PUF-Based Identification Tags and Blockchain for Supply Chain Management

Carmelo Felicetti[1] Antonella Guzzo[1] Antonino Rullo[1]
Domenico Saccà[1,2] **Francesco Pasqua[2]**

[1]DIMES, Università della Calabria

[2]OKT srl, Relatech Group

Outline

Outline

Object Authentication in Supply Chain Scenario

- Emerging scenario of business and industrial distributed applications: supply chains, where a product item (physical object) needs to be traced along every step among the involved companies, thus requiring identification by reader devices for collecting their data and storing them into a distributed ledger.

Object Authentication in Supply Chain Scenario

- Emerging scenario of business and industrial distributed applications: supply chains, where a product item (physical object) needs to be traced along every step among the involved companies, thus requiring identification by reader devices for collecting their data and storing them into a distributed ledger.
- In this scenario, the product item is required to be recognizable and distinguishable in order to be traced individually.

Object Authentication in Supply Chain Scenario

- Emerging scenario of business and industrial distributed applications: supply chains, where a product item (physical object) needs to be traced along every step among the involved companies, thus requiring identification by reader devices for collecting their data and storing them into a distributed ledger.
- In this scenario, the product item is required to be recognizable and distinguishable in order to be traced individually.
- Authentication mechanisms, therefore, play a crucial role. However, as physical objects such as product items do not have authentication capabilities, an important research issue is to provide an identity to them together with a mechanism to prove it.

Identification Tag

Identification Tag (ID Tag): an integrated circuit (IC) with unique features (digital fingerprint) which implements an authentication protocol and incorporates an I/O interface for exchanging data.

Identification Tag

Identification Tag (ID Tag): an integrated circuit (IC) with unique features (digital fingerprint) which implements an authentication protocol and incorporates an I/O interface for exchanging data.

ID Tags can be a viable solution to the problem of conferring an identity to product items that must be traced: they can be temporarily coupled to them and interact with a tag reader by means of the NFC (or RFID) technology.

Identification Tag

Identification Tag (ID Tag): an integrated circuit (IC) with unique features (digital fingerprint) which implements an authentication protocol and incorporates an I/O interface for exchanging data.

ID Tags can be a viable solution to the problem of conferring an identity to product items that must be traced: they can be temporarily coupled to them and interact with a tag reader by means of the NFC (or RFID) technology.

Physically Unclonable Function (PUF) as entropy source for secure key generations, which represents a low-cost and more secure alternative with respect to the conventional non-volatile memory-based solutions for key storage.

Aim of the Presentation

We show how the identification tag can be coupled with physical objects (product items), conferring them a digital fingerprint within a blockchain-based supply chain scenario for traceability and anti-counterfeiting of products. In particular, we illustrate how the identification tag presented here can be employed to confer identity to a product item to be tracked along its supply chain.

Aim of the Presentation

We show how the identification tag can be coupled with physical objects (product items), conferring them a digital fingerprint within a blockchain-based supply chain scenario for traceability and anti-counterfeiting of products. In particular, we illustrate how the identification tag presented here can be employed to confer identity to a product item to be tracked along its supply chain.

We describe all phases of the supply chain management process by means of the BPMN standard, in particular we use choreography diagrams to model the interactions among all entities involved in the supply chain management in terms of exchanging messages, including those that interface with the blockchain infrastructure.

Outline

A PUF-Based ID Tag

- A PUF-based, memory-less, integrated circuit for identification tags which implements an ECC-based, one-way authentication protocol, and offers numerous advantages over other state-of-the-art solutions.

A PUF-Based ID Tag

- A PUF-based, memory-less, integrated circuit for identification tags which implements an ECC-based, one-way authentication protocol, and offers numerous advantages over other state-of-the-art solutions.
- Novel highly-stable PUF model: very small chip area, adoption of a lightweight fault tolerance mechanism without recovery data and production of unpredictable and uncorrelated true random numbers.

