WHITE PAPER

A TAMPER-PROOF AND DECENTRALIZED DIGITAL IDENTITY

Aexn global undertakes to deploy a means of identification that makes digital identity verifiable and de-centralized. Through an ecosystem of alternative services and interoperability, the Secure Decentralized Identity solution will seamlessly integrate with all the solutions of both today's and tomorrow's Internet.

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

01
Introduction

1. INTRODUCTION

For the past ten years, our relationship to the Internet has been transformed to the point where almost all of our identity and life data, such as personal records or information about our tastes, habits or social environment, is available and stored in centralized databases. Additionally, institutions and companies store the customers' data in their centralized systems, but their vulnerabilities allow cybercriminals to steal the data and then sell it on the dark Web or use it to blackmail these institutions and companies.

Figures confirm this spectacular increase over the past decade and suggest an even greater one in the future. Cybersecurity Ventures predicts that the global costs of cybercrime will increase by 15% per year during the next five years, reaching 10, 500 billion dollars per year by 2025, up from 3,000 billion dollars in 2015. This represents the largest transfer of economic wealth in history, threatens incentives for innovation and investment, is exponentially more important than the financial damage inflicted by natural disasters annually, and will be more profitable than the global trade of all major illegal drugs combined. If the entire wealth stolen by cybercrime in a year was counted as a country's GDP, it would be the fourth richest country in the world1, ahead of Japan.

These figures show the importance of this cost to the global economy. Indeed, data theft not only harms institutions themselves, but also causes considerable losses both in terms of money and time. Globally, in 2020, a single data theft inflicts on average a 3.86 million dollars loss. The report also shows a correlation between the cost of a data theft and the time it takes to detect and contain the threat. The cost of a data theft is estimated to an average of 150 dollars per customers.

1. The Impact on Privacy and Security: The consolidation of personal data in centralized databases has raised concerns about privacy and security. As individuals' lives become more intertwined with the digital world, safeguarding sensitive information is paramount.
2. Cybersecurity Challenges: The increasing costs of cybercrime represent a significant challenge for both businesses and governments. To mitigate these risks, companies and institutions need to invest in robust cybersecurity measures to protect their data and their customers.
3. Economic Consequences: The rise in cybercrime has far-reaching economic consequences. It not only affects the immediate victims but can disrupt supply chains, damage brand reputation, and erode consumer trust. The predicted $10.5 trillion annual cost of cybercrime by 2025 is a stark reminder of the need for decisive action.
4. The Innovation-Investment Dilemma: The threat of cybercrime can stifle innovation and investment. Companies may become risk-averse, fearing the financial and reputational damage associated with data breaches. This can hinder technological progress and the development of new services.
5. Law Enforcement and International Cooperation: Addressing cybercrime requires international cooperation and effective law enforcement. Authorities need to work together to track down cybercriminals and bring them to justice. Additionally, harmonizing cybersecurity regulations across borders can help prevent and combat cyberattacks.

6. Public Awareness and Education: An informed and vigilant public can play a vital role in reducing the risk of cybercrime. Individuals should be educated about online safety, the importance of strong passwords, and recognizing phishing attempts.

7. Data Protection Regulations: Governments around the world are implementing data protection regulations like the General Data Protection Regulation (GDPR) in the European Union. These regulations aim to enhance data security, give individuals more control over their personal data, and impose strict penalties for data breaches
.
8. Technological Solutions: Technological advancements, such as artificial intelligence and machine learning, can be used to detect and prevent cyberattacks. These technologies can help identify unusual patterns of behavior and respond to threats in real-time.

9. Corporate Responsibility: Companies must take responsibility for protecting the data they collect. This includes regular security audits, encryption, and developing incident response plans.

10. Investing in Cybersecurity Workforce: A shortage of skilled cybersecurity professionals is a significant challenge. Investing in training and education for cybersecurity experts is critical to strengthening defenses against cyber threats

For this reason, A team of developer, developed their thoughts on technological solutions that could help solve such problem for the global economy, institutions, companies and users. They gathered a team under the name Aexnglobal, whose ambition was to develop a solution based on the blockchain's decentralized technologies and the recent work of the W3C on decentralized identity (DID3). Aexnglobal hasgrown rapidly.

Since March 2023, Aexnglobal has been developing a decentra- lized identifier called Aexnglobal web(AGC V1) and ONE, a decentralized application (dApp4) that enables the AGC V1 manage-ment. Ultimately, by decentralizing data storage, the company aims to fight the growing cost of data theft for institutions and businesses while giving AGC V1 users back full sovereignty over their data. Thus, a rich and diverse ecosystem of dApps will be developed around the use of the AGC V1 and the entire system will be powered by its utility token, the SYL.

Aexnglobal intends to revolutionize the fight against data theft on today's Internet as well as on the upcoming Web 3.05.

02

EXTERNAL TECHNOLOGIES USED

2. EXTERNAL TECHNOLOGIES

The purpose of this section is to present the external technologies that the AEXNGLOBALecosystem will rely on.

Section 2.1 presents both the network on which Aexnglobal has developed and the one on which they will develop the technological solution presented in this White Paper, namely the Binance Smart Chain.

The section 2.2 presents Smart Contracts technology.

The section 3 presents the technology developed by Aexnglobal, the AEXNecosystem.

NETWORKS & BLOCKCHAINS

BINANCE SMART CHAIN

After studying every possible technological options to provide the best service to its users, Aexnglobal implemented its ecosys- tem on the Binance Smart Chain (BSC) network.

The Binance Smart Chain is a blockchain using a proof-of-stake[6] consensus algorithm. More precisely, it uses an algorithm called Proof of Staked Authority (or PoSA[7]) that allows participants to stack their BNBs to become validators. If they provide a valid block, they receive the fees for the transactions included in that block.

1. Proof of Staked Authority (PoSA): PoSA is a unique consensus algorithm within the Binance Smart Chain. It combines aspects of both proof-of-stake and delegated proof-of-stake (DPoS) mechanisms. In this system, participants stake their Binance Coin (BNB) tokens to become validators, enabling them to contribute to the network's block validation process. This system encourages network security and decentralization, as those who hold more BNB tokens have a greater stake in the network's integrity.
2. Reduced Energy Consumption: PoSA, like other PoS-based algorithms, is more energy-efficient compared to proof-of-work (PoW) algorithms used in some other blockchains. This energy efficiency is beneficial for sustainability and cost-effectiveness, as it reduces the environmental impact associated with blockchain operations.
3. Transaction Speed and Cost-Efficiency: Binance Smart Chain is known for its fast transaction processing times and low transaction fees. These characteristics make it an attractive option for dApps (decentralized applications) that require quick and cost-effective transactions, such as decentralized finance (DeFi) applications.
4. Interoperability: Binance Smart Chain is designed with interoperability in mind, making it possible to interact with other blockchains and assets. This feature is essential for expanding Aexnglobal's ecosystem and allowing users to access a broader range of assets and services.

The network allows transactions to be carried out with fees 100 times lower and at least 10 times faster than the Ethereum network. Beyond this performance, the BSC is able to produce a new block every 3 seconds. Its compatibility with Ethereum tools and in especially its virtual machine (EVM[8]) also allows the network to be extended to all dApps on Ethereum network and their migration to BSC.

All of these advantages have led Aexnglobal to initially favor Binance Smart Chain for the aexn token (AGC V1) smart contract and the first AGC V1 smart contract.

1 Proof of Stake is a block validation method meant to achieve distributed consensus.

2 "Binance Smart Chain uses a consensus model called Proof of Staked Authority (PoSA). It's a hybrid between Proof of Authority (PoA) and Delegated Proof of Stake (DPoS). This consensus model can support a short block time and low fees, and it only requires 21 validators to run. Validators take turns to produce blocks. They essentially power the BSC network by processing transactions and signing blocks. In return for their service, they earn a reward in BNB tokens. Meanwhile, they also require daily re-election by staking governance to be able to continue to be part of the validator set. What are the requirements to be a validator? A validator needs to spin up a hardware node with the required specs, run a full BSC node, and stake a minimum of 10,000 BNB. But that's not all. These requirements are only enough to become an elected candidate. In order to actually start producing blocks, a validator candidate needs to become an elected validator. Elected validators are the top 21 validator candidates with the highest amount of voting power. They change every 24 hours through an ongoing election process, and you can check them out on the top validator list on Binance.org." (Source : https://academy.binance.com/fr/articles/a-quick-guide-to-bnb-staking-on-binance-smart-chain-bsc)

3 The Ethereum Virtual Machine (EVM) is a sub-layer system of the Ethereum platform, it is the one that allows the calculations related to the implementation and execution of smart contracts on the blockchain.

OTHER BLOCKCHAINS SUPPORT

[2023 Update] Aexnglobal evaluated the ability to deploy smart contracts (see section 2.2: Smart Contracts) or to support other DID methods (for some users and issuers/enterprises) on other blockchains.

- Flare Network: Flare10 is a new blockchain that also uses EVM and thus allows the creation of smart contracts (in Solidity9 language). This ecosystem was still not mature and did not manage to attract a real community of developers. We'll check back again this technology later next year.

- Polygon: Polygon11 (MATIC) is a second layer solution based on Ethereum (using EVM too) with a large community of developers and users. A sub-project called PolygonID12 already supports ZKP proofs. We are currently investigating this opportunity.

- Bitcoin: Bitcoin needs no introduction. Bitcoin has little support for smart contracts but can still be a good choice to create public Issuer DID or private user DID. We are investigating the support of BTCR13 DID Method for some use cases.

4 Solidity is an object-oriented programming language used by computer developers to write smart contracts.

10 Official website: https://flare.network

11 Official website: https://www.polygon.com

12 Official website: https://polygon.technology/polygon-id

13 Official documentation: https://w3c-ccg.github.io/didm-btcr/

SMART CONTRACTS

Smart contracts are intimately linked to the blockchain. Indeed, one of the characteristics of the blockchain is its immutability, i.e. the permanence of the information recorded on it. It cannot be modified or erased. It is possible to use smart contracts with the
certainty that they cannot be broken.

A smart contract helps to create AGC V1s. The AGC V1 subject[15] creates a public/private set of keys, keeps the private key and then trans- fers the public key to the smart contract. Since the smart contract makes available this public key, references and information that the user chooses to share on a case by case basis, exchanges with third parties become possible. In addition to the creation and update of the AGC V1, this smart contract

also
acts as a directory so the AGC V1 subject can manage its attributes.

It is a place where non-sensitive information is gathered, allowing the user to assemble their AGC V1 Document (AEXN[16]).

Finally, the smart contract can allow the delegation of the AGC

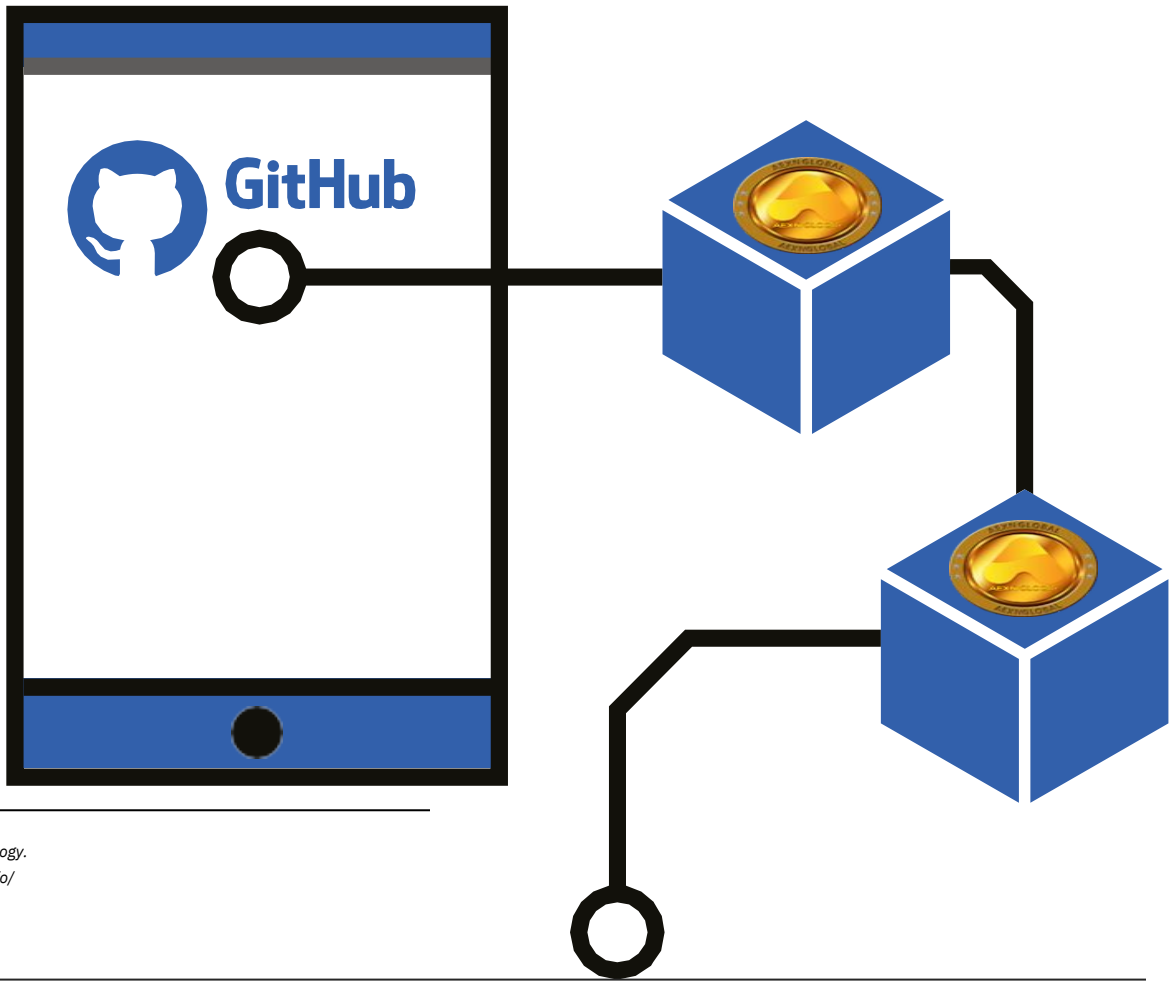
V1
control (for example, the implementation of a parental control).

