WISeCOIN

INFORMATION MEMORANDUM

April 2019

V 1.5

TABLE OF CONTENTS

ACRONYMS

AES	Advanced Encryption Standard
API	Application programming Interface
CA	Certificate Authority, entity that issues digital certificates
CCTV	Closed Circuit Television
CMS	Certificate Management System
DDOS	Distributed Denial of Service
EAL	Evaluation Assurance Level
ECC	Elliptic Curve Cryptography: is an approach to public-key cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
FIPS	Federal Information Processing Standard
HD	High Definition
HDCCTV	High Definition Closed Circuit Television
IoT	Internet of Things
mPKI	Managed PKI
NATO	North Atlantic Treaty Organization
NIST	National Institute of Standards and Technology
OISTE	Organization for the Security of Electronic Transaction https://oiste.org/
PKI	Public Key Infrastructure
PKCS#11	Public-Key Cryptographic Standard #11 describing the API to cryptographic tokens
SECaaS	Security as a Service
SHA	Secure Hash Algorithm
RoT	Root of Trust
RSA	Rivest, Shamir & Adleman encryption algorithm
SSL	Secure Sockets Layer. Secure transportation protocol replaced by TLS
TLS	Transport Layer Security. A secure transportation protocol
UN	United Nations

01 INTRODUCTION

01 INTRODUCTION

WiseCoin AG was established to secure the Blockchain and the Internet of Things (IoT) world, which is increasing in complexity and becoming more prone to cyber threats.

WiseCoin AG does this through two core service offerings:

I. WISeCoin: a new and innovative tokenized service model for authenticating people, products and machines to secure the IoT by preventing unauthorized third-party interactions.

II. WiseBlock: a service built upon our unparalleled expertise in cybersecurity to provide tailored end-to-end Blockchain solutions for organizations wanting to innovate and increase efficiency within safe and trusted technological environments.

To scale the operations, WISeCoin AG is offering the WISeSecurity token (abbreviation: WCN) to raise capital through a private sale and later through the ICO (public sale).

As an innovative, security focused Blockchain solutions provider with a very unique value proposition, WISeCoin AG has decided to invite a select group of strategic partners to participate in a private offering that will be followed by an ICO.

From an investor's point of view, both investment vehicles are highly attractive. Joining the early private sale offers an oppotunity for investors to participate in the venture's growth and strategic participation in mutually beneficial developments. By joining the tokenized equity capital, investors can trade over-the-counter directly on a secondary security token exchange benefiting from more exit options and broader exposure.

WISeCoin's ICO will target a global and highly diversified investor base and thus also increase the company's exposure among potential customers and strategic partners.

With a clear focus on cybersecurity, our mission is to enable the safe, trusted daily use of 4th industrial revolution technologies in the sectors of Internet of Things and Blockchain.

02 ABOUT WISECOIN AG

02 ABOUT WISECOIN AG

WISeCoin AG is a Swiss company dedicated to ensure that connected devices and 'things' are authenticated, validated and secure. It is a subsidiary company of WISeKey International Holding AG, a leading global cybersecurity company quoted on the Swiss Stock Exchange (SIX) since 2016. WiseCoin AG is wholly-owned by WISeKey (90% ownership) and the OISTE foundation (10%). WISeCoin AG benefits from the WISekey architecture as the first and only vertically integrated platform combining proprietary cybersecurity software and secure microcontroller for the Internet of Things ("IoT") to protect connected devices against persistent and evolving cyber threats.

Our integrated Vertical Trusted Platform combines a range of microchips with software applications that cater to our customer's specific business and security needs. The software solution is driven by proprietary technology, such as Root of Trust ("RoT") and Public Key Infrastructure ("PKI"), that enables our clients to effectively manage their digital identity, information, and communications in a single integrated platform. RoT enables us to secure electronic information through our digital certificate technology. Our PKI services deploy digital certificates used for encryption and creating tamperproof electronic "fingerprints". We enable our clients to adapt to an evolving device landscape without compromising their digital security.

The OISTE foundation created in Geneva in 1998 is a not-for-profit organization regulated by article 80 et seq. of the Swiss Civil Code. OISTE has proprietary rights upon the cryptographic Root of Trust ("RoT) that allows robust digital certification of persons and objects and WISeKey was chosen by the foundation to be the operator of it. The two entities (OISTE and WISeKey) are bound by a defined Trust Framework and Certification Practice Statement (CPS).

WISeKey is uniquely positioned to be the first mover in bringing legally enforceable transactions through Smart Contracts, certified by globally recognized SuisseID and EIDAS accreditations, to Blockchain. WISeCoin AG was therefore established to manage all Blockchain initiatives and operations of WISeKey International Holding. WISeKey International Holding has distribution of over 1 billion secure microcontrollers across 3500+ industrial clients which will form the initial basis of the ecosystem being developed.

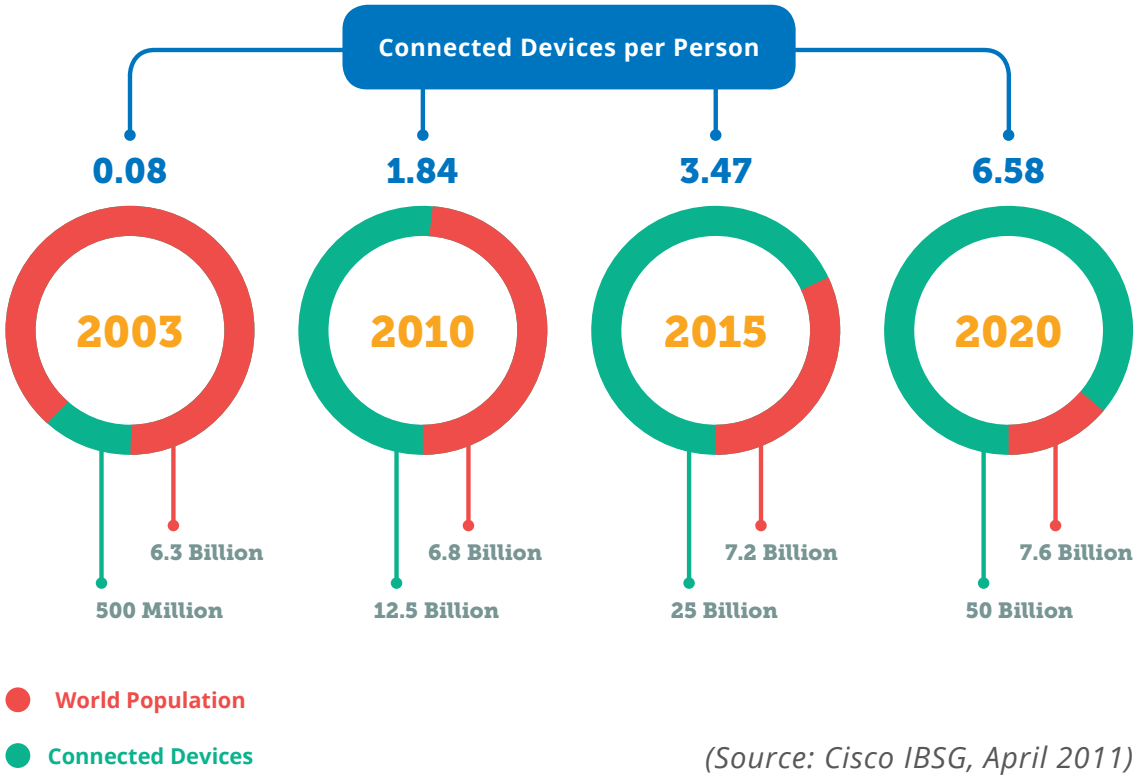
03 BACKGROUND

03 BACKGROUND

3.1 Problematic: Cybersecurity Around IoT and Cryptocurrencies

- **Internet of Things**

The rapid growth and proliferation of internet-connected devices and individuals' increasing dependence on them for personal and business purposes have exposed shortcomings in traditional security solutions. The number of connected objects is projected to increase to 50 billion by 2020[1], representing the 4th industrial revolution that will bring a new era full of technological innovations. However, while the emergence of IoT mostly represents a potential to improve our lives, the increase in its numbers creates opportunities to infiltrate security parameters. In recent years, IoT has fallen victim to several significant cyber-attacks or threats.



(Source: Cisco IBSG, April 2011)

This was evidenced in 2016, when French hosting company OVH suffered the largest distributed denial-of-service ("DDoS") attack in history[2]. The attack was perpetrated through IoT devices, such as connected cameras and personal video recorders. These connected devices are often manufactured with security as an after-thought, or even worse, without any embedded security features, resulting in significant vulnerabilities. As these devices often lack built-in automated firmware updates, these vulnerabilities often go unpatched and updates are neglected. Thus, as the number of connected devices increases, organizations' ability to trust applications and data, and authenticate devices and servers, decreases significantly. Combined with an exponentially increasing attack surface, enterprises are increasingly exposed to malicious cyber threats.

1 Dave Evans, "The Internet of things: How the Next Evolution of the Internet Is Changing Everything". Available at: https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

2 Norton Rose Fulbright, " Legal Implications of DDoS Attacks and the Internet of Things (IoT)". Available at: https://www.dataprotectionreport.com/2016/12/legal-implications-of-ddos-attacks-and-the-internet-of-things-iot/

Additional examples of the increasing cybersecurity risks posed from connected devices:

- *Mirai* (October 2016) – Mirai was a botnet, described as a "zombie army" of internet-connected devices infected with malicious software and controlled as a group without their owners' knowledge, behind a wave of major DDoS attacks[3]. The attack was carried out by infecting poorly secured devices, such as routers and internet-connected security cameras by flooding domain name system ("DNS") provider Dyn. Inadequate security made these devices relatively easy targets for attackers, who constructed a botnet large enough to carry out the largest DDoS attack ever seen and one of the first major IoT-focused attacks.

- *Reaper* (October 2017) – Reaper was a botnet that already penetrated an estimated 1 million devices and 378 million being vulnerable. Unlike Mirai, Reaper does not rely on exploiting devices with simple default credentials; rather, it exploits numerous vulnerabilities in different IoT devices, using sophisticated techniques to hack routers and various smart devices[4]. As cyber threats continue to evolve, data and identity protection will remain paramount for global enterprises.

- In January 2017, several vulnerabilities were found in St. Jude Medical's 465,000 implanted cardiac devices, allowing potential hackers to take control of them and potentially threat user's life[5].

- In July 2015, Chrysler recalled 1.4 million cars to fix their vulnerabilities to hacks once researchers were able to hack a jeep and take control of its functions and movement[6].

Cyber-attacks have become highly sophisticated, posing significant and persistent threats to IoT devices and networks globally. According to the Symantec's 2017 Internet Security Threat Report, there were more than 1,200 security breaches in 2016, resulting in 1.1 billion exposed identities. The report also noted that it takes only 2 minutes for an IoT device to be attacked[7]. Attackers deploy clandestine, advanced, and targeted attacks on less secure bring-your-own-device ("BYOD") or third-party devices to infiltrate broader networks. These attacks can remain inside a network for extended periods of time undetected, most often to steal valuable data, spread malicious malware or sabotage critical infrastructure. According to industry research, the global cybersecurity market is expected to be worth $120 billion in 2017[8]. While enterprises continue to invest billions in security technologies, existing cybersecurity software solutions and IT teams are fragmented and unable to execute a unified threat response.