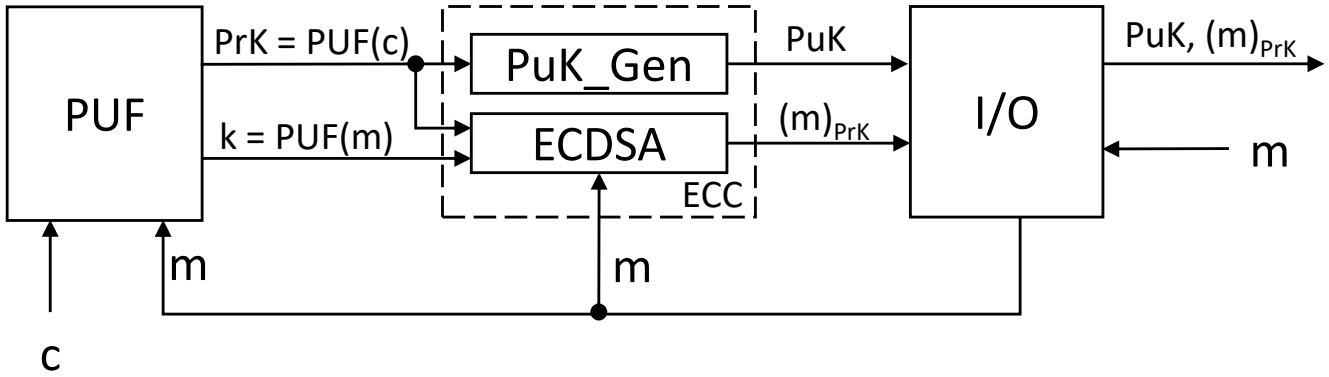
A PUF-Based ID Tag

- A PUF-based, memory-less, integrated circuit for identification tags which implements an ECC-based, one-way authentication protocol, and offers numerous advantages over other state-of-the-art solutions.
- Novel highly-stable PUF model: very small chip area, adoption of a lightweight fault tolerance mechanism without recovery data and production of unpredictable and uncorrelated true random numbers.
- The authentication protocol works without the use of any memory or shared secret, and features message authentication services, thus allowing proof-of-identity authentication of tagged objects.

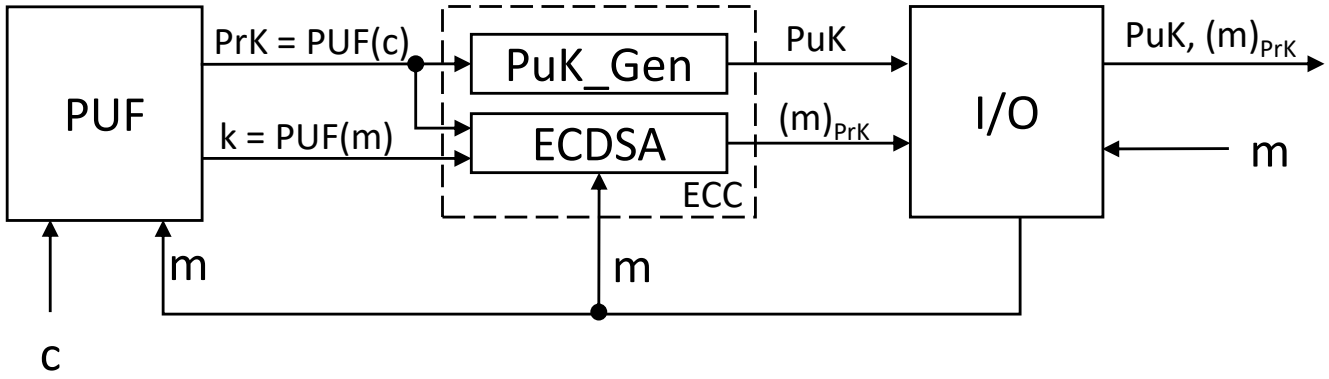
A PUF-Based ID Tag

- A PUF-based, memory-less, integrated circuit for identification tags which implements an ECC-based, one-way authentication protocol, and offers numerous advantages over other state-of-the-art solutions.
- Novel highly-stable PUF model: very small chip area, adoption of a lightweight fault tolerance mechanism without recovery data and production of unpredictable and uncorrelated true random numbers.
- The authentication protocol works without the use of any memory or shared secret, and features message authentication services, thus allowing proof-of-identity authentication of tagged objects.
- Signature verification is supported at the verifier side only.

