

**Licensable  
Technologies**

# Quantum Smart Card — "QKarD"

## Applications:

- Telecommunications: cell / smartphone; multi-party secure phone calls; videoconferencing; Voice over IP (VoIP)
- Banking and financial transactions: ATM, debit / credit card and e-Commerce
- e-Business; e-gaming; e-books; e-music; e-movies; e-gambling
- Wireless internet
- Electronic voting
- Facility and vehicle access
- Information exchange for government/defense

## Benefits:

- Future-proof encryption
- Compact
- Portable
- Wireless
- Low-cost deployment
- Does not require dedicated fiber optics
- Invulnerable to both conventional and quantum computer attacks

## Contact:

Marcus A. Lucero  
(505) 665-6569  
marcus@lanl.gov  
tmt-2@lanl.gov

Technology Transfer Division



## Summary:

The security of present-day encryption techniques for protecting electronic communications and transactions depends on the inability of computer processing power to decipher difficult mathematical problems.

With processing power increasing at an exponential rate, eavesdroppers can, in principal, decipher even the most complex mathematical problems. To make matters

even more alarming, encrypted communiqués that are secure today could potentially be archived for years until processing power catches up with the computational demands of cracking these mathematical problems. Thus, a "future-proof" encryption mechanism, that is independent of processing power, is essential to protecting valuable information.

In response to these problems, Los Alamos National Laboratory (LANL) scientists have developed a revolutionary technology entitled "QKarD" that implements the quantum mechanical laws of physics rather than complex mathematical problems to encrypt information. This technique, known as Quantum Key Distribution (QKD), uses polarized single photons to generate secret keys that can be shared between two or more parties and used to encrypt data to safeguard it from eavesdroppers. Incorporating this method of encryption into QKarD technology provides superior forward security assurances without archival attack concerns, regardless of advancements in processing power.

The QKarD is a compact, portable and wireless device that is simple to use. A user needs only to periodically insert the device into a base station for authentication, requiring both a fingerprint and personal identification number (PIN). The QKarD would then communicate seamlessly with a central trusted authority (TA) via optical fiber, from which cryptographic-quality secret random numbers are automatically uploaded. These numbers are then stored in secure memory on the device, for encryption, authentication, and access control, ensuring secure communication with other devices through the air (free-space) at remote locations. These remote devices also communicate back to the same TA to authenticate a user, provide access control, or set up a multi-party secure telephone call. Furthermore, because the QKarD generates new random numbers without the use of any pre-placed secret, it provides increased security for access to computer systems, banking and financial transactions, telecommunications, and any other function that could be referred to the TA. The QKarD could easily be envisioned as part of an Advanced Encryption Standard (AES) compliant smartphone that uses built-in quantum keys to replace conventional algorithm based encrypted communication. The QKarD system could be incorporated seamlessly into a smartphone or attached by way of a universal port.

**Development Stage:** Demonstrated proof-of-concept

**Patent Status:** Patent pending

**Licensing Status:** Available for exclusive or non-exclusive licensing and collaborative agreements.

[www.lanl.gov/partnerships/license/technologies/](http://www.lanl.gov/partnerships/license/technologies/)

An Equal Opportunity Employer / Operated by Los Alamos National Security LLC for DOE/NNSA

