SG technical contribution to ISO/IEC JTC1/SC17/WG11
Shared with Asia IC Card Forum meeting – 17 July 2019

- **A tutorial and brainstorming session for Application of Blockchain and DLT (distributed ledger technology) in the area of biometrics on smart cards**
- **Applicable to IoT devices in general**

- **By: Mr. LIN, Yih**

  Chairman, ITTC, Singapore ITSC

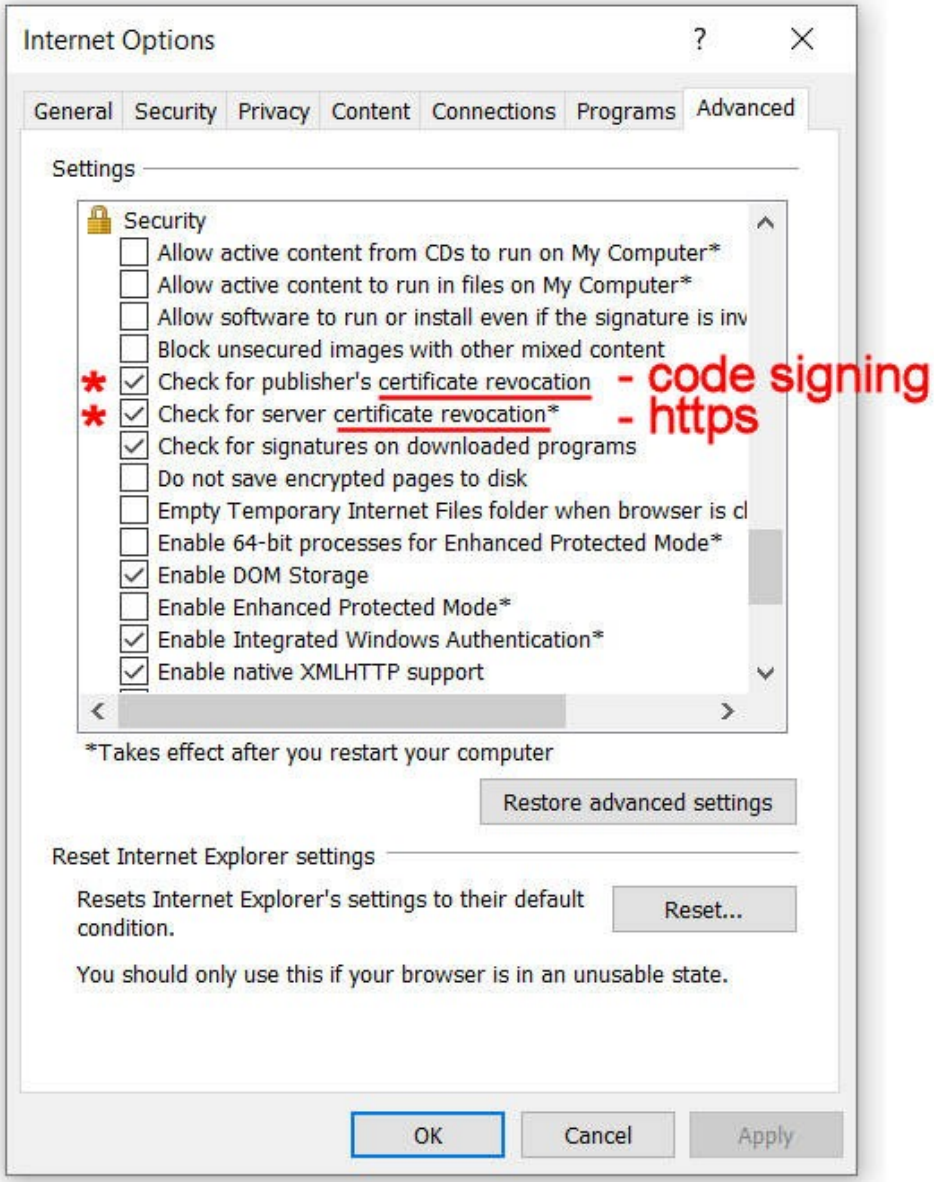
  Convenor, ISO/IEC JTC1/SC17/WG11

Known issues with classical PKI

- **Q: Classical PKI and digital signature is widely adopted, why "build another mouse trap" ?**
- **A: In order for digital signatures to be trusted, certificate revocation should (shall?) be performed**
- **A: If you don't have access to the CRL / OCSP server (e.g. no internet, firewall rules, heavy network traffic), certificate revocation cannot be done**
- **A: If the private key has been compromised but never reported, certificate revocation cannot work**

