

Public-Key-Technologie



HELP.BCSECDISI

Release 4.6C



Copyright

© Copyright 2001 SAP AG. Alle Rechte vorbehalten.

Weitergabe und Vervielfältigung dieser Publikation oder von Teilen daraus sind, zu welchem Zweck und in welcher Form auch immer, ohne die ausdrückliche schriftliche Genehmigung durch SAP AG nicht gestattet. In dieser Publikation enthaltene Informationen können ohne vorherige Ankündigung geändert werden.

Die von SAP AG oder deren Vertriebsfirmen angebotenen Software-Produkte können Software-Komponenten auch anderer Software-Hersteller enthalten.

Microsoft[®], WINDOWS[®], NT[®], EXCEL[®], Word[®], PowerPoint[®] und SQL Server[®] sind eingetragene Marken der Microsoft Corporation.

IBM[®], DB2[®], OS/2[®], DB2/6000[®], Parallel Sysplex[®], MVS/ESA[®], RS/6000[®], AIX[®], S/390[®], AS/400[®], OS/390[®] und OS/400[®] sind eingetragene Marken der IBM Corporation.

ORACLE[®] ist eine eingetragene Marke der ORACLE Corporation.

INFORMIX[®]-OnLine for SAP und Informix[®] Dynamic Server[™] sind eingetragene Marken der Informix Software Incorporated.

UNIX[®], X/Open[®], OSF/1[®] und Motif[®] sind eingetragene Marken der Open Group.

HTML, DHTML, XML, XHTML sind Marken oder eingetragene Marken des W3C[®], World Wide Web Consortium, Massachusetts Institute of Technology.

JAVA[®] ist eine eingetragene Marke der Sun Microsystems, Inc.

JAVASCRIPT[®] ist eine eingetragene Marke der Sun Microsystems, Inc., verwendet unter der Lizenz der von Netscape entwickelten und implementierten Technologie.

SAP, SAP Logo, R/2, RIVA, R/3, ABAP, SAP ArchiveLink, SAP Business Workflow, WebFlow, SAP EarlyWatch, BAPI, SAPPHIRE, Management Cockpit, mySAP.com Logo und mySAP.com sind Marken oder eingetragene Marken der SAP AG in Deutschland und vielen anderen Ländern weltweit. Alle anderen Produkte sind Marken oder eingetragene Marken der jeweiligen Firmen.

Symbole

Symbol	Bedeutung
	Achtung
	Beispiel
	Empfehlung
	Hinweis
	Syntax
	Tip

Inhalt

Public-Key-Technologie	5
Digitale Signatur	8
Ein digitales Dokument digital signieren	9
Eine digitale Signatur prüfen	11
Digitaler Umschlag	14
Einen digitalen Umschlag erstellen	15
Einen digitalen Umschlag	17
Persönliche Sicherheitsumgebung (Personal Security Environment) (PSE)	19
Das Public-Key-Zertifikat	20

Public-Key-Technologie

Dieser Abschnitt beschreibt die Grundprinzipien der Public-Key-Technologie, mit der in den SAP-Systemen die digitalen Signaturen und digitalen Umschläge erstellt werden.

Öffentlicher und privater Schlüssel

Eigenschaften öffentlicher und privater Schlüssel

Das Geheimnis der Public-Key-Technologie liegt in der Beziehung zwischen zwei Schlüsseln, dem öffentlichen und dem privaten. Die Person oder Komponente, die "signieren" will, besitzt diese beiden Schlüssel. Die beiden Schlüssel haben folgende Eigenschaften:

- Die Schlüssel sind Paare und gehören zusammen.
- Der private Schlüssel kann nicht aus dem öffentlichen Schlüssel abgeleitet werden.
- Wie der Name schon sagt, wird der öffentliche Schlüssel veröffentlicht. Der Besitzer der Schlüssel verteilt den öffentlichen Schlüssel nach Bedarf. Der Empfänger eines signierten Dokuments muß diesen Schlüssel kennen, um die digitale Signatur prüfen zu können. Um ein verschlüsseltes Dokument versenden zu können (digitaler Umschlag), muß der Absender außerdem den öffentlichen Schlüssel des Empfängers kennen.
- Der private Schlüssel muß geheimgehalten werden. Der Schlüsselbesitzer verwendet den privaten Schlüssel zum Generieren seiner digitalen Signatur sowie zum Entschlüsseln von Nachrichten, die mit einem digitalen Umschlag geschützt sind. Daher muß der Schlüsselbesitzer sicherstellen, daß **kein** Unbefugter auf den privaten Schlüssel zugreifen kann.



