Whitepaper

SEALSQ Provisioning Secure Semiconductors with NFTs

Contents

About SEAL SQ

WISeKey is a pure play cybersecurity company, with over 20 years of experience in providing digital trust and cryptographic protection. WISeKey delivers secure semiconductors, digital certificates, digital IDs, as well as SaaS platforms for proof-of-provenance, lifecycle management and blockchain-driven traceability. WISeKey customers are typically IoT vendors servicing smart buildings, smart cities, smart agriculture, drones, health care monitoring, logistics and Industry 4.0. WISeKey has even been able to successfully extend its Trust model to non-connected objects. Such objects connect through NFC or a plug when needed, and include luxury goods, health care consumables, appliance accessories, cold crypto wallets, and pieces of art.

WISeKey's certificate Authorities, Security Brokers, management systems and tamper resistant secure microcontrollers are regularly audited and accredited with highest grade WebTrust, Common Criteria (CC) and FIPS certifications.

Abstract

The value of physical objects is enhanced by creating an NFT for the digital twin on the Blockchain. The hybrid physical digital object's value is a combination of the intrinsic value of the physical object and the value of the Blockchain's immutable ledger and authenticity.

In the physical world there are assets that have intrinsic value like currency, luxury goods, and artwork. The value of physical items is well known. Digital assets are also valuable, but digital assets are easily duplicated and shared. MP3s were some of the first digital assets to be duplicated and shared. Duplication reduces the value of the digital asset.

In the digital world the Blockchain has enabled the digital assets to hold value and prevent counterfeiting. Bitcoin and digital currency pioneered the underlying Blockchain technology to enable digital assets to retain value and solve the "double spend problem". Bitcoin is structured with tokens that are "Fungible", meaning that they are identical and interchangeable. Fungibility is an essential property of any currency or cryptocurrency.

The Blockchain also enables the creation of digital assets that are unique, or "Non Fungible" through the use of "Non Fungible Tokens" (NFTs). These NFTs may be unique digital assets or linked to physical products. The value of NFTs is based on the fact that they are unique digital objects that can be owned by a Blockchain account. NFTs can be linked to existing physical objects like artwork and real estate. The NFT can also be created during the manufacture of hybrid products like electronics and consumer merchandise.

We will be exploring the physical manifestations of NFTs and showing how linking the NFT to a secure semiconductor enhances and compliments the physical value of the item and the digital value of the NFT.

ERC-1155

ERC 1155

Blockchain & NFT Overview

Blockchain Overview

Cryptocurrencies are a recent entry to the digital landscape. The cryptocurrency coins are Blockchain tokens where the integrity of the tokens use cryptographic properties. The token immutability and traceability rely on the distributed ledger. The distributed ledger solves the "double spend problem". The fundamental value of cryptocurrency is based on trust in the Blockchain properties of immutability, traceability, and integrity.

Another notable property of crypto coins is that they are interchangeable, or "fungible". Fungible is defined as "able to replace or be replaced by another identical item; mutually interchangeable". Just like US currency, every dollar has the same value and can be spent interchangeably. It doesn't matter if you have dimes, bills, or pay with a credit card. All dollars are interchangeable. Crypto coins are fungible tokens on the Blockchain.

Non-Fungible-Tokens (NFTs) are unique and cannot be interchanged. They are unique digital assets that cannot be duplicated once minted. Like unique physical assets, NFT are unique digital assets that can be owned, bought, and sold. NFTs on the Blockchain essentially recreate the familiar physical market of buying and selling for digital assets.

NFT Standards

There are many different blockchains that support NFTs, also known as "deeds". In order for NFTs to traded across many different Blockchains and distributed ledgers, there must be a standard definition. NFTs are therefore stored in a format that does not depend on the specific Ethereum compatible Blockchain it will be traded on. This enables open NFT marketplaces that use the standards described below.

ERC-721

ERC-721 is a token standard on the Ethereum blockchain that defines an API for NFTs within smart contracts. This standard provides basic functionality to track and transfer NFTs in a reliable and predictable way. The standard supports physical property like artwork and real estate, as well as digital assets like images, video, and animations. ERC 721 has become the defacto standard definition for NFTs.

