KYC’d Identity

Author: Scott Nelson
May 2019

ver 1.01

Abstract

A Know Your Customer (KYC) verified identity is needed when conducting any form of financial transaction that transfers value. Banks and financial services organizations are required by the regulatory environments of different legal jurisdictions to implement and maintain KYC processes. The requirements and processes used vary by jurisdiction and organization and are based on many factors.

The Sweetbridge Platform provides a flexible protocol for creating and managing KYC'd identity. It is not simply a KYC tool. Instead it provides the ability for anyone to create KYC components using any interfaceable tool, automated or manual process. These processes are all auditable and verifiable by audit organizations and regulators.

The output is not simply a KYC risk assessment but a shared and common KYC'd identity with credential proofs, validations and continuous monitoring where needed. These identities and credentials can be used across multiple organizations in multiple legal jurisdictions. The processes are completely configuration driven and can be interfaced with one or more databases, processes, tools or solutions to obtain proofs or validations and to perform monitoring.

The Sweetbridge KYC protocol is part of a much bigger platform that does synchronized accounting. Synchronized accounting synchronizes identity, agreements, ownership status, accounting treatments and settlement between all counterparties in real time. This means it is able to do most aspects of financial audits, process compliance and regulatory compliance in real time. The result is more than KYC, as it enables exceedingly strong AML and anti-fraud while reducing error and measuring risk.

The Sweetbridge platform is decentralized, consisting of audit nodes, identity nodes and verifiers that create a web of cryptographic proofs for identity, credentials and much more. The platform uses components that can be developed by anyone to construct modular processes for KYC, credential validation, and KYC checks. This makes the platform very extensible. Component that are created by others when used in another component can even charge royalties or fees to compensate the author and subsidies support.

The Problem

KYC processes can be frustrating to customers who don't understand why they are being asked to provide information. Existing processes frequently don't result in a unique identifier and so cause duplication of identity. Today, every organization has custom KYC processes and the results are not easily shareable or verifiable by other entities. This means that an individual or organization must provide similar information to each financial service organization.

GDPR and cyber risk further complicates KYC processes as well as the requirement that personal data on directors and owners be stored within certain legal jurisdictions. There are also regulatory risks and compliance risks of fines when KYC processes are not performed according to process documentation or regulations. This means that KYC processes tend to be expensive, bureaucratic, and time consuming while frustrating customers, leading to a delicate balance between customer experience, financial inclusion and risk management.

KYC processes are historically siloed to a single entity and other than when entities use common tools there is little shared information. This means KYC processes are fragmentary and inconsistent. Many perfectly fine individuals and organizations may be wrongly excluded by KYC processes and many KYC processes fail to detect the real risks, focusing more on bureaucratic processes to avoid fines.

The problem today is that KYC processes don't end up with an identity and credentials that can be used with any organization or in any legal jurisdiction. Furthermore an identity with credentials are not enough. The credentials along with the proof and verifications need to be accessible by other organizations, auditors and regulators when needed.

Overview

The Sweetbridge Platform supports a flexible, configurable and extensible set of KYC'd identity components. These components can be used to do KYC of individuals and organizations down to the individuals who are the ultimate beneficial owners. Its KYC process is configurable and modular, allowing it to be configured to the precise needs of the use case and jurisdiction. If the existing components can't address the unique needs in a specific case, new components can be added to the platform as needed.

KYC requires a process. Technology can help make the process more efficient but it is important that the proper process come first and foremost, not the technology. That is why the Sweetbridge platform starts at its core with configurable workflows. These workflows are designed to automate and verify any process. These workflows can integrate any external tool or database accessible via an API.

In addition, these workflows allow for humans to play a role where desired or needed. All workflows have configurable and modular inputs, outputs, validations and statuses. The Sweetbridge platform uses technology to automate and police these workflows as well as perform validations.

The platform is decentralized, storing source documents, proofs and validations at the edge of the network. This reduces risk from cyber attack and makes the network scalable. These documents and records are shareable with auditors and regulators; for documents and information where there is a low cyber risk, this happens through centralised audit nodes.

High risk information and proofs are stored on the edge device[1] in an encrypted form that uses biometrics or unique, individual specific, data to unencrypt the data. The data can only be decrypted on the device that encrypted it, making hacking difficult. High risk information and proofs are only shared in memory through encrypted peer to peer connections.

When highly confidential information is shared for audit or reverification a cryptographic signature of any verifications are added. This increases the verification of the validity of the information while decreasing the need for the data to be shared again as the number of independent verifications increases. This allows the veracity of information to be attested to but without requiring it to be shared.

