



Die einzig wahre Lösung

Secure Remote Access mit KOBIL



KOBIL 
secure your identity



Ohne die PIN geht gar nichts –
und die wissen nur Sie!

Wissen und Besitz: entscheidend für Secure Remote Access



Ohne Token bzw. Smart Card
geht allerdings auch nichts – und
selbst ein Diebstahl ist zwecklos:
Die Kombination von Wissen
und Besitz macht KOBIL Authenti-
fikationslösungen hochochsic!
sic!

Sie haben in Sicherheitstechnologien investiert, um den Zugriff auf Ihr Unternehmensnetzwerk besser zu schützen. Doch ist die Authentifikation bei VPN, Firewall und RAS mit statischem, wiederverwendbarem Passwort und Benutzernamen nicht wirklich sicher und macht Ihre Investitionen zunichte. Es ist zu leicht, auf die Frage „Wer sind Sie?“ auch als unbefugter Nutzer die passende Antwort zu geben. KOBIL schiebt dem Missbrauch einen intelligenteren Riegel vor, der sich ganz einfach implementieren lässt. Mit Einmalpasswörtern und auf der Basis digitaler Zertifikate.

Wer nicht darf, darf eben nicht. Punkt.

Sie haben Ihr Netzwerk von außen zugänglich gemacht. Für Mitarbeiter im Außendienst und Mitarbeiter mit Home-Office. Für Niederlassungen und Filialen. Für Partnerfirmen, die in interne Unternehmensprozesse eingebunden sind. Und natürlich für Kunden. Ihr Unternehmensnetzwerk muss aber sicher sein – wie ein Safe. Vor dem Ausspähen von vertraulichen Unternehmensdaten. Vor zufälligen oder beabsichtigten Hacker-Attacken. Vor zielgerichteter Sabotage.

Statische Passwörter können:

- ausgespäht werden
- erraten werden
- gestohlen werden
- abgehört werden
- gehackt werden
- von Trojanern versendet werden
- durch Wörterbuchangriffe aufgedeckt werden

Egal, welche Sicherheitstechnologie Sie nutzen – mit statischen Passwörtern ist sie nichts mehr wert

Zugänglichkeit und Sicherheit müssen also nebeneinander bestehen. Dazu braucht Ihr Unternehmensnetzwerk die Fähigkeit, intelligent unterscheiden zu können – zwischen berechtigten und unberechtigten Zugriffen.

Authentifikation: Wer sind Sie?

"Wer sind Sie?" ist die zentrale Frage beim Zugriff auf ein Unternehmensnetzwerk. Die Identität des Benutzers muss eindeutig bestimmt werden können. Nur dann ist überhaupt eine Basis für ergänzende Sicherheitstechnologien vorhanden. Statische Passwörter gehören nicht zu den ausreichend effektiven Formen der Authentifikation. Aus diesem Grund finden Sie im Produktportfolio von KOBIL Lösungen, die sich der Herausforderung auf andere Weise stellen.

KOBIL SecOVID generiert für jeden Zugriff ein neues Passwort. Bei KOBIL Smart Key & KOBIL Smart Token muss jeder, der rein will, zertifiziert sein. Mit KOBIL Trust erstellen und verwalten Sie eigenständig digitale Zertifikate. Neugierig auf mehr Details? Die erfahren Sie auf den kommenden Seiten.

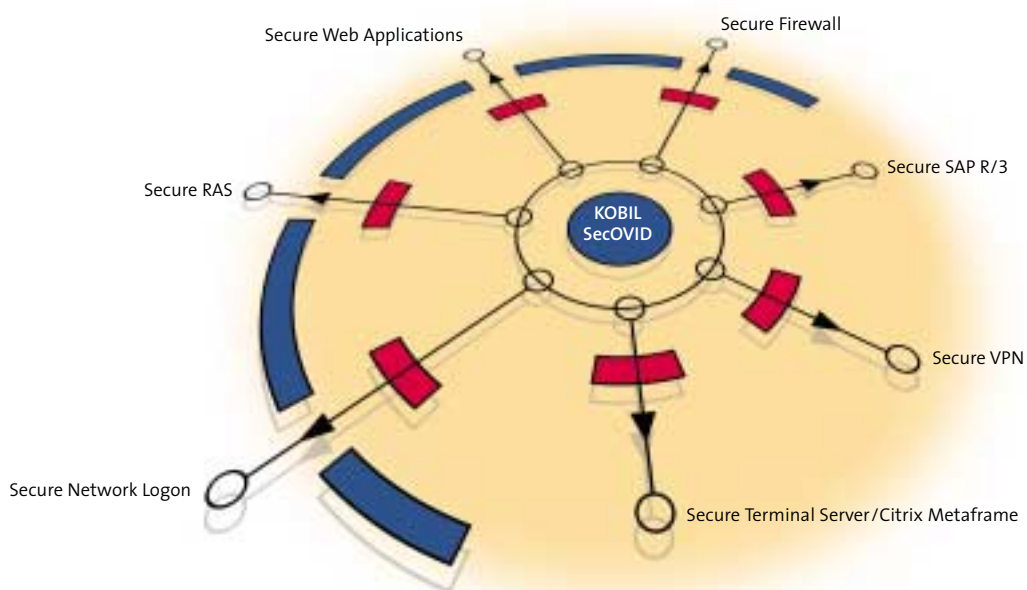
Die Lösung:

