

# Online-Banking der Zukunft ist sicher vor Phishing

## Kobil bietet mit „Mobile Futurebanking“ auf drei Säulen Sicherheit beim e-Banking

Worms, 21. Oktober 2005. Unter Kobil Mobile Futurebanking präsentiert der Wormser IT-Security-Hersteller Kobil Systems ein auf drei Säulen bauendes Angebot an sicheren Online-Banking-Lösungen: über Einmalpasswörter, PKI-basierte Lösungen mit Smart Card-Zertifikat und Kobil mIDentity Basic, dem weltweit einzigen Kartenleser mit Smart Card, Flash-Speicher und mobilen Unternehmenslösungen. Kobil mIDentity Basic hat in seinem mobilen Datensafe bereits den Browser Mozilla Firefox und die Startseite der Bank vorkonfiguriert. Die Authentifikation des Benutzers erfolgt nach Eingabe der PIN automatisch über die integrierte Smart Card. Ohne Treiber oder Software am PC installieren zu müssen, kann der Anwender seine Banktransaktionen mit dem handlichen Kartenleser an jedem beliebigen Rechner ausführen. Bei der zertifikatsbasierten Lösung erfolgt die Benutzeridentifikation ebenfalls über eine Smart Card. Die Identifikation über Einmalpasswörter erfolgt ähnlich wie beim PIN/TAN-Verfahren, bietet jedoch mehr Sicherheit und Mobilität, da der Benutzer die nur einmal gültigen Passwörter bei Bedarf elektronisch über ein Token generiert. Die einzelnen Mechanismen des Mobile Futurebanking sind miteinander kombinierbar.

Einen hundertprozentigen Schutz vor Phishing bietet Kobil Mobile Futurebanking über die dritte Säule Kobil mIDentity Basic. Da der Browser inklusive Startseite der Bank schon im mobilen Datensafe des handlichen Kartenlesers vorkonfiguriert ist, braucht der Anwender nur seine PIN einzugeben und kann gleich seine Transaktionen durchführen. Die Authentifikation erfolgt automatisch über die Smart Card. Da die Internet-Adresse der Bank fest im mIDentity vorkonfiguriert ist und nicht geändert werden kann, ist ein Umlenken des Bankkunden auf eine gefälschte Webseite nicht möglich. Des Weiteren ist keinerlei Installation, weder von Treiber noch von Software, auf dem Rechner notwendig, da der Browser auf dem mIDentity liegt und an jedem beliebigen PC gestartet werden kann. Der Bankkunde ist damit vollkommen flexibel und mobil - und dennoch rundum sicher. Ein weiterer Vorteil liegt im deutlich reduzierten Supportaufkommen für die Bank, da alle Einstellungen vorkonfiguriert werden und der Anwender über einen Read-only-Bereich arbeitet, in dem er nichts an den Einstellungen versehentlich oder absichtlich ändern kann.

Einen nahezu gleichwertigen Phishing-Schutz bietet Kobil Mobile Futurebanking über eine PKI-basierte Lösung mit Smart Card-Zertifikat. Einige Banken wie die türkische Koç-Bank bieten ihren Business-Kunden bereits ein Smart-Banking-Paket an, das aus der Software Kobil Smart Key, einem Kobil Smart Card Terminal und Smart Card mit persönlichem Zertifikat besteht. Das digitale Zertifikat auf der Smart Card schützt die digitale Identität des Kunden und sorgt für eine sichere Anmeldung an der Bankapplikation. Der Kunde muss nur die Karte ins Lesegerät stecken und seine PIN eingeben. Nur derjenige erhält Zugang zum Bankserver, der beide Faktoren erfüllt, also im Besitz der Karte ist und die PIN kennt (Zwei-Faktor-Authentifikation: Besitz und Wissen). Dadurch ist ein Missbrauch durch Phishing oder andere Passwortspionage ausgeschlossen. Der Vorteil der beiden Smart Card-basierten Lösungen ist außerdem, dass der Kunde die Smart Card für weitere Applikationen wie für die digitale Signatur und die Verschlüsselung von Daten und E-Mails nutzen kann.

Beim Online-Banking mit Einmalpasswörtern erhalten die Bankkunden als mobile Endgeräte SecOVID Token, mit denen sie Einmalpasswörter generieren, um sich damit auf dem Bankserver einzuloggen. Solche nur einmal

gültigen Passwörter sind wesentlich sicherer als statische Passwörter, die leicht ausspioniert und dann missbräuchlich eingesetzt werden können. Außerdem ersparen sie den aufwändigen Druck von TAN-Listen, da das SecOVID Token quasi eine unendliche elektronische TAN-Liste darstellt. Die Lebensdauer des Tokens ist unbegrenzt, da die Batterie des Tokens jederzeit vom Endbenutzer ausgewechselt werden kann. Alternativ können die Einmalpasswörter auch mit einem Soft-Token erzeugt werden. Dieses wird in Form einer Software zur Verfügung gestellt und kann vom Anwender auf verschiedene Endgeräte (zum Beispiel PDAs oder Mobiltelefone) geladen werden.