Thus, this smart contract is an essential tool of the ecosystem, with multiple functions.

It can be consulted on our GitHub[17] .

Synthesis

Aexnglobal has implemented its ecosystem on Binance Smart Chain, which is currently the network offering the best possible service, combining scalability, low network costs, reliability and cross-chain compatibility.



15 Subject identified by an AGW.
16 See section 3.1.2 AGW technology.
17 To consult https://aexnglobal.info/

03

AEXN ecosystem

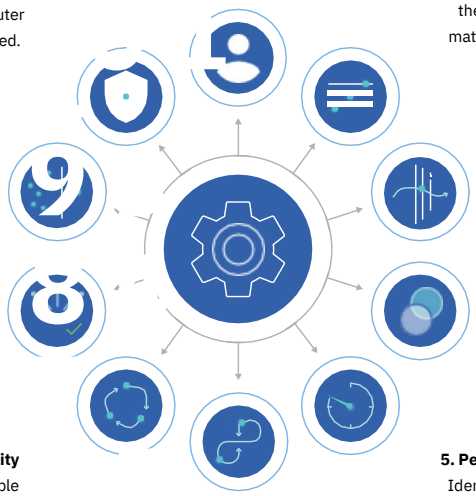
3. AEXNECOSYSTEM

AEXN GLOBAL WEB (AGW)

INTRODUCTION

AGW and Self-sovereign identity (SSI)

The Aexnglobal web(AGC V1) developed by Aexnglobal is a Decentralized Identifier (DID) based on the 10 principles of Self-Sovereign Identity18 defined by Christopher Allen. The aim of Self-Sovereign Identity, like the AGC V1, is to guarantee the users identity pro- tection against cybercriminals and their independence from private or state entities that might be tempted to take advantage of their information or use it against them. The concept of Self-Sovereign Identity seeks to revolutionize interactions between Internet users,
whether they are individuals or entities, by making interactions more secure and trustworthy.



1. Existence
The identity of individuals cannot be reduced to their digital identity; digital identity only makes accessible and public certain aspects of the full identity of individuals.

2. Control
The users must have control over their identity and the way their data is used. They are the absolute authority in this matter, and can decide to share it, to update it, to hide it.

3. Access
The users must have access to all of their data as well as the ability to modify them, without the intervention of any intermediary.

4. Transparency
The systems allowing the implementation of self-sovereign identity must be transparent both technically and in their- management. Algorithms must be open-source, free, and- must be available for review to understand their functio- ning.

5. Persistence
Identities must last as long as their authors wish, at least until they become obsolete due to technological evolution. Users must also be able to exercise their right to be forgotten.

6. Portability
The identity should not be held by a single third party, even if it is a trusted authority. A portable identity ensures that the user retains control of it, which promotes persistence.

7. Interoperability
The identity must be usable as widely as possible throughout the world, across different systems, without the author losing control of it

8. Consent
The user must give his consent to the use of his identity. Any sharing of data with anyone is subject to their express consent.

9. Minimalisation
The disclosure of data must be kept to an absolute minimum. Technical processes such as zero knowledge support this principle, and everything must be done to protect the user's privacy as much as possible.

10. Protection
User rights must be protected. If the needs of identity systems conflict with the rights of the user, the latter take precedence. Systems must also use independent algorithms, be able to withstand censorship, computer attacks, and be decentralized.

Figure : The 10 principles of SSI

The AGW technology, which relies on these principles, is a central component of Aexnglobal' solution against data theft.

How does AGW fight data theft ?

Data storage centralisation is one of the issues Aexnglobal intends to address.

When cybercriminals hack into a centralized database, they have access to every users' data which they can steal and then sell or use for wrongful purposes.

This is the first problem that the AGC V1 solves. According to the W3C19, a decentralized identifier, or DID, is unique and persistent identifier that does not require a centralized registration authority "[because it makes] use of distributed ledger technology (DLT20) or some other form of decentralized network". The blockchain and decentralized servers that form the AGC V1 technology basis enable decentralized storage of AGC V1 users personal data. It is impossible to link identity data to a specific AGC V1 user. Only the AGC V1 subject can use the data, because it is the only person that has the required private key to present them.

This way, a cybercriminal who intends to steal the personal data of AGC V1 users will have to hack each user's device one by one. This renders such practices ineffective and significantly less profitable, thus discouraging them.

The AGC V1 (Aexnglobal) addresses a critical issue by implementing decentralized identifiers (DIDs) and leveraging distributed ledger technology (DLT) or decentralized networks to ensure the security and privacy of its users' personal data. This approach offers a wide range of benefits and safeguards against data breaches, making it significantly more challenging for cybercriminals to exploit the system.

1. Unique and Persistent Identifiers: DIDs, as defined by the W3C, provide a unique and persistent means of identification without the need for a centralized registration authority. This uniqueness ensures that each user is distinct, and their identifier is not reliant on a single, vulnerable point of control.

2. Decentralized Storage: The AGC V1's underlying technology, which includes blockchain and decentralized servers, enables the decentralized storage of users' personal data. Instead of relying on a single, centralized database, data is distributed across multiple nodes, enhancing resilience and reducing the risk of a single point of failure.

3. User Data Privacy: One of the key advantages is the inherent privacy and security of AGC V1 users' data. The system is designed in such a way that identity data cannot be linked to a specific AGC V1 user. Only the individual user (AGC V1 subject) possesses the required private key to access and present their data.

The second problem that the AGC V1 solves is the spread of perso- nal data. With the AGC V1, identification and access to a website or a service may no longer require the sharing of personal data. The service could simply have access to the sequence of characters that constitute the AGC V1 (See section 3.1.2 : AGC V1 Technology) wit- hout ever being able to associate it with other information.

Also, sharing personal data with a service allows the user to choose which data is transmitted, so it is no longer necessary to share irrelevant data with them. Since services only have very limited access to the data, it cannot use it for commercial or po- litical purposes.

It is also possible to access a service without disclosing any data at all. In such case, a verified document can be issued, based on certain data and attesting that the conditions for accessing the service have been met. This process is called Zero-Knowledge Proof.

18 The W3C (also World Wide Web Consortium) is the main international standards organization for the World Wide Web.
20 Distributed Ledger Technology.

Example : In order to register to a service that requires an age verification, the AGW confirms to the service that the requirement is
met, without providing the date of birth.

Therefore, the AGC V1 defines a new era in terms of user data security on the Internet.

In the long run, it will also significantly reduce the power of large companies such as Facebook or Google, whose solutions facilitate, at the cost of massive profiling, the connection to a large number of third-party services. In fact, such power gives them an excessive amount of control over their users' Internet activi- ties, privacy and data. Moreover, their business model relies on their exploitation for profit or political purposes. Today, the right to privacy is not respected and everyone's digital life is partly controlled by GAFAM21.

The AGC V1 technology constitutes a very important example of decentralized counter-power to the Web giants. The AGC V1 allows to keep the practicality of a unique identifier while guaranteeing data security and user's sovereignty over it.

The adoption of DIDs is bound to grow considerably in the years to come. Aexnglobal' AGC V1 can be used in the same way as any other existing DIDs. Eventually and when decentralized identifiers are widely used, it may no longer be possible to request access to a DID user's data without owning one, effectively eliminating the risk of identity fraud and data theft.

A complete overview of the AGC V1 technology and its ecosystem is detailed in the following sections.

GAFAM : Google, Apple, Facebook, Amazon and Microsoft

Synthesis

AGW is a decentralized identifier that relies on the principles of Self-Sovereign Identity. Its purpose is to guarantee the independence and sovereignty of users in the management of their data by using de- centralized technologies, independent from centralized authorities and the power of governments or GAFAM. It helps fight both theft and spread of data by preventing their storage on centralized databases and by using Zero-KnowledgeProof (ZKP) methods.

21 *An acronym for the Web giants.*

AGC V1 TECHNOLOGY

Before being able to associate personal data verified by third parties with one's identity, an AGW must be created. This AGW is an iden- tifier that refers to a single user and respects the following principles :

- It cannot be assigned (or reassigned) to anyone else
- It can operate without a central authority
- It is linked to one or more cryptographic keys to verify that its owner has exclusive control over it
- It allows the retrieval of a public document, the AGW Document, which references other elements such as one or more publickeys or services

W3C DID Syntax

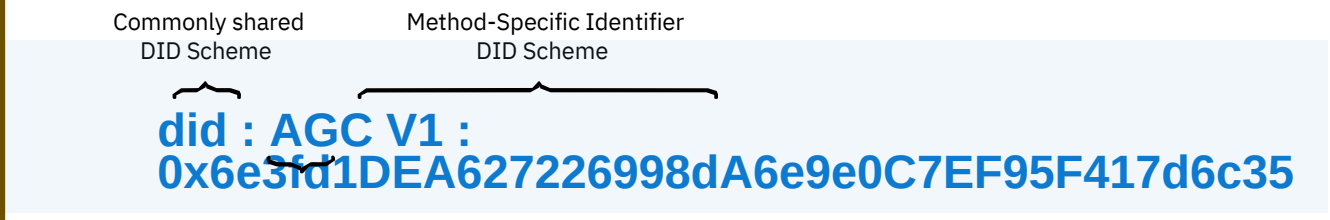


Figure : A user's AGW, unique identifier

AGC V1 Document (AEXN GLOBAL)

The AGC V1 is an identifier associated with an “AGC V1 Document” (called also AEXN GLOBAL) available on a public blockchain.

An AGC V1 Document refers to an AGC V1

The AGC V1 Document is the essential public profile of the user. It is not intended to contain much information, and since it is available
on a public blockchain, it should not contain identity information such as name and date of birth.

Section 3.1.2.4 describes the mechanisms through which new types of information can be added to the AGC V1 Document. Ongoing standardization work will define the possible contents of such document, its syntax and structure.

History and innovation about the technology

In 2017, with the first public experiments on decentralized identities, the Decentralized Identity Foundation22 (DIF) began listing the resolution methods for DIDs to form a "Universal Resolver23" that allows each service provider wishing to interact with a DID
presented by a user to retrieve the associated Document DID.

This correspondence table is referenced in the first document of the W3C working group on DIDs24.

The release of this DID document, finalized in 2019, was a major step forward as the World Wide Web Consortium (W3C) is the leading standards body for Internet technologies (such as with the creation of HTML, DOM, PNG, XML standards).

Aexnglobal will soon join the Decentralized Identity Foundation (DIF) to have its own DID method listed in the official DID resolution table.

AGC V1 Document content

As noted in the introduction to section 3.1.2, the AGC V1 is always associated with an AGC V1 Document. This document does not directly contain personal information, it essentially contains :

- sub-identifiers to localize information in the AEXN GLOBAL (AGC V1 Document)
- public keys
- information about services and public keys
- information about the AEXN's creator and creation date/update
- signature

Definition

Public keys (and indirectly public crypto addresses) are mathematically linked to private keys which must remain in their owner's wallet, under its exclusive control. Private keys are used to sign data (documents, transactions and proofs) and public keys are used to verify the validity of these signatures.

In the following example, the AGC V1 and the AGC V1 Document are linked to an individual. However, the AGC V1 can also be associated with a legal person, an object or an organization.

Here is an example of an AGC V1 Document (in standard JSON/JSON-LD format) :


```
{
"@context": "https://www.w3.org/ns/did/v1",
"id": "did:sdi:aea42randn1awa3xzhjkbvc33",
    "controller": "did:sdi:aea42randn1awa3xzhjkbvc33",
"authentication":
[{
      "id": "did:sdi:aea42randn1awa3xzhjkbvc33#authkey",
"type": "EcdsaSecp256k1KeyFID2021",
        "controller": "did:sdi:aea42randn1awa3xzhjkbvc33",
"publicKeyBase58":
"mM3wnZ3wXmC2AVvLNakc6zjZpfm3uJCwDMv6gVAnHqPV"
}],
"service":
[{
"id":"did:sdi:aea42randn1awa3xzhjkbvc33#webvc",
"type": "VerifiableCredentialService",
     "serviceEndpoint": "https://example.com/vcheck"
}],
"created": "2021-01-01T14:22:21Z",
"proof":
{
"type": "LinkedDataSignature2020",
"created": "2021-01-01T14:21:14Z",
"creator": "did:sdi:aea42randn1awa3xzhjkbvc33",
"signatureValue": "NRB43Y42Q21...1tndsf45sw=="
}

}
```


“did:sdi:aea42randn1awa3xzhjkbvc33”

As a reminder, this document is the resolution of the AGC V1

“did:AGC V1:aea42randn1awa3xzhjkbvc33”. In order to find this document, several segments must

be solved.

“did” indicates a decentralized identity protocol, just as “http” indicates a server/client communication protocol for browsing the World Wide Web.

“AGC V1” corresponds to the used DID method25.

