MySecuritas

SECURITY WHITEPAPER

Securitas

Securing applications and data throughout the lifecycle of digital services.

Securitas works methodically with the protection of digital assets from outside threats and technical vulnerabilities by adopting a secure software development lifecycle and security controls for all key services delivered to clients.

This document is intended to provide transparency around the technical and organizational security measures in place when developing and operating MySecuritas digital services.

Introduction

The goal of software security is to maintain the *confidentiality*, *integrity*, and *availability* of information resources to enable successful business operations. This goal is accomplished, more generally, through the adoption of a secure software development lifecycle (SDLC), and more specifically, through a set of security controls.

Development of MySecuritas software follows a modern paradigm, built on early security analyses (so-called shift-left), automation and secure defaults, combined with appropriately defined policies, roles and responsibilities.

Architecture

MySecuritas is a suite of separate applications sharing a common platform and application distribution framework, Securitas Digital Platform (SDP). A core responsibility of SDP is to provide CIAM (Customer Identity and Access Management) capabilities for any client-facing digital communication channel.

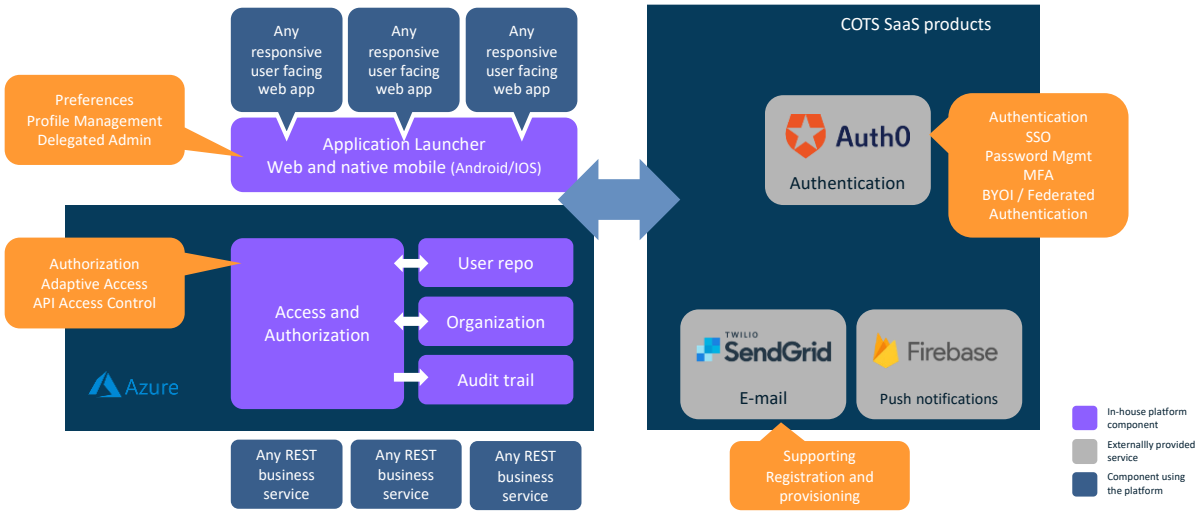

Figure 1: High level overview of the components included in the CIAM-related parts of SDP.

Authentication

Authentication is handled through the third-party provider Auth0. Users can be authenticated directly through the built-in password verification capabilities of Auth0, or alternatively through federated single sign-on with the clients' own preferred identity provider (e.g. corporate Active Directory)

When using built-in password verification, the password policy follows the latest NIST recommendations. As per these recommendations, user-provided passwords are checked against existing data breaches. MySecuritas checks over half a billion breached passwords and prevents any of those to be used.

Authorization

Authorization is managed through a set of services operating in tandem. The main control flow is provided by the Access service, which is responsible for introspecting every single request and deciding whether to allow or deny access. In doing so, the authorization service is consulted to verify that the user has the right permissions to perform an operation or access data. The Organization service is consulted to verify that access is performed in the organizational context of the logged in user.

