SIEMENS

Navigator Security concept

Secure IT architecture

The Navigator application and database servers are hosted in the data center Karlsruhe, Germany[1], by Atos and follows the IT Security Management Process.

Documented processes

Siemens' IT service provider Atos has a documented security incident management, which conforms with ITILv3 for IT Security Incident Management and ISO 27001, and with defined escalation levels and involvement of the Building Technologies Division from Siemens.

Access security

Siemens takes all the necessary precautionary measures to ensure that your Navigator transactions are as secure as possible. Access is granted via an individual user account comprising of a user name and password (passwords are stored in an encrypted form) with a minimum of 8 characters (combination of letters, numbers and special characters). The application supports two-factor authentication via SMS OTP (one-time password). The account is locked after 5 unsuccessful logon attempts.

IT service continuity and backup

Siemens' IT service provider has standard IT service continuity measures in place. In particular, backup systems are connected to the systems in the Web and application server zone with a dedicated backup network. Backed-up data is sent to another data center over dark fiber connections, where it is stored on tape libraries.

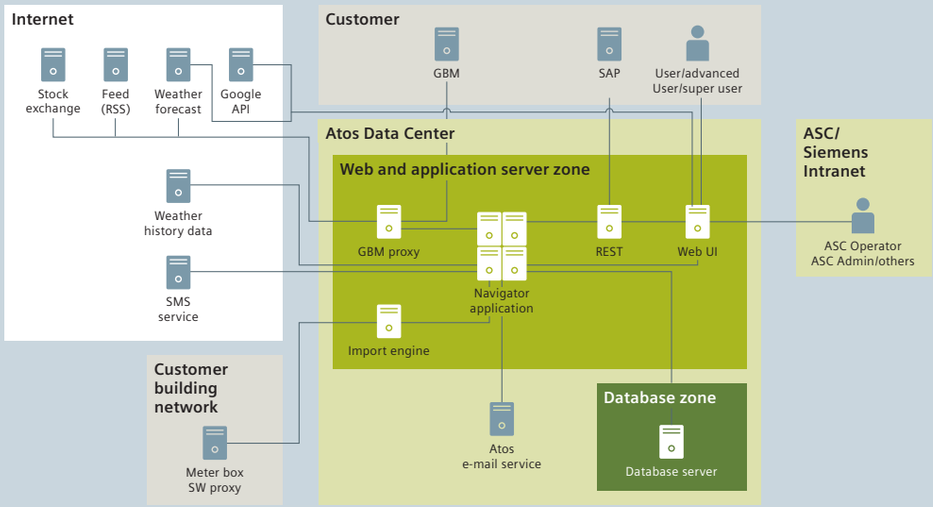
Isolation of customer data

Each customer has its own set of data that remains logically isolated from data that belongs to all other customers.

Security management

Siemens' IT service provider keeps abreast of current threats (such as zero-day exploits) for the applications and components used to provide their service. With respect to security-relevant patches, Atos the IT service provider, uses the "Security Telegrams" CERT service from Siemens to receive relevant security notifications for all standard platforms on which the Navigator application runs. "Security Telegrams" contain a criticality score. A procedure that specifies responsibilities and duties in observing security warnings is also in place. The CERT service from Siemens also informs about current threats like zero-day exploits and possible workarounds. In such a case, Siemens will decide about the implementation of a suitable workaround.

www.siemens.com/bt/navigator



The graph shows the overall system architecture with all interfaces. The overall system consists of multiple network zones with different security parameters.

Secure communication with the Navigator application server is guaranteed by a state-of-the-art encrypted https connection (256-bit SSL).

The IT service provider also runs a patch management process that covers all components used to provide the service to Siemens. This includes patches for the operating systems which are installed on the global "Siemens OS Patch Day". In between, critical patches are installed after consultation with Siemens.

Secure software development

The software has been developed according to best practices in secure software development, covering the following aspects:

- Protection against SQL injection vulnerabilities, cross-site request forgery and cross-site scripting
- Secure session handling
- Secure password management
- No disclosure of internal information (e.g. via error messages, version, absolute path names)

The software developers are trained on secure software development policies and guidelines.

The Navigator application has been tested for absence of security vulnerabilities/ flaws, using state-of-the-art security testing (code reviews, static code analysis, unit and integration testing) methodologies.

The security testing included the OWASP (Open Web Application Security Project) top ten vulnerabilities.

Security assessments

The Siemens-internal Security Assessment Team performs regular penetration tests on the Navigator application, in particular of the interfaces exposed to the Internet.

Termination of contract – data ownership

Upon termination of contract, all meter data and uploaded documents will be returned to the customer at a cost agreed upon in the service agreement.

Highlights

- Access is granted via an individual user account
- ITILv3 for IT Security Incident Management and ISO 27001 conform
- Database security prevents accidental or malicious access
- Security testing based on OWASP (Open Web Application Security Project) top ten vulnerabilities

[1] At the date of printing this document, the data center location Karlsruhe, Germany, is not certified according to ISO 27001.

Siemens Switzerland Ltd
Building Technologies Division
International Headquarters
Gubelstrasse 22
6301 Zug
Switzerland
Tel +41 41 724 24 24