Documents at the edge can be requested by anyone in the network when needed but must be authorized by the individual in control of the edge device or their agent. Individuals can have one or many hosted cloud agents. These agents can respond to information requests from authorized parties. This reduces any centralized “honey pot” of information, making cyber attacks extremely difficult and expensive. It also makes the process compliant with GDPR and jurisdictional privacy data storage laws.

Legal Identity

The Sweetbridge Platform is designed to model all forms of individual and organization structures. An organization represents a legal identity in law within a jurisdiction or state government. It represents a type of group or association of individuals who are joined together either formally or legally. We use the term organization to include a corporation, foundation, trust, partnership, marriage, sports team, and any type of group, civil or political association of people recognized by a government.

Entity identity

In the platform there are two types of entities:

1. With a Tax ID - Those with tax identity of their own, and
2. Without a Tax ID - Those with tax identity that comes from their membership or owners

An entity can be an individual or an organization. All individuals are assumed to have a tax ID (even if it is their name) but only some organizations have their own tax ids. The Sweetbridge platform models both types of identity and creates an additional cryptographic identity backed by a cryptographic credential that is considered mathematically so improbable to counterfeit as to be impossible.

The Sweetbridge identity can be invalidated at any time and one or more credentials can be invalidated by the issuer. This means that once issued, credentials and identities can be revoked as needed. Any entity can check the current validity of a credential or identity so these identities can be used to prove the identity and credentials are valid for a specific type of KYC. This provides evidence that the KYC process has been performed and is current.

[1] An edge device is a device at the edge of the network in a decentralized network and is physically under the control of its owner as opposed to cloud storage.

Use of the Sweetbridge identifier externally is optional. But, when used, it can significantly strengthen cyber security and reduce identity theft. It eliminates the need for websites and financial services to keep or hold personal data. In addition, the Sweetbridge ID is issued to each user on the platform and can be used instead of a user id / password to access the platform when adding or updating their information or the information of an organization they maintain. It can also be used to replace a user id and password system on any organization's website.

This Sweetbridge identity either requires a smartphone / tablet to verify the individual through biometrics or a computer to verify the individual through the weaker password and user id combination. Phone and in person support can also be supported for the less abled or when walk in support is desired.

Jurisdiction-Specific Credentials

All identity credentials are jurisdiction- and (optionally) organization- specific, therefore the Sweetbridge platform supports jurisdiction-specific models. Each jurisdiction in the Sweetbridge Platform can have multiple identity verifiers. Each identity verifier uses the same credential schema for the jurisdiction.

Take tax IDs for example:

- In the US individuals have a Social Security Number (SSN) but in Singapore, it is the National Registration Identity Card Number (NRIC), Foreign Identification Number (FIN), Tax Reference Number Assigned by IRAS (ASGD) or the Income Tax Reference Number (ITR).
- For organizations, such functional equivalent tax ID types include, the Tax Identification Number (TIN) for a company in the US, the Permanent Account Number (PAN) in India, the Unique Entity Number (UEN) in Singapore, and the Business Registration Identity Card Number (BRID) in Hong Kong.

The scheme for tax ID is therefore:

- Jurisdiction Code - The country code for the country this tax ID is for,
- Type - The type of tax ID when the country supports more than one
- Number - The value of the tax ID if one exists for the country
- Name credential - The name associated with the tax ID or that serves as the tax ID in countries that don't have tax IDs[2].

Identity verifiers can be audited by external auditors and / or government regulators to make sure their processes meet the government and financial organization requirements. By supporting multiple verifiers governments can decentralize identity verification and can even require multiple verifiers with higher risk entities.

[2] Some countries don't have tax identifiers such as Bahrain, or the United Arab Emirates (UAE) and others only issue them for companies such as Kuwait, Oman, and Qatar.

Entities with a Tax ID

When an entity has a tax id, the tax ID is used to determine if the entity already has a KYC'd identity. The tax identity is never stored itself. Instead, a cryptographic hash of the ID type and tax ID is stored. The real tax ID can't be determined from the hash but no two tax ids will produce the same hash. This means the hash can be used to determine if the identity already exists.

Entities without a Tax ID

When an organization does not have a tax ID of its own, the members of the organization are used to locate organizations to which the party belongs. A list of the organizations to which an individual belongs is returned when someone is adding an identity. The user can then select the organization if it already exists.