Audit

All user activity that involves access to business data is logged in a separate audit trail service, keeping track of "who", "what" and "when". Log records have different retention time depending on the impact of the underlying operation, after which they are permanently deleted. The audit trail is being used for a couple of purposes:

- Data analysis – by identifying deviating behavior, for example a large numbers of failed access attempts, it is possible to proactively identify and act on potential malicious attacks.
- Dispute resolution – in case there is a dispute over who did what, it is possible to use the logs to see the chain of events and tie them to an individual and a point in time.

Zero trust

The zero trust security model describes an approach to the strategy, design and implementation of systems where implicit trust is not assumed (e.g. by being connected to the same network). Traditionally, security controls are often performed on the perimeter, but once you are in, you gain access to multiple resources. In SDP, zero trust is applied and every application, regardless of their proximity to core resources, is explicitly authenticated and restricted by the fine-grained permissions configured for that application.

Infrastructure

The MySecuritas application suite is developed following a *cloud-native* principle and is comprised of many cooperating *microservices*. The large number of autonomous services drives the need for automation, which is beneficial also from a security perspective, since many of the controls can be performed automatically and continuously for every single line of code being added to any of the applications.

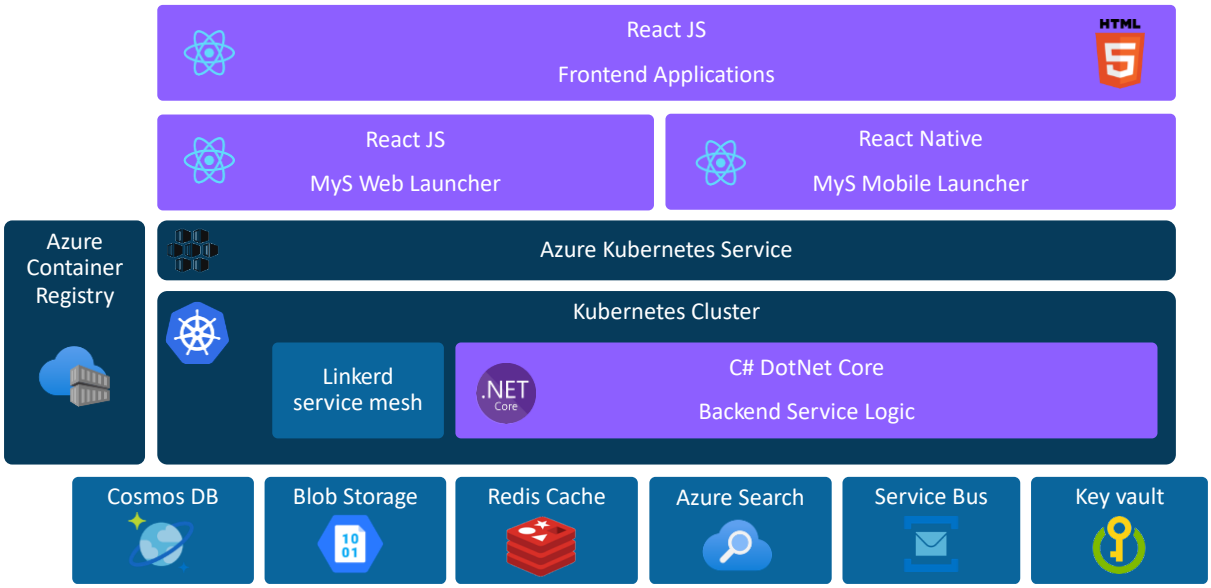

Figure 2: Layered infrastructure architecture based on microservices and extensive use of managed services provided by the Azure cloud environment.

The user facing applications of MySecuritas are delivered using ReactJS as the framework for front-end application logic. This framework provides several features that reduce the risk of vulnerabilities like injection and cross-site-scripting. Each application is developed to be responsive and is rendered optimally on both desktop and mobile devices. This allows the native

mobile client to be light weight and act as a thin wrapper around the individual business applications.

