

# Produktinformation

***bi-Cube***<sup>®</sup> Token

Technologien   Lösungen   Trends   Erfahrung

In den meisten Unternehmen und Verwaltungen nimmt das Bewusstsein für Sicherheitsfragen zu. Ein einfaches und schnelles Authentifizierungssystem ist das **bi-Cube<sup>®</sup> Token** in Verbindung mit einem SMS-Token.

## bi-Cube<sup>®</sup> Token

Der User nutzt bei einem Tokenmanagement zur Authentifizierung zwei Faktoren: eine PIN oder ein Passwort, die der User kennt, sowie einen wechselnden Code aus einem Token. Der SMS-Token bietet neben dem iSM-Tokengenerator eine weitere Möglichkeit, sichere Token zu benutzen. Dabei wird der Token jedoch nicht von einer Codekarte, USB-Stick oder ähnlichem erzeugt, sondern dem User per SMS auf sein Mobiltelefon übermittelt.

### „Das Handy ist der Schlüssel“

Anstelle zusätzlicher Hardware wird das vorhandene Handy des Users für eine zusätzliche Authentifizierung genutzt.

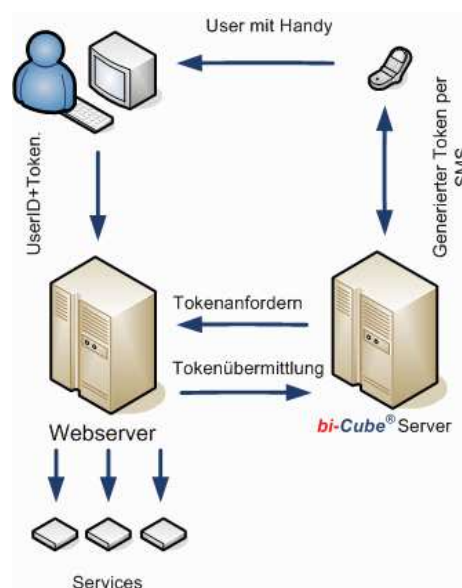
Das SMS-Token wird über eine Web-Applikation nach Eingabe von Username / Kennwort angefordert und mit einem Zeitstempel versehen. Nach Eingabe des Tokens erfolgt dann der Zugriff auf die vom Anbieter vorgesehenen Applikationen. Die Lösung ist für unterschiedliche Anwender flexibel konfigurierbar und berücksichtigt zur Definition bereitgestellter Ressourcen die derzeit gültigen Standards zum Versand von SMS.

Die Anwender dieser SMS-Lösung benötigen eine zentrale Erfassung der Zugangsberechtigten für die zu sichernden Ressourcen.

Eventuelle Änderungen der Daten werden durch das zentrale System flexibel und ohne Zeitverzögerung realisiert.

**In der heutigen mobilen Zeit der Notebooks und Handys wird ein sicheres, komfortables und an allen Orten der Welt einsetzbares Authentifizierungsverfahren immer wichtiger.**

Mit dem SMS-Token des iSM können Außendienstmitarbeiter sich an praktisch jedem beliebigen Ort sicher mit dem Firmennetzwerk verbinden.



## Ablaufschema

### ● Antragsverfahren

Nach der ersten Authentifikation (User-ID / PW) auf einer Web-Page wird der User aufgefordert, das Token, das ihm vom System per SMS auf sein Handy übertragen wurde, in das bereitstehende Eingabefeld zu übertragen.

Im technischen Ablauf wird im ersten Schritt die Korrektheit der eingegebenen Userdaten geprüft und ein Token generiert und per SMS versendet. Die entsprechende Handynummer ist dem **bi-Cube<sup>®</sup>**-Server bekannt.

Der Zeitstempel ist auf zwei Wegen skalierbar. Zum einen darf dieser Schlüssel nur für einen kurzen Zeitraum nach dem Versand gültig sein (Aktivierungszeitraum). Das zwingt den User, den Schlüssel nur dann anzufordern, wenn er wirklich gebraucht wird. Dabei sind die Zeiten zu beachten, die eine SMS typischer Weise benötigt, um übermittelt zu werden.

Zum anderen besteht die Gültigkeit des Token nach erfolgreicher erster Anmeldung für einen festgelegten Zeitraum (Sessiondauer), um permanente Zugriffe auf Netzressourcen des Anbieters zu verhindern. Dieser zweite Zeitraum muss frei wählbar sein, um den unternehmensspezifischen Gegebenheiten Rechnung zu tragen.

### ● **bi-Cube<sup>®</sup>** Server

Der einzurichtende **bi-Cube<sup>®</sup>** Server stellt eine Serverumgebung bereit, welche den Datenbankbetrieb ermöglicht. Es wird somit ein ideales Umfeld zur Verwaltung sensibler Userdaten und eine komfortable Verwaltung der generierten Token geschaffen. Der auf dem **bi-Cube<sup>®</sup>** Server einzurichtende Dienst generiert den Token und vergleicht im Aktivierungszeitraum diesen (anhand des Zeitstempel) mit dem eingegebenen Schlüssel.

### ● Web Server

Der Web-Server hält das Log-In Frame für das Login mit SMS-Token bereit und stellt die benötigte Datenbankbindung per UDP zum **bi-Cube<sup>®</sup>** Server her. Über diese Anbindung übergibt die Web-Applikation die eingegebenen Daten des Users und stellt bei Erfolg auch die Erreichbarkeit der Services sicher.

### ● SMS Versand

Der Versand der SMS erfolgt durch einen externen Service, der das durch den **bi-Cube<sup>®</sup>** Server bereitgestellte Template abholt und versendet.