Einmalpasswort und digitale Zertifikate

- Starke Zwei-Faktor-Authentifikation durch Wissen und Besitz



Wenn die Sicherheit gegen unendlich geht



KOBIL SecOVID bietet sichere Authentifikation in vielen Einsatzbereichen.

KOBIL SecOVID gibt Eindringlingen keine Chance.
Für die Authentifikation gibt es zunächst zwei Voraussetzungen: Man muss die PIN kennen. Und man muss das richtige Token oder die passende Smart Card besitzen. Praktisch bis ins Unendliche steigt die Sicherheit des Verfahrens dann aber durch das Einmalpasswort – es wird mit jedem Zugriffsversuch vom System neu erzeugt. Schlechte Aussichten für schlechte Absichten.

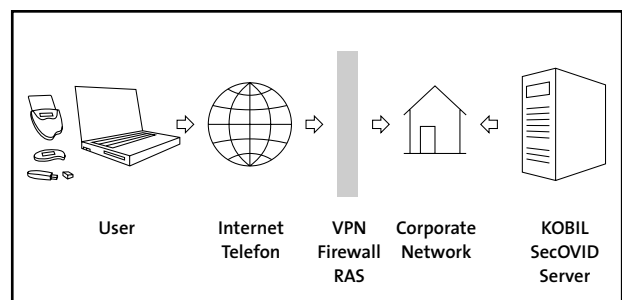
Mehr Sicherheit, weniger Aufwand

Überall dort, wo statische Passwörter verwendet werden, ist KOBIL SecOVID sicherer. Denn das Hauptelement der Lösung ist das Einmalpasswort – und das kann weder erraten noch ausspioniert werden. Die Gesamtlösung besteht aus zwei Hauptkomponenten. Auf der Benutzerseite benötigt der Zugangsberechtigte zur Authentifikation neben seiner PIN nur das SecOVID Token – ein Gerät in Größe eines Schlüsselanhängers. Alternativ lässt sich eine Smart Card verwenden, die vom portablen SecOVID Reader Plus ausgelesen wird. Die SecOVID Software und das Administrationstool werden auf einem Server innerhalb des jeweiligen Unternehmensnetzwerks installiert.

Wie erfolgt die Authentifikation?

Der Benutzer gibt sein Einmalpasswort ein. VPN, Firewall oder RAS leiten es verschlüsselt an den SecOVID Server weiter. Dieser prüft die Anfrage. Ist das Einmalpasswort korrekt, erhält der Benutzer Netzwerkzugang – und zwar nur dann.

Wie kann der SecOVID Server das übermittelte Einmalpasswort verifizieren? Beide Seiten – SecOVID Server auf der einen und Token oder Smart Card auf der anderen – verwenden einen Algorithmus und Ausgangswerte, die synchronisiert sind.



Starke Authentifikation mit KOBIL SecOVID

Die intelligente Antwort auf jeden unerlaubten Zugriff: Das Einmalpasswort-System KOBIL SecOVID

Hochverfügbar und stabil – in jeder Situation

Der SecOVID Server übernimmt die Überprüfung der Einmalpasswörter, die Verwaltung der Benutzerrechte und die Protokollierung der Zugriffsversuche. Das System ist hochredundant – die Verfügbarkeit in jeder Situation ist gewährleistet. Zugleich sorgen die Leistungsreserven dafür, dass die Sicherheit auch unter einem großen Ansturm von Authentifizierungsprozessen keinesfalls leidet.

Nahtlos integrierbar

Internationale Authentifikationsstandards wie RADIUS oder TACACS+ werden vom Server natürlich problemlos unterstützt. Was dazu beiträgt, dass sich KOBIL SecOVID in jede vorhandene Systemumgebung reibungslos einfügt.