High-level tag architecture

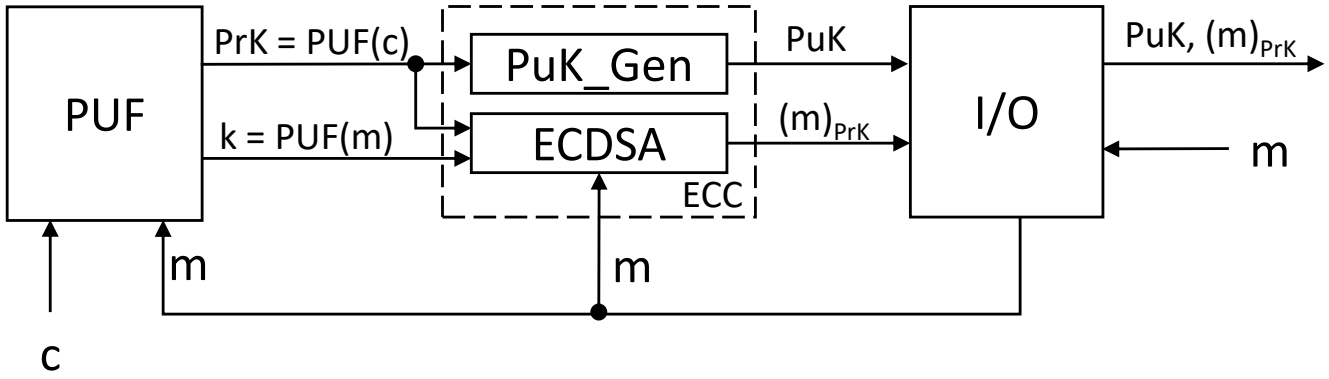


High-level tag architecture



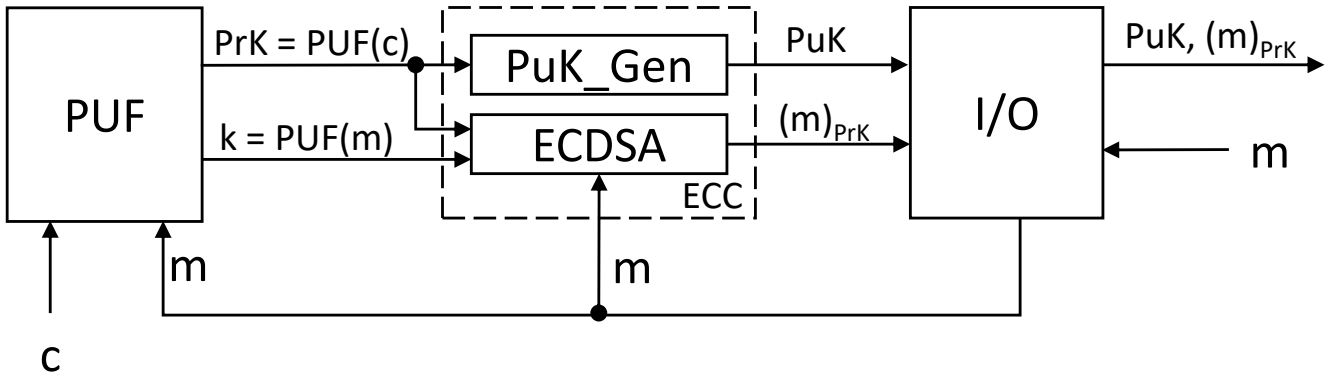
- The tag architecture consists of three ad-hoc designed hardware components: the PUF, the Elliptic Curve Cryptography (ECC) component, and the Input/Output interface (I=O).