3 Symantec, "Internet Security Threat Report". Available at: https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf

4 BullGuard, "New Reaper IoT Botnet Leaves 378 Million IoT Devices Potentially Vulnerable to Hacking". Available at: https://www.prnewswire.com/news-releases/new-reaper-iot-botnet-leaves-378-million-iot-devices-potentially-vulnerable-to-hacking-300542019.html

5 Food and Drug Administration, " Firmware Update to Address Cybersecurity Vulnerabilities Identified in Abbott's (formerly St.Jude Medical's) Implantable Cardiac Pacemakers: FDA Safety Communication". Available at: https://www.fda.gov/medicaldevices/safety/alertsandnotices/ucm573669.htm

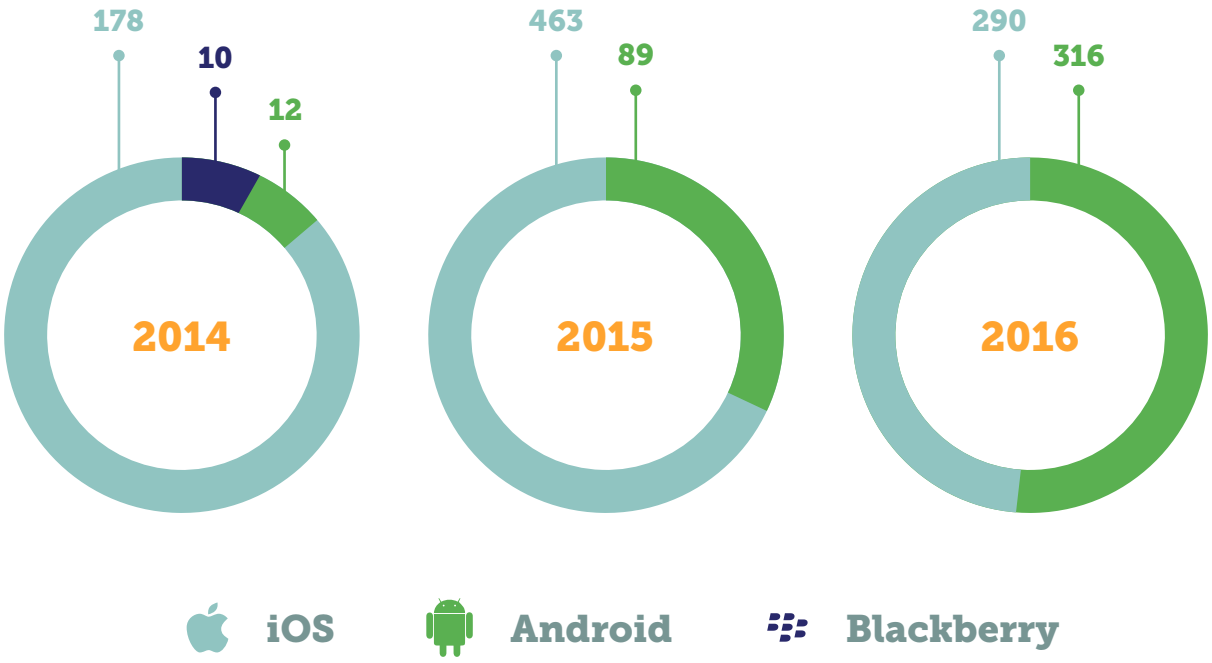
6 BBC News, "Fiat Chrysler recalls 1.4 million cars after Jeep hack". Available at: https://www.bbc.com/news/technology-33650491

7 Symantec, "Internet Security Threat Report". Available at: https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf

8 Info Security Magazine, "Global cybersecurity market to reach $120 billion by 2017". Available at: https://www.infosecurity-magazine.com/news/global-cybersecurity-market-to-reach-120-billion/

Mobile vulnerabilities reported, by operating system

Android surpassed iOS in terms of the number of mobile vulnerabilities reported in 2016



(Source: Symantec report Vol 22, April 2017):

Additionally, the rise of cloud computing and virtualization technologies have expanded organization's network perimeters, reducing IT control of critical hosting infrastructure and de-centralizing data center environments. As organizations continue to push more workloads to the cloud, individual users and their devices will be able to access sensitive data and confidential information from anywhere. Organizations often lack secure policies and procedures for the usage of these cloud services, increasing the risk of cloud application use, and once deploying a public cloud infrastructure, lose data governance as they are exposed to vulnerabilities outside of their organization. Ultimately, due to the heterogeneous nature of cloud computing environments, organizations are increasing their exposure to cyber threats from new attack vectors.

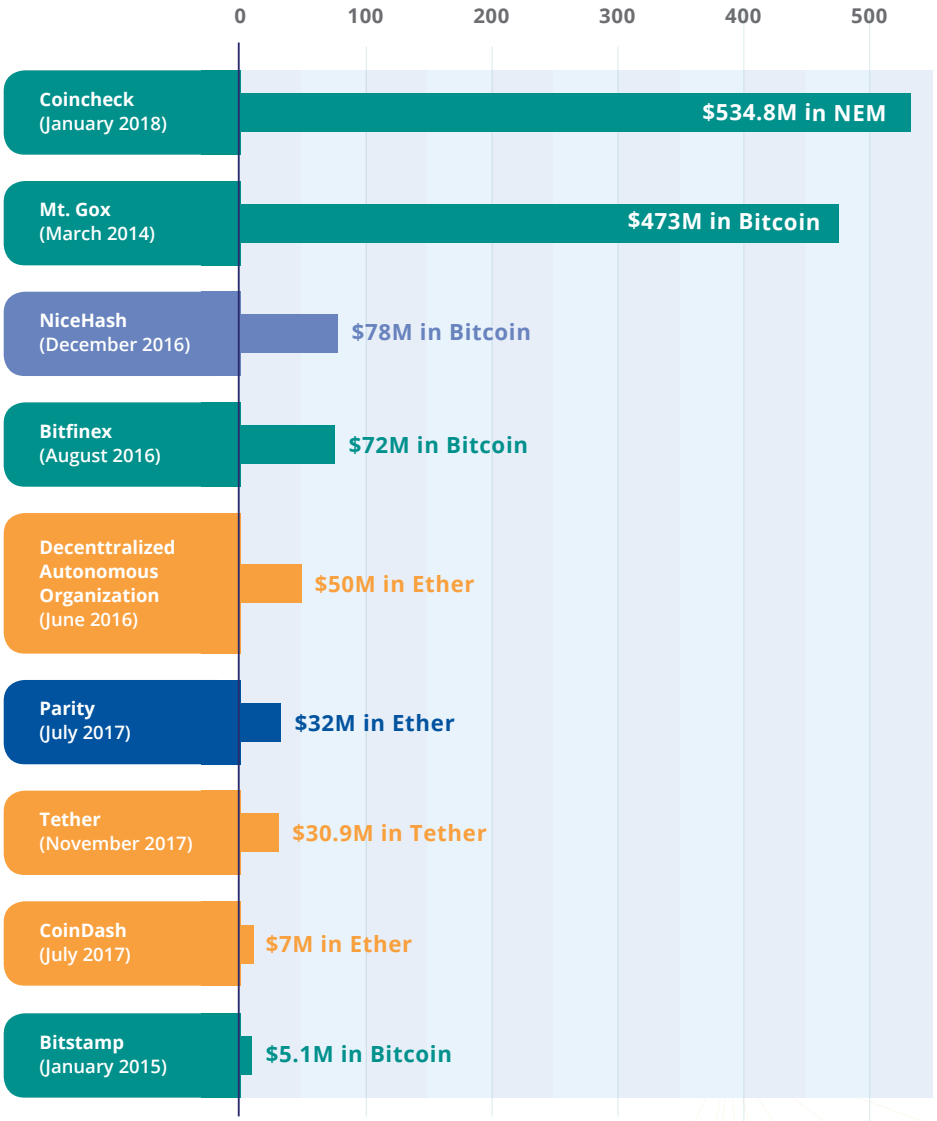
- **Cryptocurrencies**

The success of Blockchain lies into enforcing trust among the network participants. With Blockchain, it is now possible for 2 people and organizations with different interests to directly exchange value, goods and data without relying on a centralized authority. The various Blockchain technologies offer different strategies that make the data stored on the Blockchain immutable. Depending on the use case, one can prefer a strategy over another.

As cryptocurrencies have garnered more attention over the years, the number of cyberattacks has subsequently grown.

- In 2014, Mt. Gox reported a total loss of $460 million caused by a series of unrelated hacks over time, ultimately leading the cryptocurrency exchange to bankruptcy[9].
- In January 2018, CoinCheck, another cryptocurrency exchange, was reported to have lost $534 million due to a hack[10].
- In June 2018, CoinRail, also a cryptocurrency exchange, reported having lost $37 million also in a hack, causing a subsequent loss of $42 billion to the market value of cryptocurrencies[11].

Biggest Cryptocurrency Hacks and Thefts



(Source: 99bitcoins.com, benzinga.com)

9 Robert McMillan, "The Inside Story of Mt.Gox, Bitcoin's $460 Million Disaster". Available at: https://www.wired.com/2014/03/bitcoin-exchange/

10 Jake Adelstein, "Japan Cracks Down On Cryptocurrency Exchanges After $534M Heist; Police Begin Investigation". Available at: https://www.forbes.com/sites/adelsteinjake/2018/01/30/japan-cracks-down-on-cryptocurrency-exchanges-after-534m-heist-police-begin-investigation/#2c6529d85031

11 Stephen Johnson, "Cryptocurrency markets tank after hackers hit South Korea exchange". Available at: https://bigthink.com/stephen-johnson/cryptocurrency-heist-hackers-steal-millions-from-south-korean-exchange-global-market-drops-42-billion

These three prominent hacks, among many others, were all caused by one common initial problem – lack of security. According to Reuters, $1.2 billion of cryptocurrency were stolen between January 2017 and May 2018, out of which 20% have been recovered[12].

3.2 Increasing Importance of Securing Digital Identities

Cyber-attackers often target personal identity as it provides access to valuable systems and data while concealing their activity within networks. More than ever, enterprises must focus on identity as the primary constant in an ever-evolving technology and threat landscape. Thus, it is critical to effectively secure digital identities. PKI and digital certificates are the best approaches for implementing strong authentication, encryption and digital signatures, which are the building blocks of cybersecurity solutions that can be applied to diverse environments. Digital certificates provide identifying information, are forgery resistant, and can be verified because they are exclusively issued by official, trusted agencies. As identity has effectively become the new network perimeter, securing that identity is mission critical. The rapid emergence and anonymity created by the Blockchain has further accentuated the importance of securing identity.

3.3 IoT for Enterprises

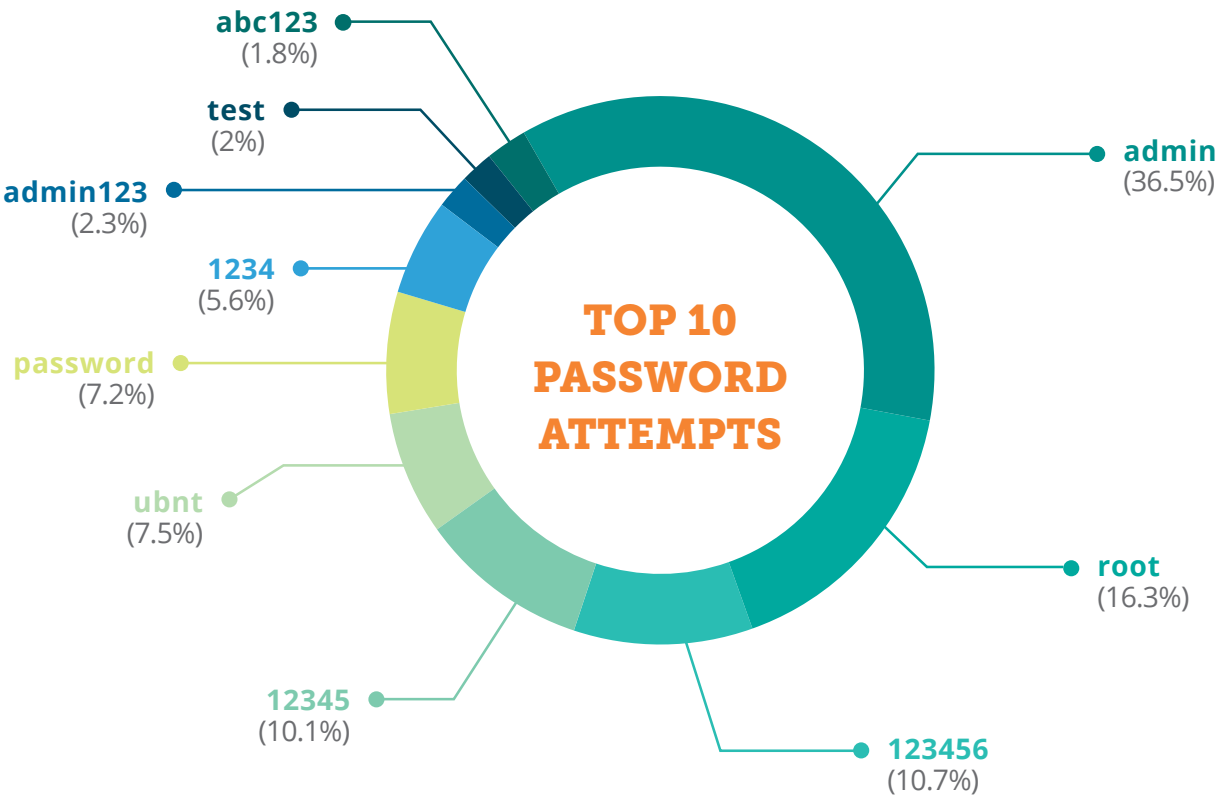
Addressing device security is a major enterprise priority in the evolution of the cybersecurity industry

The proliferation of connected devices has hastened the need to effectively secure these devices. Solving the device security problem in today's dynamic threat environment is critical for the security of all enterprises. Moreover, as enterprises become increasingly distributed, they face the challenge of securing perimeter-less borders. With the emergence of cloud and mobile technologies, the attack surface has expanded, creating greater security risks. Simultaneously, the frequency, complexity, and costs of cyber-attacks continue to rise.