Die einzelnen Mechanismen der Online-Banking-Lösungen sind miteinander kombinierbar. „Mit Mobile Futurebanking bietet Kobil unter einem Dach die passende Lösung für jeden Kundenwunsch. Alle Bereiche aus einer Hand mit einer Lösung zu bedienen kann heute nur Kobil“, so Marius Schmidtke, Teamleiter Marketing bei Kobil Systems. Sämtliche Kobil-Lösungen unterstützen den EMV-CAP-Standard, der für die starke Authentifizierung bei E-Banking und E-Commerce-Anwendungen von Eurocard, MasterCard und Visa (EMV) definiert wurde. Das Chip Authentication Program (CAP) wurde entwickelt, um Transaktionen mit Kreditkarten im Internet sicher abwickeln zu können.

#### **Über die Authentifikation mit Einmalpasswörtern:**

Die Absicherung mit Einmalpasswörtern besteht aus zwei Hauptkomponenten: Auf der Benutzerseite benötigt der Zugangsberechtigte ein Authentifikationsgerät in Verbindung mit einer PIN, zum Beispiel ein Token, eine Smart Card und Kartenterminal, ein PDA oder ein Handy. Die zweite Komponente ist der Server – bestehend aus Software und Administrationstool zur Verwaltung der Benutzer. Der Benutzer erhält von seinem Authentifikationsgerät einen numerischen Code, der auf Basis des 3DES-Algorithmus berechnet wird. Dieser Code ist nur einmal gültig. Sollte jemand versuchen, dieses Einmalpasswort ein zweites Mal zu verwenden, wird der Zugriff verweigert. Ein Angreifer kann ein abgehörtes oder ausgespähtes Passwort also nicht selbst benutzen. Wenn der Benutzer sein Einmalpasswort in die Bildschirmeingabemaske eingibt, wird es über das Netzwerkgerät (zum Beispiel VPN oder Webserver) verschlüsselt an den Server weitergeleitet und dort überprüft. Ist das Einmalpasswort korrekt, erhält der Benutzer den Zugang ins Netzwerk. Damit der Server das Passwort verifizieren kann, verwenden Token und Smart Card einen Algorithmus und Ausgangswerte, die mit dem Einmalpasswort-Server synchronisiert sind. Der Server übernimmt die Überprüfung der Einmalpasswörter (Authentifikation), die Verwaltung der Benutzerrechte (Autorisierung) und die Protokollierung der Zugriffsversuche (Accounting).

#### **Über die zertifikatsbasierte Authentifikation:**

Die zertifikatsbasierte Benutzeranmeldung basiert auf einem asymmetrischen Verschlüsselungsverfahren mit zwei komplementären Schlüsseln, einem geheimen (private key) und einem öffentlichen Schlüssel (public key). Der private Schlüssel liegt hoch sicher auf der (PIN-geschützten) Smart Card und dient zur Entschlüsselung von mit dem öffentlichen Schlüssel verschlüsselten Daten. An den öffentlichen Schlüssel gebunden dient das digitale Zertifikat als digitale Identität des Benutzers. Für die Authentifikation erfolgt der Zugriff per Smart Card mit privatem Schlüssel und Zertifikat über ein Kartenlesegerät. Das Zertifikat fungiert quasi wie ein digitaler Ausweis und bindet seinen Inhaber an den öffentlichen Schlüssel. Die Handhabung ist für den Benutzer sehr einfach: Er muss bei der Anmeldung nur seine Smart Card ins Lesegerät stecken und seine PIN eingeben.

#### **Über Kobil Systems:**

Die 1986 gegründete Kobil Systems GmbH agiert als Hersteller hochsicherer Basistechnologie im Umfeld von Smart Cards, Einmalpasswörtern (OTP) und Zertifikaten. Sicherheit ohne Einschränkungen, einfach, überall und jederzeit, zu ermöglichen, dieses Ziel hat Kobil durch langjährige Forschungs- und Entwicklungsarbeiten verwirklicht. Das Unternehmen bietet seinen Kunden heute nicht nur patentierte Basistechnologie, sondern vor allem die wichtige und umfassende Lösungskompetenz, um gemeinsam mit namhaften Technologiepartnern für jedermann die Verwendung seiner digitalen Identität bequem und gleichzeitig absolut sicher zu ermöglichen.

---

Weitere Informationen: KOBIL Systems GmbH, Marius Schmidtke, Pfortenring 11, D - 67547 Worms  
Tel.: (06241) 3004-31, Fax: (06241) 3004-80, E-Mail: marius.schmidtke@kobil.com, Internet: <http://www.kobil.com>  
Pressekontakt: Konzept PR GmbH, Andrea Finkel, Karolinenstr. 21, D-86150 Augsburg  
Tel.: (0821) 34300-15, Fax: (0821) 34300-77, E-Mail: [a.finkel@konzept-pr.de](mailto:a.finkel@konzept-pr.de), Internet: <http://www.konzept-pr.de>