MCS
microsystems group

Secure Multi Applications Code

Secured Dynamic QR Code Solution

Overview

All across the globe, public and private sectors are implementing digital transformation initiatives for a multitude of reasons. The problem, however, is their data is typically spread across different silos and is difficult to access for analysis, decision-making, and insights. Then again, centralizing data presents an attractive single point of attack and raises public outcry for data privacy. Another issue is being able to communicate just the necessary data to the right audience and, in reverse, to let the recipient know that the information came from the respective sources.

MCS Secure Multi-Applications Code (SMAC) solution will effectively and intuitively resolve these very issues in both the public and private sectors. Better yet, we can apply this solution to information about various entities, including persons, organizations, and assets.

Secure Multi-Applications Code (SMAC)

The Secure Multi-Applications Code system is a web-based information gateway that directs users to privileged information or services concerning individuals or objects of interest.

The **SMAC Issuer**, typically an authority or industry leader, owns the SMAC system and will be responsible for its use which starts with the issuance of SMAC IDs to entities within its domain. The **SMAC ID** is a secured dynamic QR Code that contains Public Data (optional), a Unique ID, and their Digital Signature, where the latter two are generated by the **SMAC Platform** web server. The QR Code standard is a commonly used, low-cost, optical technology familiar to many people, and the SMAC QR Code can be applied to pre-existing ID cards, product labels, documents, and digital media, thus compatible with any system infrastructure.

As a result of the digitalisation exercise, the SMAC Issuer has a trove of information and/or range of online services concerning individuals or objects within its database. Usually, such **Resources** are placed on the organization web servers and made accessible to third parties in a controlled manner. Subsequently, the SMAC Issuer, also a **Resource Owner**, will populate the **SMAC Platform** with the list of the web addresses of the Resources related to each entity as identified by its SMAC ID; notably the information or online services themselves are not included in the upload.

In addition, to ensure the Resources are consumed by the right party (**Resource Consumer**), the Resource Owner can dictate a combination of **access rules**, i.e., who (user account and role), when (date and time), where (geofence), what (device type), and/or how (single or multiple accesses). On the other hand, public information or services may be made accessible to all users by not specifying any access rule. Ultimately, the Resource Owner has complete control over the distribution of its information and online services.

Finally, Resource Consumers must be registered on the SMAC Platform in order to gain access to restricted Resources. Using a **SMAC Client App**, they can scan the QR Code on a SMAC ID, receive a list of accessible Resources which have passed the access rules check, and choose the Resource to be directed to.

Features and Benefits

Verifiable credentials

- SMAC gives your audience a means to verify your identity through a digital token that is secured by PKI and blockchain.

Closed-loop security

- Accessible to register users only.
- Scan by custom mobile or web app only.

Up-to-date

- Information and services are delivered directly from the providers, instead of third-party cached or downloaded versions.

Rules-based access

- The Resource Owner is responsible for managing access rights of its data and services: they are not automatically accessible to all SMAC users.

Privacy

- The SMAC ID and SMAC Platform do not store any private information.
- Instead, data remains with the Resource Owner in compliance with Personal Data Protection Act.

Analytics

- Times and locations of scans are communicated to Resource Owners in real time.
- Responses can be analysed to protect against abuse and misuse.

