DECIDEACT

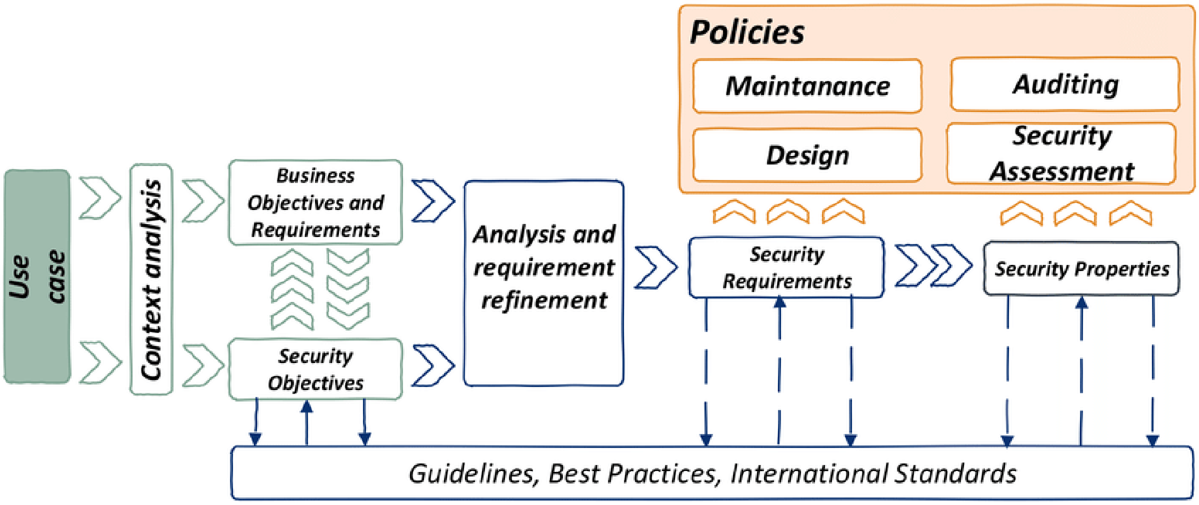
Technical specifications

Table of Contents

1. Security and Software Development

Building and deploying a secure system is an iterative process involving the entire team responsible for the product, e.g. product owners, developers, auditors, security experts and IT operations.

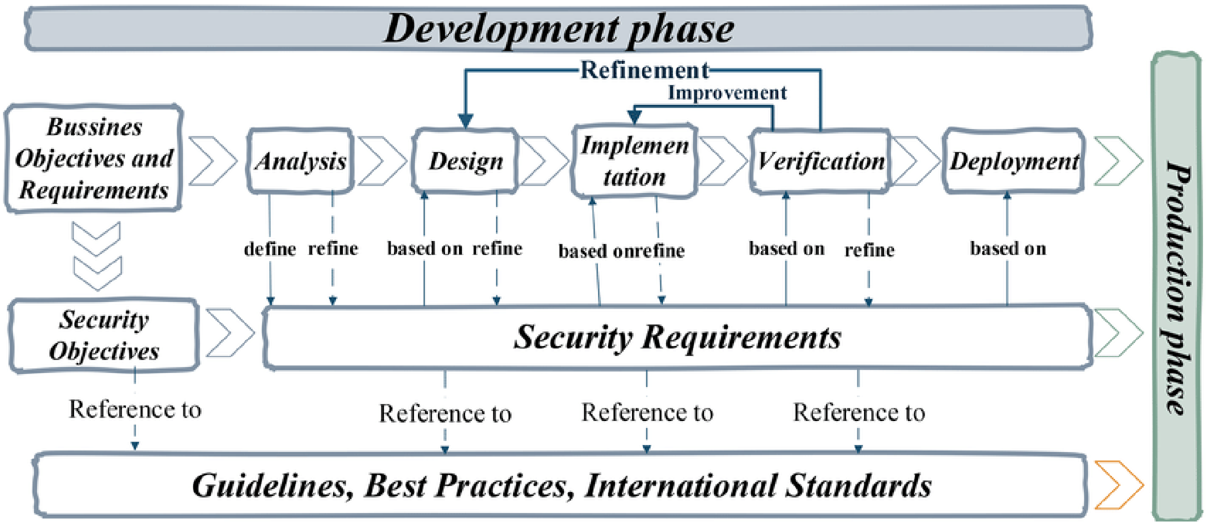
As a product evolves new features are requested and added. We use a specific development model to ensure that we live up to industry standards regarding security and best software development practices.



New features and requests are formulated by the product owner as use cases. The use cases are then analyzed by software architects in cooperation with the product owner to ensure that the team has a clear and precise view of the upcoming feature; furthermore, any security considerations are considered. This could be permissions for accessing a new API endpoint, user rights for updating a new resource, etc.

Our development team has a background from the FinTech industry where security and software development practices are subject to very strict procedures. We have used those procedures and best practices in the development process of the DecideAct system.

During software development we use TDD, Test Driven Development. This is done to ensure that the software is properly tested and that no new features added to the system will result in regression issues.