Unmanaged IoT devices represent a significant threat for enterprises due to the activity and configuration of those devices, which are often opaque or even invisible to traditional IT tools. According to Positive Technologies, a provider of vulnerability assessment, compliance management and threat analysis solutions, cites that approximately 15% of devices leave default passwords unchanged[13]. Default passwords are often the same passwords set by manufacturers on every product produced, leaving these devices vulnerable to attacks. The use of weak passwords is a security issue that has been repeatedly seen in connected device breaches, such as the Mirai and Reaper botnet attacks. The combination of increasingly connected devices, persistent threats, and poorly secured devices has created a new security paradigm which enterprises need to prioritize in today's world.

12 Gertrude Chavez-Dreyfuss, "About $1.2 billion in cryptocurrency stolen since 2017: cybercrime group". Available at: https://www.reuters.com/article/us-crypto-currency-crime/about-1-2-billion-in-cryptocurrency-stolen-since-2017-cybercrime-group-idUSKCN1IP2LU

13 Kirill Shipulin, "Practical ways to misuse a router". Available at: http://blog.ptsecurity.com/2017/06/practical-ways-to-misuse-router.html



Top 10 passwords used to attempt to log in to the Symantec IoT honeypot (Source: Symantec report Vol 22, April 2017)

Thus, with the growing number of hacks every day, Juniper Research has suggested that the average cost of a data breach will cost businesses an estimated $150 million by 2020. Additionally, they have suggested that the overall cost for businesses of hacks could reach $2.1 billion by 2019[14]. Cybersecurity Ventures has suggested that cybercrime damages would cause $6 trillion in damages annually by 2021[15].

Enterprises must address the IoT security problem and bridge the gap between device proliferation and device manageability. It is imperative for devices to be manufactured with secured microchips embedded to provide an end-to-end solution that eliminates potential security gaps that inevitably arise with the combination of various technologies.

14 Juniper Research, "Cybercrime Will Cost Businesses over $2 Trillion By 2019". Available at: https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion

15 Steve Morgan, "Cybercrime damages will cost the world $6 trillion annually by 2021". Available at: https://1c7fab3im83f5gqiow2qqs2k-wpengine.netdna-ssl.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf

04 WISECOIN AG BUSINESS MODEL

04 WISECOIN AG BUSINESS MODEL

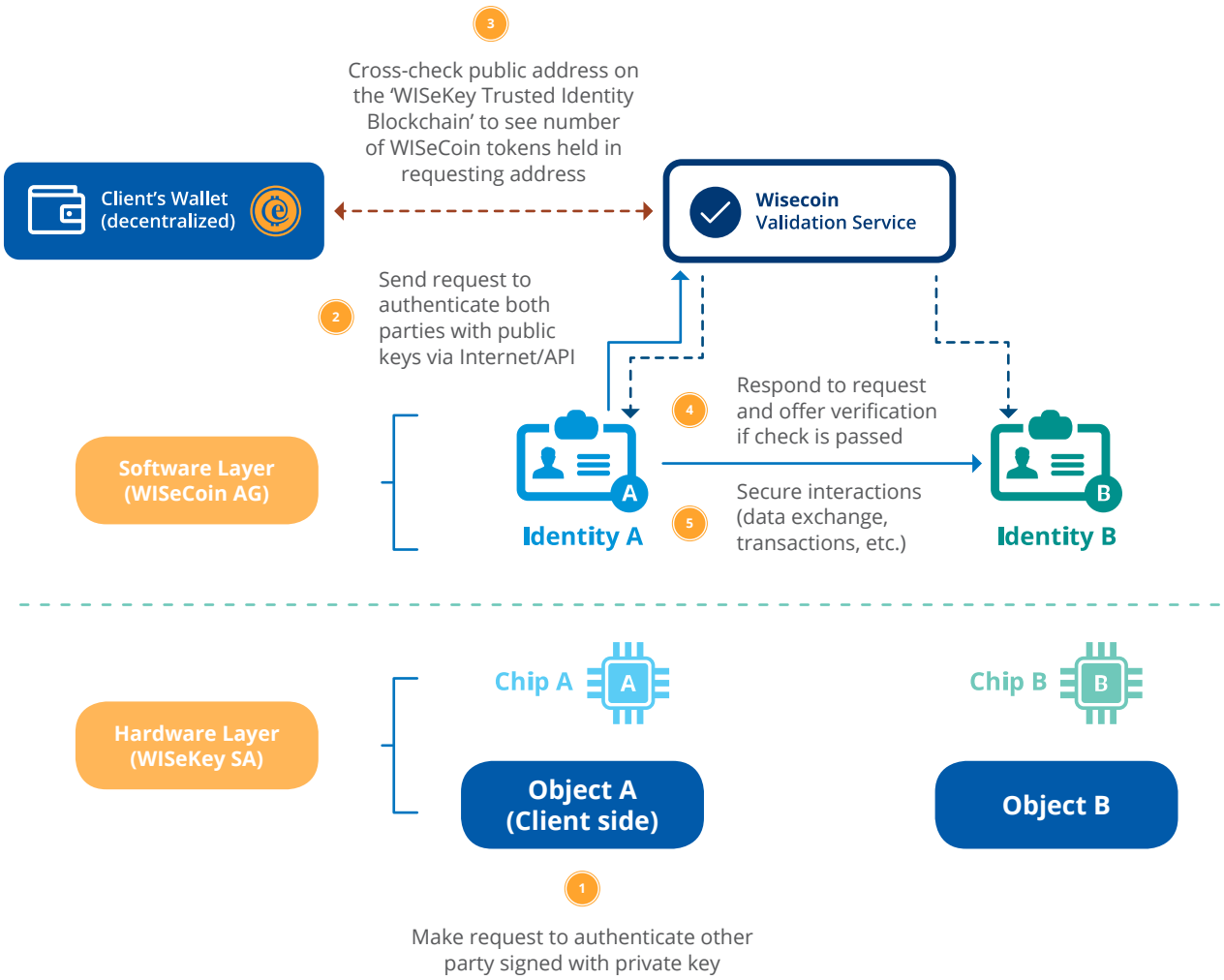
WISeCoin AG is developing a set of solutions that is complementary to the underlying Blockchains which will help objects, individuals and companies manage their identity and authentication. Its operations and business units are divided into two areas:

4.1 Internet of Things

4.1.1 Overview

WISeCoin's IoT solution enables secure digital communications from people-to-people, people-to-machines and machines-to-machines. We combine Blockchain technology, with our extensive experience in digital identities and PKI, and our expertise with secure microcontrollers to create a tokenized service offering, the 'WISeCoin' token, which is a utility token. It provides an innovative way to verify connected objects wanting to interact with one another. Through this unique service offering, WISeCoin AG aims at becoming the ubiquitous industry solution for facilitating secure IoT interactions.

The solutions provided by WISeCoin AG will allow any person, object or machine to exchange information or value in a trusted manner while significantly reducing the risk of malicious cyber threats, frauds and hacks. WISeCoins are however not a means of payment, but a service offering. It is enabled through the token which is stored in a digital wallet and entitles the holder to the service offering of the WISeCoin. The token is indifferent to the wallet provider and can be incorporated into any ERC-20 compatible wallet.

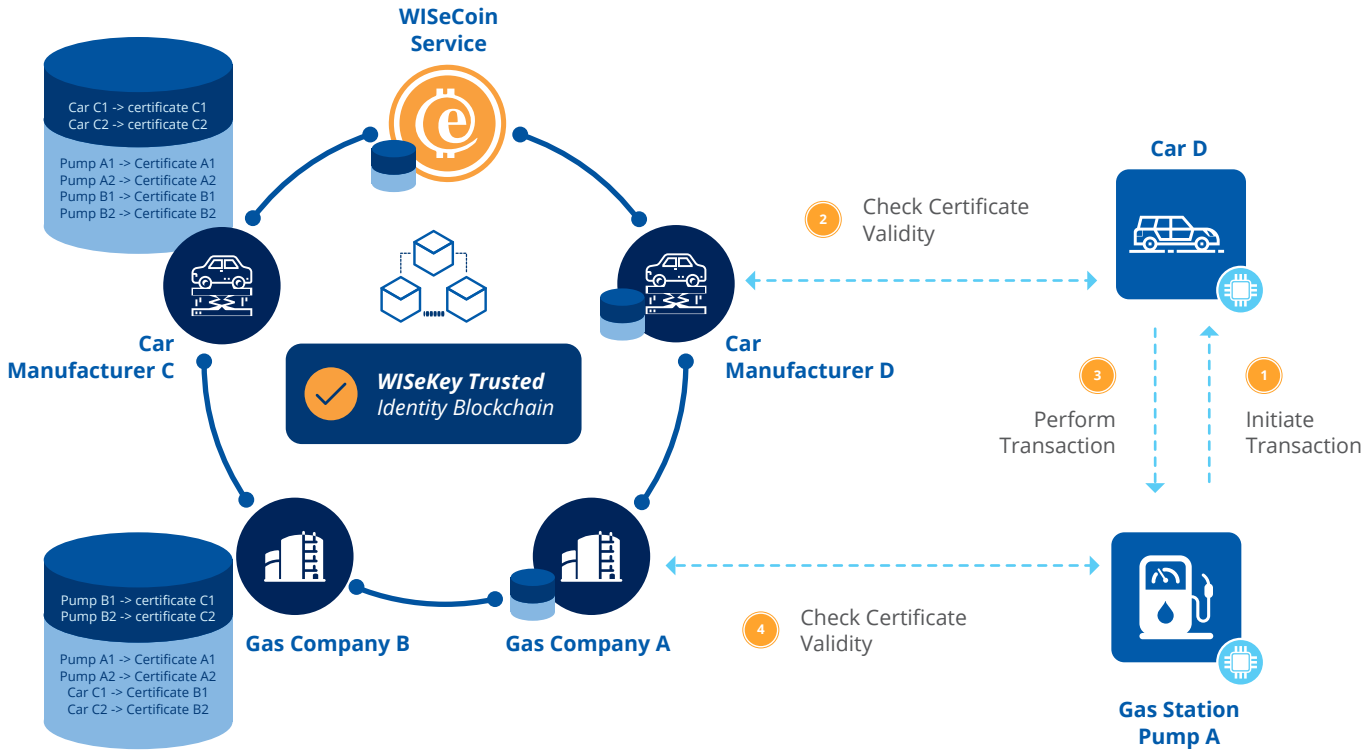


The demand for this service will be driven by the exponential growth in connected devices, the adoption of new transaction methods (such as cryptocurrencies) as well as the autonomous nature of new technological developments (e.g. self-driving vehicles and autonomous devices). We derive revenue from the sale of WISeCoins. Our core business addresses large and growing markets. According to industry research, the number of IoT devices is expected to grow from 22.9 billion devices in 2016 to 50.1 billion devices in 2020[16], growing at a compound annual growth rate (CAGR) of 21.6% from 2016 to 2020. By 2020, the IoT will be a $ 1.4 trillion Market[17]. Moreover, global IoT Security Products spending is estimated to be $12.5 billion in 2017, with the potential to grow to more than $21.2 billion in 2021.

16 NCTA, "Internet of Things". Available at: https://www.ncta.com/positions/internet-of-things

17 Machina Research and IoT AG

WISeKey Trusted Identity Blockchain



4.1.2 WISeCoin Platform

WISeCoin is a service to secure IoT interactions by allowing actors (machine-to-machine or people-to-machine) to recognize and trust each other.

The WISeCoin Validation Service (the certificate's validation authority) analyses the digital certificate of different actors to recognize and trust the identity of other parties they are interacting with. To do this, the WISeCoin token gives its token holders (stored on digital wallets) access to the WISeKey Public Key Infrastructure, which provides the verification service in order to mitigate malicious actors and hackers from compromising interactions.

WISeCoin offers a service to authenticate and validate parties to allow the exchange of information or value with each other. WISeCoin is sold directly by WISeCoin AG and generates revenue as a hybrid product/service offering. WISeCoins will not be listed on secondary markets and will be sold directly from WISeCoin AG. Therefore, WISeCoins will not be subjected to price fluctuations and will be sold on a fixed price basis.

Objects send the validation authority the third party's public key and the digital certificate for validation. WISeKey checks that the corresponding public key holds a valid WISeCoin and if so, the identity is verified. In order to get the verification, the object making the request needs to hold at least 1 WISeCoin in its wallet, which is valid for 12 months or 100 requests. WISeCoin AG can, over time, adjust the number of tokens required to get verified, the longevity of the token and entitled verifications per token.

