S D C

Secure Data Carrier

New technology for
Keyless Secure File Exchange

Invisible Data Transmission

The file is incredibly secure and unbreakable.

QUANTUM
Experts Of Data Hiding

Quantum
Smart information technology

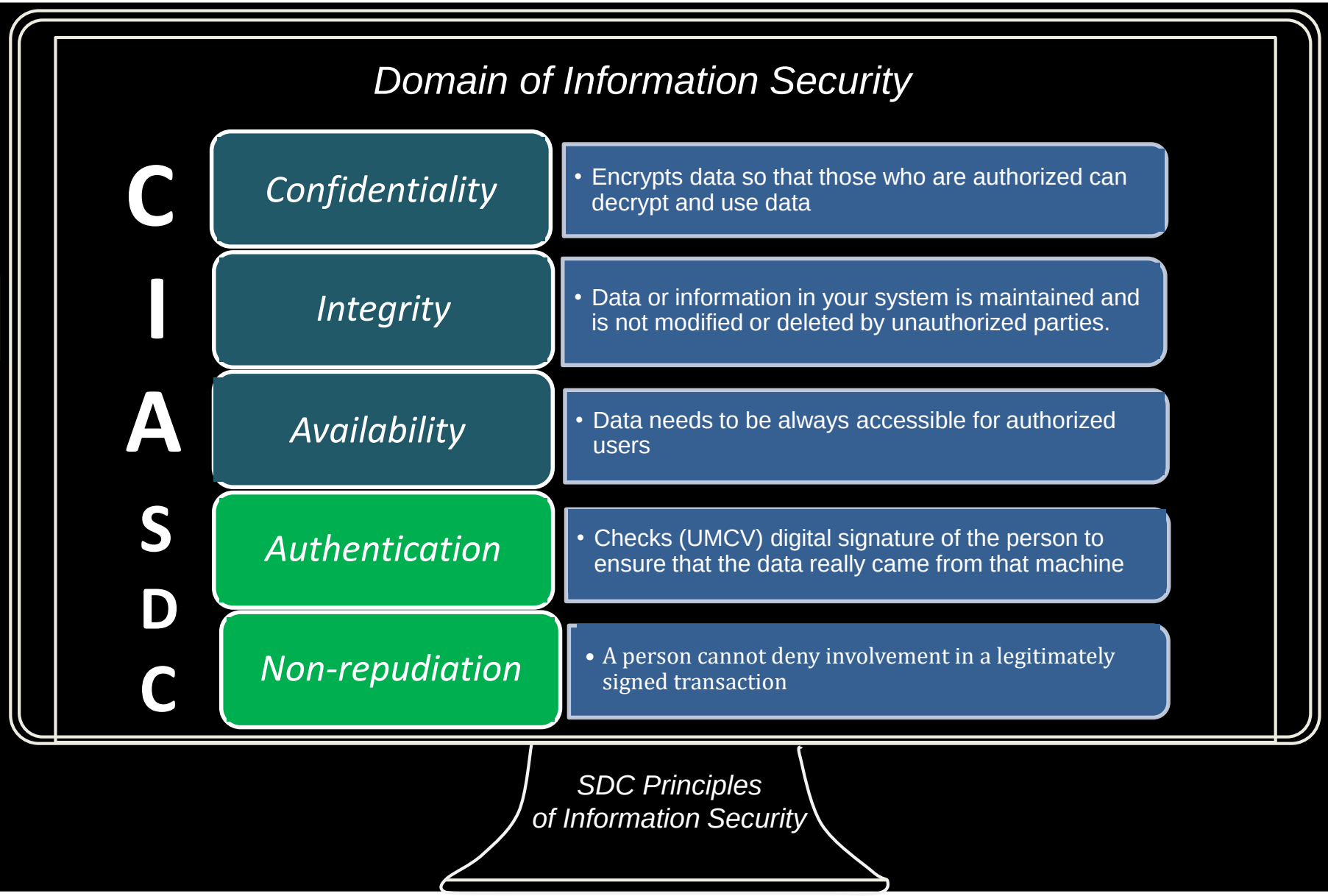
TRUSTED SECURITY SOLUTIONS (TSS)