Once the method is found (example : the smart contract 0xb9c15...98e246504 on Binance Smart Chain), the identifier is used to find the AGC V1 document. Here, the smart contract is requested with the identifier "aea42randn1awa3xzhjkbvc33" (this is a random identifier assigned when the AGC V1 is created). Whether directly through a main smart contract or through individual smart contracts, the documentation of the DID method allows to obtain the AGC V1 Document, which is called the AGC V1 resolution.

The rudimentary content of the AGC V1 Document in the figure above can be much more diverse and detailed. This example is an overview of this type of document in order to explain its different parts.

“@context”: “https://www.w3.org/ns/did/v1”

This line indicates that this is a document related to a decentralized identifier.

“id”: “did:AGC V1:aea42randn1awa3xzhjkbvc33”

The first "id" shows the AGC V1 address that is resolved by the AGC V1 Document. It is associated with this AGC V1 Document.

“controller”: “did:AGC V1:aea42randn1awa3xzhjkbvc33”

This first “controller” specifies who controls this DID and therefore who can make changes to it. This example represents the simplest case, where the identity of the controller is the same as the identity which is described in the AGC V1 Document.

This is not the only possibility. Many other cases are possible and can be useful in the following situations (non-exhaustive list) :

- A person uses several different wallets to control the same identity
- A person uses a single wallet to control several identities
- An adult manages certain parts of a child’s decentralized identity
- A person delegates certain rights over all or part of their identity to a trusted third party

```
“authentication”:
[{
        “id”: “did:sdi:aea42randn1awa3xzhjkbvc33#authkey”,
“type”: “EcdsaSecp256k1KeyFID2021”,
        “controller”: “did:sdi:aea42randn1awa3xzhjkbvc33”,
“publicKeyBase58”:
“mM3wnZ3wXmC2AVvLNakc6zjZpfm3uJCwDMv6gVAnHqPV”
}]
```

This segment describes the default authentication method of the AGWs owner. An authentication public key is inserted.

“id” which ends with #authkey allows direct reference to this seg-
ment. Here, the AGC V1 is “did:AGW:aea42randn1awa3xzhjkbvc33” but it is possible to directly show the key which serves as au- thentication.

An anchor allows to proceed and point directly to a specific seg-
ment. In this case :
“did:AGW:aea42randn1awa3xzhjkbvc33#auth- key”.

“type” gives the public key digital signature algorithm used for authentication. In this example, it is the DSA[26] using elliptic-curve cryptography[27].

“**controller**” refers to the AGC V1 responsible for this segment. Once again, it is the simplest case since the reference is identical to the owner of the identity.

“**publicKeyBase58**” is followed by the value of the public key base 58 encoded.

22 Digital Algorithmic Signature : a standardized digital signature algorithm.
23 A set of cryptographic processes particularly suited to public key cryptography.

This segment can be used by an external web service to authenticate a new user using his AGC V1.

```
"service":
[{
        "id":"did:sdi:aea42randn1awa3xzhjkbvc33#webvc",
"type": "VerifiableCredentialService",
         "serviceEndpoint": "https://example.com/vcheck"
}]
```

Verifiable Credentials are described in section 3.1.3. These Credentials are verifiable data available in the user wallet, it is sometimes useful, or even necessary to have them verified by a centralized online service. This configuration makes it easier to share a Verifiable Credential with an entity that is not part of the ecosystem.

In practice, this entity can verify a Verifiable Credential linked to this AGC V1 by going to the indicated address (in this example, "https://example.com/vcheck"), then copy-pasting it or by directly checking the Verifiable Credential in the AGC V1 Document.

```
"created": "2021-01-01T14:22:21Z",
"proof":
{
"type": "LinkedDataSignature2020",
"created": "2021-01-01T14:21:14Z",
        "creator": "did:sdi:admin42randn1awa3xzhjkbvc33",
"signatureValue": "NRB43Y42Q21...1tndsf45sw=="
}
```

\At the end of the AGC V1 Document, a digital signature can be found to authenticate the person who created it. The first timestamp refers to the document's date of creation in the smart contract and is followed by details of the signature which serves as proof, often containing a slightly earlier date.

Again, the simplest case is shown in this example, where the creator is the owner of the identity. But this is not necessarily the most frequent case. Indeed, the creation of an AGC V1 Document on a blockchain often requires the payment of data creation fees and the user is not necessarily the one who performs this tran- saction.

Example : when an AGC V1 Document is created on a smart contract on Binance Smart Chain, a user that downloads a wallet to create and manage his decentralized identity, does not necessa- rily possess BNB (Binance coin) to pay the necessary gas fees when creating this AGC V1 Document. The identity owner can the- refore be in a situation where he knows how to provide all the details to create the content of his AGC V1 Document, but needs an intermediary to help him put this document on the smart contract of the blockchain. This intermediary will pay the fees associated with the creation of the AGC V1 Document on behalf of the user.

The author of the AGC V1 Document can therefore be different from the user. However, even in this case :

The author's AGC V1 can be used to find and verify the identity of the intermediary to ensure that it is indeed a trustworthy interme- diary. Thus AGC V1 can point to the AGC V1 Document of a referenced administrator.

The AGC V1 (Aexnglobal) provides a versatile solution that extends beyond secure and private data management. It can also play a pivotal role in verifying the identity and trustworthiness of intermediaries, offering an added layer of reliability and transparency in various processes. One of the key functions of AGC V1 is to validate the identity of intermediaries and ensure that they are credible and dependable. This is achieved through the AGC V1 Document, which serves as a reference point for administrators.

Identity Verification for Intermediaries: AGC V1 acts as a tool for confirming the legitimacy and trustworthiness of intermediaries in various transactions and interactions. It enables users to rely on a secure and verified source to confirm the identity of the intermediaries they are dealing with.

This does not necessarily mean that the author can modify the information in the AGC V1 document, especially without the consent of the identity owner. The latter may indicate that they alone re- main authorized to make future modifications to their AGC V1 docu- ment or to share control with a third party.

Use case

A web service wishes to authenticate AGC V1 owners through a dedicated web page. This is a common case of authenti- cation on a website initially displayed in a desktop browser.

The server login page displays a QR Code that contains the web service address and a unique random character string (also called a "challenge").

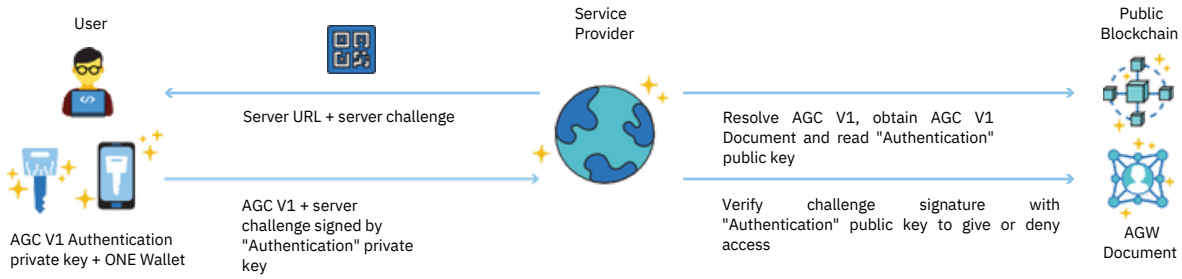


Figure : AGW owner authentication on a web server

The wallet user scans the QR Code found on the web page. The wallet asks the user if they agree to use a key linked to their AGC V1 to authenticate on this server and then, after confirmation, uses the private authentication key to sign the challenge contained in the QR Code. The wallet then sends the signed challenge and the AGC V1 (identifier) back to the server.

The web service receives the AGC V1 (acting as “username”) and
automatically follows the steps described above to obtain the associated AGC V1 Document. The service reads the segment on authentication and finds the public key linked to the AGC V1 that
can be used for authentication by default. The server must now en- sure that the AGC V1 owner has the private key corresponding to this public key. Then, the server checks the validity of the signature it has just received. If the signature is valid, the server confirms the authentication and provides access to the service.

Using an AGC V1 to do an authentication is a simple use case that
is important to understand before moving on to the description of Verifiable Credentials. Authenticating AGC V1 (Aexnglobal) for authentication represents a fundamental and straightforward use case that lays the foundation for a more comprehensive understanding of advanced concepts like Verifiable Credentials. Authentication with AGC V1 is crucial in the realm of digital identity management and offers a wide array of benefits that are essential to grasp.

Note : Within an Aex document, it is possible to assign several authentication keys to different web services and contexts, and also other keys to other uses such as message encryption and contract signature.

VERIFIABLE CREDENTIALS

In order to obtain verifiable personal information, it is necessary that a trusted issuer is previously identified and contacted. Trust in the Verifiable Credentials issuer must be established through verifiable information about their own identity and issuer qualification.

Following the example of Public Key Management Infrastructures (PKI), a chain of trust must be traced guaranteeing the reliability of the identity of all the actors in the chain, it then indirectly guarantees the reliability of the transmitted information.

In a case of a Verifiable Credential (VC) such as a family name, this information can be validated by an issuer qualified as a KYC service provider. This requires prior verification of the reliability of
the issuer's identity through its own AGC V1.

At the top of the chain of trust, the first link is the highest verified identity, the root authority. In the context of queryable AGC V1, it generally consists of the smart contract administrator's
AGC V1.

Establishing trust in the issuer of Verifiable Credentials (VCs) is a critical aspect of ensuring the reliability and integrity of personal information. Much like Public Key Management Infrastructures (PKI) employ a chain of trust to guarantee the credibility of actors in the system, VCs rely on a similar framework to ensure the authenticity of the information being transmitted.

1. Trusted Issuers and Qualifications: To obtain verifiable personal information through VCs, users must first identify and contact trusted issuers. These issuers are responsible for vouching for the accuracy of the information. Trust in these issuers is established by verifying their own identity and qualifications.

2. Chain of Trust: Much like PKI, VCs rely on a chain of trust to confirm the reliability of all actors involved. This chain of trust ensures that each entity in the network can be authenticated, indirectly guaranteeing the trustworthiness of the information being shared.

3. Validation by Qualified Issuers: For example, in the case of a Verifiable Credential, such as a family name, the information can be validated by an issuer qualified as a Know Your Customer (KYC) service provider. This necessitates a prior verification of the issuer's identity through their own AGC V1, establishing their credibility.

4. Root Authority: At the top of the chain of trust is the highest verified identity, often referred to as the root authority. In the context of queryable AGC V1 systems, this typically comprises the AGC V1 of the smart contract administrator. The root authority is the ultimate source of trust within the system.

5. Ensuring Data Integrity: The chain of trust within VCs ensures that every actor involved can be trusted, enhancing the overall integrity of the information being exchanged. This is crucial in scenarios where the accuracy and reliability of data are paramount.

6. Security and Privacy: VCs prioritize the security and privacy of individuals' data by allowing only trusted entities to issue and verify credentials. This protects users from unauthorized access and data breaches.

7. Scalability and Interoperability: The trust framework in VCs is designed to be scalable and interoperable, accommodating a wide range of use cases and facilitating seamless verification across various systems and platforms.

8. User Control: VCs also empower users by giving them control over who accesses their verified information. Users can choose to share specific credentials with selected parties.

As a reminder, it is possible to interact with other DIDs and blockchains as long as the wallet or the tool that seeks to verify a VC can trace the chain of trust of the DIDs between different blockchains (interoperability principle).

It is also possible to not make it mandatory for the root authority to have an AGC V1, but instead to have at least one identity linked to a certificate issued either by a certification authority (as is the case for SSL/TLS28), or by government agencies.

Being able to choose between different root authorities makes it possible to increase the decentralization of the architecture. Nevertheless, it will be necessary for Aexnglobal to work on suppor- ting these different authorities so that the user can easily judge the reliability of the authorities' identities.

1. Interoperability Principle: VCs and DIDs can interact with various other DIDs and blockchains, as long as the wallet or verification tool can trace the chain of trust between different blockchains. This principle underscores the importance of a seamless exchange of trust and verification across different platforms and systems, enhancing interoperability.

2. Multiple Root Authorities: It is not mandatory for the root authority to have its own AGC V1 (Aexnglobal Digital Credential). Instead, a root authority can establish trust by linking at least one identity to a certificate issued by a recognized certification authority (similar to SSL/TLS certificates) or government agencies. This approach offers flexibility in how trust is established, accommodating different trust anchors.

24 Protocols for securing exchanges over information networks.TLS is the successor to SSL.

The following case describes a simple chain of trust.