Mit besonderen Anforderungen sind Sie bei KOBIL besonders gut aufgehoben: Kombinieren Sie bei Bedarf die Vorteile des Einmalpasswort-Systems mit den Vorteilen der zertifikatsbasierten Lösungen KOBIL Smart Key & KOBIL Smart Token.

- **Mehr Sicherheit**
Durch Zwei-Faktor-Authentifikation – Wissen (PIN) und Besitz (Token / Smart Card)
- **Dauerhafte Token-Nutzung**
Austauschbare Batterien verursachen keine Kosten für Austausch und Wiedereinführung neuer Token
- **Eventsynchrone Technologie**
Verhindert Probleme der serverseitigen Zeitsynchronisierung und das Warten auf zeitbasierte Passwörter
- **Reibungslose Integration**
Durch Unterstützung internationaler Standards wie RADIUS oder TACACS+
- **Starke Performance**
Tausende von Authentifizierungen können gleichzeitig durchgeführt werden

- **Einfache Administration**
Einfache Verwaltung von Benutzerdaten über graphische Benutzeroberfläche oder textbasiertes Kommandozeilentool
- **Hohe Kosteneffizienz**
Ein ausgezeichnetes Preis-Leistungs-Verhältnis sorgt für neues Wertschöpfungspotenzial beim Schutz von Netzwerkressourcen
- **Uneingeschränkte Skalierbarkeit**
Die Lösung hält problemlos mit dem Wachstum und den Veränderungen Ihres Unternehmens Schritt
- **Mobilität**
Der Benutzer hat jederzeit und überall Zugriff auf die gewünschten Ressourcen

KOBIL Smart Key:
hier in der Alternative mit
KAAN Professional für die sichere
PIN-Eingabe über Tastatur ...

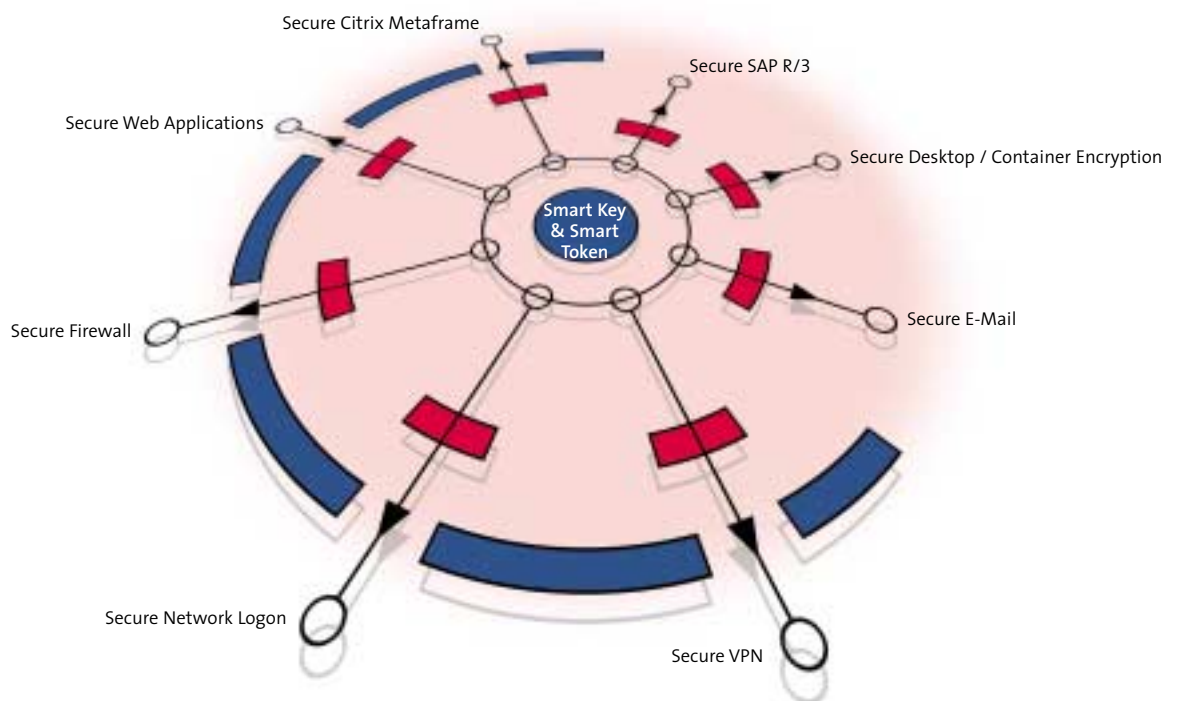


... und mit KOBIL PCMCIA B1
für den Einsatz im Notebook



KOBIL Smart Token

Der absolute Ausschluss der Öffentlichkeit



Die vielfältigen Einsatzmöglichkeiten von
KOBIL Smart Key & KOBIL Smart Token

Mit digitalem Zertifikat und privatem Schlüssel ermöglichen die Lösungen KOBIL Smart Key und KOBIL Smart Token eine starke Authentifikation und Datensicherheit. Für die verschiedensten Anwendungen. Der private Schlüssel zur Authentifikation des Zugangsberechtigten wird auf einer Smart Card gespeichert. Und ist fest an diese gebunden.