Nachfolgend wird der Schlüsselbesitzer als Unterzeichner und die zu unterzeichnende Information als Dokument bezeichnet.

Schlüssel generieren und zuweisen

Zum digitalen Signieren benötigt der Unterzeichner ein Schlüsselpaar. Eine zentrale Instanz, die Zertifizierungsinstanz (Certification Authority, CA), erzeugt diese Schlüssel und weist sie dem Besitzer zu. Die Zertifizierungsinstanz ist der zentralen Stelle vergleichbar, die die Personalausweise ausstellt. Diese Schlüssel "gehören" dem Besitzer und können zur Identifikation verwendet werden.



Alternativ zur zentralen Generierung der Schlüssel können Sie diese auch selbst generieren und dann Ihren öffentlichen Schlüssel zur Zertifizierung an die CA senden.

Verwendung einer digitalen Signatur

Ein Dokument signieren

Der Unterzeichner signiert ein Dokument, indem er mit seinem privaten Schlüssel eine digitale Signatur erstellt. Dieser Vorgang wird in [Ein digitales Dokument digital signieren \[Seite 9\]](#) beschrieben.

Public-Key-Technologie

Das Dokument wird zusammen mit der Unterschrift an den Empfänger weitergeleitet.

Eine digitale Signatur prüfen

Der Empfänger des Dokuments verwendet den öffentlichen Schlüssel des Unterzeichners, um die Unterschrift sowie die Integrität des Dokuments (die Unverändertheit des Dokuments seit der Unterzeichnung) zu prüfen. Eine Beschreibung dazu finden Sie in [Eine digitale Signatur prüfen \[Seite 11\]](#).

Einen digitalen Umschlag benutzen**Einen digitalen Umschlag erstellen**

Sie erstellen einen digitalen Umschlag, indem Sie das Dokument mit einem geheimen Nachrichtenschlüssel in einen sicheren "Umschlag" "verpacken". Der Empfänger der Nachricht muß den Schlüssel ebenfalls kennen, um die Nachricht entschlüsseln zu können. Daher verschlüsseln Sie den Nachrichtenschlüssel mit dem öffentlichen Schlüssel des Empfängers und versenden ihn zusammen mit dem Dokument. Siehe: [Einen digitalen Umschlag erstellen \[Seite 15\]](#).

Einen digitalen Umschlag "öffnen"

Der Empfänger des Dokuments entschlüsselt dann mit seinem privaten Schlüssel den geheimen Schlüssel, der zum Verschlüsseln des Dokuments verwendet wurde. Mit diesem geheimen Schlüssel kann er das Dokument entschlüsseln. Eine Beschreibung dazu finden Sie in [Einen digitalen Umschlag "öffnen" \[Seite 17\]](#).

Das Public-Key-Zertifikat

Noch stellen sich folgende Fragen: "Wie weiß man, wem welcher öffentliche Schlüssel gehört?" und "Wie erhält man den öffentlichen Schlüssel des Unterzeichners?"

Die Antworten liefert das Public-Key-Zertifikat.

Wie bereits erwähnt, braucht der Unterzeichner ein Schlüsselpaar. Ferner wurde die zentrale Instanz, die CA, genannt, die dem Besitzer die Schlüssel zuweist. Die CA weist diese Schlüssel zu, indem Sie ein digitales Zertifikat ausstellt. Dieses digitale Zertifikat enthält die Informationen, mit denen sichergestellt werden kann, daß der öffentliche Schlüssel dem genannten Unterzeichner gehört. Eine genaue Beschreibung finden Sie unter [Das Public-Key-Zertifikat \[Seite 20\]](#).

Der Unterzeichner verteilt seinen öffentlichen Schlüssel, indem er sein Public-Key-Zertifikat verteilt (z. B. direkt per E-Mail oder über die X.500-Verzeichnisdienste).