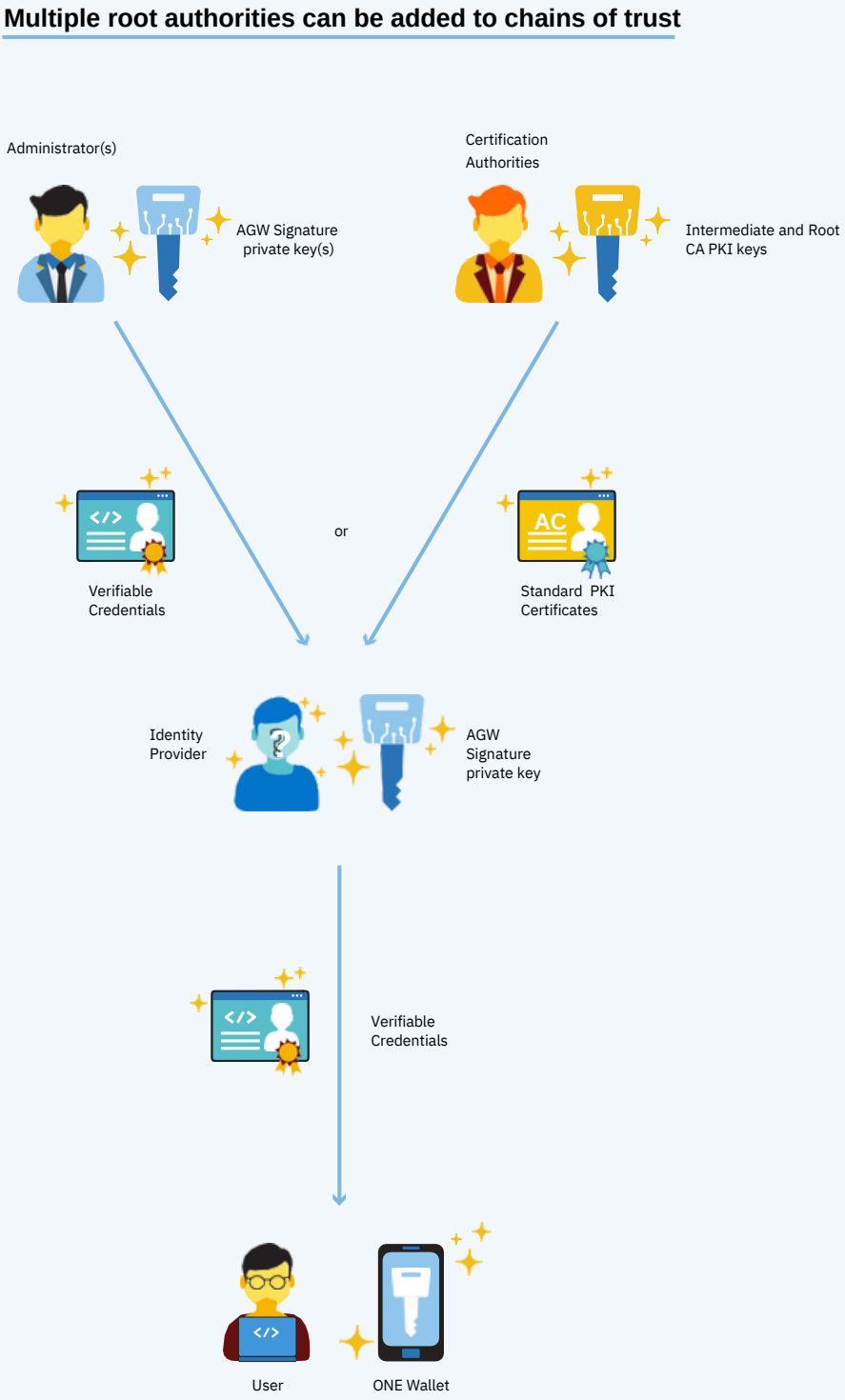


Figure : Verifying a VC also implies going up the chain of trust to check the identities involved

In order for the user to obtain a Verifiable Credential, it is necessary to request it from an identity provider (Verifiable Credential issuer) whose legitimacy has been previously verified.

As mentioned earlier, it is necessary to verify the VC issuer's legitimacy.
The diagram below details the steps of this verification procedure :

How to check if an "Identity Provider" is legit?

Check provider of AGC V1 Document
Check provider of the public profile
Check provider of the Verifiable Credential's public trace Check public Verifiable Credential (role)
Check if AGC V1 Document's issuer is admin
Check Verifiable Credentia public signature

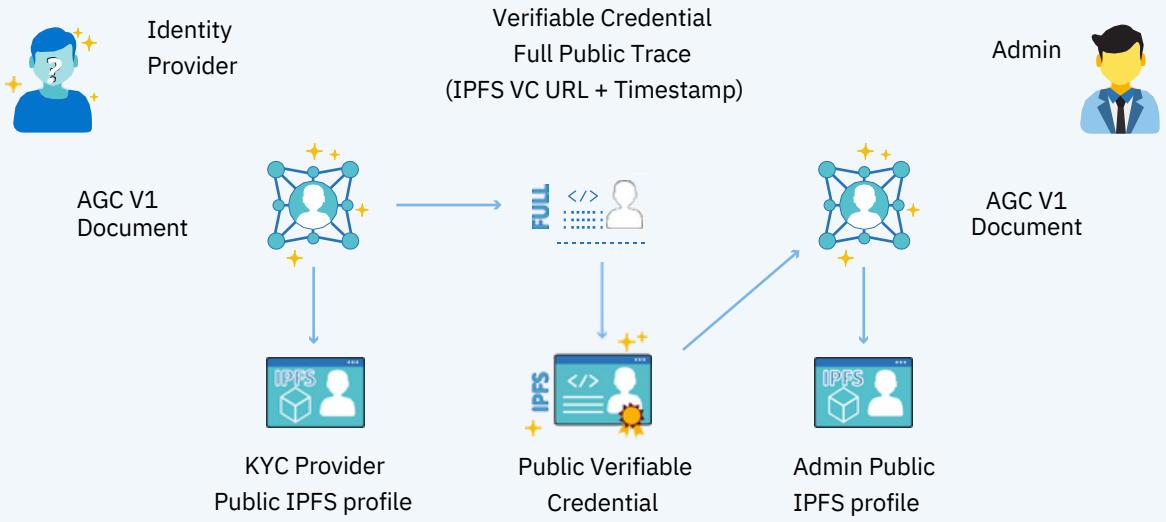


Figure : How to verify that an Identity Provider is trustworthy

The user can be directed to a VC issuer or decide on his own to go to a recognized provider. The notion of verifiable information that
can be presented several times with the same reliability will lead to changes in user behavior and pathways.

It should be noted that the owner (user) that owns a verified identity can also issue a Verifiable Credential for another user.

AGC V1 Document of a VC issuer

The figure below describes a simple use case of identity providers (public issuers of Verifiable Credentials with a clearly identified
role, separated from standard users).


```
{
      “@context”: “https://www.w3.org/ns/did/v1” ,
      “id”: “did:sdi:0x4B20993Bc481177ec7E8f571ceCaE8A9e22C02db” ,
      “controller”: “did:sdi:0x4B20993Bc481177ec7E8f571ceCaE8A9e22C02db” ,
      “authentication”: [{
      “did:sdi:0x4B20993Bc481177ec7E8f571ceCaE8A9e22C02db#keyAuth-1” ,
      “type”: “EcdsaSecp256r1Signature2019” ,
                  “controller”: “did:sdi:0x4B20993Bc481177ec7E8f571ceCaE8A9e22C02db” ,
      “publicKeyBase58”:
      “027560af3387d375e3342a6968179ef3c6d04f5d33b2b611cf326d4708badd7770”

      }] ,
      “assertionMethod” : [{
            “did:sdi:0x4B20993Bc481177ec7E8f571ceCaE8A9e22C02db#VC-Signature” ,
      “type”: “EcdsaSecp256klSignature2019” ,
      “controller”: “did:sdi:0x4B20993Bc481177ec7E8f571ceCaE8A9e22C02db” ,
      “ethereumAddress”: “0x4B20993Bc481177ec7E8f571ceCaE8A9e22C02db”
      }] ,
      “service” : [{
                  “id”: “did:sdi:0x4B20993Bc481177ec7E8f571ceCaE8A9e22C02db#Public_Profile” ,
      “type”: “Public Profile” ,
      “serviceEndpoint” : “https://ipfs.infura.io/ipfs/addresses ”
      }]

}
```


Figure Aex Document of a public issuer of Verifiable Credential

A notable difference is the availability of a public profile on IPFS:


```
{“type”: “Profile”,
“id”: “IPFS”,
“name”:
“Aexnglobal”,
“image”:
“https://ipfs.infura.io/ipfs/
QmXV2ZEMMom4Z9ciFzgNnpJ33oPipb3rzbWe4J5GBfFDSb”,
“url”: “https://www.aexnglobal.info/en/”,
“email”: “contact@aexnglobal.info”}
```


As a reminder, IPFS is a public decentralized storage space where files are referenced by their hash. Thus, the XML content of the above file comes from the IPFS file that can be easily found with an IPFS software, like the image referenced in this file. Web browsers are progressively integrating the ability to read these files on the network. For the moment, it is still preferable to use web gateway services.

Files stored on IPFS cannot be deleted voluntarily so it must be assumed that they can remain available for a long time and for everyone. It is therefore necessary to indicate only neutral and non-nominative information (example: website + generic contact email).

To verify the VC issuer's legitimacy, the user can (with the automatic help of its software portfolio) request the smart contract that manages its AGC V1. Then, the user obtains a list of

Verifiable
Credentials' traces that the issuer has previously received itself. Thus, the verifying software client can find the trace of a Verifiable Credential provided by the administrator to qualify its role as an identity provider (and VC provider) in the form of an IPFS reference (IPFS url) and a reliable timestamp information linked to the blockchain used. The IPFS reference retrieves the public content of the Verifiable Credential provided by the admin to this VC issuer. The client wallet can then verify the signature of this VC by the admin and conclude the legitimacy of the issuer.

Users can have confidence in the reliability of multiple root authorities, thanks to the support for various trust establishment methods. By enabling users to choose the trust anchor that aligns with their preferences and requirements, Aexnglobal enhances the overall trustworthiness of the identity system.

Request and receive a Verifiable Credential

Once trust has been established with the VC issuer, it is possible to request Verifiable Credentials.

Below are the steps required to obtain a Verifiable Credential :

- The user completes the KYC procedure and uses his private key to sign a request for a VC.
- The issuer verifies the signature of this request (by consulting the user's AGC V1 Document).
- The issuer uses its own private key to sign a Verifiable Credential that corresponds to the information verified in the official documents.

This operation can be performed via a web interface or API if the issuer's key is protected on a Hardware Security Module[29]. It can also be performed on a local machine with enhanced security provided by Aexnglobal, which could include a mini software wallet in the form of a smart card reserved for identity providers. The primary goal of this all-in-one solution is to secure and simplify the life of VC issuers.

- The issuer creates an "on-chain" public trace of this Verifiable Credential by associating the hash[30] of this VC with a timestamp information.
- The issuer sends the Verifiable Credential to the user who requested it.
- Identity Verification: The use of certificates from certification authorities or government agencies for root authorities ensures that the identities associated with these authorities have undergone formal verification processes. This adds an additional layer of trust and reliability.
- Identity Verification: The use of certificates from certification authorities or government agencies for root authorities ensures that the identities associated with these authorities have undergone formal verification processes. This adds an additional layer of trust and reliability.
- User-Centric Identity Management: Aexnglobal's approach places users in control of their digital identities by offering them choices regarding which root authorities they trust. This empowers users to customize their trust framework based on their specific needs.

25 HSMs are physical devices that are supposed to be tamper-proof and use cryptographic functions. They can be PCI cards, rackmount external boxes, USB devices, and more.

30 A hash is a sequence of alphanumeric characters resulting from the application of a mathematical function to a set of data. It is a one-way operation.

How to obtain a Verifiable Credential from an issuer

(ex : Verifiable Credential of a nationality from an Identity Provider)

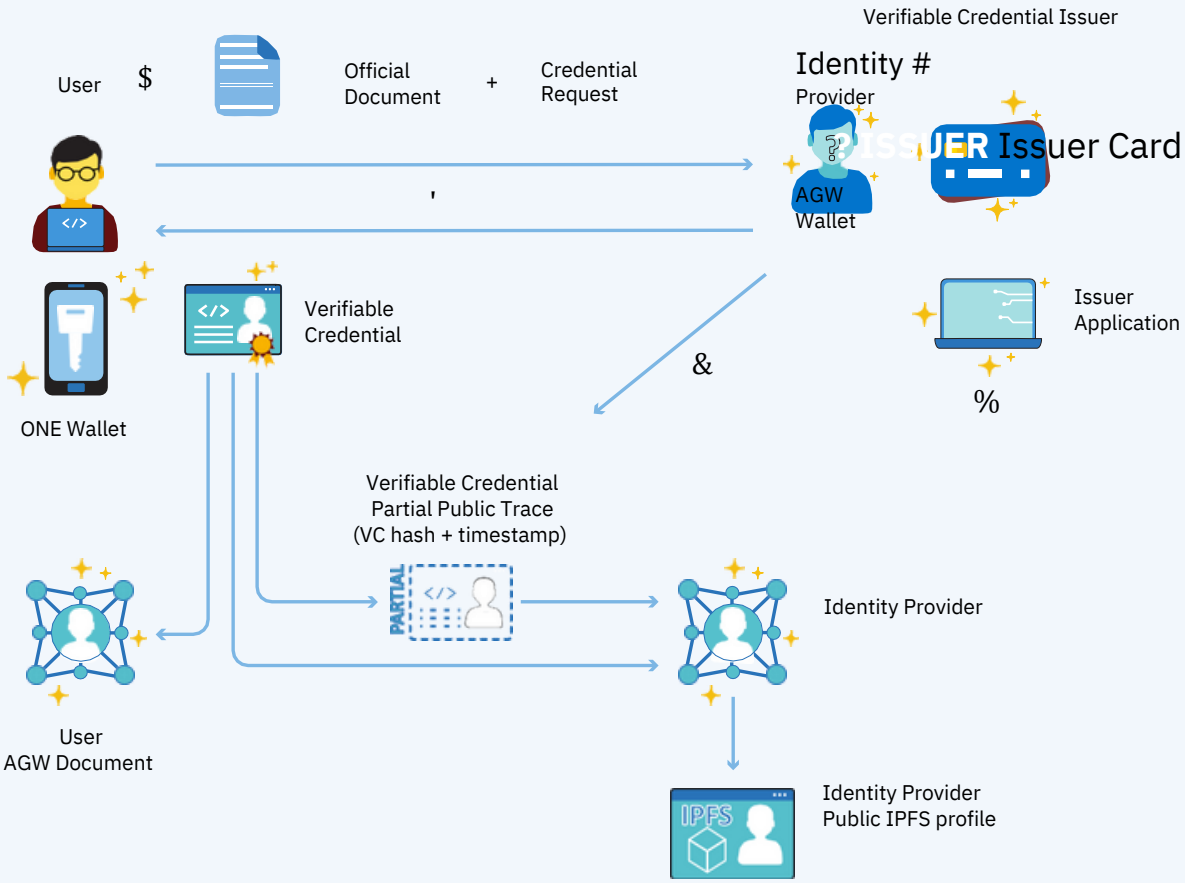


Figure : Steps to request and receive a Verifiable Credential

Verifiable Credential : creation, content and verification

A Verifiable Credential can be transmitted from its issuer to its receiver by email, face-to-face using a QR code, by file transfer, social network, API[31]. The identity wallet of the requester (first receiver) will interpret its content and perform the first total verification of this VC before importing it.