4.1.3 Token Characteristics

WISeCoin will initially be issued as a ERC-721 non-fungible token, functioning like a Trusted Digital Identity, on the Blockchain ensuring that it is publicly verifiable. WISeCoin is a utility token which offers the following characteristics:

- WISeCoins will be used to verify identities of digital wallets embedded into objects.
- WISeCoin is a product with a digital identity validation and transaction service offering and is therefore not intended as an investment, nor a means of payment.
- Its token supply is technically unlimited and can be minted and delivered to the desired wallet addresses immediately.
- WISeCoin will be initially offered at 0.10 USD per token, with a minimum purchase size of 10'000 tokens.
- After 100 verifications or 12 months, it will expire and a new WISeCoin must be purchased. The purchase of new tokens can be triggered automatically.

During the pre-sale phase, from March 2019 to April 2020, a 50% discount will be offered on the price of WISeCoin through a Token Pre-Sale Agreement. From April 2020, the WISeCoin will be offered directly by WISeCoin AG at full price.

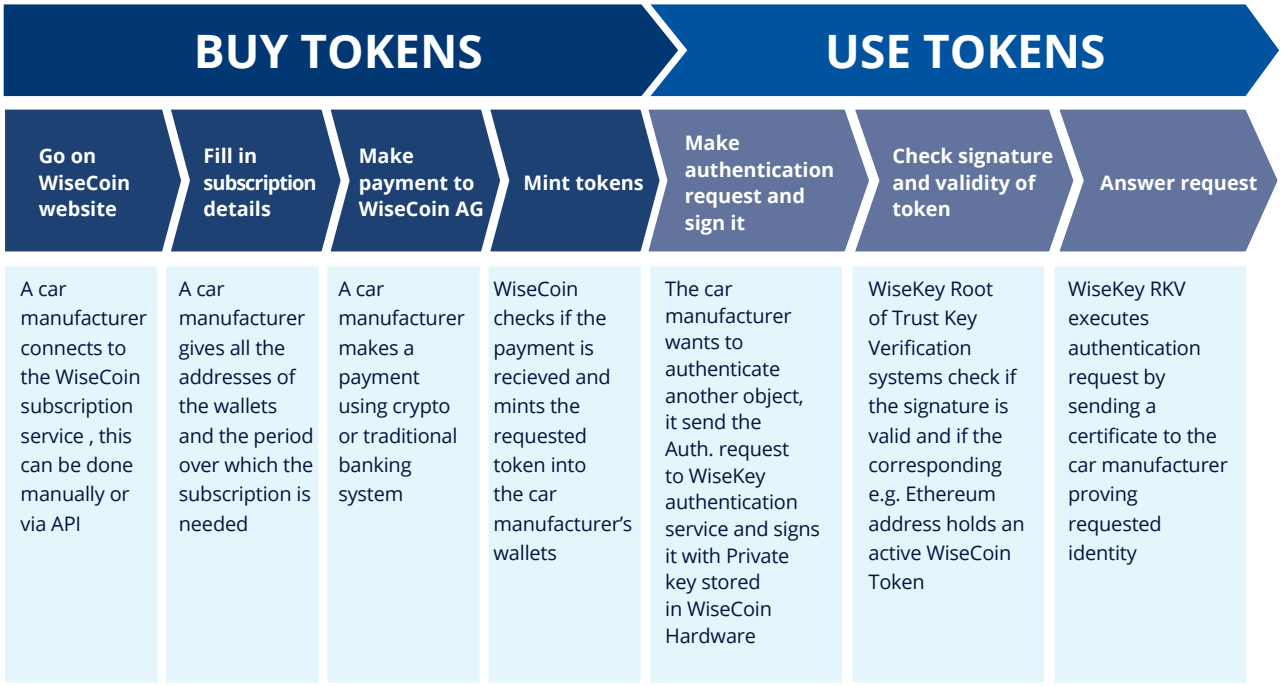
4.1.4 Application of WISeCoin

The WISeCoin Validation Service is used for the verification of the validity of digital identity of the object in real time, thus ensuring secure use of digital identities for authentication of an object connected to the Internet and the activation of attributes such as digital signing, transactions, or sending data.

The WISeCoin Validation Service is suitable for all e-services that can be used with a WISeCoin. Each validation will be charged with a WISeCoin that will represent a fraction of the transaction validation fee equivalent to 0.001 cents of dollar.

The WISeCoin platform is Blockchain neutral and allows Blockchain configurations to benefit greatly by the use of secure, private keys in place of the public keys currently used. By using private keys between the IoT signer and the IoT recipient, secure transactions and data transactions can be maintained by only approved parties – thus making it a very viable option for any sort of IoT transaction imaginable.

4.1.5 Case Study



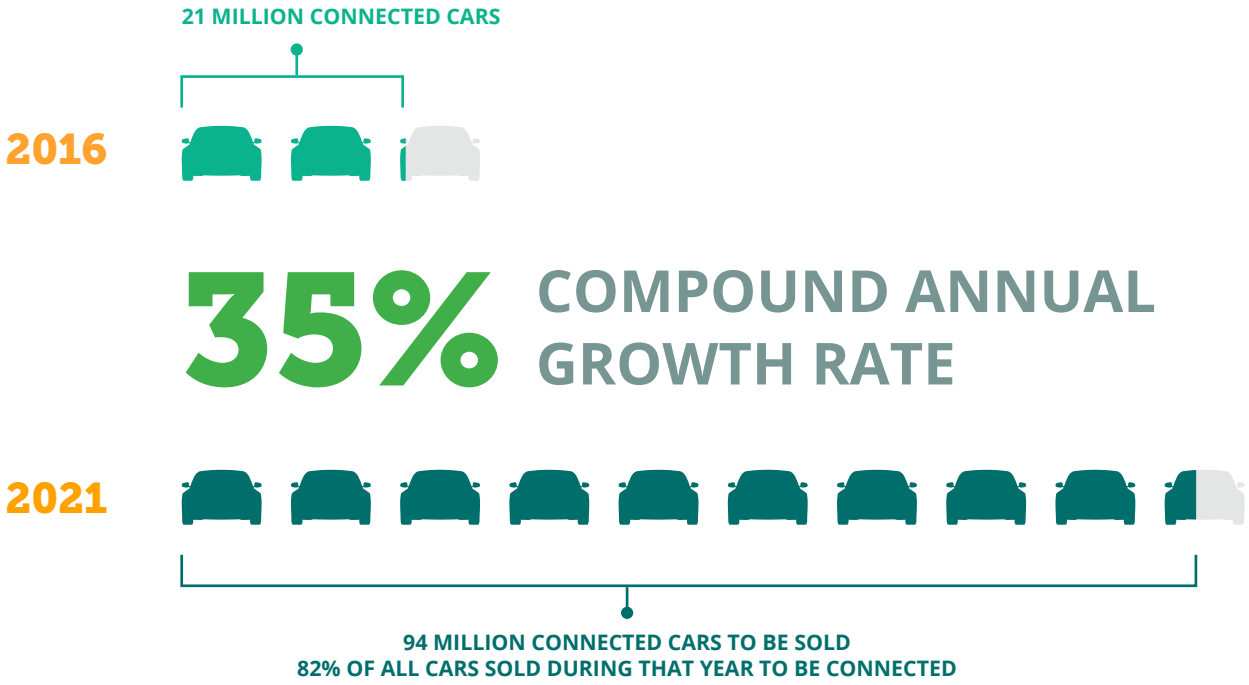
WISeKey is already providing the integration of WISeKey IoT and Public Key Infrastructure (PKI) in the manufacturer's connected car solutions allowing them to authenticate legitimate car components and enabling owners to securely interact with the car's smart features. The fact that the electric car includes a WISeKey digital certificate stored on a WISeKey microchip acting as a secure hardware module allows it to send securely the WISeCoin required to execute the transaction between the electric car and the electric charger without any intermediaries or paying any transactional fees.

Virtually all new cars on the market today include electronic technologies that could pose vulnerabilities to hacking or privacy intrusions if data security is not addressed. For example, smart cars without cybersecurity protection technology could allow hackers to gain remote access by exploiting vulnerabilities in their ecosystem of connected components and online services. As the number of cars connected to the Internet is growing quickly (to over a quarter of a billion by year 2020, as estimated by Gartner), smart car manufactures are working towards identifying and reducing potential hacking vulnerabilities in their vehicles.

The WISeCoin platform benefits from WISeKey's standardization and neutrality assets, key factors needed to achieve interoperability, and its vast experience in working with leading European automobile manufacturers to provide cybersecurity services for connected cars.

Currently, WISeKey provides PKI Services to a growing number of smart car manufacturers

and its ISTANA PKI platform is already active in several large-scale projects. As the number of cars connected to the Internet is growing quickly, smart car manufactures are working to identify and reduce potential hacking vulnerabilities in their vehicles. BI Intelligence expects 94 million connected cars to be sold in 2021, and for 82% of all cars sold during that year to be connected. This represents a compound annual growth rate of 35%, from 21 million connected cars in 2016 . In recent years, the security protections of smart cars have expanded using proven IoT technologies. There is an increased use of Secure Microcontrollers provided by WISeKey Semiconductor to authenticate individual car components within the vehicle itself and to the online services it interacts with, and to ensure that only legitimate software is installed in the car.



Each connected object is equipped with WISeKey's Secure Element, called VaultIC184, consisting of a tamper resistant silicon chip, based on a state-of-the-art securemicrocontroller allowing device manufacturers an easy integration of the chip, as well as a provisioning service, transferring the burden of device personalization to WISeKey's secure Personalization Center.

4.2 WISeBlock

4.2.1 Overview

WISeCoin AG will also be dedicated to help organizations innovate with the implementation of tailored Blockchain solutions. This service will offer specific business applications around Blockchain using our expertise in cryptocurrency, identity management, Public Key Infrastructure (PKI), and Secure Microcontrollers. The application can be diverse, from innovative supply chain solutions to helping governments establish smart city projects. WISeBlock also offers a digital wallet application, secured through hardware and software, to hold sensitive private information as well as cryptocurrencies, but also to trade and exchange them securely. The platform will also provide a distributed PKI solution, also known as DPKI.

4.2.2 wisewallet

More often than not, the architecture of a wallet that holds cryptocurrencies determines how securely held and accessible they are. While most wallets must find a compromise between security and accessibility, our wallet solution consists in providing the highest standard of security to holding, buying and selling cryptocurrencies all while remaining practical through the interface of a mobile application for iOS and Android. Our solution uses our VaultIC secure element chip, hardware secure module, and digital certificates.

User Application

End users are first equipped with a WISeKey account, which requires them to go through a KYC process upon registration. This will allow them to identify themselves when accessing the mobile application. Once in the application, users are able to manage their account and assets. With integration to exchanges, users can trade cryptocurrencies.

As an optional physical security layer, users can be equipped with a tangible 'key' taking the shape of a coin with a purpose to identify and authenticate themselves when accessing the application and performing transactions. This tangible coin is embedded with a VaultIC secure chip using Near Field Communication (NFC) technology, ensuring that its use remains as simple as a tap on the back of their phone.

Security

The highest standard of security is achieved through our Hardware Security Module (HSM). The WISekey's HSM stores cryptocurrency keys in Swiss data centers located in secured military grade bunkers. Its security architecture, which parallels those of banks, ensures that cryptocurrency keys are virtually uncompromisable. While usable through the application's interface, the latter is protected through data cyphering and several security layers upon login such as regular passwords, password patterns, fingerprint authentication, one time passwords, facial recognition, and more.

An additional yet optional security layer is provided through the tangible coin embedded with a VaultIC secure element chip. The secure element holds digital certificates which are associated to private keys made to double check and verify that actions done on the wallet application are truly by the owner of the wallet. WISeCoin AG provides a service to manage the digital certificates with a purpose of ensuring that it can be made obsolete by revoking the certificate if lost or stolen.

4.2.3 WISePhone

WISePhone Genesis (the entry-level model) and WISePhone Block (the upgraded version which will be available for purchase in 2019) deliver business and personal privacy and security enabled by Blockchain technology. WISePhone is a cost-effective and flexible platform that empowers efficiency and mobility whilst protecting intellectual property and confidentiality by transforming public networks and mobile devices into highly secure communication channels. WISeKey's Telecommunication Services Provider status under OFCOM, the Swiss Federal Office of Communications, allows the company to deploy mobile phone voice encryption solutions.

WISePhone Genesis

The WISePhone Genesis is a secure Blockchain mobile phone entirely secured by WISeKey. The WISePhone Genesis model, which can be used a business and/or personal phone, offers secure communications (email and voice), digital identity, and data on the cloud. Through a Personal Cybersecurity Hub, WISePhone Genesis model puts users in control of application permissions and offers separate secure environments to protect and separate personal and business data.

WISePhone Block

The WISePhone Block edition comes with pre-loaded with native WISeID and WISetalk, WISeKey's industry-leading, digital identity and communication app that offers encrypted, secure voice calls, conference calling, text and file transfers. WISePhone integrates WISeKey's innovative hardware and software technologies bringing to market the first and only smartphone powered by WISeCoin cryptocurrency Blockchain technology.

