



# Leap-Ahead Technologies

Miles Smid  
Orion Security Solutions

For those viewing via webcast, please submit questions to [kmwquestions@nist.gov](mailto:kmwquestions@nist.gov)

NIST CKM Workshop June 2009

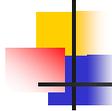
1

## What makes a leap-ahead technology in CKM?

- Leap in base technology
- Leap in security
- Leap in ease of implementation, management, or use
- Some combination of the above
- Other suggestions?



2



## Leap in base technology

---

- Computer communications
  - Made communications much easier
  - Significantly increased the need for security
- Quantum cryptography
- Network security at no extra cost
  - Dream on
  - What about seat belts and air bags
- Something else?

3



## Leap in security

---

- Automated protocol validation
- Provably secure protocols
- Quantum Cryptography
- Secure key generation, access, storage and recovery
  - There is more to the problem than just key distribution

4

## Leap in ease of implementation, management, or use

- Electronic key distribution
  - Key wrapping
  - PKI
- Identity based key management?
- Transparency
  - Cloud key management
  - Cloud secure channel
- Enterprise key management?
- Other possibilities?

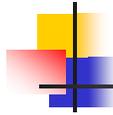
5

## A leap-Ahead would be great, but shouldn't we keep on walking

- What is wrong with current technologies? Are the flaws fatal?
- Do we see a clear leap-ahead technology at this time?
- Are there some good candidates?
- Shouldn't we continue to improve upon our current technologies and let the leaps come where they may?



6



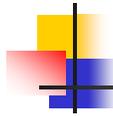
## Submit your ideas

---

NIST CKM Blog Question A

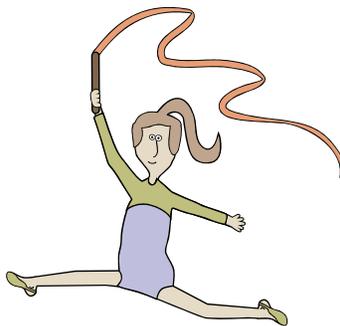
<http://keymanagement.wordpress.com/>

7



## Discussion?

---



For those viewing via webcast, please submit questions to [kmwquestions@nist.gov](mailto:kmwquestions@nist.gov)

8