High-level tag architecture



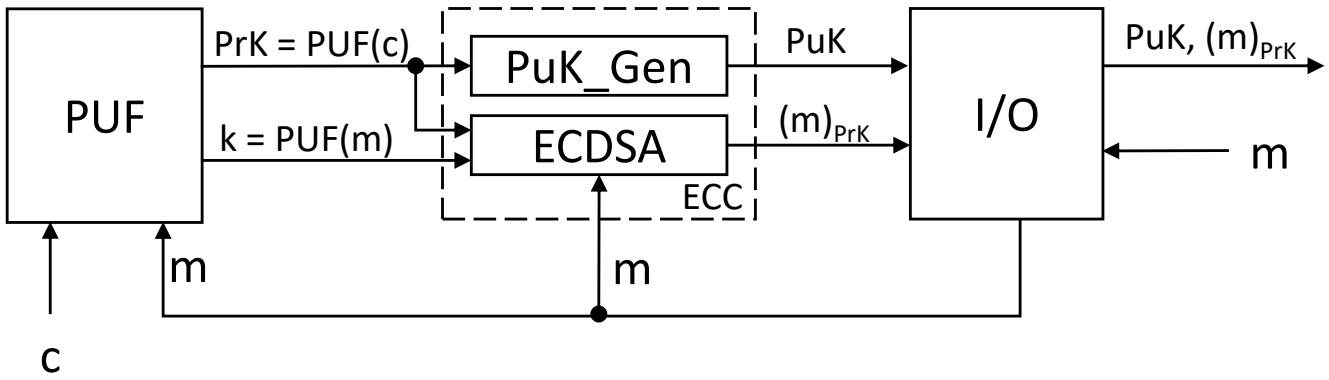
- The tag architecture consists of three ad-hoc designed hardware components: the PUF, the Elliptic Curve Cryptography (ECC) component, and the Input/Output interface (I=O).
- The PUF is used to deterministically generate the tag's private key PrK using a hardwired challenge c, and a nonce k.

High-level tag architecture



The NFC-compliant I=O component, with a bus width of 1024 bits, has two goals:

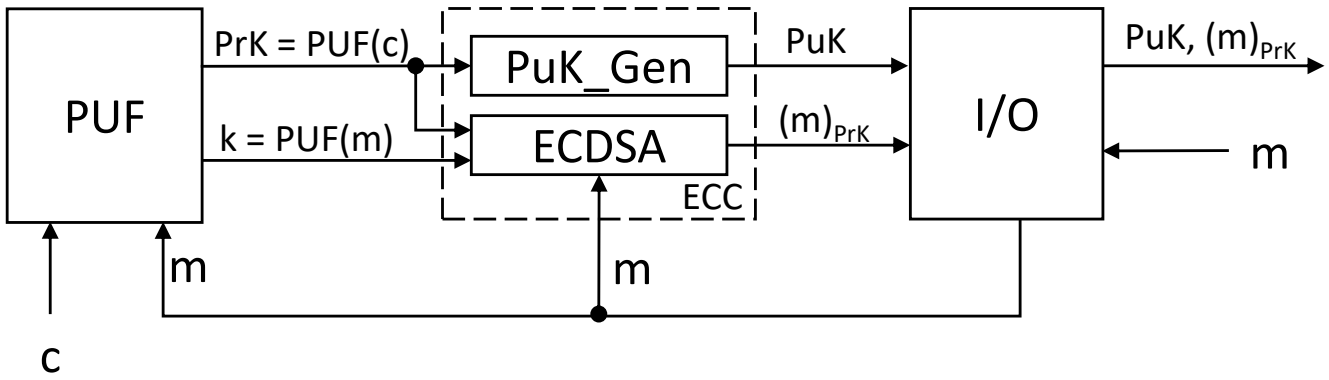
High-level tag architecture



The NFC-compliant I=O component, with a bus width of 1024 bits, has two goals:

- To enable plain text message input reception (256 bits maximum) and signed message and public key output transfer (1024 bits maximum).

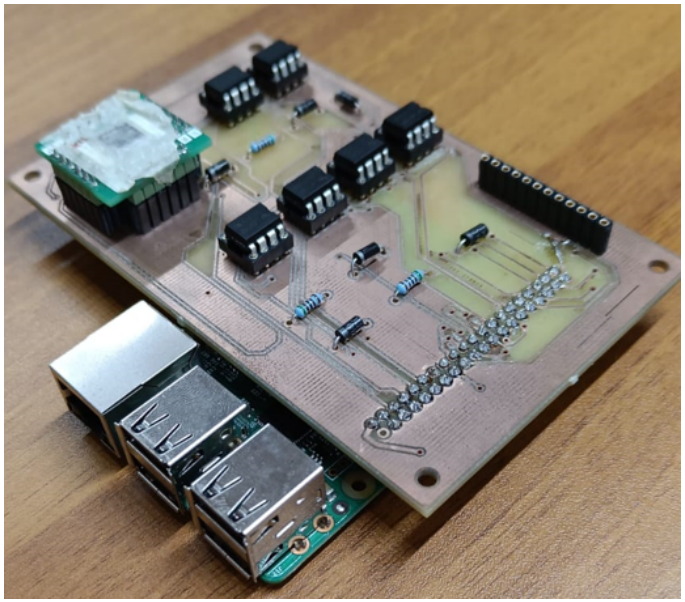
High-level tag architecture



The NFC-compliant I=O component, with a bus width of 1024 bits, has two goals:

- To enable plain text message input reception (256 bits maximum) and signed message and public key output transfer (1024 bits maximum).
- To supply power to the identification tag, being it passive in itself.