S D C

Integrity

- Output Feedback Mode shows that the data has not been altered and not compromised since it was signed

- In Output Feedback 1 bit error is Fatal to the next bit sequence, decryption will fail in the very first occurrence of error.
- SDC has a built-in encryption key to check the byte signature.
- TROJAN will never change the byte structure, but byte signature changes



QUANTUM
Experts Of Data Hiding

Types of Encryption Key

Encryption Key

Symmetric

- Single Shared Key
- Use Substitution Functions

  e.g.: DES, AES
- Block Cipher
- Fast

Asymmetric (Public Key)

- Two Keys (Private, Public)
- Use Mathematical Functions
- e.g.: RSA, ECC, EL-GAMAL
- Stream Cipher
- Slow

SDC

- Symmetric Key is injected in Ciphertext Garbage Payload
- Invisible Cipher Key
- Bit-wise Encryption
- Stream Cipher
- Memory-based encryption
- Very Fast

Encryption Algorithms

Standard Encryption

1. Substitution
2. Fractionation
3. Transposition

SDC Encryption

1. Compression
2. Dissociation
3. Substitution
4. Fractionation
5. Triple Transposition
6. Output Feedback

SDC Encryption with Bit Hiding

1. Compression
2. Dissociation
3. Substitution
4. Fractionation
5. Triple Transposition
6. Output Feedback
7. Invisible Ciphertext Conversion

NIST Recommends	1024 Bit = 128 Byte	(Not Variable-length)
AES	512 Bit = 64 Byte	(Not Variable-length)
SDC	3072 Bit = 384 Byte	(**Variable-length**)

SDC key length and output are changing every encryption process even the key and data are the same.

SDC Sophisticated Methodology in Data Security

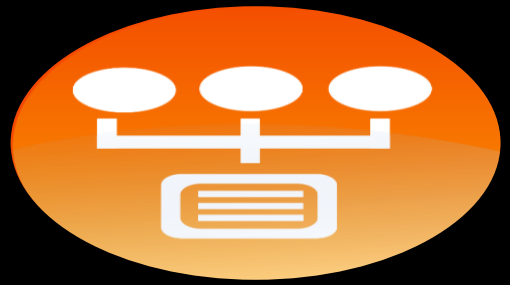
SDC Dissociation Process

Dissociation Process

Dissociation Process is one algorithm of SDC Encryption wherein it dissociates the original Characters or replaced them randomly with Dummy Characters with the same length of random characters, by this way SDC encrypts the fake or Dummy Characters, so the Ciphertext is based on Dummy Characters in order to confuse the Crypt-analyst, this process makes the encryption unbreakable.

In Short, dissociation is a process of removing the original Characters or Plaintext and replaced by Dummy Characters. The original Characters or Data are not present in the Ciphertext anymore.

SDC Sophisticated Methodology in Data Security



Triple Transposition

Triple Transposition

Triple Transposition in SDC Encryption, some of the bits are hidden already that's why SDC encryption is unbreakable, single bit mistake is fatal to the next right bit sequence, cannot be decrypted anymore.

SDC MAIN FEATURES

User / Group Certificate	• HIGHLY SECURE EXCLUSIVE DATA OWNERSHIP (HSEDO)
Steganography Technique	• Data Compression • RPP Random Pixel Positioning • Data injection into an image Pixel's Noise and Colours
Steganography Benefits	• 0% change in image size! • No change after data injection • Color will never change after data injection

HIGHLY SECURE EXCLUSIVE DATA OWNERSHIP (HSEDO)

