CDAC Comments onConsultation Note –

Solution Architecture forTechnical Interoperable Set Top Box

1. Secure channel establishment is considered for confidentiality only. It is suggested to consider Integritypart while communication between Smart Card and STB.

2. Smart Card Data definition should be standardized.
    a. Mechanism of key storing and its retrieval mechanism is to be standardized
    b. Security aspect of smart card data and key store is not there.
3. What will be the impact of this scheme on Older STB's (Smart Card based STB/Soft CAS based STB)
4. Generation of nonce is not clear (True Random Number?)
5. Generation of UK(user key) is not there in the document
6. HACK Recovery is not considered.