During our entire development phase, we follow strict security objectives and perform code analysis in order to deliver the best possible codebase. We use static code analyzers in order to maintain code consistency, govern our coding conventions and to optimize performance and avoid possible security problems.

1.1 Security

Building on the same requirements that are issued and enforced by the world's largest credit card companies, namely the Payment Card Industry Data Security Standard (PCI DSS), we have designed a system from the ground up with security in mind.

It's our aim to ensure the best possible security for your data by following these practices and procedures within our entire organization.

This includes (but is not limited to) ingress/egress traffic filtering, VPN, strong encryption of data in transit and at rest, well documented procedures and automated test suites.

1.2 Single Sign On and Enterprise Integration

Enterprise integration with SSO (Single Sign On) enables the DecideAct application to integrate directly into existing authentication systems such as Active Directory.

This ensures easy user management and integration into existing backend systems.

1.3 User authentication

For user authentication we use Auth0. This service allows us to use our own database with user information (credentials) or use SSO systems such as ADFS, Azure or similar. Furthermore, the system supports 2FA (Two Factor Authentication). Only authenticated users are allowed to fetch and/or modify data. This is governed by our authorization layer in the application. The authorization layer defines which data is available to the authenticated user, and only data that is filtered through the authorization layer is returned to the user. Each user can belong to one role (per account). The role defines the access rights in the system ranging from "Admin" (access to all) to "Reader" (read only access).

2. Technology

Working with a proven and stable technology stack is one of the core pillars in our philosophy to software design and development.

We utilize technology giants such as Cloudflare and Microsoft Azure to build a resilient, scalable and secure application platform. With strong encryption, VPN and encrypted data at rest, redundant storage and network typology we aim at the highest possible uptime and data security.

2.1 Blockchain Technology

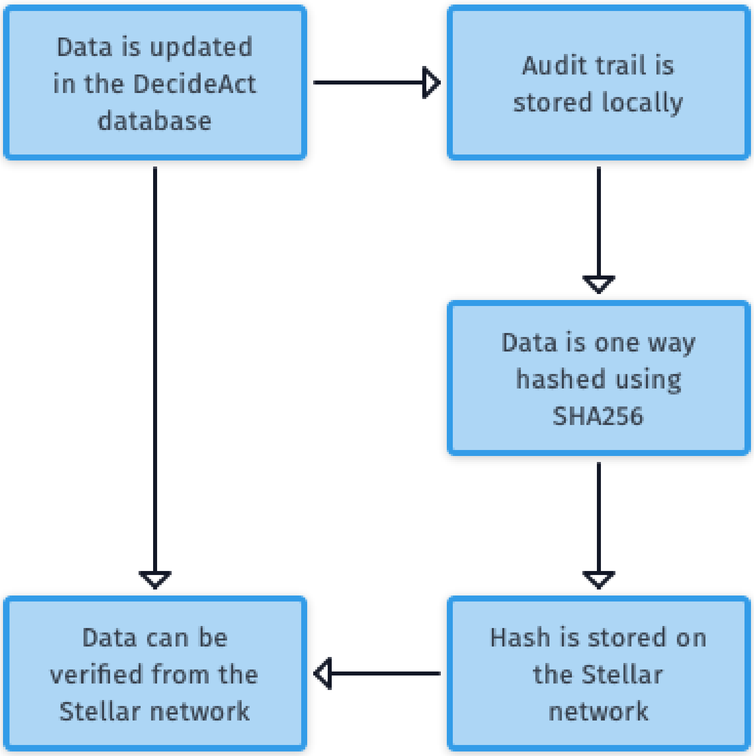
Data and data integrity is of great importance in any IT system. This is why DecideAct utilise MVCC databases to store and process data. All changes to data in the DecideAct system are audited, and to ensure the validity of the audit logs we have implemented a Blockchain validation system.

The DecideAct Blockchain validation system is built on Stellar - a global distributed blockchain network used by banks and FinTech companies. Each locally stored audit is digitally fingerprinted and stored on the Stellar network.

Data is digitally fingerprinted (one way hashed) using SHA256 and the returned hash is stored on the Stellar network. Once the hashed value is stored it can be retrieved from the Stellar network and compared to the hash value and timestamp stored in the DecideAct database.

This ensures that customers at any point in time can verify that the data stored and processed by DecideAct is valued and governed.

Data stored on the Stellar network is one way hashed value of audit data, and the hash cannot be reverse. This means that no confidential data ever leaves the DecideAct system, and we comply with all GDPR rules.


Data is updated in the DecideAct database
Audit trail is stored locally
Data is one way hashed using SHA256
Hash is stored on the Stellar network
Data can be verified from the Stellar network

Data is stored in a PostgreSQL database. Access to the database is encrypted and backups are encrypted at rest. Data can and will be removed to honor GDPR rules defined by the EU.

2.2 Browser Support

We support latest versions of Google Chrome, Firefox, Safari and Microsoft Edge.

