

Technische Produktinformation

bi-Cube[®] ID-Server
für Online-Kunden

Technologien Lösungen Trends Erfahrung

Inhalt

1	BI-CUBE[®] - TOKEN ALS KOSTENGÜNSTIGE, SICHERE IDENTIFIKATION	3
2	ZWEITE SICHERHEITSSTUFE ALS SCHUTZ GEGEN PHISHING.....	4
3	TECHNISCHE LÖSUNG	4

1 **bi-Cube**[®] - Token als kostengünstige, sichere Identifikation

Für Online - Geschäfte, insbesondere im Private Banking ist eine sichere Identifikation des Kunden für beide Seiten eine unverzichtbare Geschäftsbasis.

Die Anforderungen an die Identifikation in Richtung Sicherheit einerseits und Komfort andererseits sind in der Regel gegenläufig. Nur die duale Authentifikation bietet hier einige Möglichkeiten, beide Ziele zu erreichen.

Dieser Zielstellung entspricht die vom iSM entwickelte Lösung des **bi-Cube**[®] - Token, das bereits seit Jahren erfolgreich zur sicheren Authentifizierung im e-Business eingesetzt wird. Das Prinzip des Token besteht in der zeitabhängigen Generierung einer Zeichenfolge mit einigen internen Informationen, die verschlüsselt und komprimiert übertragen und serverseitig wieder entschlüsselt sowie in den einzelnen Komponenten geprüft werden.

Das Grundprinzip der dualen Authentifizierung besteht darin, dass die Bestätigung der Authentizität eines Kunden von zwei unabhängigen Komponenten abhängt. Im Falle des **bi-Cube**[®] - Token sind dies:

1. ein Passwort, das der User weiß und
2. ein Gerät, das der User hat und welches eine weitere Identifikation liefert, das sog. Token.

Das **bi-Cube**[®] - Token kann in 2 Varianten genutzt werden:

1. als Ergänzung der bisherigen Authentifizierung (ID und Passwort) oder
2. nur das Token - zusammen mit einer initialisierenden PIN.

Die 1. Variante hat die Vorteile, dass das die bisherige Maske beim Kunden und die Prüfung in der Bank beibehalten wird und nur durch das Token ergänzt wird. Diese Variante ist etwas sicherer als die 2. Variante, da in dieser die PIN im Token - Generator mit enthalten ist und damit dem (zwar geringen aber prinzipiell vorhandenen) Risiko des „Knackens“ des Generator - Codes unterliegt.

Für das Online Banking würden sich also 3 Stufen einer sicheren Authentifizierung anbieten, die mit unterschiedlichen Limits verbunden werden könnten.

1. Stufe: wie bisher mit User-ID und Passwort
2. Stufe: Token mit PIN
3. Stufe: User-ID / Passwort - ergänzt um das Token

Die Anmeldung des Users in seinem Bankportal erfolgt zweistufig (duale Authentifikation). Im ersten Schritt meldet sich der Nutzer z.B. in Stufe 3 wie gehabt mit seiner ID (Username) und Passwort an. Nach positiver Überprüfung wird das Token abgefragt und zusätzlich am ID-Server bei der Bank geprüft.



Mit dem Fadenkreuz kann das **bi-Cube**[®]-Token in ein Feld einer Webseite übertragen werden.

Das u.a. individuell erzeugte Token ist nur für eine Min. (konfigurierbar) gültig:

```
71E49FA2F65E815893EE299DA66383073EF4BF  
039E930C7EFCDD5C4BCF8DE3DEF452ACFCA  
03D591DCA608FEA99F5486961AC97F1C4ED16  
26F67FB8A621B12A4F2B6EC7D7C416D9B7726  
A81DF46D2183CEF0723C638B0FD0828A83BCDFAA  
336375DABF2CD4AD8CD6A
```

Als Zusatzfunktion kann der User mit dem Token - Generator auch noch Dateien auf seinem PC verschlüsseln. Eine Entschlüsselung ist nur über das Token möglich.

2 Zweite Sicherheitsstufe als Schutz gegen Phishing

Der eigentliche Kern des Problems besteht beim Phishing darin, dass der Inhalt der Überweisung in betrügerischer Absicht verfälscht wird. Deshalb wäre in einer weiteren Ausbaustufe folgendes Szenario möglich:

Die wichtigsten Daten der Transaktion, z.B. der Überweisung, werden herausgezogen, daraus ein Hashcode gebildet und dieser Code dann im Secu-Token mit verschlüsselt. Mit diesem Transaktions-Token gibt der Kunde dann die Überweisung endgültig frei. Damit kann dann auf Bankseite die „Unversehrtheit“ der eigentlichen Daten geprüft werden.

Mit dem **bi-Cube**[®] - Token kann eine Bank somit für ihr Online - Geschäft eine kostengünstige und auch „Phishing – Proof“ Lösung bereitstellen. Dies ist unter Berücksichtigung der aktuellen Diskussion ein enorm wichtiges Vertriebsargument in der Gewinnung von Neukunden und der verstärkten Online - Nutzung durch Bestandskunden der Bank.

3 Technische Lösung

Mit dem Token - Generator wird ein personalisiertes Token erzeugt.

Je nach Einstellung und damit nach Security - Anforderungen kann das Token fest an ein Device, den USB-Stick, gebunden oder dem User als Software zum Download auf seinem Rechner bereitgestellt werden. Diese Option ist damit die Sicherung, dass das Token nur auf dem übergebenen USB-Stick lauffähig ist, also nicht kopiert werden kann.



Als Fall-Back-Lösung, wenn der Kunde sein Secu-Token nicht verfügbar hat und bei der Bank seine Handy-Nr. hinterlegt ist, kann auch ein SMS-Token genutzt werden. Zum Versand des SMS-Token bietet das iSM einen entsprechend gesicherten Webservice als Dienstleistung an. Ob ein Kunde das SMS-Token nutzen kann, ist in seinen Daten hinterlegt.

Bitte geben Sie Ihr Token ein.

1. Tokenart wählen

Security-Token

SMS-Token

Handynummer

49 [redacted]

SMS-Token anfordern

2. Token eingeben

[redacted]

Übernehmen

Token mit Pin

Das PIN-gesicherte Token kann dem Nutzer vor dem Ausgeben auf einem Memo-Stick generiert werden.

Erst nach Eingabe der PIN startet der Token-Generator.