The WISePhone Block edition comes with a native crypto Wallet, is equipped with a HSM (Hardware Security Module) device and integrates the WISeKey SuisseID Digital Identity enabling cloud based qualified signing capabilities certified by the Swiss Government and in compliance with the EU General Data Protection Regulation (GDPR).

The WISePhone Block Wallet also uses WISeKey's Blockchain-as-a-Service ("BaaS") technology to conduct secure contactless payments and it is compatible with most of the existing Blockchain technologies.

Additionally, WISePhone's Block suite of applications offer voice and text encrypted communication features (WISeTalk), reflecting sophisticated security mechanisms and advanced end-to-end encryption technologies. Furthermore, WISeID keeps user's data and digital assets protected inside an encrypted enclave (replicated in a secure swiss cloud), while WISeAccess provides additional secure authentication factors to access the WISePhone suite of applications.

Since 2010, WISePhone.ch voice encryption products and services have been used by large user groups in public and private organizations and recently, the technology was upgraded to provide voice encryption services for a wider consumer platform, targeting global markets. Today, the platform hosted in Switzerland inside WISeKey's zero-risk bunker deep in the Swiss Alps, provides Secure Cloud Storage solutions allowing users to securely exchange sensitive data and Identity Management with WISeID.

4.2.4 Distributed PKI Solution

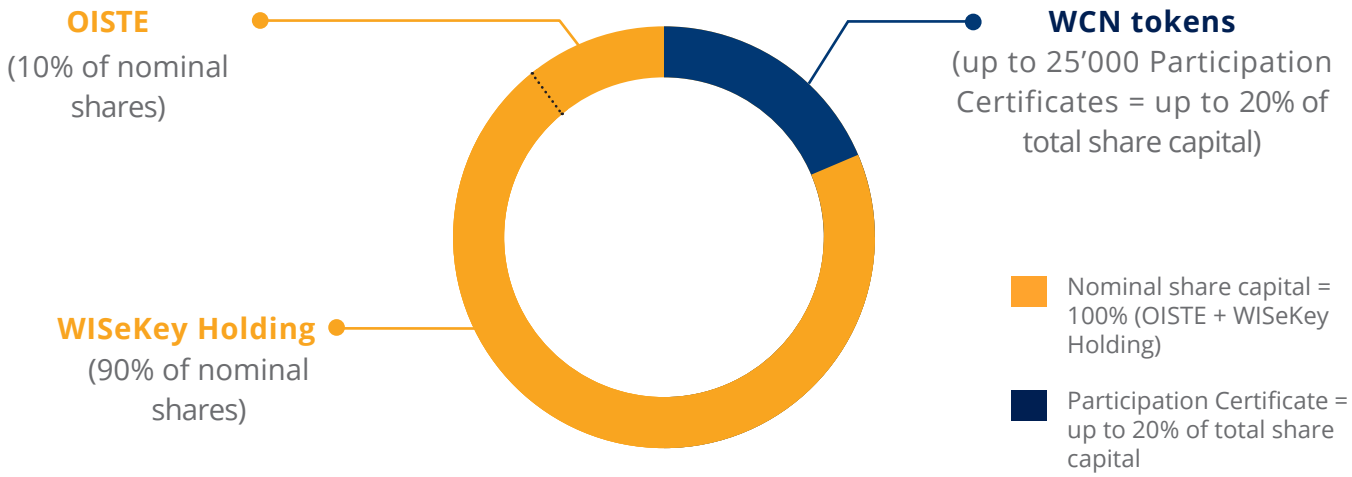
Distributed PKI consists in the implementation of a PKI where the digital certificates are shared and verifiable on a Blockchain network. This particular implementation presents the advantage to give a better defense against the man in the middle attack . This will offer an innovative solution for our clients looking to implement a PKI and is particularly suitable in a cross-organizations or cross-sites environment.

05 WISECOIN TOKEN (WCN)

05 WISESECURITY TOKEN (WCN)

5.1 Overview

WISeCoin AG will develop the infrastructure for verified intra object interactions as well as cryptocurrency storage solutions through its own digital wallet solution. To facilitate its development, as well as to provide an investment opportunity in WISeCoin AG, WISeCoin AG is issuing a WISeSecurity Token (WCN) in a private sale to institutional investors and corporate partners and later a public sale through an ICO.

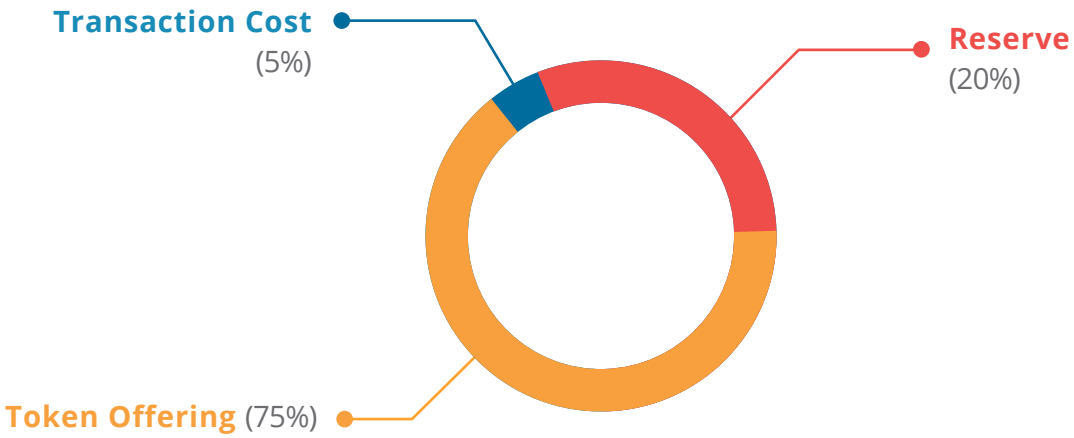


WISeCoin AG will offer WCN tokens of which 100 WCN tokens correspond to 1 participation certificate. Consequently, up to 25'000 registered participation certificates at 1.00 CHF will be issued via an authorized participation capital increase. The WCN tokens will embody the potential claim on the entire participation capital of the WiseCoin AG representing by the participation certificates. Up to 20% of its equity capital as participation rights through the sale of the WCN token. Subject to Swiss law, both nominal share and participation rights certificate holders have equal claim to dividend rights.

- 100 WCN tokens correspond to and can be exchanged into 1 WISeCoin AG non-voting share (participation rights) participation certificate of CHF 1.00 nominal value.
- If WISeCoin AG issues a dividend, WCN token holders have the right to receive dividends on a pro-rata basis of the equity capital subject to the annual general assembly's decision.
- WCN is planned to be listed on regulated token exchanges in 2019.
- In limited events (including liquidation and exit events) an exchange of WCN tokens into shares may be mandatory.

Symbol	WCN
Sale Type	Private and Public Sale
Token Type	ERC20
Total Token Supply	2,500,000 WCN
Price per Token	1 WCN = 9.38 CHF
Hardcap	CHF 17,587,527
Minimum Investment	CHF 1 million for Private Sale CHF 1,000 for Public Sale
Lockup Period	12 months
Dividend Claim	Participation Certificate
Sale Periods	Private Sale: March 2019 - May 2019 Public Sale (ICO): April 2019 - July 2019
Accepted Currencies	CHF, ETH, BTC

5.2 WISeSecurity Token Distribution



- 75% of all minted WCN tokens will be offered for purchase to investors. The private sale will commence in March 2019 and stay open until May 2019. A public sale (ICO) will happen in April 2019 to July 2019.
- 5% of the proceeds of the token sale will be used to cover the transaction costs. These costs are the following:
  - Legal fees
  - Blockchain Valley Ventures Advisory fees
- 20% of WCN tokens will be held as reserves at 2 year vesting period.

06 TOKEN OFFERING

06 TOKEN OFFERING

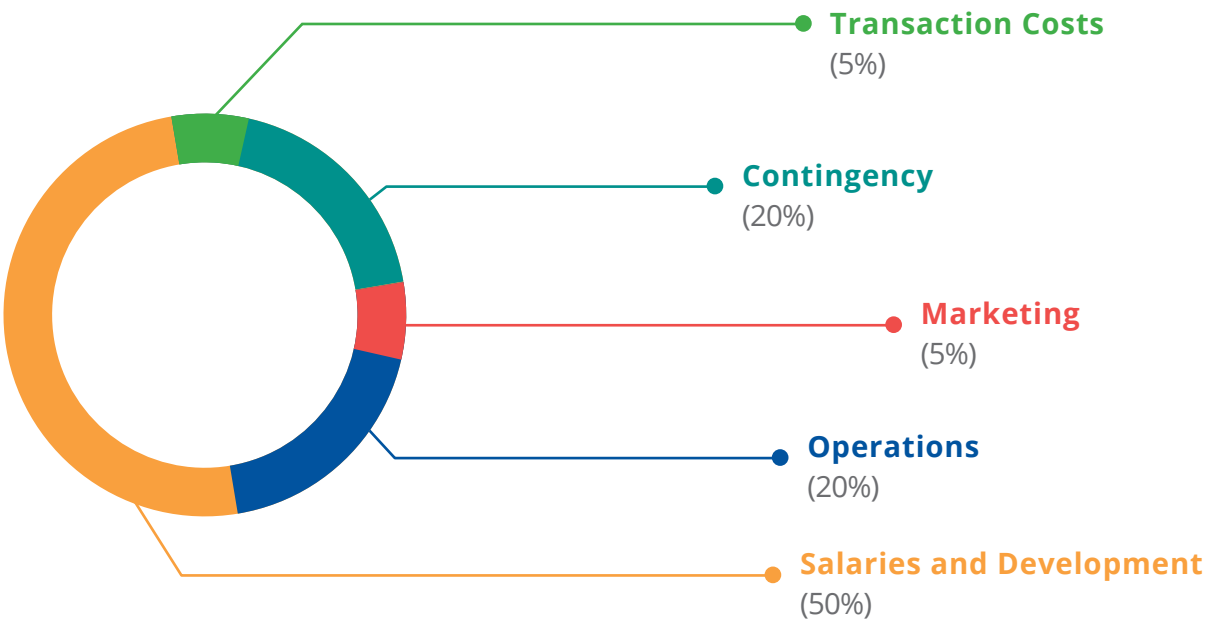
6.1 Overview

There are two phases for the fundraising of WCN tokens. The first phase will be through a private sale of the WCN tokens from March 2019 to May 2019 for credited and institutional investors. The second phase will occur through a public sale (ICO) starting in April 2019 to July 2019.

Regarding the private sale and at the request of the investor and his own costs, he may have the opportunity to put payments for the WCN token into a third party escrow arrangement. Once the WCN token is issued and delivered to the Buyer, the funds will be released, whereby the Buyer benefits from a secured transaction.

6.2 Use of Proceeds

The use of proceeds concerns both of the funding phases (private and public sale).



- Salaries and development (50%)* – the team consists of software engineers, business developers and fintech specialists. This financing allows for WISeCoin AG to scale up its team and accelerate the rollout of the WISeCoin platform.
- Operations (20%) – Usage of PKI, data centers, SGA. WISeCoin AG would look to purchase or lease the relevant IT infrastructure from WISeKey International Holdings.
- Contingency (20%) – Reserves for unforecasted costs
- Marketing (5%) – Partnerships to create websites, blog, social media channels and videos
- Transactions costs (5%) – Legal, Advisory

The envisioned use of proceeds described above are provided for illustrative purpose only, and WISeCoin AG reserves the right to allocate the resources, including proceeds from the private or public sale of WCN tokens in a different way at its sole discretion.

*Salaries and development:

1) Develop wallet functionality to offer secure digital identity and key management for Secure Microcontrollers and objects.