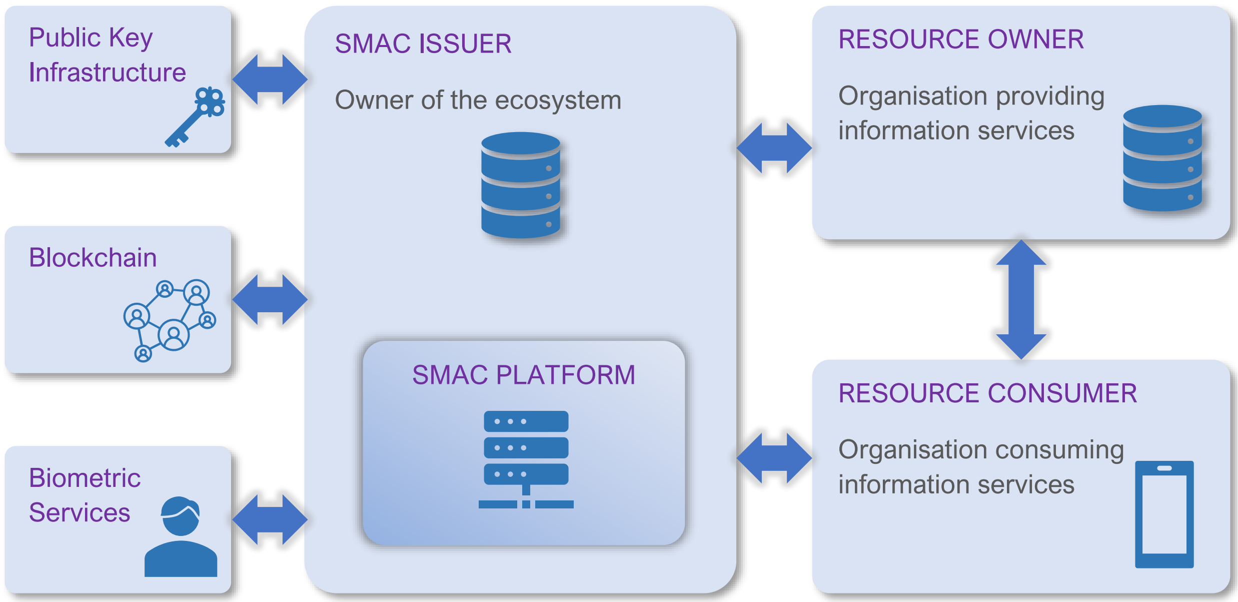
Expandable

- New Resource Owners and Resource Consumers can participate in the SMAC system at any time; adding to the number of applications served by the SMAC IDs.

Scalable

- The SMAC Platform implements a RESTful API and can be deployed on the Cloud or on-premises.
- More than 10^{38} SMAC IDs can be provisioned by one SMAC Issuer.

SMAC Ecosystem



Public Key Infrastructure

Blockchain

Biometric Services

SMAC ISSUER

Owner of the ecosystem

SMAC PLATFORM

RESOURCE OWNER

Organisation providing information services

RESOURCE CONSUMER

Organisation consuming information services

Example Use-Cases

Personal Identification

The SMAC ID can function as a mobile-friendly verifiable credential that acts as a token for multi-factor authentication, giving individuals access to electronic healthcare records, online government services, digital KYC by financial institutions and authentication for government benefits distribution among others.

Expanding upon the power of the internet and SMAC Platform, individuals can register their SMACs and create online profiles. Subsequently, the individual can populate their profile with a wide array of contents, such as:

- Personal particulars for use by the authorities.
- Health records for use by medical practitioners.
- Financial records for use by banks.
- Education records for use by learning institutions and future employers.
- Age or date of birth for the purchase of cigarettes, alcohol, medication and other restricted goods.
- Custom information (as digital documents, images, URL, vCard, etc.) targeted at various individuals, corporates or groups.

For example, according to the prescribed rules, a bank officer can scan a loan applicant's SMAC and download the latter's financial records during office hours, but such a request would be rejected if done outside office hours.

Furthermore, corporations and institutions can produce official, signed attestations and have them added to individual profiles to be shared with interested parties in the future. For example, a university can produce academic transcript and qualification, and attach them to a student's profile.

Asset Profiling

Aside from people, the usage of SMACs can be expanded to assets. SMACs can be created and attached to physical assets of value, to be used as a means of identifying the asset. Subsequently, Resource Consumers may obtain relevant information about the asset while Resource Owners attach data throughout the life of the asset. Furthermore, since the SMAC is attached to the asset, transfer of asset ownership can be registered and duly recorded. Moreover, historical records may be transferred along with the asset. Such dynamic data provides actionable, up-to-date information and opens up unlimited use-cases.

