Embedded security

Requirement analysis and design of a secure
update mechanism for an IoT gateway

Customer requirements

The scope of the project was a requirement analysis for the creation of a secure update mechanism for an IoT gateway. To ensure security the update image needed to be testable for completeness, correctness, and authenticity (genuineness and origin). Also changes to the content of an update package were to be reliably detected.

A process was to be established that ensures secure generation of the asymmetrical key pair and secure handling, storage, and administration of the signature key.

A reliable signalling and download mechanism was also to be specified.

comlet solution

A process for generating an asymmetrical, cryptographic key pair was defined based on the recorded requirements. It is following the dual-control principle. The passphrase was distributed and multiple instances of the private key were securely archived. Finally, the process was integrated into the client's existing process structures. Therefore the definition and documentation of the various responsibilities have been a pre condition. In addition, the signing process was integrated into the release/update management process.

Aspects like secure communication with the back end and supervision leading to VDE certification were taken into account during the definition of the update process.

Technology used

openSSL, MS Office, Confluence/JIRA

comlet

comlet Verteilte Systeme GmbH I Amerikastr. 27 I 66482 Zweibrücken I Tel. +49 6332 811-100 I Fax +49 6332 811-315 I www.comlet.de I info@comlet.de