Building a Transparent Supply Chain – Knowing the Provenance of Foods in Superstores

Clément Petit - Supervised by: Konstantinos Markantonakis
Information Security Group, Smart Card and IoT Security Centre

The Smart Card and Internet of Things Security Centre

Introduction

As consumers are more and more inclined to favour responsibly sourced products and transparent organisations, it is becoming increasingly important to have a transparent supply chain.

Supply chain transparency allows the producer to monitor various aspects, which would otherwise be very difficult:

- Quality
  Monitor all suppliers within the supply chain to only work with quality and trusted producers.
- Sustainability
  Ensure products are ethically sourced and produced. A 2015 study shows 66% of consumers are willing to buy from a responsible company. [1]
- Compliance
  Allows companies to see if its suppliers comply with various acts (Modern Slavery Act etc.)
- Consumer trust
  In 2016, a study showed that over 90% of independent consumers would be loyal to a transparent producer. [2]
- Procurement
  Enable JIT delivery structure by optimising supply chain resilience through transparency. The Business Continuity Institute found that in 2018, 73% of supply chains have suffered at least one disruption, with 34% coming from 2nd tier and lower suppliers.

Objectives

Create a more observable and tamper-proof supply chain for suppliers and third party organisation, while maintaining user privacy.

More specifically:

- Maintain user privacy
- Scalable structure
- Tamper-proof design
- Maintains company security

Technology

The underlining technology behind this project is blockchain; Ethereum. Ethereum is a distributed public ledger, which implies anyone can access it, and anyone can submit transactions.

Every user has a digital signature based on a private/public key pair, which is used to verify every transactions made on the blockchain.

Blockchain is particularly apt for increasing transparency due to its unique characteristics: [4]

- Decentralised
  No single organisation has validation control over the transactions made to the blockchain.
- Persistent
  Invalid transactions would be discovered very quickly, and once data is in the blockchain, it cannot be removed
- Anonymous
  There is no data that could directly link users to transaction (such as IP addresses).

Tamper-proof

It is important that when a transaction is made, it cannot be tampered with by unauthorised users.

This is achieved using Keccak-256 hashing algorithm, followed by a signed version of this hash (using ECDSA). Each message sent to the blockchain is divided into two parts; the plain message and the bytes containing the verification.

The first part (plain message) also contains a transaction count. The second part (bytes) contains a hashed and signed version of the plain message. The message (including the transaction count) is hashed locally, then signed using the user's private key, as demonstrated in fig.1.

The blockchain network will then verify the signature and ensure it is signed by the correct Ethereum address. *column break >*

It will also hash the plain message and compare it to the hashed messaged sent in the second part of the message. If these are equal, it means the message has not been tampered with.

As the transaction count is also signed and hashed, this prevents replay attacks against a user, as if this number has changed in the plain message, it will no longer match the signed hash and it won't be accepted. [5]

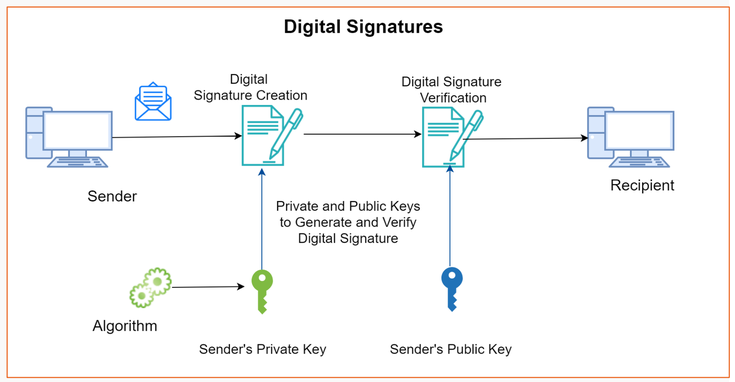

Fig. 1: Signing process for supply chain.

Conclusion

The final product shows a tree structure of a supply chain. All the current suppliers are displayed, as well as their current shipping status. Although expandable, it currently only shows the provenance of each supplier.

The software prototype focusses on creating the secure and one that supports a zero-trust architecture. Any supply chain could be safely observed as if from the root company by third party regulatory companies by simply aquiring the root contact address.

Submitting and receiving information is also secure for suppliers in the chain, as it is outside a company's security levels; no login details need to be produced and no personal database is accessed.

The software is also expandable and can include supplier attributes such as time due, certifications (RSPO, USDA Organic, Green Seal etc.) and other statistics.

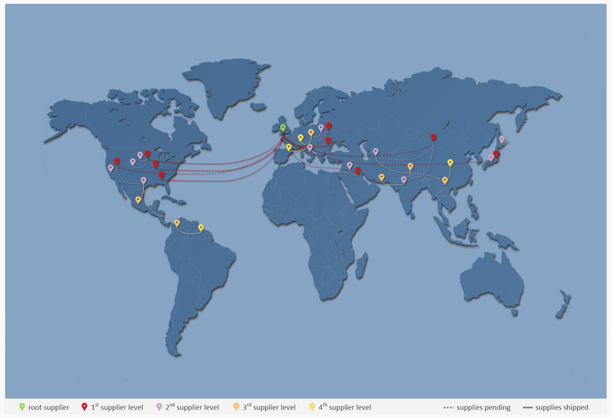

Fig. 2: Typical supply chain visualisation

Fig. 3: Supplier info

Contact

Web: https://scc.rhul.ac.uk/
Email: ClementAMPetit@gmail.com

References

[1]https://www.nielsen.com/us/en/insights/report/2015/the-sustainability-imperative-2/
[2]https://www.fooddive.com/news/why-food-transparency-is-a-valuable-investment/425503/
[3]https://www.thebci.org/uploads/assets/uploaded/c50072bf-df5c-4c98-a5e1876aafb15bd0.pdf
[4]https://ieeexplore.ieee.org/document/8029379
[5]https://github.com/ethereum/wiki