More information can be found at this link: https://eips.ethereum.org/EIPS/eip-721

The ERC 1155 standard outlines a smart contract interface that can represent any number of fungible and non-fungible token types. While the ERC-721 standard's token ID is a single non-fungible index and the group of these non-fungibles is deployed as a single contract with settings for the entire collection. In contrast, the ERC-1155 Multi Token Standard allows for each token ID to represent a new configurable token type, which may have its own metadata, supply and other attributes. NFT marketplaces use this standard to minimize the impact on the network and save on transaction fees.

More information can be found at this link: https://eips.ethereum.org/EIPS/eip-1155

NFT Value

For an NFT that started as a physical object or "Digital Twin", the owner's credentials, ownership history, expert appraisals, and notarization of authenticity will be used to establish the NFT's value. The medium of the digitization and the smart contracts are also contributing factors to the value of digital twins

Digital Certificates for NFTs

A significant contributor for added value is to require a cryptographically signed certificate from a certifying authority.

The certified origin of the NFT becomes vitally important in determining the value. Just as biometric authentication paired with a password is more secure than either one individually, the second factor of a certificate introduced in the process of minting the NFT can add value and integrity to the NFT.

For example, an NFT that has a certificate that it is an original Picasso with a certified owner, can have a higher value than one that only claims to be a Picasso without the certification of the artwork or owner.