2) Develop a Software Development Kit (SDK) to:

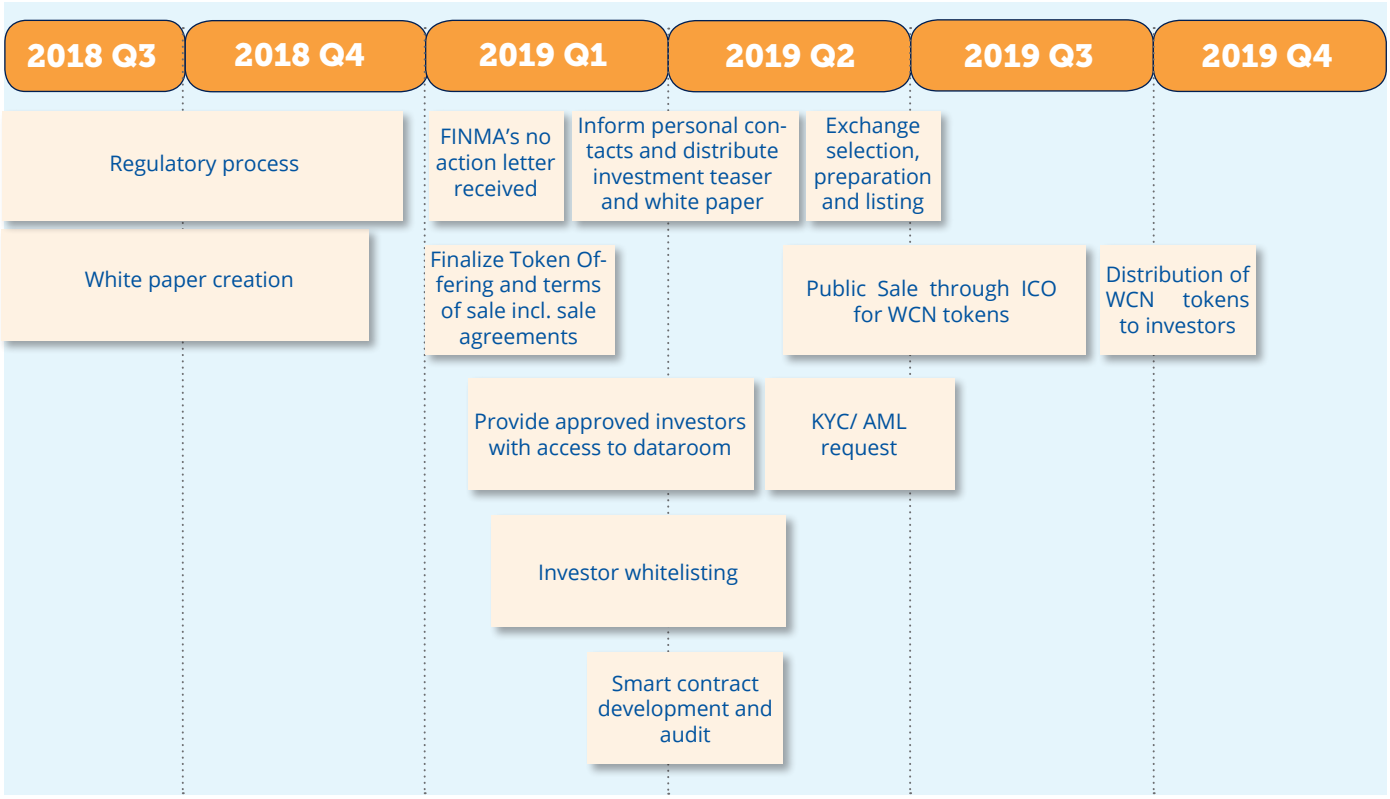
- Connect Identity/ Digital Certificates and WISeKey Secure Microcontrollers to 3rd party solution providers through gateways.
- Connect Identity/ Digital Certificates to any type of Blockchains (IOTA, Ethereum, Bitcoin, Cardano, Hyperledger, Corda, etc.)
- Integrate Crypto Wallet functionality into objects and applications.
- Enable secure, legally enforceable transactions between objects and wallet holders, which will be recorded on the Blockchain.

3) Develop the WISeKey Trusted Blockchain of identities

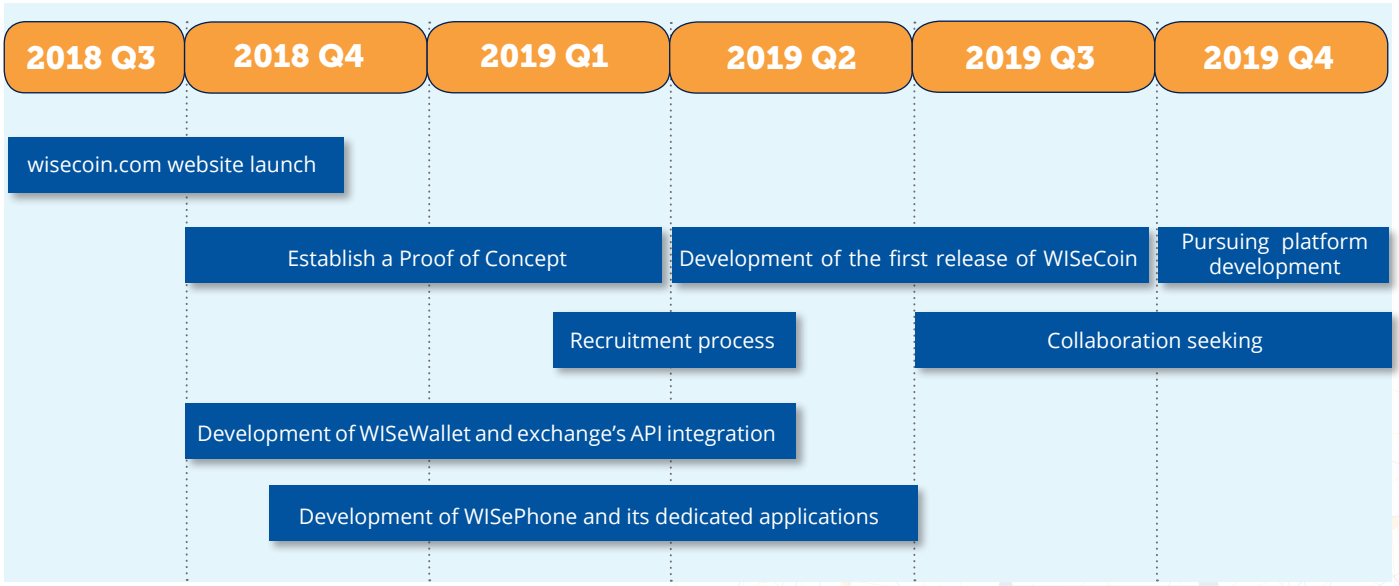
07 ROADMAP

07 ROADMAP

STO Process



Platform Development



08 TEAM

08 TEAM

8.1 Core Team

Carlos Moreira - Chief Executive Officer

At the head of the WISeCoin AG project is the founder, chairman and CEO of WISeKey, Carlos Moreira. Being a UN Expert of Cybersecurity and Trust Models and member of the World Economic Forum Global Agenda Council for Future IT and Software, his credentials are backed by 20 years of experience in digital identity and IT security. This makes him a seasoned leader for the team that implements his vision for the WISeCoin AG project.

Pedro Fuentes - Chief Security Officer

Pedro Fuentes is the Chief Security Officer of WISeKey. With over 20 years of experience in information security and PKI, Pedro is considered a specialist and a certified professional in the area (CISM, ISO27000, MSCP and more). As the Chief Security Officer of WISeKey, he supervises the PKI aspect of the WISeCoin AG project.

Peter Ward - Chief Financial Officer

With a significant amount of experience in the fields of IT, FMCG, Retail/Distribution, Medical Equipment and Plastics industries, Peter Ward is a Chartered Management Accountant that has also worked for several industry leaders, giving him a deep and specialised understanding of Change Management, Process Improvement, Business Integration and Restructuring and more. As the Chief Financial Officer of WISeKey, he also oversees the financial aspects of WISeCoin AG.

Hans Schwab – CIO / Managing Director

More than 30 years of experience in areas of technology, with a focus, over the past decade, on developing tools and applications to disrupt counterfeiting, illicit trade and fraud. He spent ten years in various management positions at the World Economic Forum in Geneva, including as a member of the executive board.

Carlos Moreno - Team manager and head of partnerships

Throughout his career, Carlos Moreno has worked extensively in executive roles on strategic projects for both national and multinational companies in the financial and industrial sectors giving him 18 years of experience in Sales Engineering, Sales Management and Business Development. During the course of the development of the WISeCoin AG project, he manages the team and the partnerships involved to make the project come to fruition.

Gaetan Egloff - Information System Developer

Equipped with prior project management experience in banks, the medical sector, the oil industry and more, Gaetan Egloff has provided significant contributions to WISeKey's growth since 2009. Also with a Bachelor of Science in Computer Science, Gaetan is committed to enhancing and integrating applications into the WISeCoin AG project.

Andreas Moreira - Project Manager WISeCoin & Cryptocurrency

Having completed his Bachelor of Science in Computer Science from University of Webster and École Polytechnique Fédérale de Lausanne, Andreas Moreira was assigned with the WISeCoin AG project. Equipped with a deep understanding of Blockchain and cryptocurrencies, Andreas is able to provide a fresh and innovative direction to the project.

Julien Ducor - WISeCoin ICO Manager

Julien Ducor completed a postgraduate degree in Finance at Imperial College. With experience in trading for major banks in London and Geneva, Julien Ducor also moved to Blue Lakes Advisors to work in Private Equity, a field he would later become an expert in. In April 2017, he started trading, investing, and mining cryptocurrencies. For the WISeCoin AG project, he works in business development and in the enhancement financial structure to improve its efficiency and sustainability.

Florine Dromard - Blockchain Developer

While studying Computer Science, Florine Dromard simultaneously worked part time as a developer. After graduation, she worked as an IT Consultant and stayed in the banking world for four years. Prior to joining the WISeCoin AG Team, she took different roles in the IT field, including as developer in Blockchain projects. Florine Dromard now uses her prior knowledge in Blockchain to ensure that the WISeCoin AG project takes the right steps in implementing this new technology.

8.2 Advisors and Extended Team

BLOCKCHAIN VALLEY VENTURES

Blockchain Valley Ventures

With a deep know-how and insight into the Blockchain ecosystem as well as significant ICO experience, Blockchain Valley Ventures is a Swiss venture firm that focuses on incubating, developing and investing into Blockchain-enabled businesses.

09 ANNEXES

09 ANNEXES – UNDERLYING TECHNOLOGY

9.1 Root of Trust for Digital Identities

What is PKI?

A public key infrastructure (PKI) is a set of roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption. PKI facilitates the secure electronic transfer of information for a range of network activities including, but not limited to, e-commerce, internet banking and confidential email. PKI enables parties to identify one another by providing authentication with digital certificates and allows reliable business communications by providing confidentiality through the use of encryption, and authentication data integrity and a reasonable basis for nonrepudiation through the use of digital signatures.

PKI uses public/private-key pairs—two mathematically related keys. Typically, one of these keys is made public, by posting it on the Internet for example, while the other remains private. Public-key cryptography works in such a way that a message encrypted with the public key can only be decrypted with the private key, and, conversely, a message signed with a private key can be verified with the public key. This technology can be used in different ways to provide the four ingredients required for trust, namely: confidentiality, authentication, integrity, and nonrepudiation.

What is a Certification Authority?

In order for these technologies to enable parties to securely communicate, one important question must be answered. How will we know in the digital world that an individual's public key actually belongs to that individual? A digital certificate, which is an electronic document containing information about an individual and his or her public key, is the answer.
This document is digitally signed by a trusted organization referred to as a Certification Authority (CA). The basic premise is that the CA is vouching for the link between an individual's identity and his or her public key. The Certification Authority provides a level of assurance that the public key contained in the certificate does indeed belong to the entity named in the certificate.

What is a "Root Certification Authority"?