A Verifiable Credential can be transmitted from its issuer to its receiver by email, face-to-face using a QR code, by file transfer, social network, API[31]. The identity wallet of the requester (first receiver) will interpret its content and perform the first total verification of this VC before importing it.

A Verifiable Credential can be transmitted from the entity issuing it to the intended recipient through various means, such as email, in-person interaction using a QR code, file transfers, social networks, or application programming interfaces (APIs). The requester's identity wallet, which serves as the initial recipient, will interpret the content of the VC and conduct a comprehensive verification of the credential before importing it.

31 Application Programming Interface (API) : a set of functions and procedures allowing data communication between applications.

VERIFIABLE CREDENTIAL

Figure : Example of a Verifiable Credential given by a university to one of its members

The Verifiable Credential contains the following information:

- A header to indicate the nature of the file
- Metadata. In the figure above, they contain the issuer's AGC V1 as well as a creation date. But they may contain other

information such as expiration date, associated image, revocation mechanism

- Data involved in the initial request
- AGC V1 of the receiver/owner
- Information previously verified by the issuer (in this case, the university’s membership)
- Proof in the form of a signature with the issuer’s private key dataset

The Verifiable Credential is sent to its owner, who can check it and present it on request.

Each new receiver will also be able to verify the VC themselves.

The verification consists of going back to the Verifiable Credential and checking :

- The owner's AGC V1 ■ The issuer's AGC V1 ■ The Verifiable Credential's signature

How to verify a Verifiable Credential

(ex : Member Credential from University)

6 User provides Verifiable Credential
7 Verifier checks user AGW Document
8 Verifier checks Issuer/Identity Provider AGW Document Verifier checks if Issuer/Identity Provider is legit
9 Verifier checks Verifiable Credential's public trace (timestamp)
:

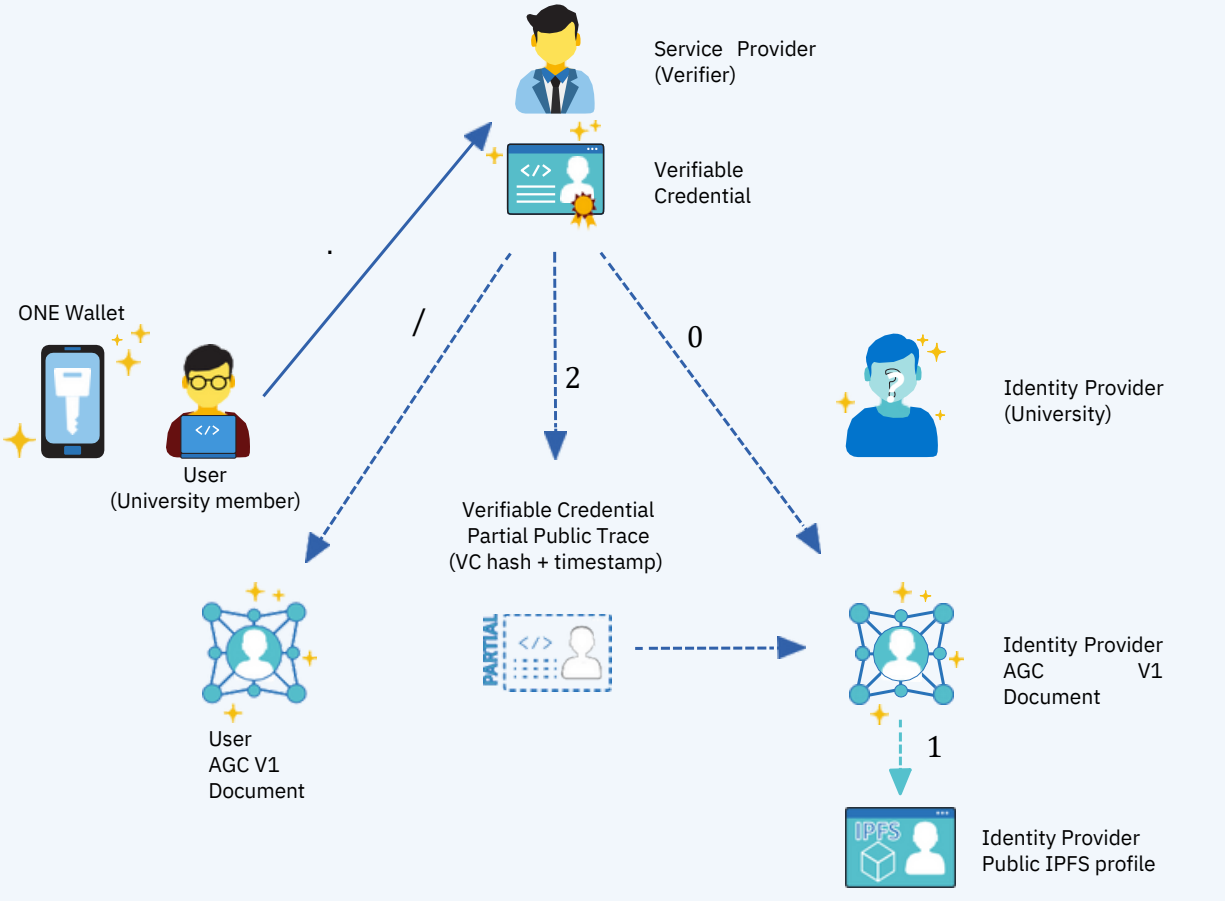


Figure : Steps to verify a Verifiable Credential

Verifiable Presentation : request, content and verification

The presentation of the Verifiable Credential is generally done through another file format, the "Verifiable Presentation". This file takes the Verifiable Credential and associates it with a signature linked to a challenge sent by the VC requester, to avoid any form of reuse.

How to request and obtain a Verifiable Credential from a VC owner

; Requester provides a random challenge, a domain (which can be a website domain or any identifier giving context) with details about which credential is requested and a reason for the request.

< Owner of the VC reads the domain, details and reason and is asked to sign the collected information: credential + domain/ context + requester's challenge. This content, once signed, becomes a Verifiable Presentation.

= Requester checks VC owner AGC V1 Document from blockchain, checks if signature is valid and checks if Verifiable Credential is genuine.

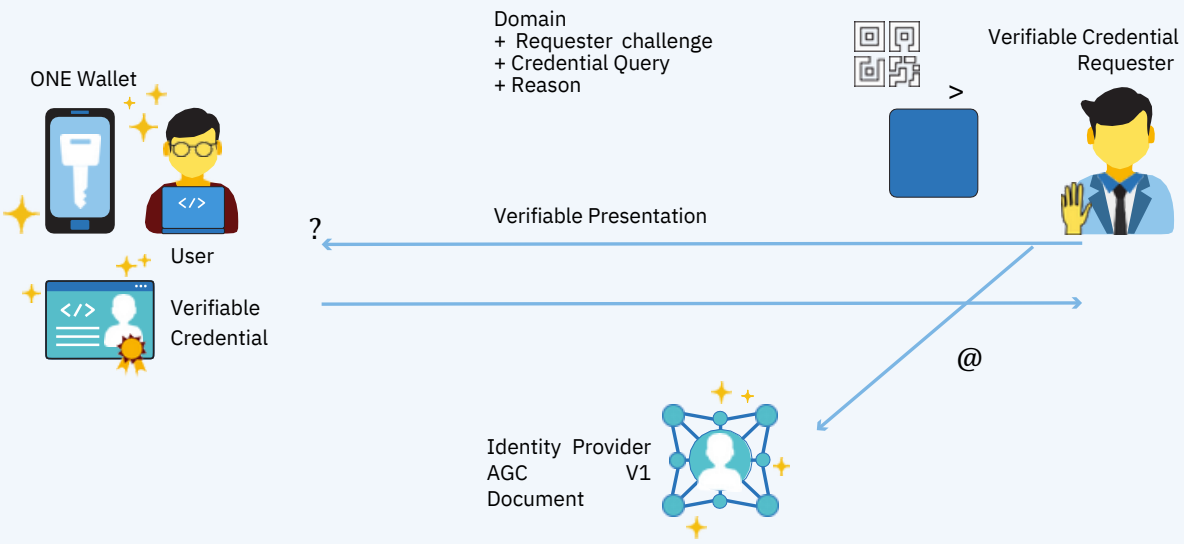


Figure : Request and acquisition of a Verifiable Presentation (signed Verifiable Credential)

Each Verifiable Presentation is unique and specific to the context of a given request and event. The request can be presented in the form of a QR code directly readable on the application ONE (see section 3.2).

VERIFIABLE PRESENTATION

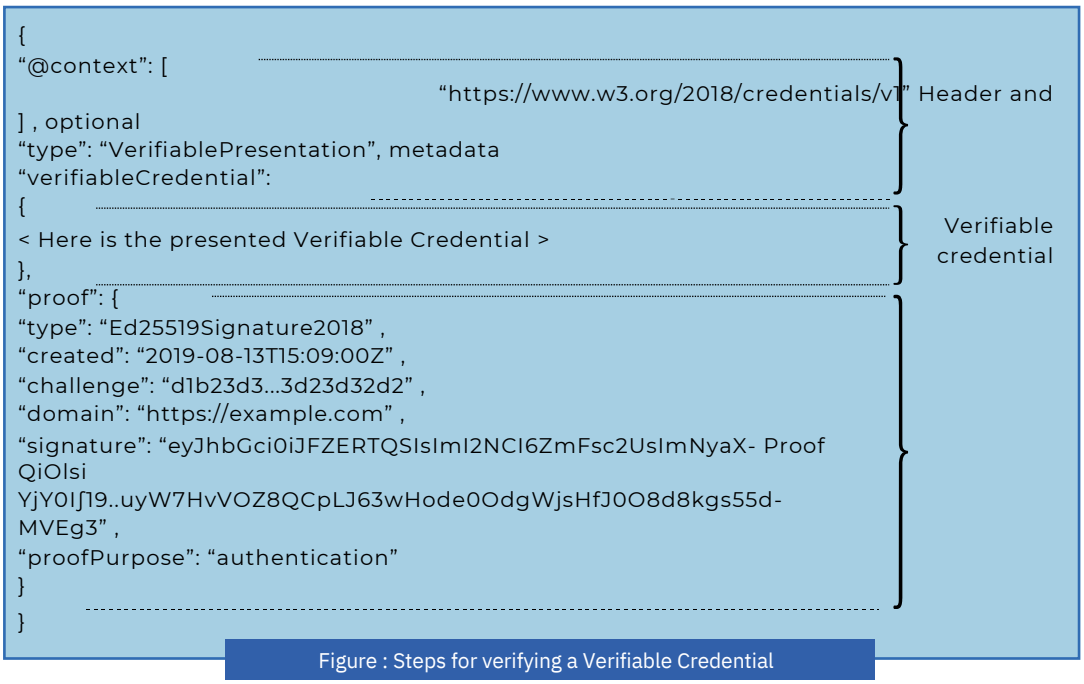


Figure : Steps for verifying a Verifiable Credential

Therefore, the Verifiable Credential and wallet owner is informed about the context before signing it, in order to create the Verifiable Presentation.

The Verifiable Presentation can be sent back to the requester via an address specified in the request details (or in “domain”) or visually with a QR code if the request was made face to face.

The requester or anyone else intercepting the Verifiable Presentation cannot reuse it in any other context.

The requester, who receives the Verifiable Presentation, can therefore verify that he is dealing with the right owner of the Verifiable Credential. The requester needs to verify the Verifiable Presentation's signature through the owner's AGC V1 Document (be- fore verifying the Verifiable Credential).

AGC V1
LIFESPAN

The right to be forgotten is essential when it comes to digital identity data. The AGC V1 user can consult the history of their portfolio
use at any time to better exercise their right to be forgotten. It is possible for a user to publicly revoke an AGC V1 (report it as deactivated). If the user manually destroys his private key, no one will be able to modify or access the contents of their identity wallet.

1. Transparency and Control: AGC V1 places transparency and control in the hands of the user. Users can access and review the history of their portfolio usage at any time. This feature empowers them to understand how their data is being used and make informed decisions about exercising their right to be forgotten.

2. Public Revocation of AGC V1: AGC V1 users have the option to publicly revoke their AGC V1, essentially reporting it as deactivated. This means that they can proactively signal that a particular AGC V1 should no longer be considered valid. This feature ensures that users have a say in the ongoing relevance of their data.