ID Tag Prototype



The PUF itself is ad-hoc hardware, fabricated through the EUROPRACTICE Consortium, connected to a Raspberry Pi board by means of a signal-levelling custom interfacing printed circuit, connected to the expansion pins. We leverage the board's already available software substrate for the other components.

Outline

ID Tag and Blockchain for supply chain management

- ID Tag can be effectively employed in a blockchain-based application for supply chain management. Blockchain and ID Tag are combined to provide a supply chain framework for traceability and anti-counterfeiting of products

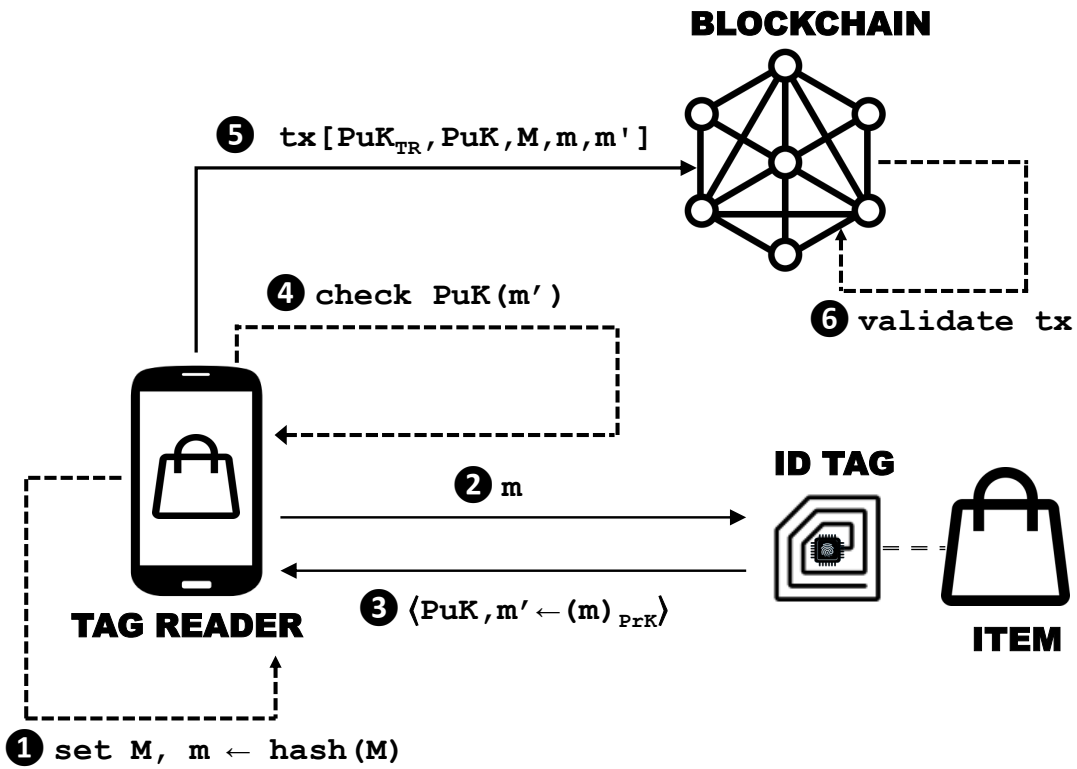
ID Tag and Blockchain for supply chain management

- ID Tag can be effectively employed in a blockchain-based application for supply chain management. Blockchain and ID Tag are combined to provide a supply chain framework for traceability and anti-counterfeiting of products
- During an enrollment phase, a product item is coupled with a tag to make the product anchored to a robust, trustworthy identifier