QUANTUM
Experts Of Data Hiding

USER KEY CERTIFICATE

- SDC uses local Certificate based on user machine
- SDC Certificate based on Local Server
- SDC Certificate & CA file Key Infrastructure
- SDC has 6 factors of authentications (UMCV)
- SDC Integrity verifications on both (Data and Machine)
- Sending Data to specific/exclusive users based on Certificate Credentials
- In OTP the Key is sent to the partner, not the message
- In SDC Dummy Characters are sent to the partner, **Not** the key

Compromised key equals Compromised Data

(UMCV)
USER MACHINE CREDENTIALS VERIFICATION
&
MULTI-FACTOR AUTHENTICATION

USER MACHINE CREDENTIALS VERIFICATION

User Windows Credential

- Username
- User Password
- Encryption Key

User Machine Credential

- Mother Board
- HD Smart Ser. No.
- Processor/CPU

The Data are being authenticated and verified
by UMCV using the 6-Factor Authentication

SDC KEY VALIDATION TECHNIQUES

Users can exchange secure documents securely, only targeted user/users are allowed to open the encrypted documents.

QUANTUM
Experts Of Data Hiding

1. **Group Certificate (CERK)**
   - Certificate Member Verification
   - User's Machine Credential Verification
   - CA File Signed Key Verification
2. **External User (CREDK)**
   - User's Machine Credential Verification
   - Encryption Key Verification from UMCV
3. **Personal Credential (SDCK)**
   - Personal Machine Credential Verification
   - Encryption Key Verification from UMCV
4. **SDC Encryption (SDC)**
   - Using Key-Shift in Encryption Key

Note: *Key-Shift Key Generation is an exceptional process that cannot be reversed by any means. The Key output is unpredictable.*

SDC Safe Note (SDCSN)

Steganography

SDCSN Sophisticated Technique
for Secure Data Transmission

The Art of injecting invisible File Content
into an image Pixel's Noise & Color

The decent way in sending confidential/classified documents
to any Internet channel of communication.
Encryption is suspicious.

SDC Safe Note (SDCSN)

SECURITY BENEFITS

Chest X-ray (radiographic) image contains Sensitive Data For highly protection and secure transmission

SDCSN Steganography technique

SDC Safe Note is the solution to protect and transmit sensitive information inside an image in a hidden and secure way without any change in the **image size and color**.