Vielseitig und unkompliziert einsetzbar

Der private Schlüssel fungiert bei KOBIL Smart Key und KOBIL Smart Token als digitale Identität. Gespeichert ist er im Kartenchip einer Smart Card. Ohne den Besitz der Smart Card und die Kenntnis des PIN Codes lässt sich dieser private Schlüssel nicht nutzen.

Zusammen bilden diese zwei Faktoren eine unüberwindliche Hürde – zum Schutz unterschiedlichster Applikationen. Neben dem Remote Access kann man das Windows Domain Logon im LAN sichern – alles auf Basis der Smart Card. Ebenso unkompliziert ist die Verschlüsselung und Signatur von E-Mails und Dateien.

Das KOBIL Smart Token ist Lesegerät und Smart Card in einem. Und damit gezielt für Mobilität ausgelegt. Schön wirtschaftlich ist es auch, denn die Smart Card im SIM Format lässt sich leicht austauschen oder personalisieren. Was eine längere Nutzungsdauer des Geräts erlaubt.

Wie erfolgt die Authentifikation?

Der Zugriff erfolgt per Smart Card mit privatem Schlüssel und Zertifikat über Smart Card Terminals oder USB Token. VPN oder Firewall reagieren auf einen Zugriffsversuch mit einer Challenge in Form einer zufälligen Zahlenfolge. Beim User wird die Challenge mit dem privaten Schlüssel signiert und zusammen mit dem Zertifikat zu VPN oder Firewall zwecks Prüfung zurückgeschickt. Befugte Benutzer erhalten Zugang zu den Netzwerkressourcen.

Die Vorteile der zertifikatsbasierten Lösungen KOBIL Smart Key und KOBIL Smart Token können Sie mit den Vorteilen des Einmalpasswort-Systems KOBIL SecOVID kombinieren. Problemlos mit nur einem Hardware-Element realisierbar – ideal für Ihre Anforderungen.

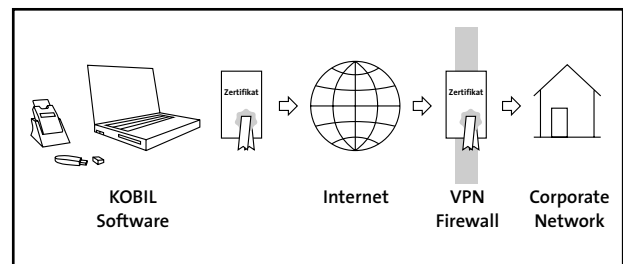
Hochsichere Schlüssel für Ihre digitale Identität: KOBIL Smart Key & KOBIL Smart Token

Die Festplatte kann nichts verraten

Mit KOBIL Smart Key und KOBIL Smart Token können Sie sowohl Ihre Dateien verschlüsseln als auch mit der Container Verschlüsselung eine bestimmte Laufwerkspartition inklusive aller darin gespeicherten Dateien schützen. Pro Session ist nur eine einmalige Authentifikation notwendig, was den Komfort der Lösung noch steigert. Schneller und einfacher geht Sicherheit nicht. Kommt dann – etwa auf Reisen – das Notebook abhanden, dürfen Sie ganz gelassen bleiben. Ohne Smart Card und PIN lässt sich nicht auf verschlüsselte Daten zugreifen.

Variabilität bei den Hardware-Komponenten

Der Unterschied zwischen KOBIL Smart Key und KOBIL Smart Token liegt vor allem in den Hardware-Komponenten. KOBIL Smart Key bietet Variabilität bei den Smart Card Terminals – optimiert für Ihren Bedarf. Für den PCMCIA Slot von Notebooks gibt es einen passenden Leser. Bevorzugen Sie ein externes Smart Card Terminal können Sie zwischen Ausführungen ohne Tastatur und – für eine noch sicherere PIN Eingabe – mit Tastatur wählen.



