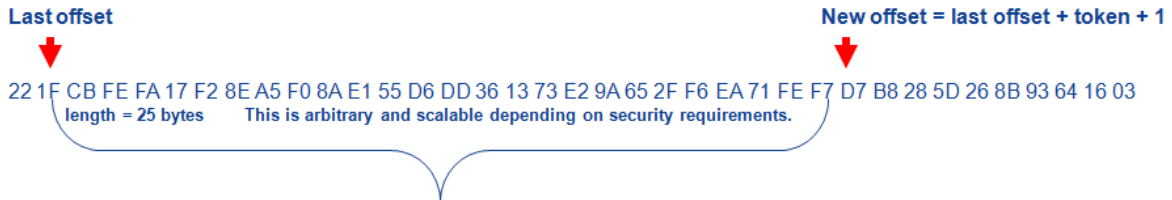
NOKIA

DIVA is always polling ahead in a stream and comparing a token (portion of key stream) that has never been created or used before. That is what makes it an unbreakable one-time-pad.

### 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. If they are identical then the

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



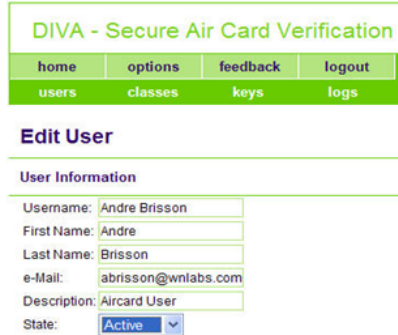
The system is synchronized for the next continuous authentication query.

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 % accurate – only two DIVA outcomes

Someone tries to steal a key.

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

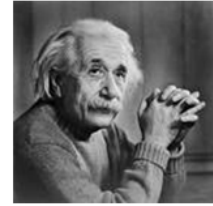


DIVA - Secure Air Card Verification	
home	options
feedback	logout
users	classes
keys	logs

### Edit User

User Information

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



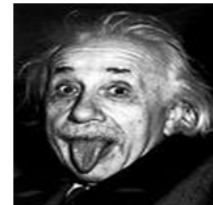
- The legitimate key and server offset dynamically updates with this use independently.
- The pirated or spoofed key (if possible) is no longer synchronized with the server and the legitimate key.
- The pirate will be detected if he makes a login attempt.
- The pirate can't access network. Stolen copy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

This is the only outcome we have ever seen.

**NOKIA**

### 2. The pirate somehow steals a key and logs on 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.



Gotcha Hacker!

**NOKIA**

Dynamic Distributed Key Infrastructure Virtual frameworks (DDKI) and Dynamic Identity Verification and Authentication One-Time-Pad authentication

<http://www.wnlabs.com/products/SecureSessionManager.php>

## **Two things you must remember about WN, DIVA and DDKI**

It works seamlessly without direct integration with PKI and any other security frameworks or controls.

It is NOT only about encryption. That is a small part. Whitenoise technologies perform all network security controls with a single distributed key.

- perfect identity
- secure network access
- continuous dynamic authentication
- authorization
- signature
- non-repudiation
- inherent intrusion detection
- automatic revocation
- and yes, encryption

**NOKIA**