ID Tag and Blockchain for supply chain management

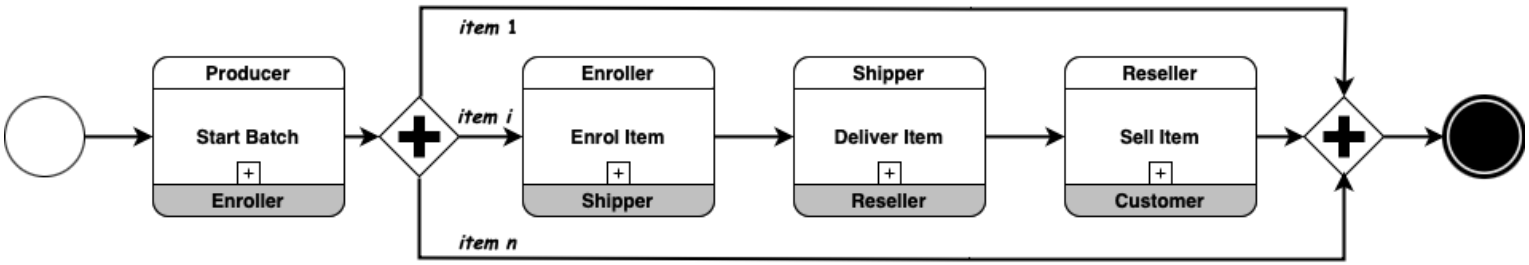
- ID Tag can be effectively employed in a blockchain-based application for supply chain management. Blockchain and ID Tag are combined to provide a supply chain framework for traceability and anti-counterfeiting of products
- During an enrollment phase, a product item is coupled with a tag to make the product anchored to a robust, trustworthy identifier
- The item is then traced by means of other tag readers in the various phases along the entire supply chain. Readers collect relevant information about the phase into a transaction that is sent to the blockchain to be validated by a suitable smart contract checking the status of product distribution, thus enabling supply chain actors (e.g., producer, distributor, and consumer) to track and trace their entire production and delivery

A generic authentication phase for supply chain management



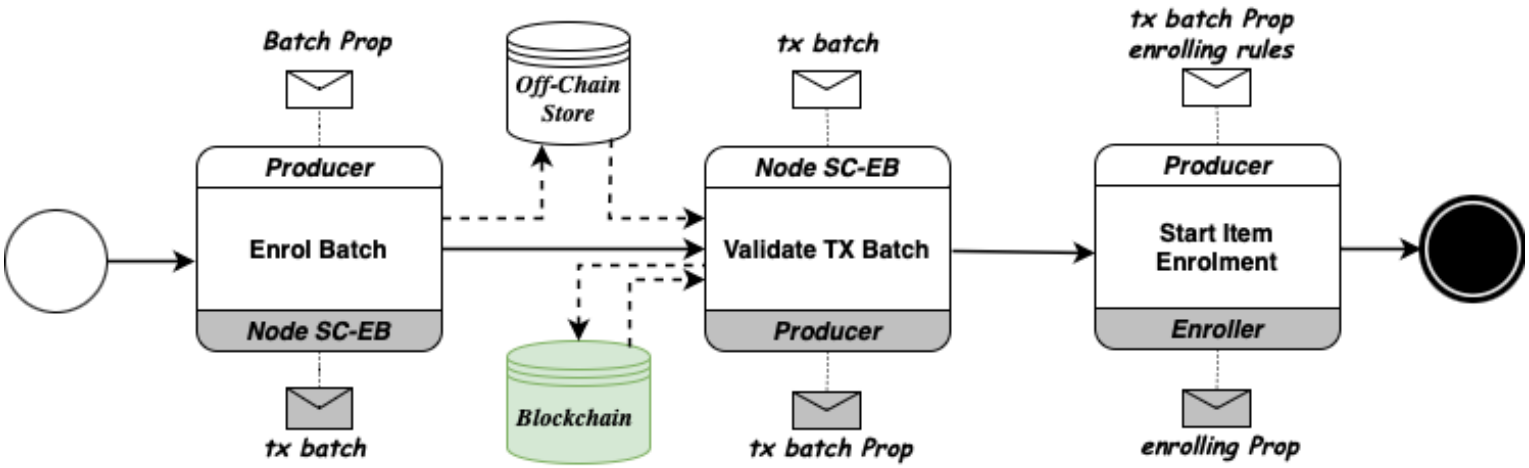
The figure describes the steps of a generic phase in the blockchain application scenario.