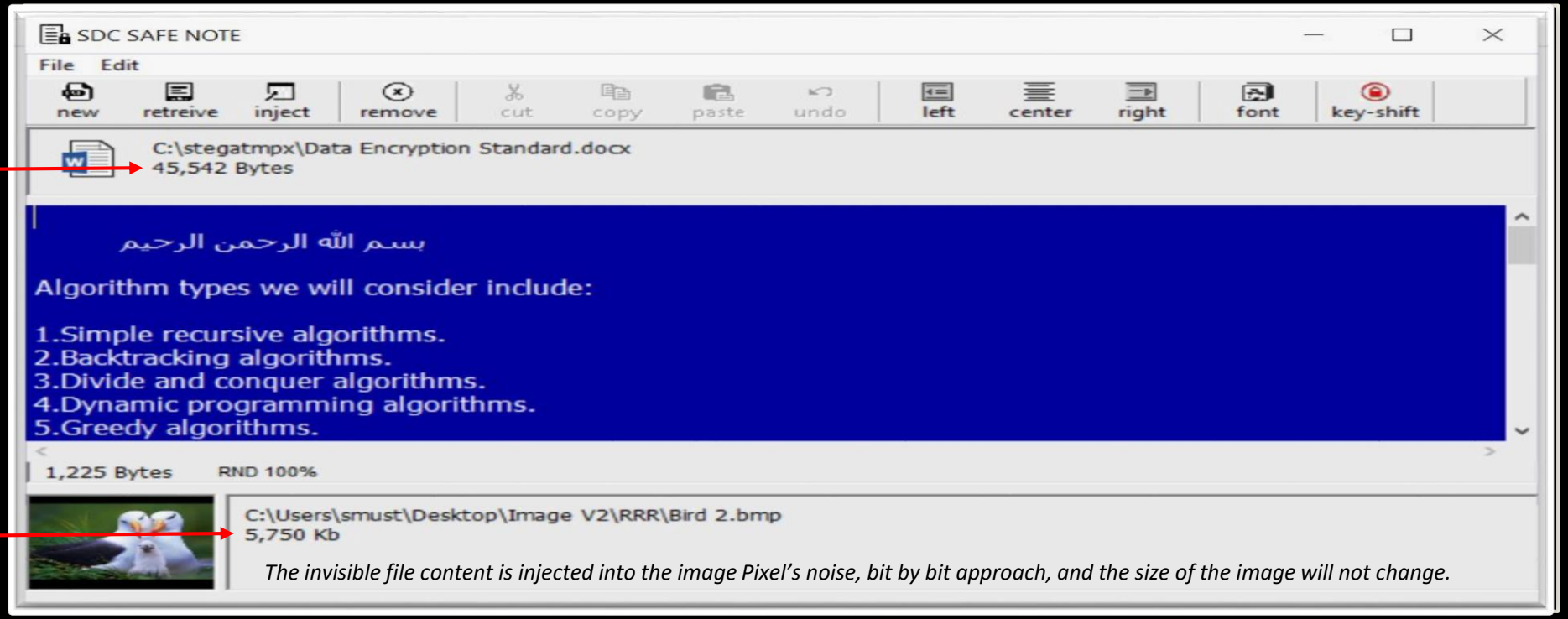
SDCSN Technique

- **Crypto-Secure Steganography (CSS)** is to inject compressed and encrypted Data inside an image Pixel's noise making it totally invisible for human eyes due to the noise data manipulation process.
- **Random Pixel Positioning (RPP)** ensures that even when it is known that the image is a data carrier, it is impossible to retrieve and access the original injected data.

SDC Safe Note (SDCSN)