Starke Authentifikation mit KOBIL Smart Key & KOBIL Smart Token

• Mehr Sicherheit

Durch Zwei-Faktor-Authentifikation – über Wissen (PIN) und Besitz (Smart Card)

• **Container Verschlüsselung**
Schützt individuell bestimmte Laufwerkspartitionen und bietet neben Gruppenverwaltung und Netzwerkfähigkeit eine optimale Integration in die Windows Plattform

• **Einfache Integration**
Unterstützt internationale Kryptografie Standards wie MS CAPI oder PKCS#11

• Out-of-the-box-Lösung

Standardisierte Plug-and-play-Software

• Höchste Sicherheit

Keine privaten Schlüssel mehr auf der Festplatte oder im Browser gespeichert

• Einfache Handhabung

Schnelle Installation und intuitive Benutzerführung

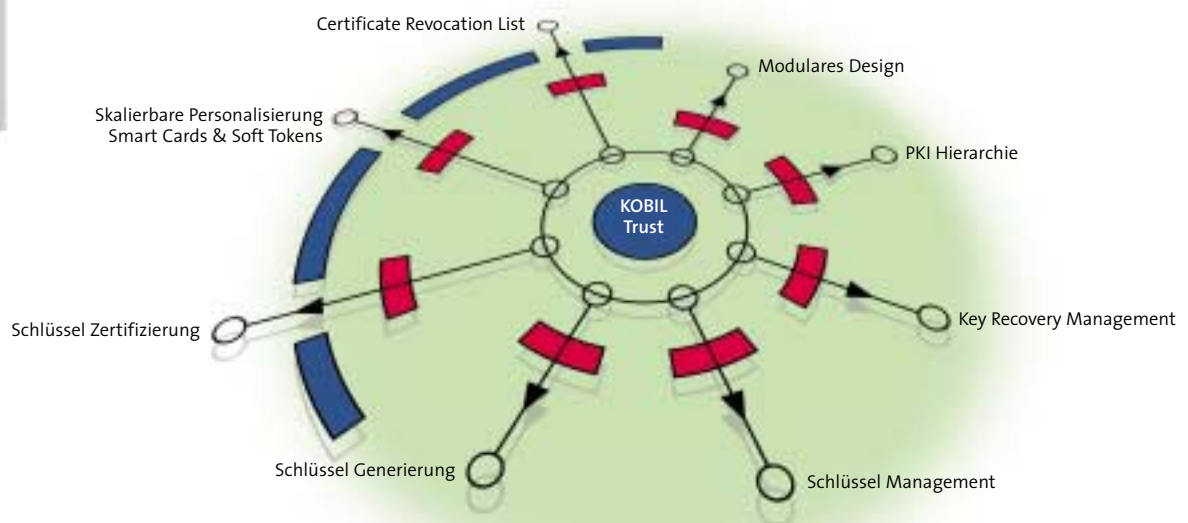
• Flexibilität

Mehrere private Schlüssel und digitale Zertifikate für unterschiedliche Applikationen auf einer Smart Card möglich

KOBIL Trust zur Ausgabe, Verwaltung,
Verifizierung und Zertifizierung
digitaler Schlüssel



Dass Sie sind, wer Sie sind, ist zertifiziert



KOBIL Trust bietet umfangreiche Features
zur Sicherung Ihrer digitalen Identität.

Auf der Benutzenseite ermöglichen KOBIL Smart Key und KOBIL Smart Token zertifikatsbasierte Applikationen. Die perfekte Ergänzung finden Sie ebenfalls bei uns – KOBIL Trust. Mit dieser umfassenden Trustcenter Software-Lösung schaffen Sie eine leicht integrierbare unternehmenseigene Public Key Infrastructure – zur Ausgabe, Verwaltung und Verifizierung digitaler Zertifikate. Alles aus einer Hand.

Maximal flexibel – offen für die Zukunft

KOBIL Trust setzt sich aus drei Hauptkomponenten zusammen, die den Workflow optimal ergänzen – KOBIL Trust RA, KOBIL Trust CA und KOBIL Trust IS. Mit konsequent objektorientiertem Design ist KOBIL Trust offen für zukünftige Entwicklungen und unterstützt alle gängigen Standards und Schnittstellen. Das Konzept bietet zahlreiche Möglichkeiten: von der einfachen Out-of-the-box-Lösung bis hin zu einer individuell angepassten Corporate PKI.

Ihr virtueller Notar: KOBIL Trust RA

KOBIL Trust RA ist das Eingangsportal von KOBIL Trust.

Behält die Übersicht: KOBIL Trust IS

KOBIL Trust IS verwaltet Ihre PKI. Es veröffentlicht die Zertifikate in einem Verzeichnisdienst, liefert sie aus und archiviert sie. Für die Verlängerung der Zertifikate sorgt KOBIL Trust IS genauso wie gegebenenfalls für deren Sperrung. In Verbindung damit aktualisiert es die Sperrlisten regelmäßig. Optional lässt sich eine Key-Recovery-Funktion einrichten, mit der Benutzer private Schlüssel sicher verwahren und wiederherstellen können.

