
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.

- 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.