Cybersecurity Technology as a Trade Facilitator

Pedro Fuentes

Trust Services Manager, WISeKey

Positive Vs Negative approaches to Security

Negative approach

Security Measures prevent the "bad guys" to steal data or corrupt systems

Positive approach

Security Measures allow to safely achieve our goals and improve our performance

For a climber, the goal of securing its progress in the mountain is to safely reach the summit, not just preventing a fall

The Pillars of Information Security

Authenticity

The transaction is done among the genuine parties

Confidentiality

The data is only visible for the authorized parties

Integrity

The data can't be manipulated once the transaction is settled

So, what do we need?

Digital Identity, to ensure the authenticity of any access to data or transaction sent

Encryption, to protect data while in transit or at rest

Anti-tampering seals, to ensure electronic transactions can’t be manipulated

Tackling the problem: The Traditional PKI Approach

Identity, encryption and integrity can be obtained with x.509 Digital Certificates:

- The certificate itself is a credential that can be linked to an entity and used to authenticate a transaction
- Encryption can be implemented using well-known public-key cryptography
- Integrity can be obtained by adding digital signatures to the transactions

Tackling the problem: The New Blockchain Approach

Disclaimer:

Blockchain is one of the most over-hyped technologies in the last 10 years

Actually... it can't solve all the problems of humanity

And... in many cases there are other options that should be considered

But... it's a disruptive technology that can bring unique benefits

Tackling the problem: The New Blockchain Approach

Identity and integrity can be obtained from blockchain-based implementations:

- Blockchain uses also Public Key Cryptography that can be used to authenticate the transactions
- Integrity can be obtained by adding digital signatures to the transactions

(Blockchain doesn’t provide confidentiality)

Pros and Cons

	Pros	Cons
Traditional PKI	• Standards-based • Can provide authentication and integrity • Well-known and proven • Regulated, auditable • Legal validity	• Trusted Third-Parties are required • Doesn't provide a transaction store • Scalability can be a challenge • Usability issues
Blockchain	• Provides a transaction store • Great for Transaction Integrity and Track&Trace • Transaction automation (smart contracts) • Scalable in most cases	• Not well-defined standards • Can't easily provide authentication • Multiple and changing implementations • Not regulated, not easily auditable • No legal framework • Privacy issues

What about Trade Facilitation?

- PKI is well aligned with UN/CEFACT recommendations for the Authentication of Trade Documents (ECE/TRADE/C/CEFACT/2014/6), proposing standard-based implementation that can provide document signatures and authentication

- Blockchain, even not being a mature technology, can cover adequately certain needs for integrity assurance of the trade life-cycle, specially where we can’t rely on Trusted Third Parties

Our proposal…

We should build synergies among both worlds, in such a way that:

- The traditional PKI can be used (where available) as an identity layer and a mean to digitally sign transactions with legal validity (when required)
- The Blockchain can be used to ensure the integrity of the transaction flows and track securely the status changes of merchandises

In parallel, there should be real efforts to regulate the blockchain in order to gradually enable better control, homogeneous implementations and legal validity