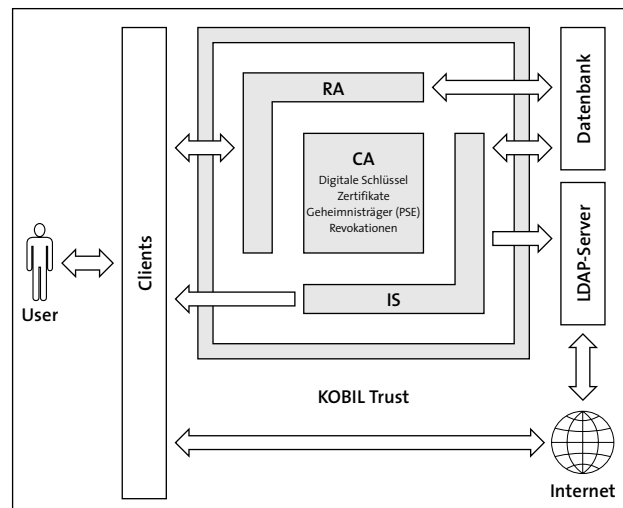
- **Hohe Skalierbarkeit**
Von kleineren Out-of-the-box-PKI-Lösungen bis zur großen, individuellen Corporate PKI
- **Flexibilität**
Die modulare KOBIL Trust Architektur wächst mit – und lässt sich immer wieder den wechselnden Anforderungen des Unternehmens anpassen
- **Optimale Bedienungs-freundlichkeit**
Schnell implementierbar, intuitive Benutzerführung
- **Integrierbarkeit**
Genügt den Anforderungen unterschiedlichster Sicherheitsrichtlinien
- **Maximale Interoperabilität**
Basiert auf offenen, internationalen Standards (z.B. X.509 v3) und Protokollen und unterstützt verschiedenste Unternehmensapplikationen
- **Personalisierung**
Frei konfigurierbare Module mit direkten Schnittstellen zur Chipkarten-Personalisierung

Ihre firmeneigene Identitätsvergabe: KOBIL Trust

Als PKI-Registrierungsinstanz sammelt und verwaltet es Zertifizierungs- und Revokationsanträge, prüft und korrigiert die Antragsdaten gemäß Ihrer Policy. Zertifikatsanträge können in einem Registrierungsbüro, über einen Webbrowser, aus vorhandenen Datenbank-einträgen oder PKCS#10-Anträgen generiert und an KOBIL Trust CA verschickt werden.

Vertrauen in digitaler Form: KOBIL Trust CA

KOBIL Trust CA stellt alle Funktionen einer Zertifizierungsinstanz bereit. Indem es entsprechende PKI-Schlüssel, X.509-Zertifikate, personalisierte Geheimnisträger (PSE) und Sperrlisten generiert. Die frei konfigurierbaren Module von KOBIL Trust CA besitzen Schnittstellen zur skalierbaren Personalisierung von Chipkarten.