Data injected into the image

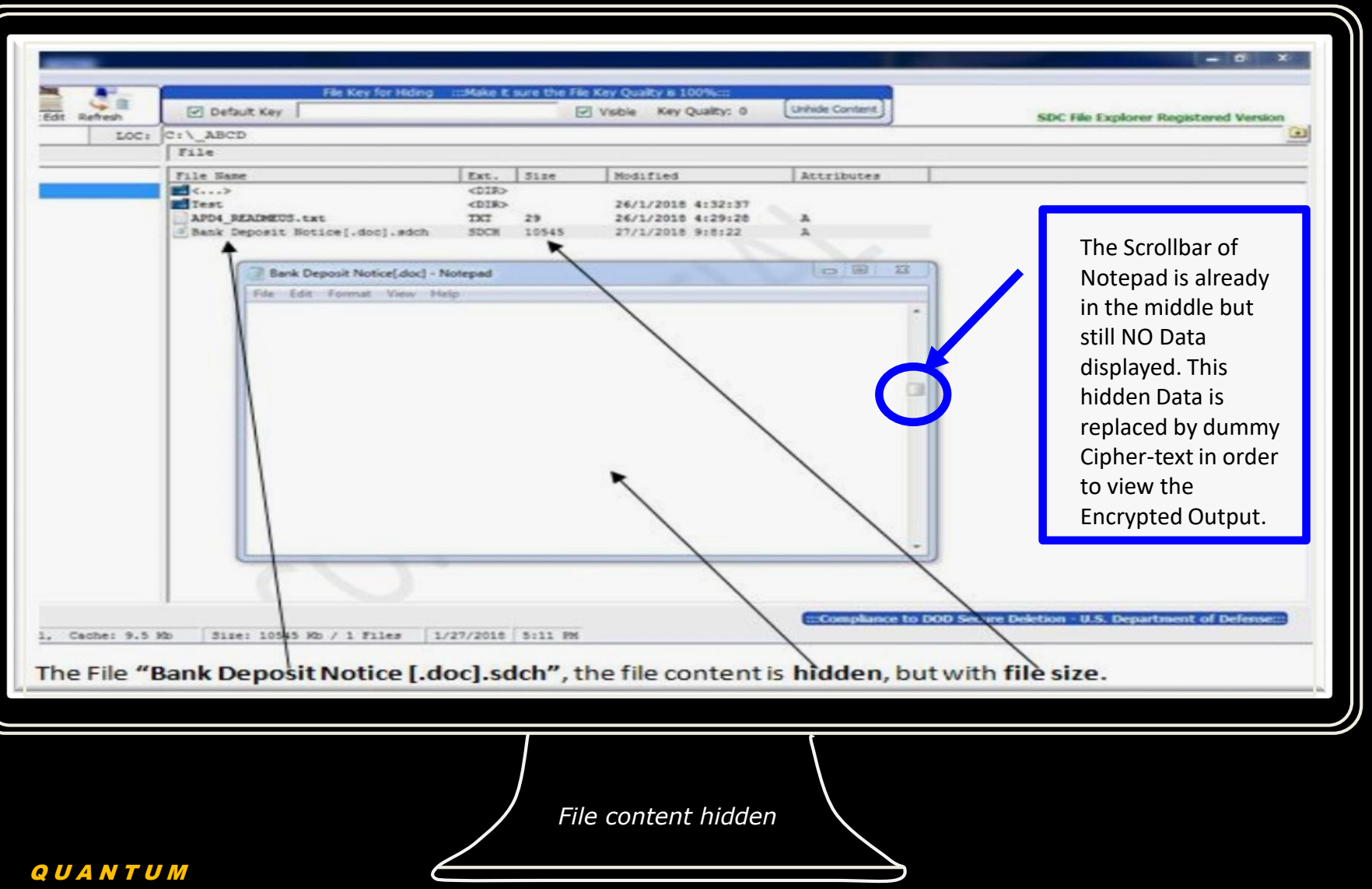
Actual image Size



After Data injection image size will not change

QUANTUM
Experts Of Data Hiding

TRUSTED SECURITY SOLUTIONS (TSS)



The Scrollbar of Notepad is already in the middle but still NO Data displayed. This hidden Data is replaced by dummy Cipher-text in order to view the Encrypted Output.

SDC makes the file content hidden but you can see the File size, and cannot be seen by any Hex Editor Utility or by any means to recover the hidden bits of data of a file or a document.

File content hidden

QUANTUM
Experts Of Data Hiding

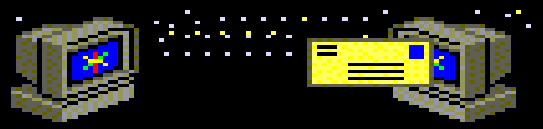
SDC PROTOCOLS STRATEGIC BENEFITS

Invisible File content

STRATEGIC BENEFITS OF SDC PROTOCOLS

SDC can transmit data of **All Types** to different internet connection protocols such as TCPIP, UDP, HTTPS, FTP, and SFTP, etc.

Also, **SDC** can transmit Confidential data on public communication channels such as Facebook, Messenger, WhatsApp, and Emails.



Users can exchange secure documents securely, only targeted user/users are allowed to open the encrypted documents.

SDC SECURITY FEATURES

National Security Agency – NSA Recommendations

3072 bit is advised to encryption programmers worldwide by NSA of America to be used beyond the year 2030 because NSA has a conclusion that encryption below 3072 bit will become weak and vulnerable and possibly be broken.