Entities with unique names

Entities such as individuals in Qatar or registered companies in EAU typically have unique official names. These names can usually be verified with governmental sources or by providing documentation such as a birth certificate, partnership agreement or publishing of a DBA (Doing Business As). When an entity has a unique name, the hash of this name is the key used to find an existing identity.

Entities without unique names

Entities without unique names, such as a marriage, or companies in Bahrain, are uniquely identified by their set of membership. Their identity is the combination of the identities of their members. These hashes are hashed to produce a unique hash for the entity that represents the identity hashes for each member.

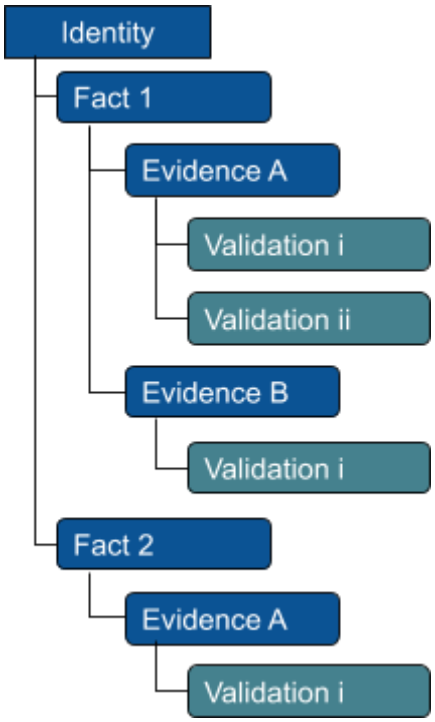
Signing of identity

These identities and each credential is cryptographically signed by each validator. This allows both the veracity of the identity and the source of the validation to be determined. Credentials are good until they are revoked. Identity validations nodes in the network can validate any signed credential is valid and was signed by the specific party.

KYC processes

There is no single process to do KYC for all cases. KYC is about risk management and regulatory compliance. The KYC process that is acceptable for one country or organization might not be sufficient for another. The KYC process for an entity that only spends a few dollars a day might be different than the one that spends millions a day. In addition, KYC can't be a one time event. Regulations change, new risks are identified and the nature of transactions change.

Regardless of the type of KYC performed in one jurisdiction, the only process that needs to be done in another is around any differences in the requirements. KYC breaks down into a process that is made up of three repeating patterns[3]:



1. An assertion of a **fact**. eg. “My name is x”, “The company name is y”, etc.
2. One or more **evidence** of the claims. eg. a passport with the individual’s name, the look up in an official registry of the company name, etc.
3. The method for **verification** of the evidence. eg. look up the passport to see if it is valid in a government database, audit that the server is talking to the official registry site.

Any KYC process relies on a series of these patterns on multiple facts which might have optional rules to give users a choice around the ways they prove a claim and options around ways to verify each proof.

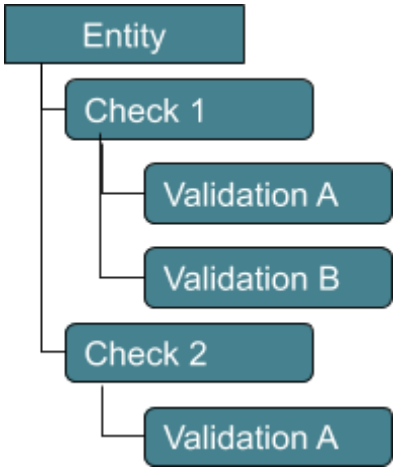
Each fact, evidence and verification is treated separately in the platform. As requirements change or fact proofs expire, only the claims which aren’t proven need to be provided and reverified.

This means that if a company identity is KYC’d in Hong Kong with a foreign corporation as the owner in Singapore, that the Hong Kong process for KYC of the Singapore company can be different than the Singapore process for the Singapore company. However, they both can rely on common proofs and verifications or extend proofs and verification which refines the risk in both jurisdictions. This means that the more jurisdictions on the platform, the better the results when dealing with multi-jurisdictional entities.

The Sweetbridge platform supports temporal KYC that expires, incremental KYC that gets strengthened over time, and risk scored KYC that quantifies the quality of the KYC. Also, the way KYC is done can be different by entity type within a jurisdiction or for a jurisdiction. For example, the process for doing KYC on an individual within Argentina might be different from the process used in the US for KYC on a company who has an Argentinian owner.

The identity of an individual or organization stays the same but may not be considered as KYC’d in all jurisdictions or for all uses. It also means that KYC’d identities become stronger when more jurisdictions join the Sweetbridge platform.

[3] Blue indicates the data is stored at the edge and green that it is stored centrally.