The server side of MySecuritas is provided through a Kubernetes cluster using the Azure Kubernetes Service, which leverages *health-probes* to monitor and maintain service availability. Within the Kubernetes cluster, all communication between services is encrypted and mutually authenticated using a service mesh which provides granular, service-based access control.

Starting with .NET 8, all container images enabled non-root application execution, and all services run in a non-privileged context. This reduces the impact of someone exploiting a yet unknown vulnerability by gaining access to a service runtime. Shell and remote shell access is removed from containers, further reducing the capabilities gained in the event of a security breach.

Being true to the principles of microservices, each service manages its own data and in doing so there are various persistence mechanisms that are optimal for different purposes. All data persistence is provided using separate managed services which greatly simplifies management and guarantees high service levels, standardized backup procedures and continuous patching.

Cloud and Network Infrastructure Security

Hosting Regions

The MySecuritas infrastructure is hosted in the EU/EES area, currently in EU West (the Netherlands) and EU North (Ireland)

Network Communication Security

All communication to and from the service is encrypted using TLS (Transport Layer Security), min TLS 1.2, and using certificates signed by third-party certificate authorities. TLS is a standardized protocol suite designed to maximize both compatibility and security. It is used ubiquitously for secure communication across the Internet.

Data Confidentiality and Security

Application-level Security

Data access is restricted based on roles and permissions. Permissions are enforced in an organizational context where access must be given explicitly to a location in the organization. All information pertaining to a higher organizational level is automatically restricted. Access control is applied exclusively in the back end and is managed in a single, central location.

Database-level Security

Application access to databases is managed through service principals, secured by Azure AD, eliminating the need for application credentials to be known by developers and support staff. Databases are encrypted at rest using 256-bit AES encryption and cloud provider managed keys which are rotated automatically. Encryption at rest is *on* by default. There are no controls to turn it off.

Firewalls

Only HTTPS traffic is allowed into the application cluster. Developers and support staff who need access directly to the internal system components connects through a separate management channel and the Azure CLI tool using strong encryption and integration with Azure AD.

Backups

Back-ups are performed continuously on all persisted data with the following properties:

- Transaction logs are backed up continuously.
- Database backups are performed continuously.
- Backups have a 7–15-day retention period.
- Backups are automatic and do not require user interaction.
- Backups are encrypted using AES encryption with a 256-bit cloud provider managed key.
- Data has restore-in-time versioning capabilities.
- Data is replicated in real-time in a disaster recovery site.

Availability and redundancy

All services within MySecuritas are hosted in at least two, physically separated, environments to maintain a high level of resilience in the case of a disaster. The datacenters are engineered to provide 99.999% availability. To ensure reliable network communications, diverse fiber routes and redundant hardware is utilized to protect critical components from failure or service disruption. Datacenters have dedicated 24x7 uninterruptible power supplies (UPSs) and emergency power support, which includes on-site generators that provide backup power.

Product Security

Penetration Test

The MySecuritas Platform and applications are subject to penetration tests performed by a trusted third party on a regular basis, yearly or shorter if justified by a major release. The most recent penetration test was performed in December 2024 with highly satisfactory results.

MySecuritas does not suffer from any critical vulnerability. The security review identified 10 vulnerabilities of the following security risk levels. The Medium severity finding pertained to Multi-Factor Authentication (MFA) being enabled but not enforced for a development tool and hence not MySecuritas directly. This vulnerability was immediately resolved.

- *0 Critical*
- *0 High*
- *1 Medium – Indirect finding*
- *5 Low*
- *4 Information*

“The overall conclusion is that it is a modern application that demonstrates a robust security posture, with recurring testing and assessment for continuous improvement”

Application Security Verification Standard

MySecuritas is governed using the OWASP ASVS framework. In conjunction with penetration test, compliance verification towards testable ASVS controls is performed.