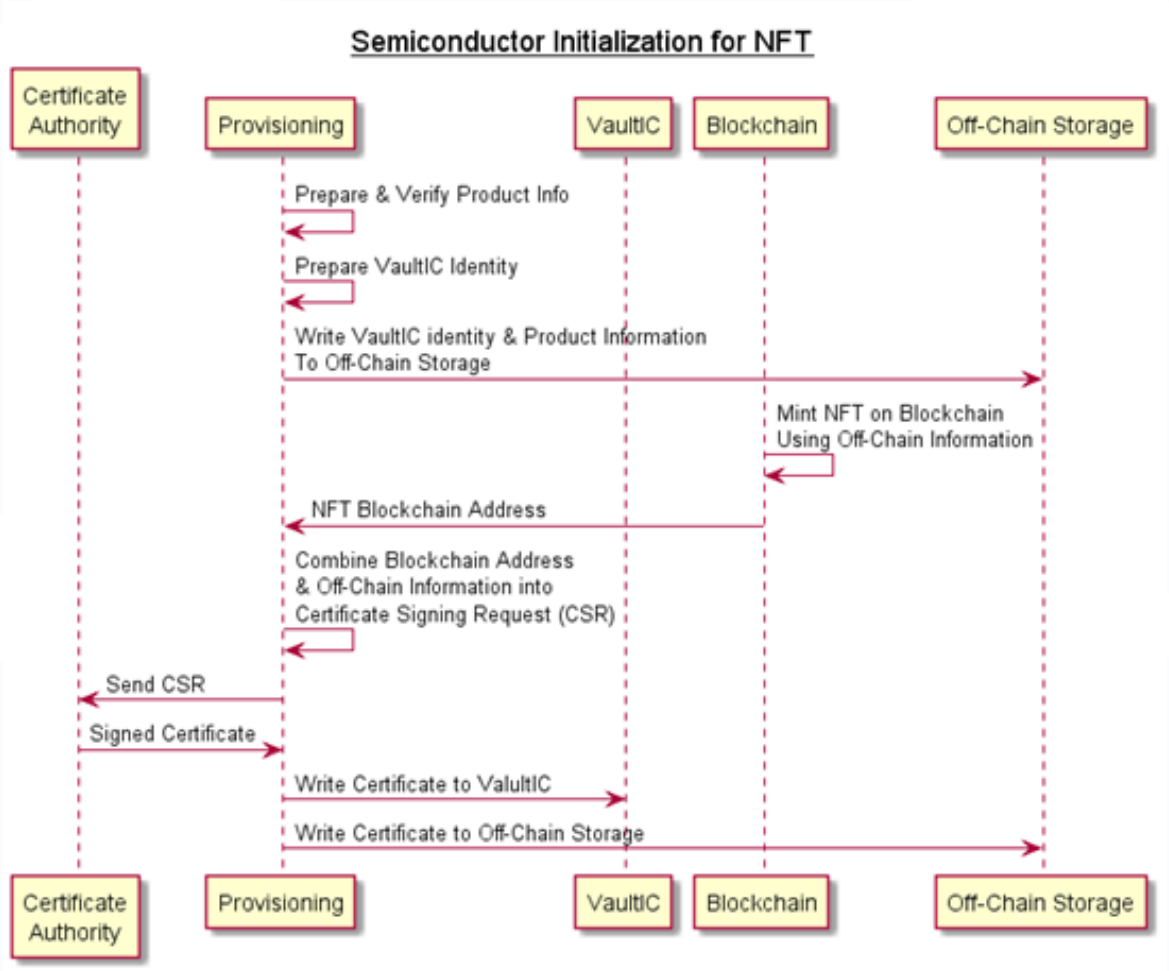
Immutability & Historic Value

As the NFT continues its digital life, the ownership can change multiple times. Each time the ownership changes, the record of previous owners, will can remain as permanent record on the Blockchain. In this way the ownership history will also be a contributing factor for the value NFTs.

Provisioning Process

Creating a hybrid physical-digital identity that is linked to the Blockchain involves cryptographically relating a physical identity to the Blockchain identity. This combination of secure identities provides the assurance, reliability, longevity, and immutability that is required to for both the NFT and the physical item to retain long term value.

The sequence of event shown below is representative of the process that takes place during provisioning. This process relates a PKI certificate with the essential elements of the NFT's identity on the Blockchain. It then provisions that certificate into a secure semiconductor.



Steps for provisioning.

1. First verify that the product that the NFT will be created for. This is an essential step to ensure the resulting NFT retains its provenance, authenticity, and long term value.

2. Next the identity of the secure VaultIC semiconductor is established. This identity is in the form a unique public private key pair that is embedded in the secure VaultIC semiconductor.

3. The resulting product information is combined into a patent pending format that ensures the that the resulting NFT is not corrupted, incomplete, or ambiguous. This structure is written to Off Chain Storage since it can be detailed and consist of a large amount of data.

4. The NFT is then created (also referred to as “minting”).

5. After the minting process, the NFT has a specific address on the Blockchain. This address is returned to the provisioning server.

6. The provisioning server then combines the Blockchain address with the VaultIC identity and the product information to create a Certificate Signing Request (CSR)

7. The CSR is signed by a certificate authority using the INeS Certificate Management Service. The end result is a valid certificate that cryptographically links the Blockchain NFT with the physical product.

8. The certificate is written back to the secure VaultIC semiconductor and the Off Chain Storage

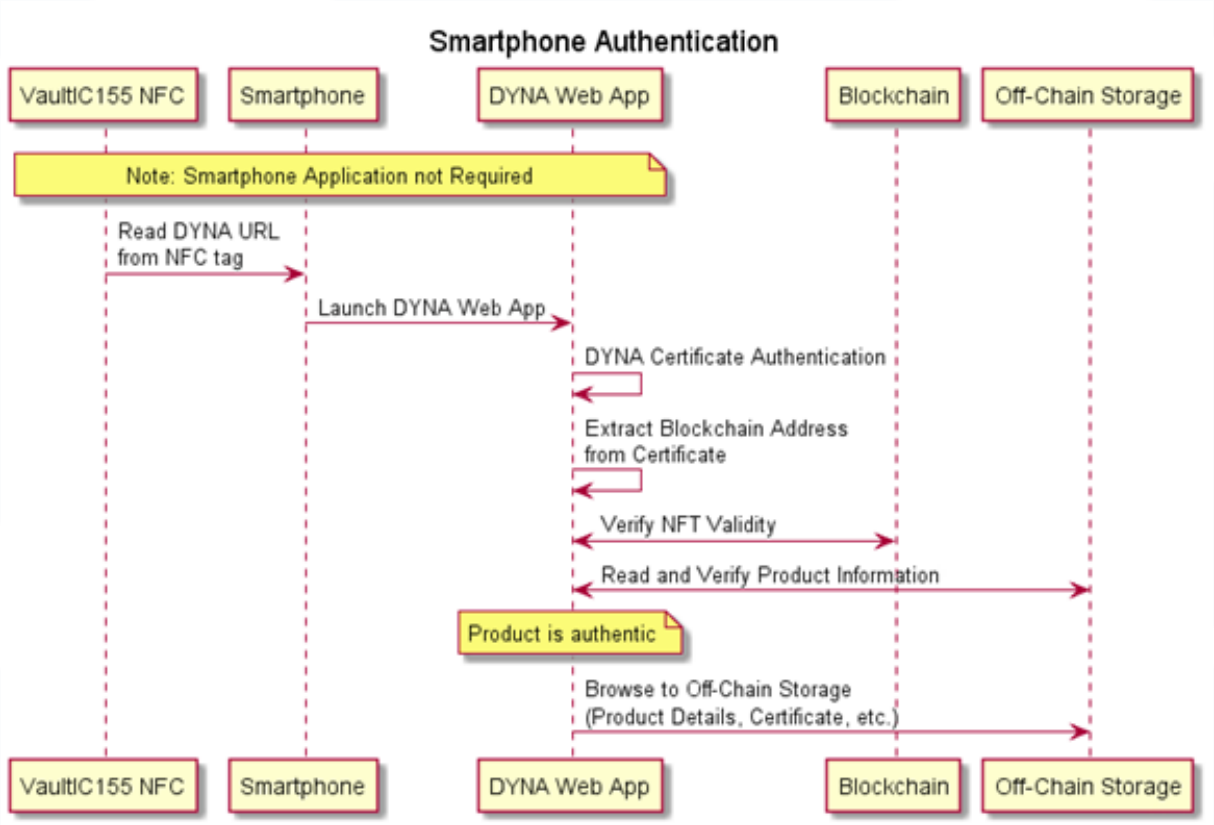
The end result is a physical item that is contains two immutable identities that are cryptographically linked, one from the secure semiconductor and it’s PKI certificate, the other from the Blockchain.