3. User-Initiated Data Destruction: One of the most powerful aspects of AGC V1 is that users can manually destroy their private key. When a user takes this action, it becomes virtually impossible for anyone, including AGC V1 administrators or external entities, to modify or access the contents of their identity wallet. This ensures the ultimate privacy and data control for the user.

UNVERIFIED AGC V1

The AGC V1 features a quick creation function. Any user can use this functionality. It can be activated at a service terminal, a payment point or even a control point.

This function will initiate the creation of an imperfect digital identity which its holder can then complete. The temporary digital identity can be reduced to a minimum of a single piece of information so its owner can take possession of it. In such case, an e-mail address may be sufficient.

An unverified AGC V1 consists of :

- An identity element such as contact information (e-mail address or phone number)
- A function allowing the newly created identity to move to a higher level of verification, involving the use of KYC

The creation of an unverified AGC V1 may be associated with a future incentive benefit offered to the customer or user. The final acqui- sition of this advantage or of the specific right that was granted will require the completion of the AGC V1, via a connection through the decentralized application ONE, or to a service of the official site that will be made available to users.

AGW INTEROPERABILITY

Interoperability and standards compliance (services and resolution methods) are important goals for the AGC V1. They are ensured through compliance with W3C (World Wide Web Consortium) standards and the work of the DIF (Decentralized Identity Foundation).

Synthesis

The AWG is a unique character string identifying a user or another resource. It is linked to a public AWG Document and available on a blockchain that contains functional information such as sub-identifiers, public keys. It also contains information about the creator of the document, its creation date, updates and a signature. It does not contain any kind of identity information.

Each AWG subject owns an identity wallet where its Verifiable Credentials are stored. These credentials are issued by third parties at the beginning of the chain of trust (institutions, companies, organizations or verified users) that contain information related to the identity of the AWG subject, as well as a signature that proves that it has not been modified and a timestamp certifying the issuance time. When the AWGsubject wishes to prove an information to a third party, it issues a Verifiable Presentation which may contain information, about one or more Verifiable Credentials or the sole proof of validity of the information without distributing any other data (Zero- Knowledge Proof).

The AWGcan be verified with a KYC (Know Your Customer) or can stay unverified for a quicker use. It will also be inte- roperable with all other decentralized identifiers (DID) and blockchains.

INTRODUCTION

Context

The following sections aim to define the outlines of the ecosystem built around the wallet ONE. This project is part of the work on decentralized identities which aims to use blockchain to prove the authenticity of personal data and provide a better framework for accessing this data.

The ONE wallet project is rooted in the concept of self-sovereign identity, wherein individuals have complete control over their personal data. Blockchain technology serves as the foundation for this digital identity ecosystem, allowing users to independently manage and verify their identity information.

At the heart of this ecosystem is the innovative use of blockchain to instill trust and authenticity into the digital identity sphere. By leveraging the immutable nature of blockchain, the ONE wallet ensures that personal data is verifiable and tamper-resistant.

Multi-identity wallet

Today, our digital life is made up of a multitude of personal data that are not easily verifiable and abusively requested each time a user account is created. Web services that request them don't usually have any particular interest in getting this data. Until now, each Internet user had neither the tools to manage the dissemination of their identity data nor the means to contribute to track or fight against the collection of data.

Moreover, proving one's identity and attributes is a real challenge in a world that is moving ever more towards the digital age.

Digital identity management includes the management of :

1 User registration and attribute validation phase

2 User identification and authentication on the basis of his verified data

3 Verifiable Credentials reception, storage and presentation

4 Access to services and transactions on the basis of these Verifiable Credentials

Thus, the user is informed of the companies' identity and is demonstrating part of his information in order to access the services they offer. The consent to the presentation of information may be accompanied by a context or a usage agreement (temporary proof, storage duration, potential sharing).

1. User Registration and Attribute Validation: This initial phase involves the creation of user accounts and the validation of personal attributes. Users often find themselves supplying a wealth of information without proper validation, leading to concerns about data accuracy and privacy.

2. User Identification and Authentication: The core of digital identity management lies in the identification and authentication of users based on verified data. In this phase, it becomes essential to ensure that users can be accurately identified and authenticated in a secure manner.

3. Verifiable Credentials: The reception, storage, and presentation of Verifiable Credentials are central to this ecosystem. Users should have the capacity to securely manage these credentials, offering proof of their identity and attributes when necessary.

4. Access to Services and Transactions: Access to online services and transactions is predicated on the presentation of these Verifiable Credentials. Users are empowered to choose which information to share and can be selective in the attributes they reveal. Importantly, they are informed about the identity of the companies requesting this information, promoting transparency.

5. Informed Consent: The consent to present specific information can be accompanied by contextual details and usage agreements. These may include parameters such as temporary proof, data storage duration, and the potential sharing of information, thus ensuring that users maintain control and agency over their data.

Online service providers generally take on the role of identity provider. If not, they delegate this activity to third parties, mostly Web giants and social media.

Through various regulations, governments are trying to :

- Regulate the use of personal data to limit their misuse (GDPR32), often for customer profiling purposes
- Strengthen authentication security levels on the most sensitive online services (PSD2, eIDAS, TSP)

In terms of security, the best practices pushed by these regulators are based on the same cryptographic bases that are well known to crypto-assets enthusiasts: hash functions, data encryption, strong authentication, data and transaction signatures.

Generic cybersecurity and crypto-asset security are already being combined with, for example, the use of FIDO (strong authentication protocol developed by the Web giants and endorsed by regulators) on certain hardware wallets such as Ledger, Trezor and Bitbox or, the support of message encryption in the Metamask software wallet33.

Conversely, some crypto wallets can now perform message signatures outside the usual framework of crypto-asset transactions and transfers.

Traditional centralized cybersecurity actors such as certification authorities can also benefit from this convergence.

One and Aexnglobal ecosystem

ONE is a decentralized application that acts as the control tower of the AGC V1 user's identity.

The decentralization of this app allows it to be independent of any third party authority by freeing itself from all intermediaries that could potentially exert control over users. This dApp, short for decentralized application, allows interoperability of all services that use AGC V1 solution and it represents the gateway to the AEXN ecosystem.

Each presentation of personal data made by the wallet owner is added to a local searchable history (including nature of data, recipient, context, date and time).

The dApp ONE also features a wallet to manage the user's AEXN tokens and their issuance.

1. Decentralization for User Empowerment: ONE's decentralization is its hallmark feature. By operating independently of third-party authorities, it grants users unprecedented control over their digital identities. Users are no longer beholden to intermediaries, and they can assert their digital sovereignty.
2. Enabling Interoperability: ONE acts as a catalyst for interoperability among all services that leverage the AGC V1 solution. This means that various services can seamlessly communicate and interact within the AGC V1 ecosystem. This interconnectedness simplifies user experiences and makes the AGC V1 ecosystem more versatile.
3. Gateway to the AEXN Ecosystem: Beyond its role in AGC V1, ONE serves as the gateway to the larger AEXN ecosystem. It bridges the gap between various services and users, offering a unified entry point to the diverse offerings and opportunities within the AEXN ecosystem.

32 General Data Protection Regulation (EU) 2016/679.

33 Portfolio management extension, allowing easy access to decentralized applications from a web browser.

ONE : CHARACTERISTICS AND PILLARS

PRIMARY FEATURES OF ONE

- Creation of a user space
- Sending and receiving AEXN GLOBAL COIN(AGC V1)
- Receiving, storing and using Verifiable Credentials
- Complete history of the account's interactions
- Services related to the use of cryptographic keys listed in its AGC V1

  (strong
  authentication, electronic signature, data encryption)

THE 4 PILLARS OF ONE

- Protection of personal data

ONE uses the AGC V1 solution in all services that will enable users to connect to it, in order
to protect user data. It will also provide a direct access to AGC V1 settings and a history of
all interactions resulting from the user's activity.

- Scalability and adaptability

Through various decentralized applications available on the ecosystem, ONE can adapt to the needs of each user.

- ID wallet

The ID wallet will be used to receive and store Verifiable Credentials issued by trusted third parties and to issue Verifiable Presentations.

- AEXN wallet

The AEXN GLOBAL wallet integrated directly into ONE will make it possible to receive or send token and to be able to access various services of the ecosystem independently.

KNOW YOUR CUSTOMER SERVICE

KYC & AML for financial institutions

One of the great strengths of ONE is the storage of Verifiable Credentials linked to KYC, Know Your Customer, which makes it possible to comply with AML, Anti-Money Laundering regulations.

This advantage of Aexnglobal' solution aims to considerably reduce the costs in time and money for companies subject to these
legal requirements.

The financial sector, represented by payment institutions, banks, traditional financing platforms and also new crypto providers, are subject to numerous rules (KYC and AML).

The fight against fraud, money laundering and terrorist financing is reflected in the need to repeatedly ask their users for a certain amount of information and proof of identity (when opening an account for example).

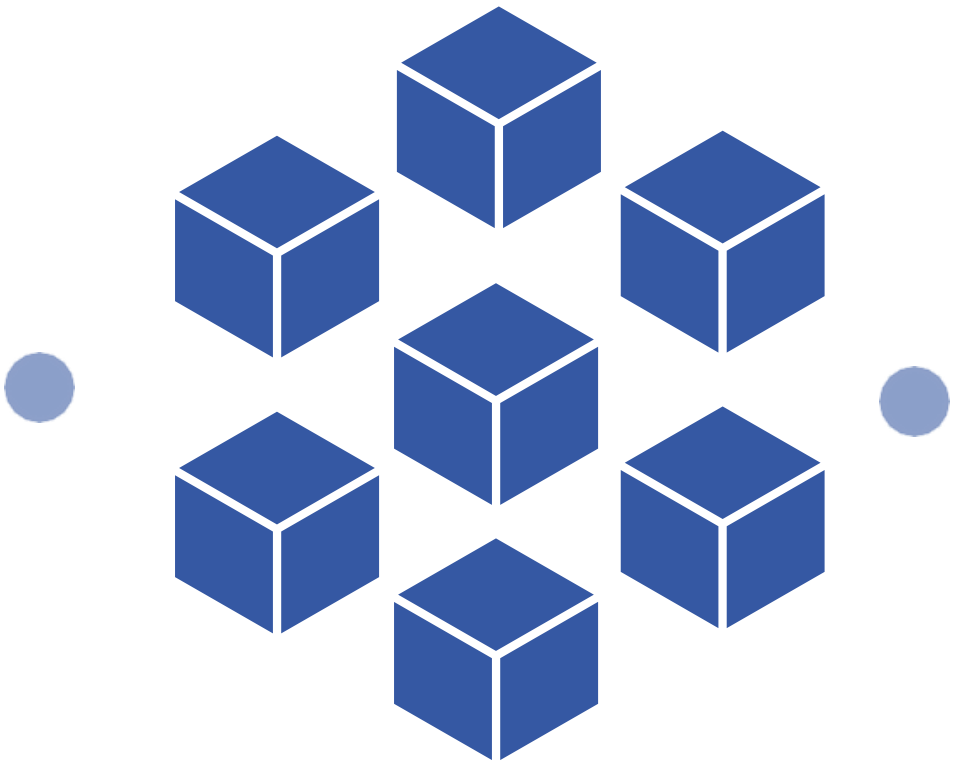
Each bank spends around 60 million dollars a year on KYC processes.

Aexnglobal could save financial institutions a large part of this amount with the AGC V1 and ONE application.

KYC Cost

The cost of KYC that requires access to a third party service may either be covered by the service providers or by the customer depending on the business plan of each service.

KYC is not a necessity by nature, but it may be a prerequisite for service provision, in which case the cost of KYC could be included in the purchase of a service. Once KYC is performed, it will be valid for all services requiring the same level of verification.



ONE TECHNOLOGY

Nowdays, the attributes of online accounts are often hosted by the service that created them. Therefore, the online Service Provider (SP) also acts as an Identity Provider (IDP) with its own authentication portal (Single Sign On).

Service Provider with integrated Identity Provider

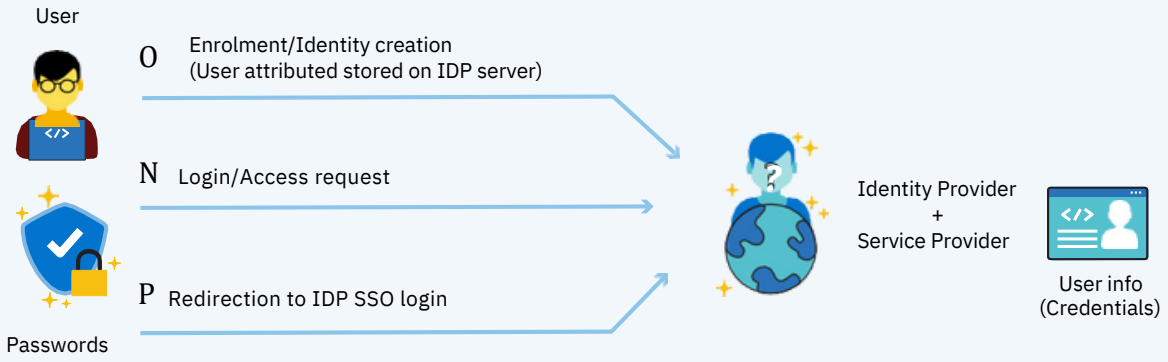


Figure : The Service Provider (SP) creates the user's account and its attributes

The roles of identity provider and service provider can be dissociated. This is the principle of account openings and information sha- ring through authentication on social networks gateways.

