miaa Guard
taking care of digital access

Blockchain and access management

miaa Guard’s reference framework consists of enterprises that want to engage with their eco-system of B2B and B2C users and monetise their digital services. Our customers typically protect their digital services against abuse and data leakages while serving millions of users with millions of access decisions per day. To enable our customers’ API gateways to rely on access decisions at those scales, miaa Access Management offers split-second decisions combined with super-scalable access governance. This article gives a view on how blockchain technology can enrich miaa Access Management.

Split-second access decisions

To enable our customers to decide instantaneously whether to process or reject traffic, miaa Access Management issues bearer access tokens. These tokens are issued to a requesting front-end to be used by the enterprise’s API gateway, Enterprise Service Bus, or business API’s. The tokens are secured, short-lived and bear the on-the-spot access decision.

In this context, dependability is key. As such, miaa Access Management is built from the ground up for dependability in terms of governance, security, throughput, availability and resilience. For example, miaa Access Management has proven to support a domotica installation that can be controlled in real-time via Amazon Alexa, and without Amazon knowing anything about the user and his installation.

For propagating the access decisions, miaa Access Management builds on open standard protocols and formats. Thanks to the use of open standards, our customers can integrate miaa Access Management using widely available libraries and out-of-the-box solutions. In fact, the API economy is increasingly building on these standards in areas such as the Internet of Things, Open Banking and MedTech.

Because of their volatile nature, it is very unlikely that blockchains would be used for propagating access decisions; such decisions may expire before the blockchain consensus protocol completes. And while dependability is key for access decisions, other characteristics of blockchain such as non-repudiation are less relevant in this context.

Super-scalar access governance

The access decisions produced by miaa Access Management are governed by the customer’s unique business policy. To produce an access decision, miaa Access Management’s rule engine takes into account not only core-identifiers but also relationship-identifiers and the context of the request. While core-identifiers may include gender and birthdate, relationship-identifiers are unique for an enterprise and include claims such as “I’ve paid for this subscription,” “I’m a colleague of this person,” “I’m the installer of this device,” and “I’ve enrolled for this event.” And while core and relationship-identifiers may be relatively static, the context of an access decision may include geolocation, type of device, time of day, level of authentication and interaction history.

While core-identifiers may become decentralised using blockchains to serve self-sovereign identity, relationship-identifiers are typically kept close to the enterprise because of their confidential and proprietary nature. In the words of Gartner, Homan Farahmand, July 12, 2018: “*For decentralised* *identity to take root, enterprises need to view core-identifiers and relationship-identifiers as two distinct constructs. Core-identifiers can be decentralised and drive relationship-identifiers for different enterprises. However, each enterprise still has to manage its own relationship-identifiers for each person to address other identity governance and access management requirements."*

miaa Access Management has been designed from the ground up to consult core-identifiers at external sources in real-time during the self-service processes. It currently consults data at authoritative directories such as national registers (e.g. eID) and sector registers (e.g. IQvia IMS Health). It also consults customer and subscription data in the customer's CRM and ERP systems.

miaa Access Management uses this data to verify self-serviced claims of the end user, so-called identity proofing. After validation, the status of the claim is updated from 'pending' to 'confirmed' or 'rejected.' Confirmed claims are then used by the rule engine for its real-time decision making. miaa Access Management also enables an enterpriser's back office to revisit the status of an identifier, for example for reasons of unpaid bills, misbehaviour or resignation.

Consuming blockchain data

Thanks to its built-in ability to consult core-identifiers at external sources, miaa Access Management offers enterprises the option to swap or supplement these sources with blockchain based sources. Our customers, however, currently wait until a suitable blockchain of core-identifiers has reached critical mass. In the words of Gartner, David Anthony Mahdi, March 2018: "*Blockchains for decentralised identity are still early and approaches are maturing, but PoCs are the common state."*

Due to their confidential and proprietary nature, we do not expect our customers to maintain their relationship-identifiers in a blockchain. In the words of Swift, Damien Vanderveken, March 8, 2018: *"To roll blockchain out to all of Swift's members, we estimate that 100,000 sub-ledgers must be created, making them extremely unwieldy to maintain, upgrade or configure. This is to avoid confidential information being seen by rival banks."*

Producing blockchain data

To derive access decisions, miaa Access Management uses relationship-identifiers, next to core-identifiers and context. From a governance and auditability perspective, our customers find it crucial to control any change in the state of a user's relationship-identifiers. miaa Access Management maintains a secured ledger for historic evidence of any such change.

There are instances where these changes need to be made publicly available. For example, the emerging user-managed authorisation standard of the Kantara initiative, of which miaa Guard is an active member, presents a standard for 'consent receipts.' A consent receipt provides proof that a user has given his consent for processing his private data within a specific context and under specific conditions.

For example, proof that a patient approved that his doctor views and updates components of his health record during a consultation. Even though the patient may withdraw his consent at a later stage, it must still be proven that he had given his consent at that point in time.

Because long-term immutability and accessibility are key for such historic evidence, our customers may opt to keep such records as smart contracts in a blockchain. In the words of Kantara, Eve Maler, June 19, 2017: "*The Kantara working group will issue recommendations for good practice on use of smart contracts to facilitate individual autonomy and enable equitable and efficient participation in transaction ecosystems."*

On the horizon of miaa Guard

The market of externalised authorisation management and tokenised access control is growing exponentially with the growth of the API economy in areas such as the Internet of Things, PSD2 and MedTech. In the words of Gartner, Gregg Kreizman, March 6, 2018: *“Ensure your IAM provider supports OpenID Connect.”*

And also in the words of Gartner, Erik Wahlstrom, 30 October 2017: “*The OAuth 2.0 framework is the preferred API security method for providing access control to REST-based APIs, but it takes time to master*.” miaa Access Management takes the complexity out of these frameworks. In fact, miaa Guard is already taking care of digital access for global brands and continues to expand its population of active users.

The roadmap of miaa Access Management includes support for public blockchains for self-sovereign identity and private blockchains for consent receipts.