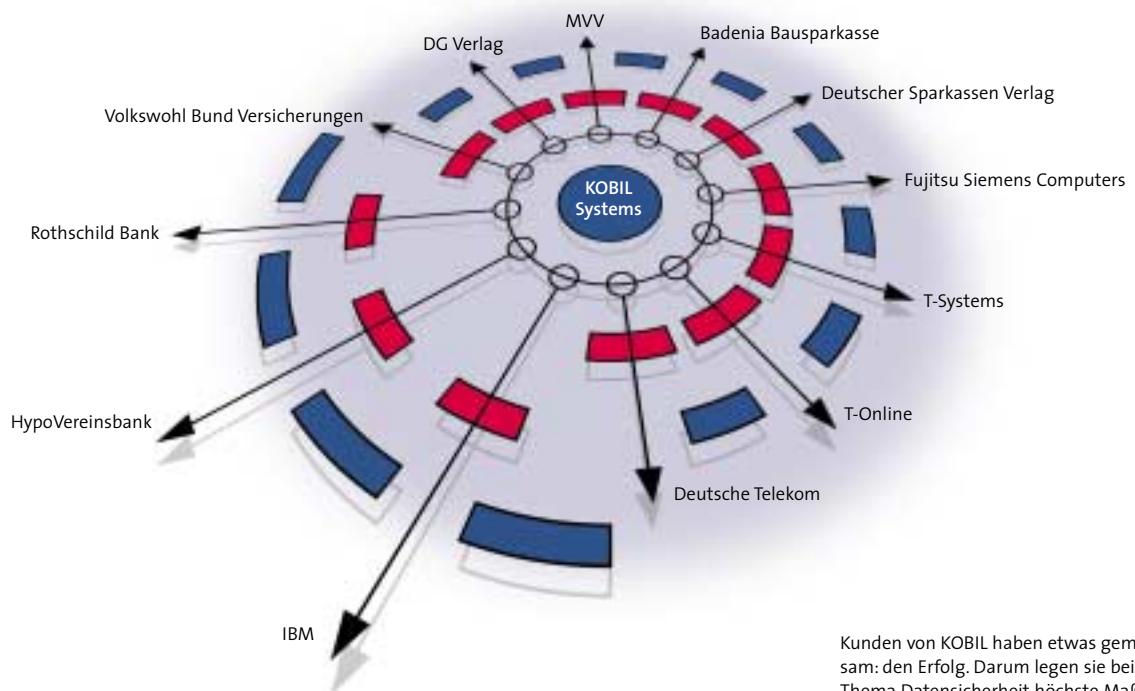


Die Architektur von KOBIL Trust



Ihr Eintritt in die Welt des Secure Remote Access – hochsichere Authentifikationslösungen von KOBIL. Dank starker Zwei-Faktor-Authentifikation über Wissen und Besitz. So sieht die einzig wahre Lösung aus!

Warum Microsoft und SAP uns als Partner wählen



Kunden von KOBIL haben etwas gemeinsam: den Erfolg. Darum legen sie beim Thema Datensicherheit höchste Maßstäbe an. Was die Zuverlässigkeit und praktische Handhabung der verwendeten Lösungen angeht genauso wie in Hinsicht auf die wirtschaftliche Effizienz.

Ob Einmalpasswort oder zertifikatsbasierte Lösung: In beiden Fällen geht es um intelligente Technologie im Kampf gegen den Datenmissbrauch. Damit Sie diesen Kampf gewinnen, steht KOBIL mit einem integrierten Lösungsportfolio an Ihrer Seite. Wie es auf diesem Gebiet eben nur einem Spezialisten möglich ist. Und natürlich entwickeln wir fleißig weiter – für Top-Kunden.

**KOBIL SecOVID:
Informationsbereitstellung über Portale**

Die Volkswahl Bund Versicherungen setzen auf die starke Authentifikation mit KOBIL SecOVID. Schließlich geht es beim Zugriff der Makler auf das versicherungseigene Web Portal um sensibelste Kundendaten – der Zugang erfolgt entweder direkt oder über das Meta Portal des VDG. Dr. Dieter Ackermann ist verantwortlicher Hauptabteilungsleiter Systementwicklung. Er zeigt sich beeindruckt: "Kompromisslose Sicherheit und einfachste Nutzbarkeit – unsere Makler können sich jetzt noch effizienter der Kundenbetreuung widmen." Aus den bislang 500 Usern werden daher Ende des Jahres 7.000, die mit KOBIL SecOVID tagtäglich beste Erfahrungen machen.

10.000 zufriedene PKI-Anwender

Die Koç-Bank (Türkei) – mit über 100 Niederlassungen eine der größten Banken in der Türkei – setzt auf KOBIL Smart Key für sichere Web-Authentifikation. Grund dafür ist die große Zufriedenheit der Firmenkunden der Koç-Bank, die die PKI-Lösung als Web-Authentifikation sowie zum Verschlüsseln von Daten und E-Mails nutzen. Um in Zukunft allen 60.000 Firmenkunden eine sichere Web-Authentifikation beim Online-Banking bieten zu können, will die Koç-Bank ihre Lizenzen dementsprechend erweitern.

Die Kunden erhalten ein "Smart-Banking-Set", bestehend aus dem Chipkarten-Terminal KAAN Standard Plus, einer PIN-geschützten Chipkarte und bereitgestellter Software. Bei einer Umfrage wurden die mit dem Smart-Banking-Set angebotenen Dienstleistungen mit gut oder sehr gut bewertet. "Mit KOBIL Smart Key haben wir das sicherste E-Banking in der Türkei und einen deutlichen technologischen Vorsprung vor den Mitbewerbern", erklärt Hishem Md. Laroussi, stellvertretender Geschäftsführer der Koç-Bank.