SDC SECURITY FEATURES

3072 bits compliant with NSA Key Requirements beyond the year 2030

1. Secure Key Management
2. Flexible Key Usage
3. Key-Shift is Secure
4. Bit-Hiding is Unbreakable
5. Injected Data into the image is inaccessible
6. No Key or password to memorize
7. Keyless Secure File exchange
8. Strong password is generated automatically by SDC
9. Secure user keys from known key loggers
10. Secure and Exclusive Data Ownership
11. All Data Security Functions are non-repudiation.
12. The encryption process is done in memory , not on Hard Drive
13. Unbreakable encryption due to Dissociation Process and Variable length key
14. SDC is Bit Level Encryption, then Converted into Invisible Ciphertext
15. User Key Certificate is Uncompromisable due to UMCV - User-Machine Credentials Verification

SDC COMPETITIVE ADVANTAGES

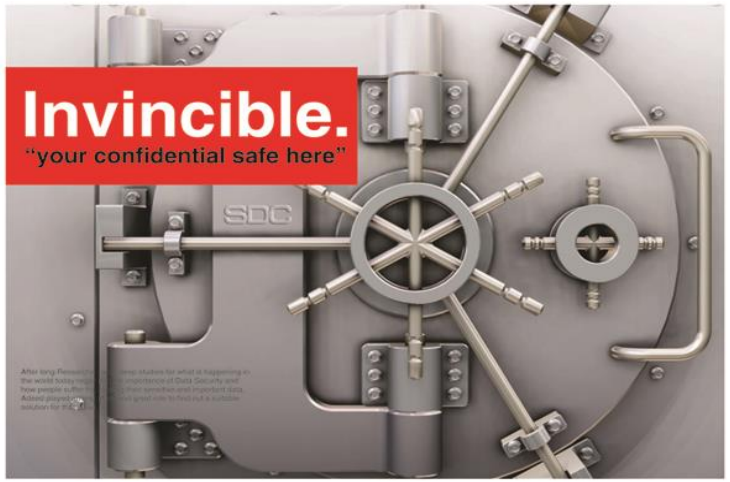
Seq	Encryption Process	SDC	AES
1	Is Ciphertext Fixed length using the same key?	NO	YES
2	Is Ciphertext changing using the same key?	YES	NO
3	Variable Key Length	YES	NO
4	Key size	3072	128/192/256
5	Substitution	YES	YES
6	Fractionation	YES	YES
7	Transposition	YES	YES
8	Dissociation	YES	NO
9	Compression	YES	NO
10	Invisible Bit Hiding	YES	NO
11	Key Injection	YES	NO
12	Output Feedback Mode	YES	NO
13	Are Data transfers using all Protocols	YES	NO
14	Is Data injected/inserted is Accessible	NO	YES
15	Where Encryption process is done?	Memory	HD
16	Is the Image size changed after Data injection/insertion?	NO	YES

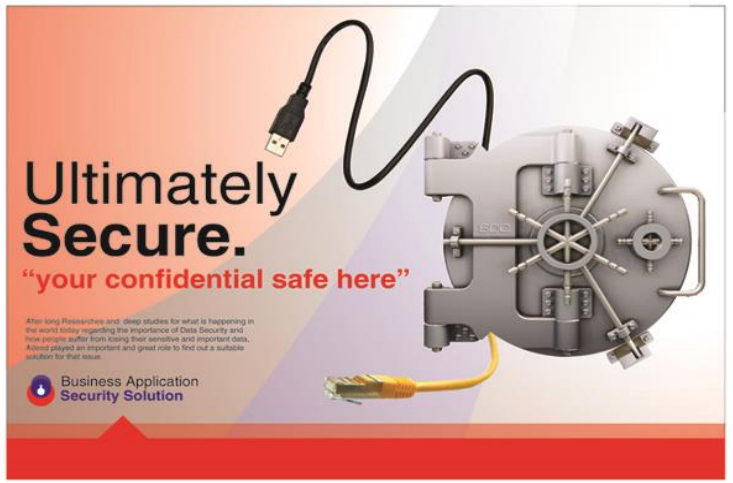
SECURE DATA ACCESS CONCEPT

Please always remember that any Cipher that is visible to the eyes of the attacker is vulnerable to attack and the vulnerabilities can be exploited at any point in time, just time matters.

SDC invincible cipher

TRUSTED SECURITY SOLUTIONS (TSS)






101001101
thank you
Quantum Encryption