In addition to facts, KYC processes frequently want perform checks[4] that individuals or organizations are good actors or are in good financial standing, such as:

- Are they on government black lists or watch lists?
- Are they politically exposed individuals?
- Do they have criminal backgrounds or connections?
- Does their credit rating meet minimum requirements?
- Have they recently filed for bankruptcy or been a director of an organization that filed for administration?
- Etc.

Admin Agent

When KYC is being done on an organization an executive admin who is not a director or a paralegal in a law firm may frequently be asked to provide information and act as the administrator for the process. The Sweetbridge Platform therefore supports the ability for anyone to provide information about a company even if they are not an owner or director. However, the information is not considered as validated until it is signed by a director.

This allows the directors of an organization to delegate the tedious work to others and then sign their acceptance of the information as accurate at anytime prior to being considered verified. Once the credentials or identity has been issued, any additional information must be provided by an Authorized Party.

KYC for individuals

KYC for individuals typically consists of:

1. Proving the individual's identity (name), citizenship and tax ID (where applicable) using one or more government-issued credentials
2. Proving where the individual resides using one or more methods so they can be contacted, investigated or served legal documents.

The Sweetbridge platform supports a variety of ways to do this via automated means such as uploading a passport, the government ID or driver's license, using live facial recognition and AI to prove you submitted your passport and you are a live person. Using credit information to prove your address or utility bills, etc.

The process is modular so either existing workflows can be used or the workflow can be customized using existing modules or new modules can be created and added to the platform when needed for specific use cases. Any required searches to determine if an individual is in good financial standing, is not a bad actor, and is not politically exposed are also configurable.

[4] Green in the diagram indicates that data is stored centrally.

KYC for companies

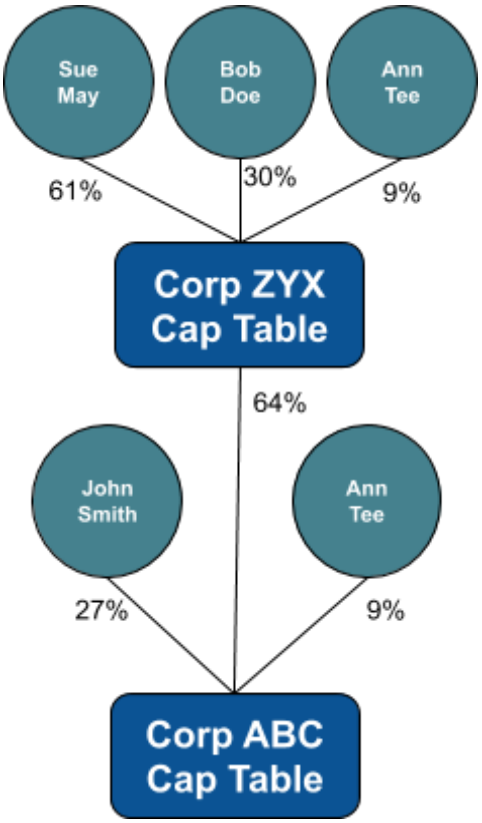
There are lots of ways to do KYC on companies and KYCing of a company means something different in many use cases and contexts. At a minimum, it is typically verifying that there is an entry in an official government registry and the tax ID matches a tax identity with the company name.

Optionally organizational KYC can include many other verifications such as:

- The list of owners who control a specific percent or more of the company
- The list of directors or officers of the company
- The list of parties that have influence or control over the company
- The business type and commercial activity classification
- The primary sources of income or revenue
- Evidence the company is in good standing
- The KYCing of the directors and owners
- Determination of the Ultimate Beneficial Owners (UBOs)
- KYCing of UBOs
- Validations that no UBOs are doing business with sanctioned customers
- Determining the risk posed by business activity with specific customers or vendors
- Enhanced due diligence of UBOs

Ultimate Beneficial Owner

Due to the multi-jurisdictional nature of ownership, the KYCing of the UBO for some companies can be very difficult if not impossible. The Sweetbridge platform allows the setup of separate workflows for ownership in a specific jurisdiction or set of jurisdictions. Workflows can also be contingent on the type of organization such as public vs private.



UBO detection can either require KYC to be done on those in control or with influence. When desired the UBOs can be KYC'd until they resolve to an individual. This requires tracing the directors / officers and owners who are in control of specific percentages of the business.

To facilitate this, the platform supports a tree of ownership with capital tables for each entity and director/officer lists. Keeping the capital table maintained can be difficult when the company is publicly traded, has a lot of equity trading or is public and no automated means of receiving updates exists.