Service Provider with Identity Provider

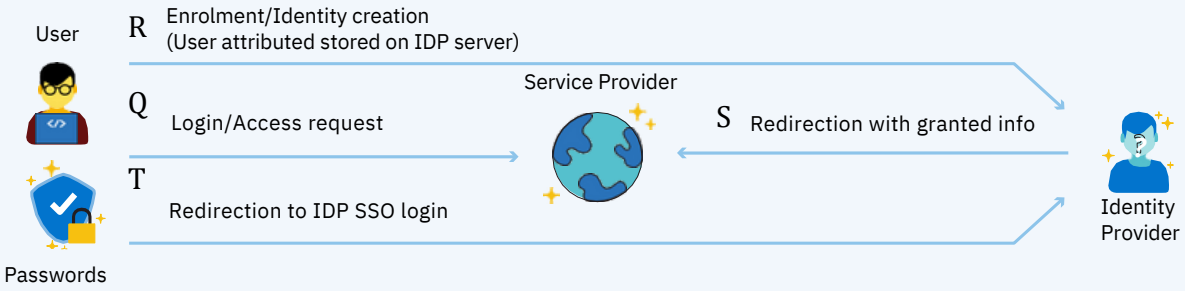


Figure : The Service Provider (SP) uses the attributes of an account that is created with an external Identity Provider (IDP)

Transition to decentralized architectures

In a decentralized architecture, digital assets are assigned in reference to a public address that depends on a private key kept by the user, in their wallet. The user only performs transaction signatures that are verified.

Wallet (locally generated keys) for crypto assets (blockchain)

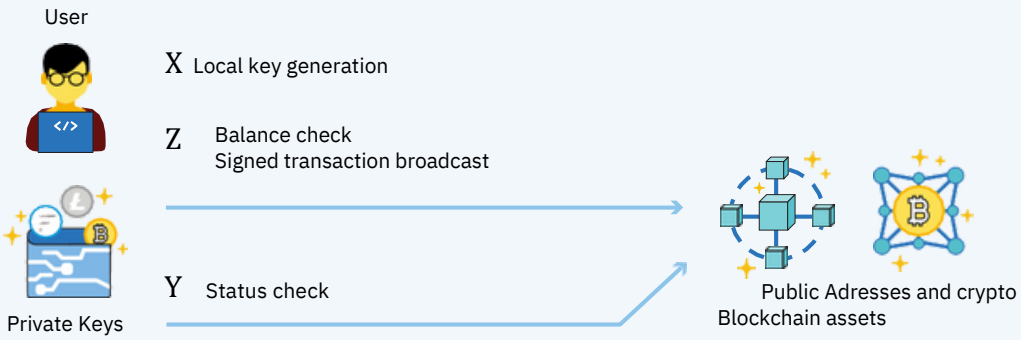


Figure : No personal information is kept outside the local wallet of the AEXNholder

It is also possible to receive and control Verifiable Credentials with the wallet ONE.

Wallet ONE : AGC V1 and crypto asset management

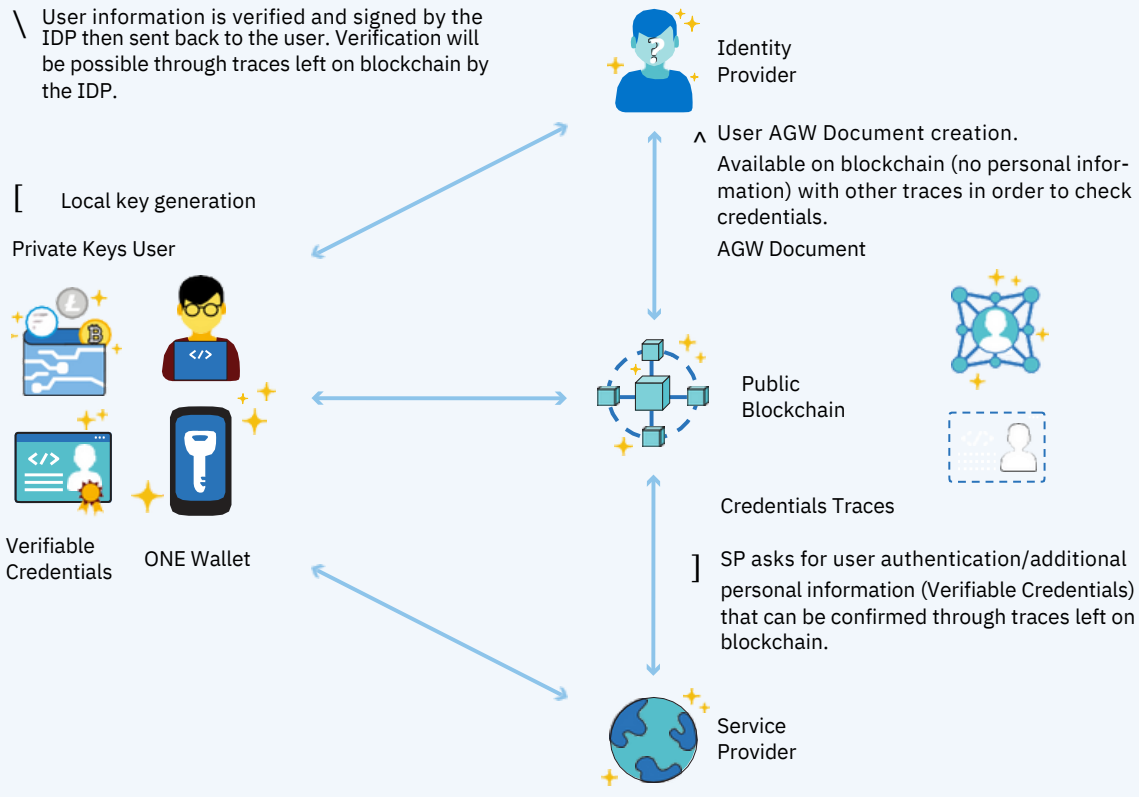


Figure : Wallet ONE is used to receive and control Verifiable Credentials

The wallet that controls the private key linked to the user's AGC V1 must be able to manage the Verifiable Credentials it receives and
must also :

■ Demonstrate cryptographically to the Identity Provider (IDP) ■ Obtain files referenced in the Verifiable Credentials on cen-
that it has control over its AGC V1 tralized and decentralized storage spaces
■ Test the validity and verifiability of the Verifiable Credentials
provided by the IDP

- Store Verifiable Credentials
- Distribute Verifiable Credentials on the right communication channels
- Use other cryptographic keys specified for other uses (encryption, generic signature, signature for authentication)
- Manage some DIDs from other channels for the purpose of interoperability and scalability

This Wallet can benefit from significant progress made by Hierarchical Deterministic Wallets[34]. It also offers a simplified backup and restores procedures.

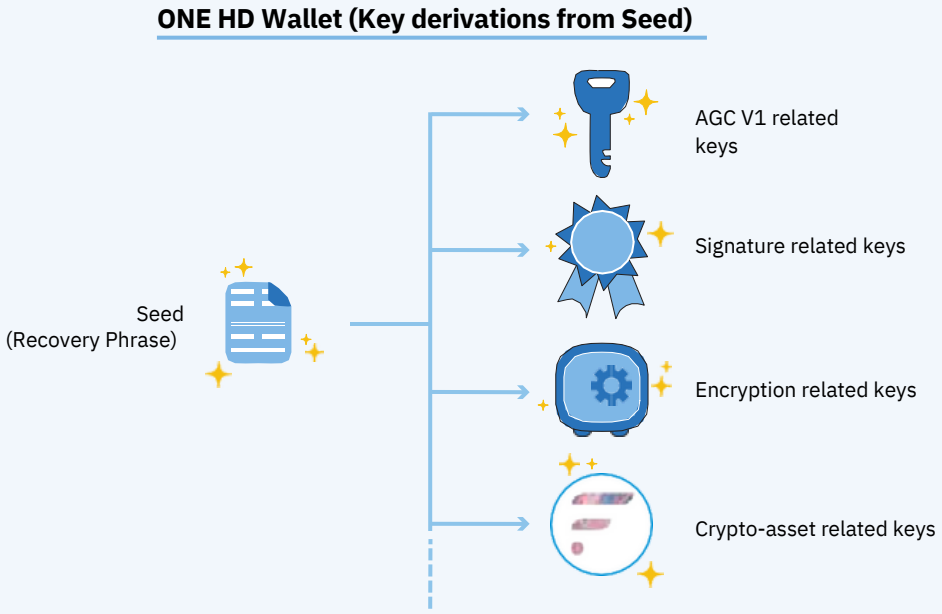


Figure : HD Wallet ONE manages all the private keys essential to all cryptographic uses

Web interfaces

Several optional web services can simplify the use of DIDs and Verifiable Credentials:

- A directory to list services for users, whether they are issuers,
- A host for public Verifiable Credentials when necessary subjects or verifiers of Verifiable Credentials
- A wallet web version for users who need to manage a com-
- A verifier of Verifiable Credentials allowing the creation of mon identity that can be automated challenges (QR codes scan) and the reception and verification of Verifiable Presentations

Synthesis

ONE is the control tower of the AGC V1. This decentralized app enables the interoperability of the services in the AEXN GLOBAL ecosystem. It will act as an identity wallet (DID wallet) by storing the user's Verifiable Credentials and allowing the delivery of Verifiable Presentations as well as the management of the utility token.
The ability to perform KYC through ONE will greatly facilitate the management of legal requirements for companies subject to them, while greatly reducing costs.

34 "HD Wallet" enables the generation of many private keys from a single initial secret called seed.

AEXN GLOBAL COIN(AGC V1)

CHARACTERISTICS

NETWORKS

Currently, the AGC V1 is a BEP-20 token operating on Binance Smart Chain network.

ISSUANCE AND ESCROW

AEXN GLOBAL COIN(AGC V1)

■https://aexnglobal.info

■All Social media Live

■Total Supply =111111 lakh

only

(0x6e3fd1DEA627226998dA6e9e0C7EF95F417d6c35)

■10% INSTANT Developer wallet (11111 AGC V1)

■90% Smart Contract Lock next 10 years.

(99999.90)

■Auto mining going to Developer wallet Daily (27+ plus AGC V1). Next 10 year's

■(AGC V1)SMART-CONTRACT-ADDERSS

LEGAL OPINION & TOKEN CLASSIFICATION

For now, three Legal Opinions have been formulated, in Japan, Singapore and Saint Vincent and the Grenadines, all three recognize the AEXN as a utility token.

AUDIT

AEXN Smart Contract was audited by the hexon, and its report is available on https://aexnglobal.info/

AEXNPURPOSE

ISSUING VERIFIABLE CREDENTIALS

The AEXN token is involved in the payment of certain services, such as the issuance of certain Verifiable Credentials and the payment of certain apps.

In order to reward the use of AGC V1s and Verifiable Credentials, an amount in AEXN can be distributed to the users at the time of the creation of the first AGC V1s, to the issuers of the first Verifiable Credentials, and even to some verifiers.

1. Payment for Verifiable Credentials Issuance: Users can utilize AEXN tokens to cover the cost associated with the issuance of certain Verifiable Credentials. This payment mechanism ensures that users have a seamless way to access and utilize Verifiable Credentials while maintaining the security and integrity of the ecosystem.
2. Access to Applications: AEXN tokens serve as the means of payment for various applications within the ecosystem. Users can use these tokens to unlock premium features, access specific services, or engage with decentralized applications that enhance their digital identity management experience.
3. Rewarding User Engagement: To promote and reward active engagement with AGC V1s and Verifiable Credentials, a system is in place to distribute AEXN tokens to various participants. This distribution includes rewards for the creation of the first AGC V1s, issuers of the initial Verifiable Credentials, and even some verifiers who actively participate in the ecosystem.
4. Encouraging Adoption and Use: The allocation of AEXN tokens to users, issuers, and verifiers serves as an incentive to encourage the widespread adoption and use of the AGC V1 and Verifiable Credential solutions. It recognizes and appreciates the contributions of key players in the ecosystem.
5. Strengthening the Token Economy: The AEXN token's involvement in these various aspects of the ecosystem bolsters the token economy. It creates a vibrant and sustainable ecosystem where users have a clear incentive to engage and participate actively.

Indeed, as explained above, once the AGC V1 of each user is created, they need to obtain Verifiable Credentials that are provided by trusted issuers. These credentials certify certain information about the user's identity. It can be a KYC (Know Your Customer), a diploma or certificate issued by an employer.

Users will also be able to exchange Verifiable Credentials by be coming issuers themselves, thus creating a peer-to-peer network of trust.

APP LIBRARY

When third-party applications use the Aexnglobal ecosystem, a library can be set up with the possibility of purchasing these applications or services with SYL.

PAYMENT GATEWAY

A payment gateway will be implemented in ONE to simplify and standardize exchanges within the application.

The standardization of the payment method among all users allows for the acquisition of Verifiable Credentials regardless of the users and issuers' local currencies.

1. Streamlining Transactions: The introduction of a payment gateway in ONE simplifies the process of conducting various transactions within the application. Users, issuers, and service providers can seamlessly engage in financial interactions without the need for complex or cumbersome processes.

2. Enhancing User Convenience: The payment gateway is designed with the user's convenience in mind. It offers a user-friendly interface and straightforward procedures for executing payments, making the digital identity management experience more accessible and efficient.

3. Standardizing Payment Methods: One of the fundamental objectives of the payment gateway is to standardize payment methods across all users.

4. Cross-Currency Transactions: The payment gateway's standardization of payment methods transcends currency barriers. It allows users to engage in transactions, including the acquisition of Verifiable Credentials, with ease, irrespective of the native currencies in their regions. This cross-currency compatibility contributes to a more inclusive and globally accessible ecosystem.