The process of provisioning a secure VaultIC semiconductor can be accomplished both with a contact version and with the wireless NFC version. The contact version of the VaultIC will be soldered onto a circuit board then used for embedded verification. The wireless NFC version of the VaultIC can be verified using any NFC wireless reader, including iPhone and Android smartphones.

NFT Verification

The process of provisioning and verifying can be accomplished both with a contact version and a wireless NFC version of the secure VaultIC semiconductor. The verification below will focus on the secure VaultIC 155 NFC device verified with a smartphone.

The sequence below uses the proprietary DYNA authentication technique available on the VaultIC 155 NFC tag. This technique enables a single tap read of the tag and does not require a smartphone application. Using the DYNA authentication technique simplifies the verification of both the VaultIC 155 and Blockchain identities.



Steps for Verification:

1. The Smartphone reads the DYNA URL from the VaultIC 155 tag. The DYNA URL includes the VaultIC 155 Certificate

2. The Smartphone browses to the DYNA Web App using any browser that is available

3. The DYNA Web App verifies the VaultIC 155 identity

4. The DYNA Web App extracts the Blockchain Address from the VaultIC 155 certificate

5. The DYNA Web App verifies the Blockchain identity and determines the location of the Off Chain Storage

6. The DYNA Web App reads the Off Chain Storage and verifies that the VaultIC 155 identity is paired with this NFT

7. The product has now undergone Multi Factor Authentication (MFA) and can be declared authentic

   a. For the PKI verification of the VaultIC identity
   b.For the Blockchain Identity
   c.For the association of the identities

8. The DYNA Web App can now redirect to the off-chain storage

The DYNA authentication technique is only one of the possible sequences to authenticate the NFT. All of the possible techniques for verifying the NFT will include the following elements:

1. Verify the PKI chain of the NFT certificate

2. Verify possession of the VaultIC identity private key \

3. Verify the Blockchain identity

4. Verify that the NFT information is associated with the VaultIC identity

When each of these elements is in place and have been verified, the NFT and product will have the enhanced value of being a hybrid digital physical NFT

Use Cases

Among the different use cases for linking secure semiconductors to NFT information are linking existing physical objects such as artwork, linking electronics to NFTs during manufacturing such as consumer electronics, and tracking products throughout their Manufacture Shipping End Use lifecycle.

For each of these use cases, having a hybrid digital physical product means that it exists both in the physical world and the metaverse. Its value is can be increased based on its multi universe existence.

WISeArt NFT

The hybrid NFT has a natural application in WISeArt. The NFTs in the WISeArt marketplace are the digital twins of the previously existing artwork that they represent. It is essential that the provenance, copy rights, authenticity, and immutability are well established at the time of minting. Going through the process of provisioning a VaultIC 155 NFC tag will ensure that the artwork is authenticatable and will retain its value.