A PKI can be described as a hierarchy of Certification Authorities, and at the top level there's always the "Root Certification Authority", the top-level of a given PKI, and represents the 'trust anchor' for the chain of trust, signing and endorsing the Certification Authorities in the hierarchy. Major operating system and browser vendors embed and distribute the Root CA certificates for many public CAs, and enterprises may add to these by distributing the Root CA certificates of internal PKIs to their users. As applications will trust any valid certificate that chains up to a Root CA that is in its trust store, extra precautions to protect the integrity of the Root CA and its private signing key must be taken. It is leading practice for Root CAs to be 'offline' and/or 'air gapped' from other networks, and only brought online in a controlled environment to issue certificates to other intermediate/issuing CAs, subordinate CAs, cross-

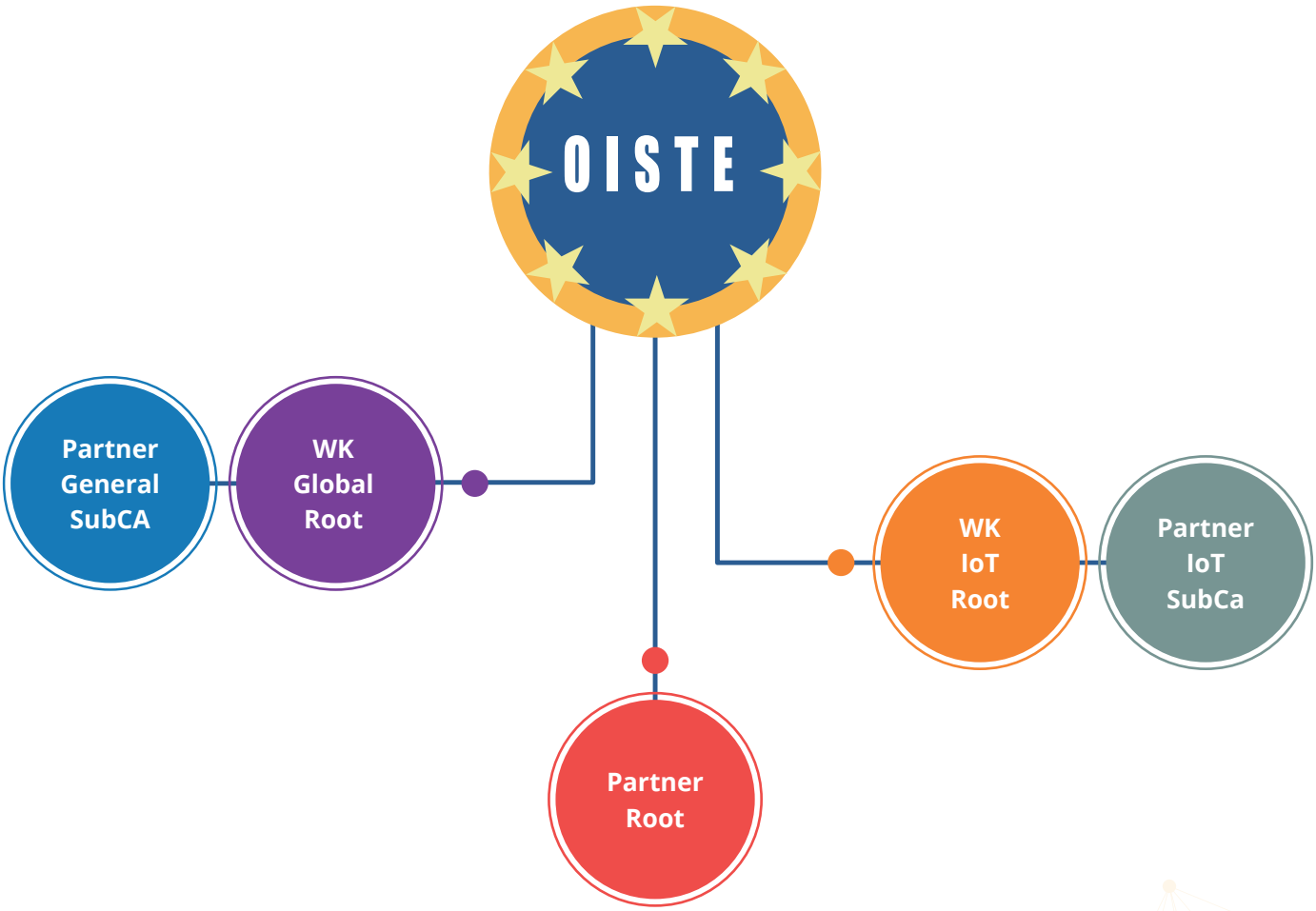
certificates, and CRLs.

What is a Root of Trust?

As explained in the previous sections, a PKI can be seen as a hierarchy of certification authorities, but also as a set of roles, policies, and procedures needed to manage the infrastructure. All this is known as a "Trust Model".

Beyond the technicalities of a Root Certification Authority, it's critical to consider how the Trust Model is controlled and who has this control. The combination of recognized Root Certification Authorities and a solid Trust Model is the only mean to build a true "Root of Trust".

At the heart of this strategy is the OISTE-WISeKey Cryptographic Root of Trust which has been actively used since 1999 by over 2.6 billion desktops, browsers, mobile devices, SSL certificates



and Internet of Things' devices. The OISTE WISeKey Cryptographic Root of Trust is ubiquitous and universal, and a pioneer in the identification of objects.

OISTE stands for "Organisation Internationale pour la Sécurité des Transactions Electroniques" (International Organization for the Security of Electronic Transactions). The OISTE Foundation, created in Geneva in 1998, is a not-for-profit organization regulated by article 80 et seq. of the Swiss Civil Code. OISTE is recognized by the United Nations as a non-profit organization

with an ECOSOC status, which allows the Foundation to participate in international programs promoting the democratization of access to new technologies, especially with respect to the provision of access to the digital identity as a fundamental right.

This unique combination of a Root of Trust managed by an independent, worldwide recognized organization like OISTE, and the operation of the PKI with cutting-edge technologies brings a unique value that no other competitor in the industry can demonstrate to the market, but the OISTE-WISeKey Root of Trust.

9.2 INeS – IoT Device Security

The Security Broker INeS, connected to your IoT platform such as IBM Watson*, Amazon Web Services* and many others, is the heart of the secure management of your assets. It gives you the tool to remotely manage your entities, one by one or by type, family or whatever defined common characteristic. This management goes far beyond the basic type of management IoT platforms generally propose, like device deployment, update and deprecation.

It starts with the optional remote Certificate Provisioning. Devices can be manufactured with an integrated Secure Element VaultIC. Only at initial connection to a network, a device receives its digital identity and certificate through a secure channel setup between INeS and the Secure Element (based on Secure Channel Protocol #11), thus allowing devices to be manufactured regardless of the back-end system it will be connected to. More about this is presented in the section Just-in-time Onboarding below.

Once a device is in operation, its digital identity can be controlled, revoked and renewed by the administrator through the Entity Control Interface of INeS.

Thanks to the intelligent use of certificates, INeS allows a device to remain operational in a sort of a secure fail-safe mode, in case its digital identity or certificate becomes compromised. This allows a continuity of service while steps can be taken to investigate on and renew certificates of the device in question.

Furthermore, INeS performs the authentication and validation of the messages coming from the different IoT devices, can add encryption or decryption if required and transfers messages to background applications, with the indication of the actual level of trust one can place on the message and the device.

On top of this INeS provides intelligent entity management, with secure firmware download and dynamic device attributes handling based on business logic that can be defined through configurable workflows. The entity management, with authentication and rights management concerns not only the IoT devices in the field, but the business processes and applications

INeS comes as a managed platform, or SECaaS, but can be licensed as a security add-on to your IoT back–end on-premises.

Just in time onboarding

Typically, to operate in the Internet of Things, controlled by INeS, a device requires two certificates prior to become operational on the network:

- Maintenance cloud certificate: this is a device certificate with its sole purpose of establishing a TLS connection with the cloud for initial enrollment of the device, or if ever the main device certificate gets compromised. It is flagged as such and the security broker INeS takes appropriate measures when communicating with a device using this certificate.
- Secure Channel certificate: This certificate is used to establish an end-to-end secure link between the certificate management system, represented by INeS, and the secure element VaultIC. This allows a private key and new certificate to be sent and installed on VaultIC in a completely protected manner, remotely, and securely.

The onboarding process itself starts with the first connection to the network. Using the Maintenance cloud certificate, a temporary authentication is done by the network and a secure TLS session is established.

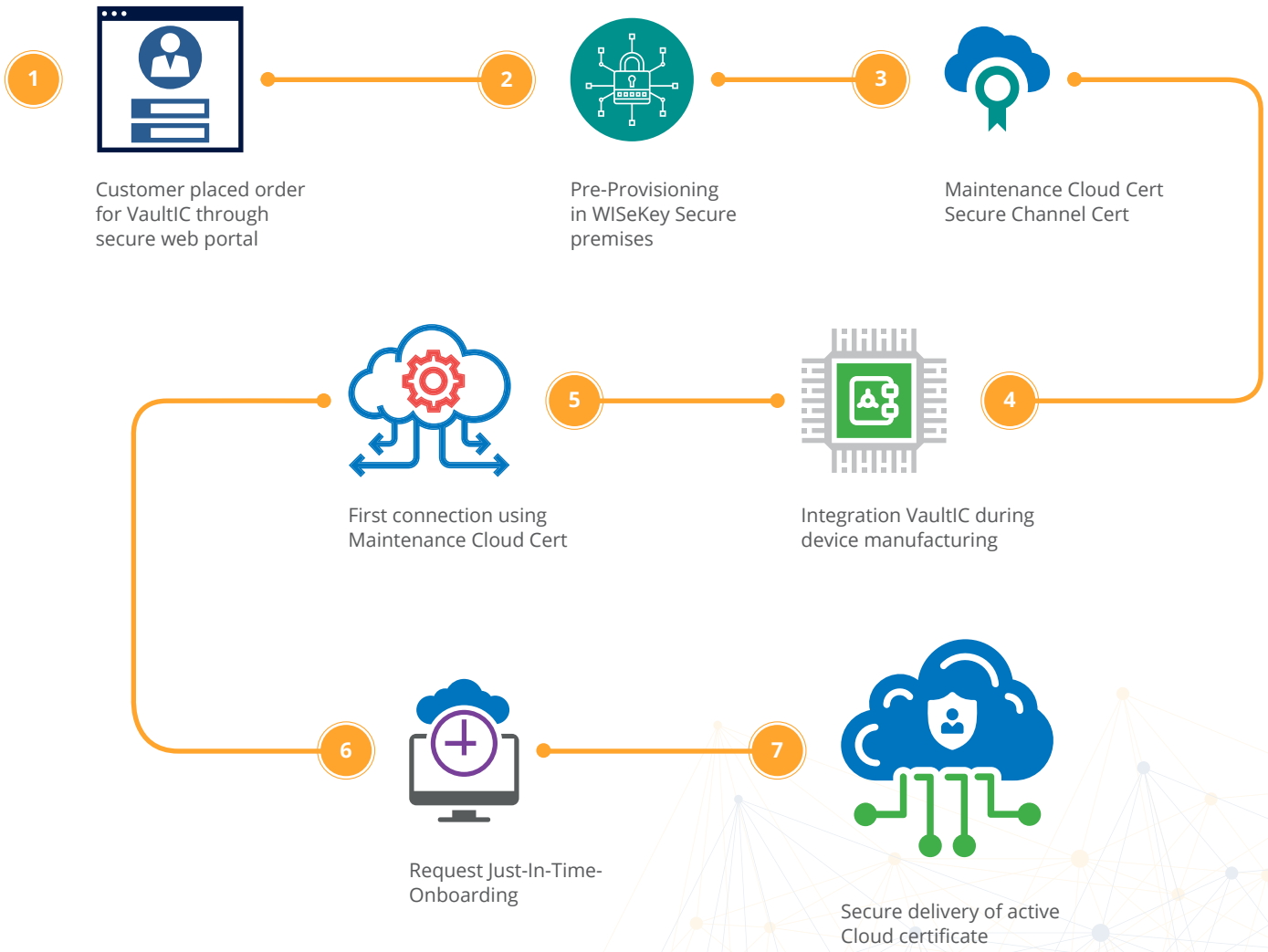


Figure 1: Step by step approach illustrating the Just-In-Time-Onboarding process using the unique combination of VaultIC and INeS

The Security Broker INeS becomes aware of this connection, and following the conditions set out in the workflow, it determines the type of certificate required for the device. A mutual authentication is done between device and INeS based on the Secure Channel Certificate (SCP11), and a related end-to-end secure communication link is set up to download the new certificate and private key into the device.

The device disconnects and can now use the new cloud certificate for further connections to the network.

WISeKey IoT

The seamless integration of VaultIC and INeS, linked to WISeKey's certificate Management System ISTANA is called WISeKeyIoT.