5. Seamless Access to Verifiable Credentials: Users and issuers no longer face the challenge of currency conversion or disparities in payment methods. The payment gateway paves the way for a streamlined and unified experience, ensuring that individuals can easily access and utilize Verifiable Credentials as part of their digital identity management journey.

This method simplifies the acquisition of Verifiable Credentials for the user. It allows the user to pay trusted issuers of commer- cial Verifiable Credentials or other fee-based services through a single wallet while maintaining traceability of transactions.

CORTEX

AEXNGLOBAL will be particularly useful in the launch of the Cortex pro- ject, which aims to revolutionize advertising targeting by strongly implying the consent of their owner and the preservation of per- sonal data. Advertisers will be able to target users who have consented to be targeted, without them sharing their personal data. A portion of the advertising revenue will also be shared directly with users via an incentive-based AEXNGLOBAL reward.

In addition to the obtained Verifiable Credentials, the user will also be able to add additional personal information.

Cortex litepaper will be released in 2022.

Alongside the Verifiable Credentials they obtain, users will also possess the capability to augment their digital identities with additional personal information within the ecosystem.
The release of the Cortex litepaper is anticipated in the year 2022, and this document is expected to provide comprehensive insights and details about the Cortex project.

AEXNGLOBAL is poised to play a pivotal role in the upcoming launch of the Cortex project, which sets out to transform the landscape of advertising targeting. This innovative project places a significant emphasis on ensuring the explicit consent of data owners and the preservation of their personal data. The ultimate goal is to enable advertisers to effectively target users who have willingly granted their consent for such targeting, all the while ensuring that users do not need to divulge their personal data. This not only ushers in a new era of user-centric advertising but also strengthens data privacy and security.

Key Components of the Cortex Project:

1. User-Centric Advertising: The Cortex project puts users at the forefront of the advertising equation. It centers on obtaining explicit consent from users before delivering targeted advertisements. This approach ensures that users are in control of the data they share and the ads they encounter.

2. Data Privacy Preservation: One of the fundamental pillars of the Cortex project is the preservation of personal data. Advertisers will be able to reach their intended audience without the necessity of users divulging sensitive personal information. This safeguards user privacy while still delivering relevant advertisements.

3. Incentivized User Participation: A groundbreaking element of the Cortex project involves the direct sharing of a portion of advertising revenue with users. This incentive-based model rewards users for their participation in the advertising ecosystem. Users can reap benefits from their engagement, creating a more equitable and rewarding advertising experience.

4. Enhanced Transparency: Cortex introduces a heightened level of transparency into advertising operations. Users can trust that their data is protected, and advertisers can access a consent-based, engaged user base. The ecosystem fosters trust and openness, contributing to a more harmonious relationship between advertisers and users.

5. AEXNGLOBAL Integration: AEXNGLOBAL's role in the Cortex project is instrumental. It provides the infrastructure and mechanisms necessary for secure, decentralized data management, user consent tracking, and the distribution of incentives. AEXNGLOBAL ensures the robust functioning of the project and fosters user trust.

Synthesis

AGC V1 is the utility token of the AGC V1 ecosystem. It is a BEP-20 token running on Binance Smart Chain. It will be used
to issue Verifiable Credentials, to access services inside the AGC V1 ecosystem, and as a payment gateway to simplify and standardize exchanges within an ecosystem that many countries will be able to use, in various currencies.

5. USE CASES

The following sections describe possible use cases for the AGC V1 without being exhaustive.

VISION AGC V1

Aexnglobal has partnered with Swiss Biometrix[35] to develop a ter- minal called ThermoVSN that will integrate the AGC V1 technology in a new network called Vision AGC V1 in order to secure their users' biometric data.

VIDEO GAMES

The use of AGC V1 in the video game industry will profoundly change the video game ecosystem. Aexnglobal will launch a first phase of experimentation with the use of its decentralized identifier. Multiplayer video games face a lot of problems related to the use of cheating software.

Using such third-party programs is prohibited, and most often results in bans for players who use them. There is a problem, however, because while banning a cheater's account makes that account permanently inaccessible, there is no guarantee that a cheater will not return to the game with another account. Thus, any punishment can be circumvented, and the persistent cheater can freely come back to ruin the experience of other players. The AGC V1 will be able to be combined with a unique anonymous ID to alleviate this problem while incorporating various features that will pave the way for a new user experience.

The AGC V1, or Aexnglobal Digital Credential, is designed to provide a robust framework that ensures both anonymity and the utmost security for personal and biometric data. This technology represents a significant advancement in the realm of digital identity management and privacy. One of the key pillars of its design is to guarantee full compliance with the stringent standards set forth by the General Data Protection Regulation (GDPR) concerning the processing and storage of personal and biometric data.

Key Features of the AGC V1 Ensuring Anonymity and Security:

1. Robust Data Encryption: The AGC V1 incorporates cutting-edge encryption mechanisms to safeguard the confidentiality of personal and biometric data. By employing strong encryption protocols, it ensures that data remains inaccessible to unauthorized parties, upholding the highest security standards.

2. Decentralized Storage: One of the hallmark features of the AGC V1 is its decentralized data storage approach. Personal and biometric data are stored in a distributed manner, reducing the risk associated with centralized data repositories. This ensures that data is not concentrated in one vulnerable location, enhancing overall security.

3. User-Controlled Data Sharing: AGC V1 places control firmly in the hands of the data owner, allowing them to determine when and with whom they share their personal and biometric information. This granular control ensures that data is only accessed as per the user's explicit consent, aligning with GDPR principles.

4. Consent Tracking: Consent is a fundamental aspect of data privacy regulations such as GDPR. The AGC V1 incorporates consent tracking mechanisms, ensuring that data processing occurs only when explicit user consent is obtained. This transparency and accountability align with GDPR's requirements for lawful data processing.

The unique identification of each user will be possible after a KYC procedure and will make both player sanctions and rewards effective.

Also, Verifiable Credentials containing a history of players will allow recruiters or other players to have knowledge of each player's positive and negative history.

Verifiable Credentials can also be used to certify players' expe- rience in different games, thus facilitating recruitment to teams and guilds.

Based on these Verifiable Credentials, it will also be possible to organize teams according to the level of the players or to grant connection authorizations according to their age, experience or level.

35 For your information: https://swissbiometrix.com/

36 It includes functions such as "aimbot", "triggerbot", "wallhack" and "ESP" functions. They are common functions in first-person shooter (FPS) video games. Such programs analyze data that the player receives so he can trace his opponents (wallhack, ESP), facilitate aiming (aimbot), or even make it automatic (triggerbot), leaving no chance for a regular player.

ANTI-FRAUD TICKETING

In a concerted effort to combat fraudulent activities and prevent the resale of tickets on the black market, ticketing sites are exploring a novel approach. They are considering the implementation of a secure digital identity solution, such as the Aexnglobal Digital Credential (AGC V1), to enhance the verification process. This innovation aims to establish a strong link between the purchaser of a concert ticket and the individual who will be attending the event. By requesting an AGC V1 from customers, ticketing sites can ensure that the person making the purchase is indeed the same person who will be physically present at the concert.

Key Aspects of this Innovative Approach:

1. Enhanced Ticketing Security: The integration of AGC V1s adds an additional layer of security to the ticketing process. This measure significantly reduces the risk of fraudulent ticket purchases and unauthorized resale on the black market.

2. User Authentication: The request for an AGC V1 serves as a robust method of user authentication, verifying the identity of the ticket holder. This alignment between the ticket purchaser and the concert attendee bolsters the integrity of the ticketing process.

3. Prevention of Unauthorized Resale: One of the primary objectives of this approach is to curtail the unauthorized resale of tickets at inflated prices. By linking the ticket to a specific individual's AGC V1, it becomes more challenging for tickets to be resold on the black market.

4. Promoting Accountability: Ticketing sites, in adopting this methodology, are promoting greater accountability within the ticketing ecosystem. This not only benefits genuine concertgoers but also fosters transparency and trust in the industry.

DATING APPS

The AGC V1 can play a key role in order to strengthen security on dating sites and applications. Issuing a KYC in the form of a Verifiable Credential on the AGC V1 user's ID Wallet will give the assurance that the person registered on the dating site or application is who they claim to be.

LINKS

■AEXN GLOBAL COIN(AGC V1)

■https://aexnglobal.info

■All Social media Live

■Total Supply =111111 lakh only

●90% Smart Contract Lock next 10 years. (99999.90 AGC V1) , Auto

mining going to Developer wallet Daily (27+ plus
AGC V1). Next 10 year's.

●10% INSTANT Developer wallet (11111 AGC V1)

■ (AGC V1) SMART CONTRACT ADDRESS-

0x6e3fd1DEA627226998dA6e9e0C7EF95F417d6c35

■Market https://coinmarketcap.com/dexscan/bsc/

0x6e3fd1DEA627226998dA6e9e0C7EF95F417d6c35

■MARKET =
https://www.coingecko.com/AGC V1/BUSD=
0x6e3fd1DEA627226998dA6e9e0C7EF95F417d6c35

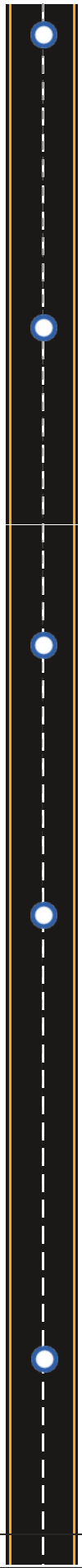
■MARKET
https://www.geckoterminal.com/bsc/pools/
0x6e3fd1DEA627226998dA6e9e0C7EF95F417d6c35

■DEFi EXCHANGE -https://pancakeswap.finance/swap?outputCurrency=

0x6e3fd1DEA627226998dA6e9e0C7EF95F417d6c35

■DEFi EXCHANGE--
https://www.dextools.io/ auto swap/=
0x6e3fd1DEA627226998dA6e9e0C7EF95F417d6c35

6. ROAD MAP



JULY 2023

• Public alpha testnet of AGC V1 smart contract on BSC • Private alpha of ONE wallet app
• Private alpha of KYC VC issuer
• Private alpha of enrolment web services and authentication via VC KYC

SEPTEMBER 2023

• Private alpha and demonstrator of e-sport services (gaming e-reputation)
• Private alpha of the online verifier (VP with challenge) • Verifier's private alpha and online hosting (VP without challenge)

NOVEMBER 2023

• The launch of the gaming portal will leverage decentralized finance (DeFi) and incorporate Aexn Global Coin for transactions.
• Users will have the option to both buy and sell Aexn Global Coin.
• BattleMoney.Live will become fully operational and accessible online, as outlined in the roadmap.

DECEMBER 2023

• Private alpha of services for biometric access control (Facial recognition demonstrator)
• Private alpha of separate VP verification app
• Public beta testnet of AGC V1 smart contract
• ONE's private beta
• Private beta of the online verifier (VP with challenge)
• Private beta and online hosting (VP without challenge)
• Private Beta of VC KYC issuer
• Open source codes for e-sport tools
• Opening of enrolment web services code and authentication via VC KYC

JANUARY 2024

• AFC Trading.live our own centralized cryptocurrency exchange will be launched.

DECEMBER 2023

- Other blockchains support investigation
- Alpha version of Web + HSM service centralizing management tools on issuer's side
- Rewards alpha service for using Verifiable Credentials
- SDK Beta for integration into third party applications
- Audits and stress tests

APRIL 2024

- Version 1.0 of KYC VC Issuer with rewards (KYC AEXNAirdrop)
- Rewards beta service for using Verifiable Credentials
- Public version 1.0 of ONE
- Public version 1.0 of online verifier (VP with challenge)
- Public version 1.0 and online hosting (VP without challenge)

MAY 2024

- DeFi Wallet with Chat Gpt AI.

SECOND TRIMESTER 2024

- Commercial public services of Verifiable Credentials issuers including KYC
- Beta version of Web + HSM service centralizing management tools on issuer's side
- Public SDK for integration into third-party applications
- Opening of authentication integration source codes for CMS/SSO

THIRD TRIMESTER 2024

- Version 1.0 of Web service + HSM service centralizing management tools on issuer's side

More coming

7. UTILITY PORTAL

AEXN GLOBAL UTILITY

- WWW.AGCV1.COM FOR STAKING
- GAMING PORTAL BATTLEMONEY.LIVE
- DEFI WALLET
- ALL API PORTAL WITH AGC V1 PAYMENT GATEWAY
- CENTRALIZED EXCHANGE AFCTRADING.LIVE

Contact

- AEXN GLOBAL COIN(AGC V1)
- https://aexnglobal.info

8. CONCLUSION

Data theft is one of the major challenges our society is facing. Its cost to companies and consequently to the global economy is enormous, and it significantly hinders entire sectors of economic activity.

Aexnglobal' solutions make it possible to effectively tackle these problems. Based on the 10 principles of Self-Sovereign Identity, Aexnglobal' decentralised identifier, the AGC V1, enables users to maintain control over their identity and their data.

Solutions built around Aexnglobal' decentralized architecture will help reduce the need to store personal data on centralized servers, while reinforcing the reliability of the presented information and the authentication of its owners.

The decentralized app ONE, which enables the control of the AGC V1, will also simplify KYC (Know Your Customer) and AML (Anti-Money Laundering) procedures.

Cortex advertising services will benefit advertisers and users, allowing them to target Internet users in a more ethical manner that respects their privacy and personal data, while rewarding them in SYL.

With these new tools, Aexnglobal is committed to build an open and collaborative Internet of Trust for the future.

Contact

■AEXN GLOBAL COIN(AGC V1)

■https://aexnglobal.info