codecta.

Case Study
Healthcare Identity Management

Overview

Country or Region:
Germany / Austria

Customer Profile
Hospital – private property
Relaxation and Mental
Healthcare center

Business situation
Strong identity management, identification, authentication and authorization of an patient or group of patients or staff, on an application, system or comprehensive healthcare IT environment, is absolutely essential and key feature in digital approach and transformation of any healthcare company.

Solution
Required features of flexibility and extensibility are important parts of current industry standards, OAuth2, OpenID and OATH, and is the best way to implement all requirements from strategic point of view.
Red Hat Keycloak opensource solution is foundation of the platform we use. To enhance functionalities set, Codecta implemented various set of proprietary solutions, different authentication and identity providers, and OATH based authenticator (softtoken) as strong identity device (iOS and Android).

Benefits
Keep close to standard is a guarantee of flexibility and long-term functionality of implemented solutions. Enhanced with specific proprietary implemented components, is the best way to meet any requirement by customer, or specific group of users, and yet to keep top level security as it is required by healthcare companies.

Protecting privacy of patient and its healthcare data

Protecting privacy of patients, as well as hospital or any other healthcare institution staff members, and its healthcare data, from user or administration point of view, is absolutely essential aspect of healthcare business in commercial or public institutions.
Second important aspect of enough flexible and modern solution is accessibility and user friendly environment, ready to use before, during and after the stay at healthcare facility. It must be able to be used in platform manner, one identity provider for different entities, hospitals, clinics, and similar facilities.
Identity management is primarily used to authenticate patient or hospital staff member on a system, and ascertain whether the patient is allowed or prohibited access to a particular system.

It is usually required that identity management consists of various phases, including the patient/staff authentication, the level of authorization and the type of roles and level of access a patient or hospital staff member may have.

From accessibility and usability point of view, it is required that authentication mechanisms are simple to use, its enrolment and/or activation must be easy to explain, so it can be accepted by patients of all ages. In case of patients with significant disorders, system must be able to provide authorization of third person (caregiver), to access patient data, with low or full access rights. Impersonation, option to access full patient profile by using caregiver authentication devices, is also one of the very useful functionalities.
For medical centers of an open type, it is important to enable patient self-registration and simple onboarding procedure to healthcare system, with only basic facility data by default.

Contrary to the requirements for accessibility and ease of use, there are requirements of strong identity devices and high-level secure authentication mechanisms. Guarantee of patient privacy, and protecting its healthcare data is one of the key features of any healthcare information system.

Situation

As one of the oldest human social activities, medical care is a very conservative discipline with established rules and methodology, and by its nature it is slowly changing and modernizing, above all in accepting technological achievements by patients of all ages.

In order to achieve any improvement in information systems, the system must be designed as an adequate match to existing procedures, so that staff and patients can easily and quickly accept and use it.

In addition, the system must meet the highest security standards, as it includes information on patient healthcare data and staff member activities.
After all, the system has to be sufficiently beneficial and optimized so that returns of investment can be made in the acceptable period of time.

Solution

Based on previous experiences, Codecta provided the platform oriented solution, that includes Web and mobile solutions, designed in coordination with experienced medical administration and medical informatics experts.

Top level security is implemented by using customized Redhat Keycloak Identity and Access Management solution.

Strategy key point was to stick to the current modern industrial standards, OAuth2 and OpenID, and OATH to create strong identity authentication devices (softtokens), for multiple platforms.

By customizing Keycloak functionalities, Codecta empowered platform and enabled functionalities such as:

- multiple OATH devices per user
- user/caregiver impersonation for patient profile
- automatic creation of new users

- customized authorization flow for safe profile update by user, and user onboarding (mobile device apps)

To enable various set of devices to be used by patients, Codecta developed set of customized proprietary authentication providers, for multiple device types:

- OATH-based authenticator devices (G-authenticator-like softtokens), and multiple devices per user
- OATH softtokens for different mobile platforms (iOS, Android)
- Different mobile platforms OATH based OTP generators (iOS, Android)
- Easy enrolment of any new OATH device
- e-mail OTP authentication provider
- Security hologram tags (Authentic Vision) authentication providers

To achieve required ease of use, for multiple OATH based devices, we enabled self-enrolment of new devices, for any existing user/patient.

As first OATH softtoken device is added by administrator (and system privileges and access rights are set to high level), each subsequent device can be added by patient himself, through few simple steps and scanning of QR code for device activation.

In addition, customized Identity providers enables authentication and user onboarding by using existing customer profiles, such as social networks or other services providers accounts.

Benefits

The most important expectations were to meet ease of use for patients of all ages, and maintain highest security level along with it.The best confirmation of the achieved goals was the use of the system by the elderly people, without any major issues.

Maintained security level was confirmed by numerous pen-tests without any critical findings at any aspect of implemented authentication and identity management system.

Customized Codecta authentication providers

enabled implementation of all requirements by customer, and enabled us to overcome the current system constraints.

Customized Identity providers enabled use of various existing patients profiles for authentication, such as social networks profiles or other service providers accounts.

Platform approach enabled patients to use same identity providers and authentication mechanisms for multiple hospitals/clinics, and every improvement of authentication providers was applied to all platform members.