

**SECURE PASSWORD GENERATION AND MANAGEMENT USING NFC AND
CONTACTLESS SMART CARDS**

ABSTRACT OF THE DISCLOSURE

Various embodiments are directed to securely generating and managing passwords using a near-field communication (NFC) enabled contactless smart card. For example, a secure password may be generated by generating a random number via a random number generator of the contactless smart card and converting the random number to one or more human-readable characters. In another example, a secure cryptographic hash function of the contactless smart card may generate a hash output value, which may be converted to one or more human-readable characters. The human-readable characters may be used as the secure password or it may be transformed to add more layers of security and complexity.

[FIG. 5]