KYC components can calculate the UBO by walking the ownership tree and capital tables until they reach individuals. In the example above the ultimate ownership for Ann Tee is 9% of Corp ABC plus the 9% of 64% or 5.76% plus 9% which equals 14.76%.

As already discussed KYC is about risk management. Even the directors of a company may not know the identity of parties that control companies which control them. This information may be considered confidential such as with trusts. Therefore, the platform allows proofs to be anything a jurisdiction allows such as entities approved by the government or by a financial services organization.

When all of the UBOs are within the same legal jurisdiction this is relatively simple to do full KYC processes for validation of UBOs. When ownership is through a foriegn individual this is also straightforward in most cases. However, in some countries it may not be possible to use the same validation methods for evidence on organization KYC so the platform supports jurisdiction defined workflows to deal with what is legal or supported in each jurisdiction. In the end, some percentage of foreign ownership typically need to be processed manually.

The platform supports tracking of UBOs and integration with external sources that provide APIs to automatically reevaluate ownership of organizations. Countries such as the UK have made this easy through their Companies House; other countries, particularly in tax advantaged locations, have not.

Authorized Parties

When the KYC'd identity is for an organization or when an individual has a Power of Attorney to act on behalf of another individual, the power to act on behalf of another entity must be proven. The platform supports a protocol for allowing entities to delegate authority to individuals to act on their behalf or update information on their behalf.

Authorized parties must have a KYC'd identity themselves. There can be two types of authorized parties:

- Legal - a legal document exists that authorizes such as the minutes of a board meeting.
- Informal - No legal document exists but a director / officer has authorized the individual.

Like everything in the platform what is acceptable evidence and validation can be determined by legal jurisdiction or organization.

The use of authorized parties credentials can extend to authorizations that go beyond the maintenance or submission of KYC information on the platform. These authorizations can be used to enable authorizations to access and update company or individual information within the financial services entities themselves.

Identity Protection

A side effect of having a cryptographically secure KYC'd identity of individuals, directors, officers and authorized parties is that it can replace user id and password based logins. These identities can be used to verify identity over the phone, on websites, or in person. This can be done through any platform integrated with a platform e-wallet[5] and a simple API that can be integrated into the organization's websites or backend systems.

[5] "e-wallet" refers to an electronic device or online service that allows an individual to make electronic transactions, hold electronic credentials and provide an electronic version of identity.

This enables a highly trusted and secure eWallet based identity solution that governments and companies can use to verify identity. Since each verification of the identity checks to see if the identity has been revoked, the loss or theft of a device that possesses the eWallet can be simply revoked by contacting the identity provider or through a simple website interface. Once revoked the identity cannot be used for any process within the network.

Components

The platform uses pluggable components that make the KYC process and credentials easily extensible. Though the identity credentialing used in KYC components can be anything, by default, the platform uses the peer to peer and DLT-based Sovrin protocol for credentials and identity. Individual identities use the MyCUId KYC protocol unless another protocol built on top of the Sovrin protocol is desired. The platform can support multiple credential validation protocol at the same time.

Enhanced AML

The platform supports tracking of transactions, agreements, identities of trading partners and can even do real time accounting through the Synchronized Accounting protocol. This means that all or only a subset of financial transactions can be reported to the platform. This enables cross organization AML and regulatory risk management. See details on our Synchronized Accounting for more details.

Summary

The Sweetbridge Platform is designed to address the KYC needs of any government, legal jurisdiction, organization or process. These processes are built from modular and reusable components. These components automate the collection of facts, provides evidence that the facts are true and validations that evidence can be validated by authoritative sources.

The platform issues cryptographic identities and verifiable credentials for facts while checking external sources for additional information. All processes can be audited in advance and any process conducted can be verified by external nodes that can use cryptographic proofs to prove the process was followed. This means that non-manual processes can be audited in real time.

All information only needs to be provided, evidenced and verified once and this can be done in a decentralized fashion but audited centrally. Every fact, evidence and validation can be proven to have been done or not done with the party and time it was performed. All information can be shared when needed but no high risk information is stored centrally, significantly reducing cyber-risk. Once KYC’d identities exist they can be used for many things other than proving KYC to a financial entity. They lay the foundation for highly secure identities which can be used instead of weak user id and password methods of verification.

The Sweetbridge platform is designed with KYC’d identity being only the first step in a new digital economic framework that includes digital signing of agreements, real time auditing of financial transactions and the tracking of ownership, rights and obligations.