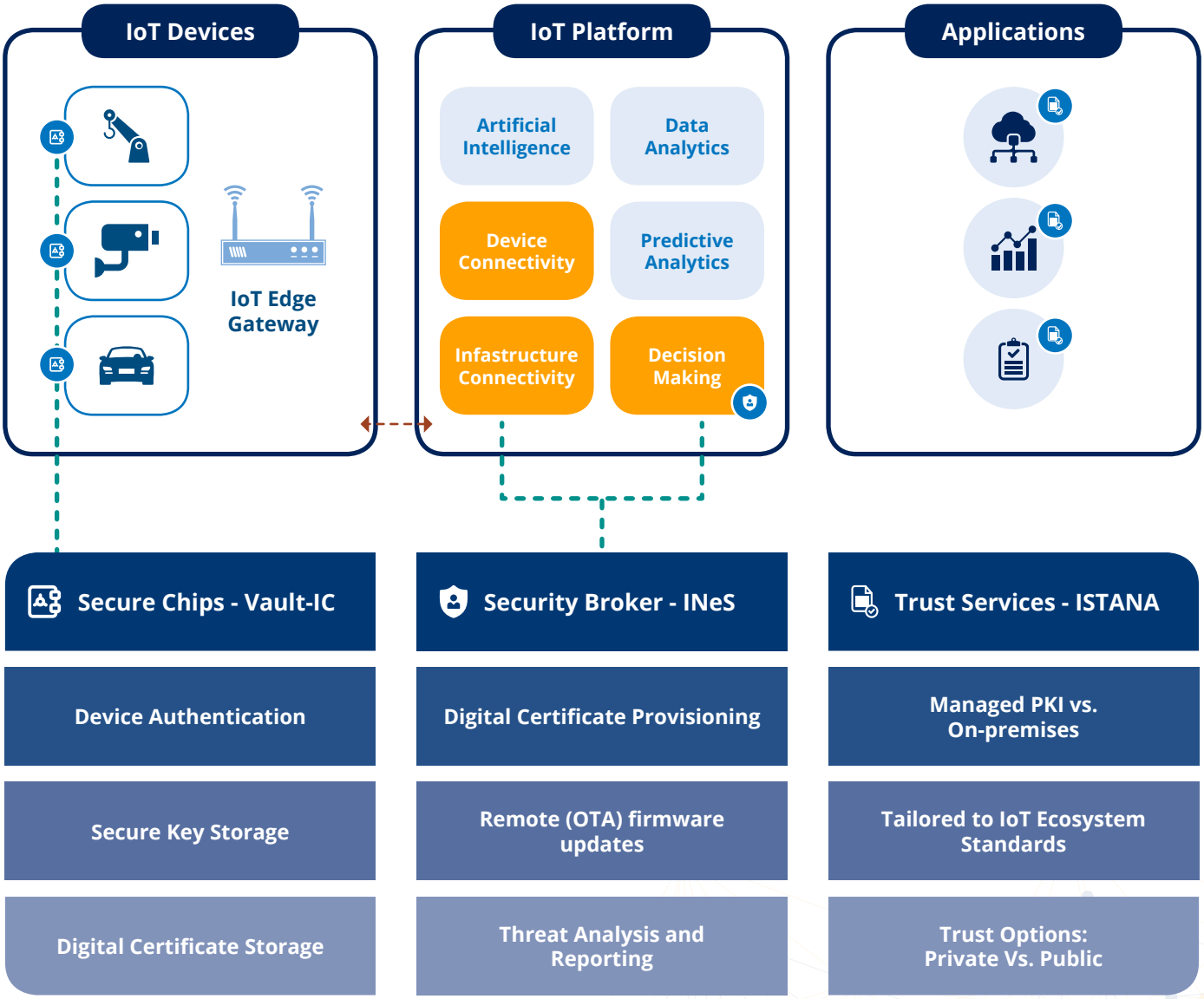


Figure 2: The seamless integration of VaultIC on the device with INeS in the back-end gives an extremely strong end-to-end security solution

As a purpose-made solution for IoT, it combines the strength of VaultIC and INeS to serve one goal: enabling the user trust in the devices, the application and the data.

It brings you the following benefits:

- WISeKeyIoT is a full security solution build by from end-to-end by the specialist of both mPKI solutions and secure microcontrollers, giving you the certainty that no security leaks exist in the 'glue' that otherwise would hold together a multi-party security offer.
- WISeKeyIoT makes it easy for you to be compliant with regularly requirements such as GDPR, as its entity manager controls exactly which information is available to whom.
- Deploying pre-configured secure elements storing the sensitive assets in your devices eases production processes, as no secrets need to be handled and no communication with a back-end is needed on the production floor.
- The intelligent certificate management of WISeKeyIoT allows you to guarantee continuous operation of devices, even if maintenance of the certificates is required and devices would not be allowed to communicate otherwise.
- Using digital identities in a device is far from a one-shot job. Certificates need to be checked, maintained, revoked, and reissued. INeS eases the administrator's job and guarantees full secure deployment, modifications and life cycle control of devices, be it secure firmware updates or certificate renewal, both for individual entities or in bulk operations.
- Real end-to-end encryption, based on state-of-the-art technology and algorithms ensures confidentiality and protects your system's communication.

As a bonus, the use of tamper resistant secure elements in your devices guards them against counterfeiting and possible theft of intellectual property, protecting your brand image and investments.

9.3 WISeKey Semi-Conductors

A device or object can be authenticated over the network using Public Key Cryptography , if it has a digital identity, consisting of a digital certificate and associated device private key. The network sends a cryptographic challenge to the device that signs it using its private key. The network will check the authenticity by verifying the signature, using the public key and certificate of the device. The authenticity of the device is established based on the assumption that only one device in the world can have knowledge of the private key. Therefore, the private key is supposed to remain unique and not used on any other device.

So, how to be assured that the private key is kept secret and cannot be copied into another device? The Web is full of articles describing successful attacks on systems, revealing secrets that were supposed to be protected. Storing and using a private key on a device without enough logical or physical tamper resistance will sooner or later result in the key being found and cloned. And the trust we had in the devices, and by extension the whole system, disappears forever.

For applications where security matters, like credit cards, mobile telephony, passports and the like, it is commonly recognized that the best solution for protecting sensitive assets of a device is to use a Secure Element.

A Secure Element provides an extremely high level of protection, existing specifically for the purpose of performing its pre-programmed security routines. These cryptographic services and functions, executed in a physically and logically hardened environment, include low-level cryptographic methods and algorithms needed for authentication and data encryption/decryption as well as secure storage of essential data items, such as private keys, CA (Certificate Authority) and user certificates, user credentials and configuration data. It allows to unconditionally trust a device and its communications, because its assets are unbreakably linked to it.

WISeKey propose Secure Elements in the form of a physical companion chip named VaultIC.

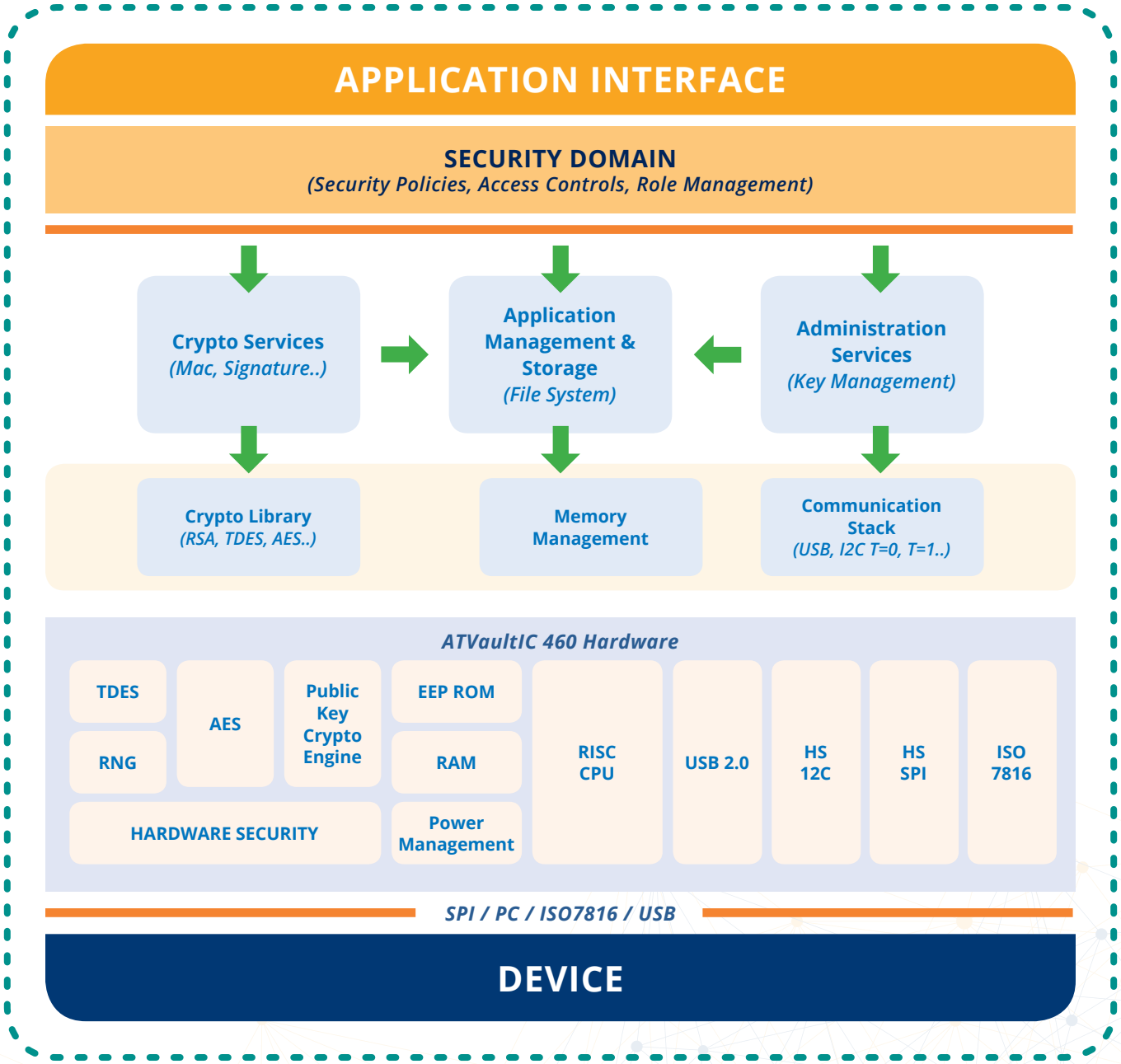


Figure 3 Architecture of VaultIC secure element

VaultIC is a product family of tamper resistant Secure Elements to be used as a companion chip to the IoT-device host processor. VaultIC embeds configurable cryptographic tool boxes for Authentication, Confidentiality and Integrity executed in a secure environment. The tool box proposes a variety of standard and NIST recommended algorithms and key lengths (e.g. ECC, RSA, ECDSA, AES, SHA...). VaultIC embeds on-chip tamper resistant data storage capabilities (NVM) for keys, certificates and customer data. VaultIC also features a True Random Number Generator to guarantee the entropy needed for high-level cryptographic services (not achievable in software).

The VaultIC low-power consumption profile makes it a viable solution to meet the limited power budgets of the embedded IoT nodes.

VaultIC comes with an API and middleware including secure boot, secure device firmware update and a secure communication (SSL/TLS, PKCS#11) stack.

Secure Elements, such as WISeKey's VaultIC, provide multiple advantages when compared with software-based security, including:

- Crypto keys and other security materials are stored in secure memory under the control of secure hardware and firmware, beyond the reach of any software attack.
- Protection against physical attacks, also referred to as tamper-resistant. Certifications such as Common Criteria EAL level 5+, provide the highest level of protection available in the industry.
- Digital signature and verification like ECDA are performed within the Secure Element, using FIPS 140-2 level 3 approved algorithms, thus relieving the main processor from this resource intensive task.
- True Random Number Generation is performed within the Secure Element hardware, delivering true randomness that is vital for high quality generation of encryption keys; Software security solutions cannot achieve this and are limited to Pseudo Random Number Generation, weakening encryption and security.
- Secure elements come with the secret assets pre-provisioned. There is no need for a costly security process to load the assets in the devices during production; simply plug and play.
- The integration of a hardware secure element in a device gives control over production and avoids over production and grey markets.

The WISeKey's designed hardware platform used by the VaultIC module is recognized by international standards and used by banks and government organizations. It is certified Common Criteria EAL4+/5+, while the whole product VaultIC is certified by the US FIPS 140-2 Level 3 (version 2011).

Provisioning

One of the great advantages of the secure Element VaultIC is that it comes pre-provisioned with the required secrets for the device. During the manufacturing of the device, there is no need to process these secrets in uncontrolled environments one can encounter at OEM in low-wages countries; by simply integrating the VaultIC in the electronics of the device and one has a trustworthy equipment without any extra cost in the manufacturing process.

How is this done?

A customer enters a purchase order for a batch of chips on WISeKey's secure VaultITrust Web portal. This triggers the generation of the required certificates in our Certificate Authority, and the creation of an input file for the personalization of the chips in our secure production environment. Our certifications like Common Criteria and Webtrust guarantee the highest grade of security for this process.

An output file is created, posted on the web portal and retrieved by the customer. This file contains the data needed in operation, like for instance chip serial number and related certificate (but not he private key of course).

If the customer uses the Security Broker INeS, described below, as a managed service, this operation will be completely transparent.

DISCLAIMER

This communication expressly or implicitly contains certain forward-looking statements concerning WISeCoin AG and its business. Such statements involve certain known and unknown risks, uncertainties and other factors, which could cause the actual results, financial condition, performance or achievements of WISeCoin AG to be materially different from any future results, performance or achievements expressed or implied by such forward-looking statements. WISeCoin AG is providing this communication as of this date and does not undertake to update any forward-looking statements contained herein as a result of new information, future events or otherwise.

This information memorandum does not constitute an offer to sell, or a solicitation of an offer to buy, any securities, and it does not constitute an offering prospectus within the meaning of article 652a or article 1156 of the Swiss Code of Obligations or a listing prospectus within the meaning of the listing rules of the SIX Swiss Exchange. Investors must rely on their own evaluation of WISeCoin AG and its securities, including the merits and risks involved. Nothing contained herein is, or shall be relied on as, a promise or representation as to the future performance of WISeCoin AG.

WISECOIN

General-Guisan-Strasse 6,
Zug 6303, Switzerland

+41 22 5943 0000

www.wisecoin.com