This process will not only enable the NFT to retain its value, but also allow for authentication of the physical artwork when you have possession of it.

Brand Protection

When a product is manufactured, part of the value is in the brand reputation that manufactured it. When that brand is compromised by a counterfeit product, the whole brand suffers and is devalued.

When using a VaultIC secure semiconductor during manufacturing and linking to an NFT allows it to be tracked throughout the product lifecycle. The materials and process can be tracked back to their origin and the manufacturing location and processes can be immutably captured on the Blockchain. As the product changes possession during shipping and logistics, each step can be captured.

The end result is that between the Blockchain records on the distributed ledger and the secure semiconductor, counterfeiting the product becomes virtually impossible. The transactions are immediately transparent, immutable, and impossible to change.

Conclusion and Key Takeaways

The value of physical objects is enhanced by creating an NFT for the digital twin on the Blockchain. The hybrid digital physical object's value is a combination of the intrinsic value of the physical object and the value of the Blockchain's immutable ledger and authenticity. Having the digital Blockchain and the physical PKI identities mutually linked gives an assurance of authenticity in the same way that Mult Factor Authentication increases the security for personal identities.

WISeKey's VaultIC semiconductors, secure provisioning, and INeS PKI technologies compliment each other to provide authenticity for many use cases including existing physical products like artwork and products that begin their existence simultaneously in the metaverse and the physical world.

Acronyms and abbreviations

API	Application Programing Interface
CA	Certification Authority, entity that signs digital certificates
CC	Common Criteria
CMS	Certificate Management System
CSR	Certificate Signing Request
EAL	Evaluation Assurance Level Used with CC certification to specify the level of verification (e.g. CC EAL5+)
ECC	Elliptic Curve Cryptography, a public Key cryptography algorithm
ECDH	Elliptic-curve Diffie–Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
ECR	Ethereum Request for Comments
FIPS	Federal Information Processing Standard
ICA	Issuing Certificate Authority
ID	Identity
IoT	Internet of Things
IP	Intellectual Property
MFA	Multi-Factor Authentication
NFC	Near-Field Communication
NFT	Non-Fungible Token
NIST	National Institute of Standards and Technology
OISTE	Organization for the Security of Electronic Transactions https://oiste.org/
PKI	Public Key Infrastructure https://en.wikipedia.org/wiki/Public_key_infrastructure
ROT	Root of Trust. The foundation for cryptography.
SaaS	Software as a Service
SE	Secure Element
SHA	Secure Hash Algorithm
SSL	Secure Sockets Layer. Secure transportation protocol replaced by TLS
TLS	Transport Layer Security. A secure transportation protocol
WiFi	Wireless Fidelity

References

[NIST] NIST SP 800-90B: Recommendation for the Entropy Sources Used for Random Bit Generation, January 2018

[FIPS] NIST FIPS 140-3: Security Requirements for Cryptographic Modules, March 2019

[CC] CC:2022 Release 1

[VIC408] WISeKey: VaultIC 408 Summary Datasheet, March 2022

[VIC292] WISeKey: VaultIC 292 Summary Datasheet, xxx 2022

[AWS] Device Manufacturing and Provisioning with X.509 Certificates in AWS IoT Core

[AppNote] WISeKey: Secure IoT Device to Cloud Solution

Disclaimer

Information in this document is not intended to be legally binding. WISeKey products are sold subject to WISeKey Terms and Conditions of Sale or the provisions of any agreements entered into and executed by WISeKey and the customer.

The products identified and/or described herein may be protected by one or more of the patents and/or patent applications listed in related datasheets, such document being available on request under specific conditions. Additional patents or patent applications may also apply depending on geographic regions.

For more information, visit www.wisekey.com

Release date: December 2022

Contacts

SEAL SQ SA
Avenue Louis-Casaï 58
1216 Cointrin
Switzerland
Tel: +41 22 594 3000
Fax: +41 22 594 3001
SEAL SQ Semiconductors
Arteparc Bachasson • Bât A
Rue de la carrière de Bachasson
13590 Meyreuil • France
Tel : +33 (0)4 42 370 370
Fax : +33 (0)4 42 370 024

Email: sales@SEAL SQ.com
Stay connected with @SEAL SQ