Embedded Security

Anforderungsanalyse und Entwurf eines sicheren
Update-Mechanismus für ein IoT-Gateway

Anforderung des Kunden

Gegenstand des Projektes war eine Anforderungsanalyse zur Erstellung eines sicheren Update-Mechanismus für ein IoT-Gateway. Um dies sicherstellen zu können, sollte das Update Image auf Vollständigkeit, Korrektheit und Authentizität (Echtheit der Herkunft) prüfbar sein und Änderungen des Inhaltes sicher erkannt werden können.

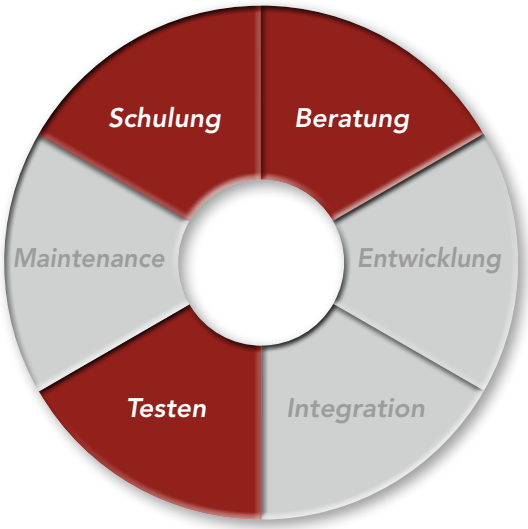
Es sollte ein Prozess etabliert werden, der eine sichere Erstellung des asymmetrischen Schlüsselpaares, einen sicheren Umgang sowie eine sichere Ablage und Verwaltung der Signaturschlüssel gewährleistet.

Des Weiteren sollte ein zuverlässiger Signalisierungs- und Download-Mechanismus spezifiziert werden.

Lösung comlet

Aus den erarbeiteten Anforderungen wurde ein Prozess zur Erstellung eines asymmetrischen, kryptographischen Schlüsselpaares definiert. Dieser basiert auf dem 4-Augenprinzip. Es erfolgte eine Aufteilung der Passphrase und der gesicherten Mehrfacharchivierung des privaten Schlüssels. Abschließend wurde das Vorgehen in die vorhandenen Prozessstrukturen des Kunden integriert. Die Definition und Dokumentation der jeweiligen Zuständigkeiten war hierfür Voraussetzung. Darüber hinaus wurde der Signierungsprozess in das Release / Update-Management integriert.

Auch Aspekte, wie die sichere Kommunikation zum Backend und die Begleitung zur Zertifizierung durch den VDE wurden bei der Definition des Update Prozesses berücksichtigt.



Verwendete Technologien

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