Vertrauen ist gut – Referenzen sind eindeutig

**KOBIL Smart Key & KOBIL Trust:
Einbindung mobiler Mitarbeiter**

"Wir haben nach einem hochsicheren System gesucht, das uns Flexibilität bietet – und genau das haben wir bekommen!" Volker Fierhauser ist Leiter des PC-Service-Zentrums der Bausparkasse Badenia AG. Sein Lob gilt KOBIL Smart Key und der Trustcenter-Software KOBIL Trust. Mehrere Hundert Außendienstmitarbeiter können sich jetzt von unterwegs sicher in das Unternehmensnetzwerk einwählen. Mit einer zertifikatsbasierten Authentifikation über ein VPN – und bei Bedarf direkt auf dem Notebook Daten verschlüsseln. Volker Fierhauser: "Alle Komponenten sind tief integriert. Wir verfügen damit heute über ein modernes und leistungsfähiges System zur VPN-Absicherung."



Das neue Headquarters in Worms, Deutschland

Ihr Weg zu KOBIL ist nicht weit

Der KOBIL Fachhändler hat eine Menge cleverer und smarter Ideen für die Optimierung Ihrer Netzwerksicherheit. Vertrauen Sie auf seine Kompetenz – und auf das KOBIL Portfolio. Sicher ist sicher.

Strategische Partnerschaften für starke Authentifikation und Datensicherheit

Microsoft

Von den Partnern Microsoft, T-Systems und KOBIL Systems wird die Lösung KOBIL Smart Key angeboten. Auf dem Markt ist das Produktbundle für starke Authentifikation und Datensicherheit unter der Bezeichnung T-TeleSec NetKey für Windows XP erhältlich. Neben der Software umfasst es ein Smart Card Terminal (KAAN Standard Plus mit USB-Anschluss) und eine (T-TeleSec NetKey E4) Smart Card. Das mitgelieferte T-TeleSec Standard Zertifikat mit Gültigkeit von einem Jahr lässt sich nach Bedarf verlängern. Ebenfalls möglich ist die Verwendung von Zertifikaten anderer Anbieter.

T-TeleSec

Der Produktbereich T-TeleSec gehört zur Deutschen Telekom AG. Unter dem eigenen Produktnamen OneTimePass bietet das Unternehmen die Einmalpasswort-Lösung KOBIL SecOVID an. Für die Nutzung brauchen Kunden auf ihrem Server keine Ressourcen bereitzuhalten, denn die Authentifikationssoftware wird ausschließlich beim zentralen T-TeleSec Trust Center installiert. Die hohen Absatzahlen zeigen den enormen Bedarf an mehr Sicherheit in der Datenkommunikation.

Unser Profil

- Gründung des Unternehmens 1986
- Headquarters in Worms, Deutschland
- Niederlassungen in Europa
- 60 Mitarbeiter
- Kernkompetenz: Smart Card basierte Security-Lösungen und Smart Card Terminals
- Enge Kooperation mit Wissenschaftlern aus dem Bereich der Kryptographie
- Entwicklungsteams in Deutschland und Zentral-europa
- 35 % der KOBIL Mitarbeiter im Bereich Forschung und Entwicklung tätig
- Produktionsstätten in Europa und Asien
- Kunden aus allen Bereichen, darunter Deutsche Telekom, Badenia Bausparkasse und HypoVereinsbank
- Zertifiziert gemäß DIN EN ISO 9001:2000

Unsere Technologie-Partner

- Cisco
- Citrix
- F-Secure
- Microsoft
- Nortel
- SAP
- Stonesoft
- T-TeleSec
- Deutsche Telekom
- Watchguard
- NCP
- Cherry

KOBIL – das integrierte Lösungsportfolio für starke Authentifikation und Datensicherheit



KOBIL SecOVID

Starke Authentifikation auf Basis von
Einmalpasswörtern

- Secure Firewall • Secure SAP R/3 • Secure VPN
- Secure Terminal Server/Citrix • Secure RAS
- Secure Web Applications • Secure Network Logon



KOBIL Smart Key & KOBIL Smart Token

Datensicherheit und starke Authentifikation auf Basis
digitaler Zertifikate

- Secure SAP R/3 • Secure E-Mail
- Secure Network Logon • Secure Web Applications
- Secure Firewall • Secure Citrix Metaframe
- Secure VPN • Secure Desktop/Container Encryption



KOBIL Trust

Trustcenter Software zum Management
digitaler Zertifikate

- Modulares Design • PKI Hierarchie
- Key Recovery Management • Schlüssel Management
- Schlüssel Generierung • Schlüssel Zertifizierung
- Certificate Revocation List
- Skalierbare Personalisierung Smart Cards &
Soft Tokens



KOBIL Smart Card Terminals

Basis für sichere E-Business Applikationen

- E-Business • E-Banking
- E-Government • E-Payment