A good example of such applications is the motorcar. When a motorcar is first licensed for road use, it is registered on the SMAC Platform and will be provisioned with a SMAC ID. Alternatively, this can be done once at any time during the life of the motorcar. Subsequently, various stakeholders may contribute their respective information about the motorcar, including:

- Vehicle ownership certificate and license status by transport authority
- Insurance policy and panel of workshops by insurer
- Vehicle fitness test report by Inspection agency
- Maintenance records by service centres
- Loan and account status by financier
- List of additional drivers allowed by owner

Access to the above information would be determined by combinations of abovementioned rules which would be further defined by the existing law, standards and industry practises. For example, license status of the motorcar might be accessible to Consumers located within the country but not to Consumers located abroad. Another example is where the transport authority is allowed to view the insurance status to facilitate license renewal but not its financial records.

Such programs may be initiated by a government agency, vehicle manufacturers, insurers, financiers, or any private enterprises. Having said that, the greatest level of benefits is realised when all stakeholders are involved. Aside from vehicles, the use of SMAC and SMAC Platform can be applied to other assets, such as industrial machines, medical equipment, firearm, etc.

Supply Chain Management

The SMAC and SMAC Platform-enabled end-to-end tracking and traceability solution allows every actor along the supply chain to check the identity of an individual product or a batch of products and access relevant information, from the manufacturer to the consumer.

The SMAC Platform will generate SMACs and maintain a database of unique SMACs and details of the product to which they are assigned – what the product is (e.g. "Eau de Parfum 20ml"), and if necessary a serial number and/or batch number, certification record, date of manufacture, location of manufacture, best-before date, or any other information that the manufacturer wishes to store. The Supply Chain system will also provide content and services to consumers via a mobile app, including instructions and warranty registration – any text information will be provided in the user's own language, based on the language settings of their mobile device.

The manufacturer will request a set of SMACs for each batch of products, using a web-based interface – they may specify a unique serial number for each item or each batch of items, to be encoded as part of the universally unique SMAC for each item. The SMACs will be generated by the SMAC Platform, and transmitted as images over a secure (encrypted) channel to the manufacturer. These will then be printed, either on the product packaging or on labels to be affixed to the product packaging, and used to track each item. Manufacturers will also be able to request batch SMACs, to assign to batches or consignments of items, which can be printed on labels affixed to the outside of boxes, pallets, shipping crates, or other containers.

The Supply Chain mobile app will provide a method for retrieving information from a SMAC printed on a product. Each actor along the supply chain will be able to display the relevant information, based on their role as specified when installing the Supply Chain mobile app. Role assignment must be approved by an administrator responsible for supply chain verification – for example, the owner of a retail store might be given a code by the product supplier, allowing them to authenticate themselves as a registered retailer and log in to the Supply Chain mobile app in the 'retailer' role. Authority to create and manage user accounts and assign roles will be delegated down the supply chain – for example, a distributor might be delegated authority to create user accounts with a limited set of roles, allowing them to create user accounts for employees so that they can view item and shipping information on scanning a SMAC.

The Supply Chain mobile app will also be available to consumers – this will provide consumers with a way to check the authenticity of goods before they purchase them. On scanning the SMAC on an item, consumers will be informed immediately whether the item is genuine or counterfeit, based on their location. The Supply Chain system has a record of where each product is going to be sold, and even allows retailers to register when the product arrives in-store, so if the user's location does not match the location of the retailer associated with that individual product, the app reports that it is a counterfeit bearing a copied SMAC.

Secure Documents

Proof of original documents (as created by a document originator such as a bank, university or law firm) have typically been undertaken manually through seal stamping or certifying. Unfortunately, with advances in modern technology, these types of documents are open to manipulation through digital scanning, editing and printing. A reader assessing the validity of the document probably has to enquire with the document originator.

We have created a new process and solution to prove validity of an original document by providing access to a digital version of the original document in a 100% secure and tamperproof way.

Document issuers and users will embed a newly created SMAC onto the original document. From a digital copy of the original document, a unique hash value (the document's DNA) is calculated for that document and is stored for future reference. For added security, the document's unique ID, metadata and hash value may be stored on a blockchain.

A document secured by SMAC allows the originator to ensure that it is only opened by the right people at the right place and at the right time. The SMAC Platform provides the document originator with the ability to dictate recipient permissions: who opens it, when they open it and where they open it. Furthermore, the authenticity of the downloaded documents can be verified by Resource Consumers by comparing them against their hash values and blockchain records.