Example of CRL settings in Internet Explorer

- **Revocation check can be turned on / off**
- **If check is “on” but there is no access to CRL server, code signing verifier won’t prompt you - it just times out !**



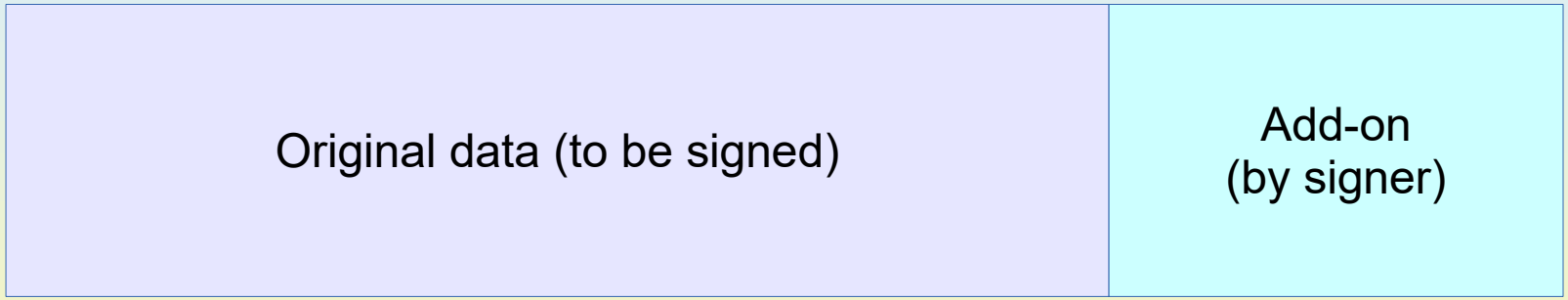
What can Blockchain & DLT offer ?

- **An alternative to public / private key technolgy**
- **Does not displace PKI, can be complementary**
- **Distributed verification – need not trust only one or a few servers, decision by consensus, majority**
- **It is intentionally, meant to be "costly" to "sign" a piece of data (but does not require public / private key)**
- ***Signing is "costly" but verification is fast, low cost***

What is “costly” ?

- Years ago, people have suggested that to fight “spam”, make sending emails (messages) “costly”
- Refine the same idea – make “signing” data “costly”
- Idea#1: Make it time consuming (e.g. 10 minutes)
- Idea#2: Make it demanding on hardware such as memory, IO bandwidth (e.g. 8GB graphics cards)
- Idea#3: Signer will lose real money, license or other consequences if they are proven to be irresponsible
- A combination of all the above and variants

Implementation (basic idea)



- **Signer adds additional block to original data**
- **The new block must meet an established requirement (e.g. SHA-3 of the new block must be less than a pre-agreed limit)**
- **Hence the signer will spend time or resource to find the correct Add-on that fulfills this requirement**

From a single block to a chain

Hash of previous block # N-1	Data block # N	Add-on (by signer)

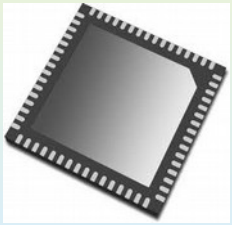
- **Where processing logic requires a sequence of data blocks, adding a Hash of the previous block creates a Blockchain**
- **For example: a fingerprint raw image can pass through a pipeline of processing units – capture, signal process, rotate, resize, align, feature extract, store, compare**

So what’s next ?

- **Brainstorm / Discussion**

Q&A – Idea generation

- **Q: Can we use BC/DLT to establish trust of biometric verification by BSoC ?**
- **Q: If transaction needs to be fast, can use BC/DLT ?**
- **Q: Can PUF (physical unclonable function) be used as Add-On given we don't need mathematical property (e.g. primeness for public / private key) ?**
- **Q: Use BC/DLT for trustable, enrolled, reference data ?**
- **Q: Use PC / card terminals as "signers" ?**



THANK YOU !

- **Hope to have a good discussion at the Madrid meeting !**