Overall supply chain process



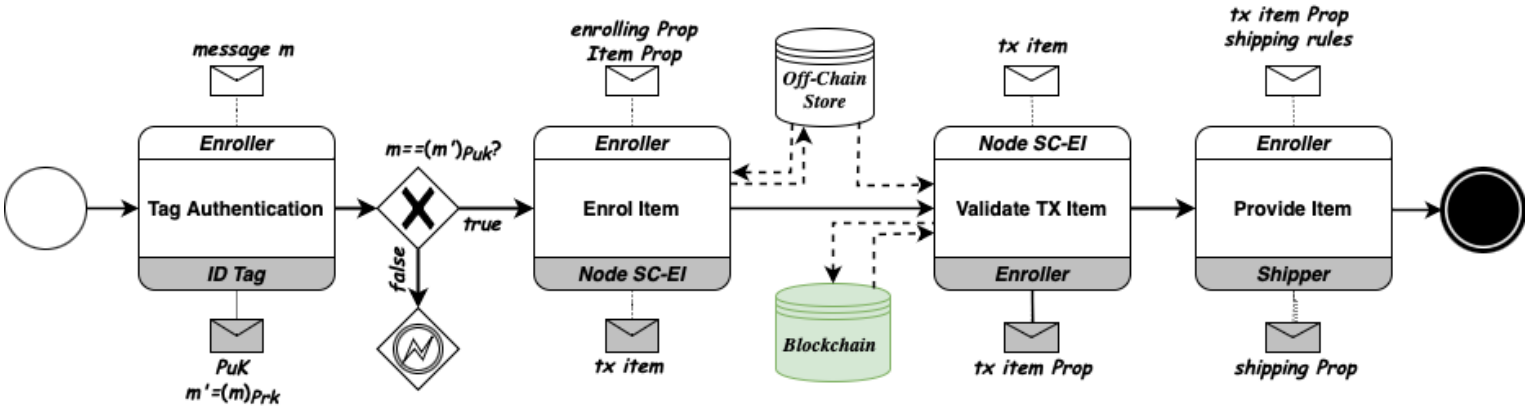
The figure describes the overall process. The reference context is a company of luxury products (items) that are packaged in batch of n items.

Enrolling a batch of items



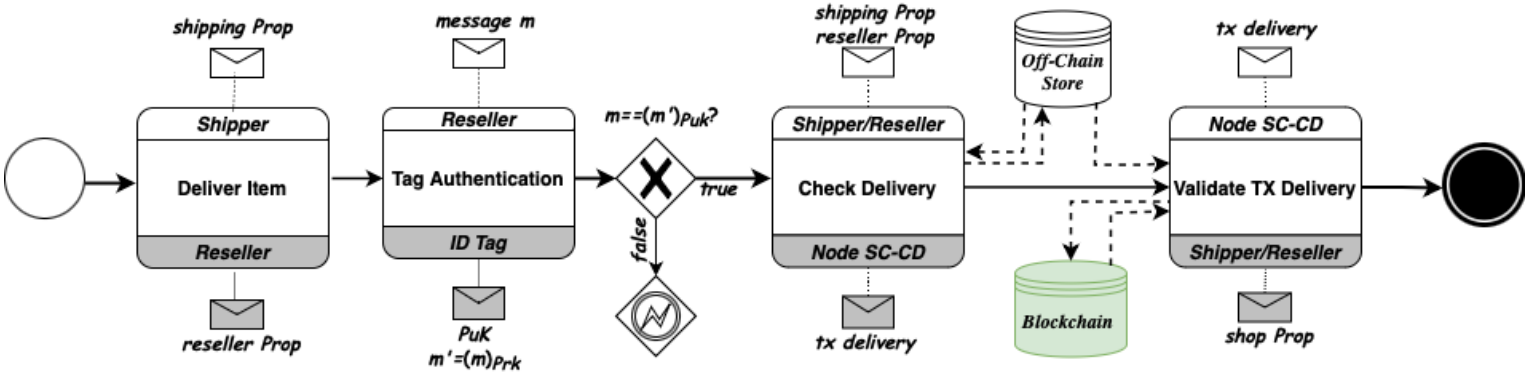
The Producer stores the main batch properties in a repository (called *O -Chain Store*) and registers the batch enrolment as a blockchain transaction. With a little abuse of BPMN notation, the interaction with the blockchain is represented by including an entity called *Node SC-EB* that is in charge of interfacing an ad-hoc Smart Contract (SC) to enrol a batch (EB).

