miaa Guard
taking care of digital access

Person-driven Access Management

What do we offer?

When enterprises make their platforms available on the internet e.g. via the cloud and an app, they will enforce their security policy 'to keep the bad guys out'. Conversely, consumers want protection of their records, especially when these become available through cloud apps. This leads to the following challenge: "How can you keep access to digital services and shared management of digital records and smart devices under strict control, while scaling up to millions of end users, with a mix of professionals and consumers?"

This is where miaa Access Management comes into play. It provides a platform with APIs for *person-driven access management*. The user is central to this. Our customers can concentrate on their digital transformation and opening up their platforms. We offer them the tools to make this happen in a controlled and secure way.

Because access control is on the critical path as a kind of front door, we offer those APIs as a cloud service with optimal protection and optimal response times and availability.

What does this mean for our customers?

Our customers typically go through some sort of digital transformation. Traditional access control is controlled by the enterprise, not the consumer, and is led by a static security policy. Access rights are assigned to users via a CRM, a directory and a back office. This is difficult to maintain for populations of millions of users. Moreover, it becomes difficult to take into account GDPR rules and complex heterogeneous relationships.

Because this is difficult to control, miaa Access Management takes as the basis the persons and their real life. It determines in real-time whether someone is granted access or not on the basis of elements that the person can manage himself and that fits with his own personal environment. This makes it scalable to millions of users. Our model is unique.

Our platform provides mechanisms for managing a person's attributes and relationships, for self-regulating workflows of invitations and approvals, and for the protocols for enforcing the access rules. The following elements are key for miaa Access Management: personal attributes relative to the enterprise, personal relationships, intuitive workflows, consent and the enterprise's security policy.

What type of personal attributes are involved?

Traditional identity management systems aim to collect personal data with a view to targeted marketing, e.g. gender, age and contact details.

miaa Access Management, on the other hand, collects data that characterises a person in the context of the enterprise. E.g. "Is she a paying subscriber?" "Is she a health care provider?" "Is he a certified installer?" "Is he a recognised breeder of a particular dog breed?" So, attributes are specific to the enterprise and concern the qualification or role that the person plays in the ecosystem and also the history such as paying a subscription or going through a certification. This is

a model that is less sensitive with regard to GDPR and that on the other hand provides much more valuable information to derive global access rights (so-called coarse-grained access control).

What type of personal relations are involved?

Traditional access systems only view the relation from a person to an application. Social media have familiarised consumers with digital relationships.

miaa Access Management builds on this by using the relation from a person to a digital records and smart device to derive access rights.

This relational model is surprisingly powerful in digitally unlocking B2B2C use cases, in which the relationship between professionals and consumers is made explicit. For example, “I am the installer of this device, of which this person is the owner.” Or, “I am the doctor who manages the health record of this patient.” Or, “I am the payer of this subscription and this is my family member who also gets read permissions.” Our customers experience this as an extremely powerful model to derive granular access rights from an intuitive model (so-called fine-grained authorisations).

What type of intuitive workflows are involved?

Traditional models for assigning access rights rely on a back office, using for example a CRM, a user directory or a subscription management system.

miaa Access Management goes much further with a series of intuitive workflows that make it possible for them to be handed over to the end user. E.g. a workflow where the installer of a device invites the owner of the device to take over part of the management. Think of an alarm system or a charging station for electric cars. The owner can then accept that invitation and register himself with it. By accepting the invitation as owner, we can deduce certain access rights. The owner can then again invite a family member as co-administrator for a certain zone of the alarm system.

With another workflow, people can sign themselves up and ask to be approved by someone else or by a system. E.g. “a child can apply and request approval from one of the parents.” Or, “a doctor can register with the recognition being verified against Iqvia IMS Health.” Or, “a person can register as a colleague and ask for approval from his team leader.”

Yet another workflow allows you to invite people to confirm a sort of pre-registration sourced from a mail list.

How does consent fit into this?

Consent is actually a specific form of authorisation: a person gives a service provider permission to use his personal data for certain purposes.

We go much further in this: a person not only gives permission to the service provider but can also indicate who can view or modify his file. E.g. The file of his dog in which the pedigree, the vaccinations, behavioural attributes and the weight progress are stated. Or also, A patient record. This allows a person to give permission that parts of her file can also be viewed by a certain nurse in a care institution. Or that certain data can be used in an anonymous way in clinical statistics. The latter helps to provide MedTech platforms with very rich data in a legitimate way.

How does a security policy fit into this?

A Security Policy is actually a specific form of authorisation. A security policy determines the game rules. E.g. A rule may stipulate that in order to add vaccinations to the file of a particular dog, you must be a licensed veterinarian, you must have a care relationship confirmed by the owner with that dog, and you must use the special app with 2-factor authentication. Another example: premium subscription can be shared, but not a standard subscription unless you pay.

Why is miaa Access Management so unique?

miaa Access Management is offered by a European player with experience of security in the banking and medical sectors and with an eye for consumer-friendliness. New protocols (such as OAuth, IoT device flow, and UMA) allow strong security at the level of B2B, MedTech and FinTech. New technologies (such as microservices and graph databases) allow millions of relationships to be managed and split-second authorisation decisions to be made.

miaa Access Management combines these new protocols and new technologies. Its unique self-service model tackles the challenge: “How can you give access to digital services and keep the shared management of digital records and smart devices under strict control, while scaling up to millions of end users in a shared ecosystem of professionals and consumers.”