DecideAct is accessible via HTTPS only, and all API calls are always encrypted. Furthermore access to our database is encrypted and database backups are encrypted at rest. Access to the system is furthermore protected by firewalls (inbound and outbound rules).

2.3 Cloud

DecideAct is hosted in the Cloud by Microsoft Azure (Europe) and the processing is regulated according to the Data Processing Agreement.

The ISO certification data for Microaoft Azure can be found here: https://learn.microsoft.com/en-us/azure/compliance/offerings/

3. Communication, Synchronization and Data Processing

Communication between the frontend and backend system is handled via a secure GraphQL API. All communication is encrypted between the browser and the backend system using strong encryption (HTTPS). Data received by the backend system is processed immediately and updates are pushed out to connected clients via an encrypted WebSocket connection. This will give a live and real time user experience of the interface.

Data can furthermore be imported and exported via dedicated and secure APIs. We use industry standard data formats (GraphQL) for easy export of data to external systems and we can provide custom solutions for enterprise customers.

Our API endpoints support both data pull (queries) and data push (mutations) communication allowing the biggest flexibility when integrating with 3rd party systems.

User administration can be managed by synchronizing data from Microsoft AD servers and other similar systems; this is part of our enterprise integration.

3.1 Service Level Agreement (SLA).

DecideAct’s Service Level Agreement (SLA) defines terms and conditions for maintenance and customer support performed by DecideAct Solutions IVS for the customer.

The Service Level Agreement covers the software known as DecideAct, which is a tool used to account for and monitor strategic initiatives as related to the corporate strategy at hand.

The Service Level Agreement is valid when the Customer has a valid subscription for products covered by the Service Level Agreement.

The SLA will for example inform you about:

- **Customer support** regarding error report handling and incident management, workaround solutions as and when needed and requests for information only.

- **Incident Management** informing about requesting service or submitting incidents, error reporting, support opening hours and response and resolution time.

- **Exclusions** describes DecideAct’s obligations and responsibilities regarding feature requests etc. from the clients.

- **System Management** will inform you about the availability of software and services hosted by DecideAct, DecideAct Backup and Restore plan and other important communication about disturbance or downtime.

For detailed information on the rights of DecideAct‘s customers concerning the Service Level, please read the Service Level Agreement: https://www.decideact.net/service-level-agreement/

4. API Integration

DecideAct offers various secure pull/push APIs for easy integration with 3rd party systems. This allows external systems to synchronize data with DecideAct (import and export of data in a secure fashion).

In addition to our standard APIs, we can provide custom API integration for enterprise customers on request.

Our development team can assist with the technical integration of enterprise solutions.

Major 3rd party systems such as Microsoft Power BI, Grafana, Tableau.com and SAP (just to name a few) can communicate directly via GraphQL and fetch data from the DecideAct system.

Furthermore, data can be updated via GraphQL (via mutations). This allows 3rd party systems to update data for Initiatives and KPIs in the DecideAct system directly when data is available. This could be from any external system.

We aim to keep our API open for any 3rd party application; this will ensure the biggest flexibility for customers and ease of integration.

5. GDPR

In DecideAct we sign a data processing agreement (DPA) with all our customers, in which the rights of our customers concerning the protection of personal data are stated. As part of DecideAct‘s (the Data Processor’s) services to its Customers (Data Controllers), DecideAct processes data relating **to** employees of DecideAct‘s customers (DecideAct‘s users)**.**

The DPA will for example inform you about:

- **Personal data and data processing** such as which data DecideAct processes on behalf of its cutsomers, for which purpose and which activities the processing of the Personal Data includes.
- **Instructions and confidentiality** regarding handling of the user‘s data, such as notifying the customer without undue delay after becoming aware of a personal data breach, and follow the procedures in Article 33 of the EU Regulation 2016/679 on General Data Protection (“GDPR”).
- **Security** to protect the Personal Data, the Data Processor must implement appropriate technical and organisational measures in such a manner that the processing meets the requirements set out in the GDPR. Such measures are determined and adjusted on a regular basis with due consideration for the current technical level, expenses, and the nature, scope, context and purposes of the processing and the risks to the rights of natural persons, cf. Article 32 of the GDPR.
- **Sub-processors** in accordance with Article 28 of the GDPR, e.g. regarding information requirements (including list of sub-processors) and integrations with third Party Services.
- **Assistance to the Data Controller** by DecideAct to ensure that all obligations under Art. 32-36 of the GDPR and other applicable data protection and information security legislation are met, i.e. security measures, notification of supervisory authorities, notification of individuals, preparation of data protection impact assessments and prior consultation of the supervisory authorities.
- **Availability of information** in order to demonstrate compliance, audits etc.
- **And other information on how DecideAct ensures compliance** of the EU Regulation 2016/679 on General Data Protection (“the GDPR”)

For detailed information on the rights of DecideAct‘s customers concerning the protection of personal data handling subject to the General Data Protection

Regulation (the „GDPR“), please read the Data Processing Agreement which is annexed to DecideAct‘s Terms and Conditions: https://www.decideact.net/terms/

In our Terms and Conditions we also describe our dataprocessor role and the personal data that we store.