Enrolling an item



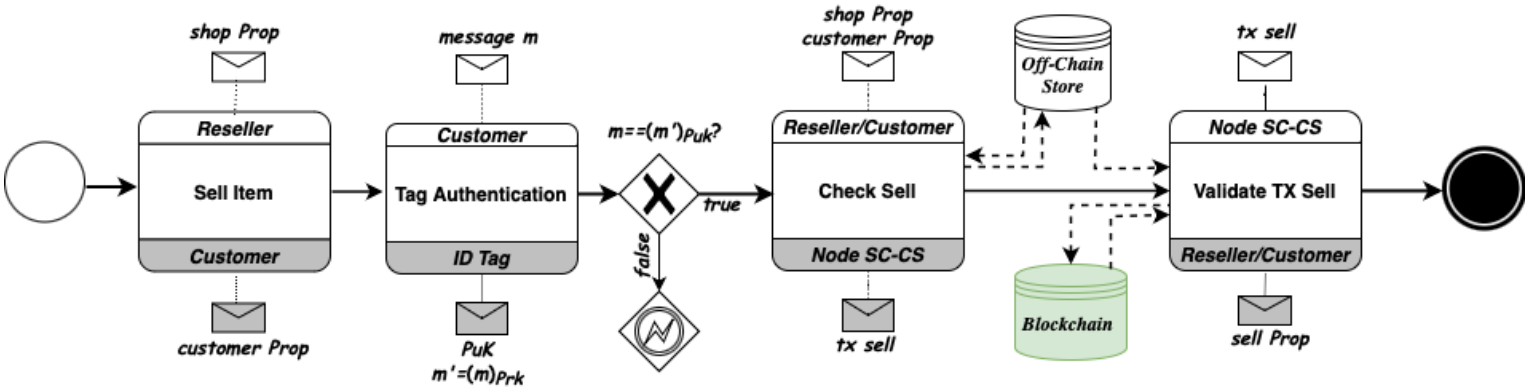
After having successfully authenticated the ID Tag associated to a batch item, the specific product properties (e.g., pictures or video of it) are stored in the Off-Chain Store, the transaction for the item enrolment (including the ID Tag public key *PuK* and the hash of relevant off-chain data) is registered on the blockchain and, then, the item is entrusted for the delivery to a shipper – for simplicity, the two participants are assumed to belong to the same company.

Delivering an item



The main task is *Check Delivery*: after ID Tag authentication, the Reseller is required to recognize the features characterizing the item that have been stored in the repository with hash registered in the blockchain – a simple solution is an ad-hoc app displaying pictures or videos, with potential Machine Learning use as an improvement to be investigated further. The Shipper is also included as initiating participant to express the fact that the transaction must be signed by both Shipper and Reseller.

Selling an item



The figure describes the selling item sub-process, which is similar to delivering item sub-process. The main difference is in the task *Check Sell*, for which multi-signed blockchain transactions should be avoided for the customer's (and business' as well) sake. The customer acknowledgment for the transaction is to be differently registered - also this issue is to be further investigated.

Outline

Main Results

An identification tag architecture, immune to tag cloning and modification attacks, and how it can be employed to confer identity to a product item to be tracked along its supply chain. The tag acts as a possession factor that only the object must have, or have access to, in order to perform authentication.

Main Results

An identification tag architecture, immune to tag cloning and modification attacks, and how it can be employed to confer identity to a product item to be tracked along its supply chain. The tag acts as a possession factor that only the object must have, or have access to, in order to perform authentication.

All phases of the supply chain management process by means of the BPMN standard, in particular we use choreography diagrams to model the interactions among all entities involved in the supply chain management in terms of exchanging messages, including those that interface with the blockchain infrastructure.

Further Work

Advanced machine learning techniques have been proposed as countermeasures against the re-application attack, i.e., a tag stolen and used by an object other than the one used in the enrolment phase.

Further Work

Advanced machine learning techniques have been proposed as countermeasures against the re-application attack, i.e., a tag stolen and used by an object other than the one used in the enrolment phase.

In particular, two architectures based on deep convolutional neural networks and adversarial machine learning have been proposed, which cover two different scenarios based on whether the products of interest represent an item in a batch of similar products, or vice-versa, a unique object with its own characteristics.

Thank you for your attention.