Security in the Development Process

Technical teams are organized with a bounded context and access is provided according to Principle of least privilege (POLP). All team members are covered by confidentiality clauses and NDAs. Background checks are performed by local authorities according to local laws and regulation.

All developers and technical staff undergo security training focusing on the common vulnerabilities regularly published by OWASP. Security is generally recognized to be hard to bolt on to an existing solution and has been an integral part of the daily development work of the MySecuritas applications.

Traceability

Activity logs are enabled which provides information when any resource is modified, or administrative actions are performed.

- Database Logs provide information about connections, duration of session and connected user details.
- Audit trail records are not possible to manipulate, regardless of authorization level.

Security controls

Several security controls are implemented as part of the automated build and release pipelines and passing these controls is a pre-requisite for putting any new functionality in production.

- Static code analysis is performed automatically on any code change. The code is scanned for many potential vulnerabilities and flagged directly in the pull request.
- Vulnerabilities in external libraries, i.e. dependency scanning, is performed continuously and any vulnerable version is flagged together with information on which version is needed to not be exposed.
- Peer review is performed on all changes through pull requests where at least one additional developer needs to scrutinize the code change before it is committed to the main code base.
- The *Responsible Disclosure* program encourages white hat hackers to find vulnerabilities in the MySecuritas applications and rewards are paid in proportion to the potential impact.

Patch handling

All managed services are automatically patched as part of the cloud service setup. The components containing custom developed code runs in containers built from public standard base images. All containers are subject to container scanning which identifies known vulnerabilities. Most often it is enough to update the base image to a newer version, but in some cases, there are patches that needs to be applied manually. For these situations the DevSecOps capability team provides patched base images in a private repository and all applications are automatically using the patched version when being redeployed.

Personal Data and Privacy

All MySecuritas applications are designed and developed after the introduction of GDPR and *privacy by design* has been a guiding principle throughout the development of all individual applications as well as the Securitas Digital Platform.

Third Party Services

Microsoft Azure

The core MySecuritas platform runs in the Microsoft Azure public cloud environment, including managed services for databases, container runtime, virtual networks, and backups. All Azure resources are provisioned in the EU/EES area.

Microsoft only provides infrastructure support for Azure resources. Microsoft personnel does not have access to Securitas or client data stored in MySecuritas applications.

Access to client data by Microsoft operations and support personnel is denied by default.

Auth0 (provided by Okta)

User authentication is managed by Auth0. The personal information kept in Auth0 is limited to the users' e-mail address. The Auth0 tenant used by MySecuritas is hosted in the EU/EES area.

Firebase

Firebase is used to send push notifications to both Android and IOS devices. The service is using an anonymization scheme where each user device is identified by a random identifier which is regularly rotated. The service provider is not able to link the messages with end users, hence the information is not classed as personal information.

Sendgrid (provided by Twilio)

The service for sending e-mail messages is provided by Sendgrid. MySecuritas sends links over email instead of the content itself, to avoid including any sensitive information. For example, if a user shares a guard report, the email will contain a link to that report instead of the report contents. Sendgrid does not store emails or their contents, nor does it store the recipient e-mail address (except for logs). Transactional logs related to the email are deleted after 30 days. The only personal information processed by Sendgrid is the e-mail address of the recipient. Sendgrid does not guarantee that all data processing takes place within the EU/EES but is committed to the standard contractual clauses (SCC) as set forth by the European Commission.

Mixpanel

Mixpanel provides usage analytics based on anonymized user information. Users are able to opt-in to collection of personal information for analytics purposes. Mixpanel is hosted within EU/EES.

PII Retention

PII captured as part of a MySecuritas user account is stored for 12 months of inactivity after which the user is requested to login to retain the data and access. No action on this request results in an account deletion including all related PII after 1 month.

Self-service functionality is in place for any user to delete their account and related PII from the system.