Mit den Informationen des Public-Key-Zertifikats (insbesondere welcher öffentliche Schlüssel und welcher Hash-Algorithmus zu verwenden sind) prüft der Empfänger die Signatur des signierten Dokuments. Der Empfänger weiß auch, daß dieser öffentliche Schlüssel diesem Absender gehört, da das Public-Key-Zertifikat auch von einer CA unterzeichnet wurde. (Der Empfänger sollte diese CA ebenfalls kennen und ihr vertrauen.) Der Empfänger kann auch die Gültigkeit der Unterschrift der CA überprüfen, da deren Unterschrift und öffentlicher Schlüssel ebenfalls in dem Public-Key-Zertifikat enthalten sind.

Weitere Informationen finden Sie unter:

- [Ein digitales Dokument digital signieren \[Seite 9\]](#)
- [Eine digitale Signatur prüfen \[Seite 11\]](#)

- [Einen digitalen Umschlag erstellen \[Seite 15\]](#)
- [Einen digitalen Umschlag "öffnen" \[Seite 17\]](#)
- [Das Public-Key-Zertifikat \[Seite 20\]](#)

Digitale Signatur

Definition

Die digitale Signatur hat für die Verarbeitung digitaler Daten dieselbe Funktion wie die handschriftliche Unterschrift für gedruckte Dokumente.

Verwendung

Mit der digitalen Signatur können Sie digitale Dokumente "unterschreiben". Digitale Signaturen identifizieren den "Unterzeichner" eines digitalen Dokuments eindeutig und schützen außerdem die Integrität des Dokuments. (Bei der Überprüfung der digitalen Signatur werden Änderungen in signierten Dokumenten entdeckt.)

Integration

Sie können digitale Signaturen in SAP-Systemen in Verbindung mit einem externen Sicherheitsprodukt verwenden oder ohne ein solches Produkt. Wenn Sie ein externes Sicherheitsprodukt in Verbindung mit dem SAP-System verwenden, können Sie nicht direkt im SAP-System verfügbare Funktionen nutzen wie [digitale Umschläge \[Seite 14\]](#) oder die Authentifizierung von Einzelpersonen über Smartcards.

Für bestimmte Anwendungsgebiete jedoch (z. B. die Schnittstelle SAP ArchiveLink Content Server HTTP), genügt die digitale Signatur allein ohne daß die zusätzlichen Funktionen eines externen Produkts benötigt werden. Daher liefern wir die [SAP Security Library \[Extern\]](#) (SAPSECULIB) mit dem SAP-System. Weitere Informationen erhalten Sie in der Dokumentation zur Anwendung, die die digitale Signatur verwendet.

Beispiel

Beispiele für die Verwendung digitaler Signaturen in SAP-Systemen finden Sie unter:

- [Digitale Signatur im QM \[Extern\]](#)
- [Verarbeitung von Herstelleranweisungen \[Extern\]](#) in Abschnitt [Rückmelden von Istdaten \[Extern\]](#)
- Schnittstelle SAP Content Server HTTP 4.5 im Abschnitt [secKey \[Extern\]](#)

Ein digitales Dokument digital signieren

Einsatzmöglichkeiten

Sie signieren ein digitales Dokument aus denselben Gründen, aus denen Sie normale Dokumente unterzeichnen. Aufgrund der Art und Weise, in der Sie eine digitale Signatur erstellen, können Sie außerdem die Integrität des Dokuments überprüfen. (Falls das Dokument nach der Unterzeichnung verändert wird, wird die Unterschriftenprüfung fehlschlagen, siehe [Eine digitale Signatur prüfen \[Seite 11\]](#).)

Hier einige mögliche Gründe für das digitale Signieren eines Dokuments:

- Um zu bestätigen, daß Sie das Dokument gelesen oder genehmigt haben (z. B. Genehmigen von Anfragen).
- Um sich gemäß der Bedingungen des Dokuments zu verpflichten (z. B. Abschließen nicht in gedruckter Form vorliegender Verträge oder Kaufen von Produkten über einen Online-Katalog).
- Um die Integrität der Daten zu schützen (z. B. Unterzeichnen von Archiven zu Auditing-Zwecken).

Voraussetzungen

Zur Erstellung digitaler Signaturen benötigen Sie ein Schlüsselpaar. Ein Schlüssel ist öffentlich, einer privat. Wie Sie diese Schlüssel erhalten, hängt von der Public-Key-Infrastruktur Ihres Unternehmens ab.

Außerdem benötigen Sie ein digitales Dokument, das unterzeichnet werden soll.

Ablauf

Als Endanwender geben Sie normalerweise nur an, daß Sie ein Dokument signieren wollen und das System erledigt alles Weitere.

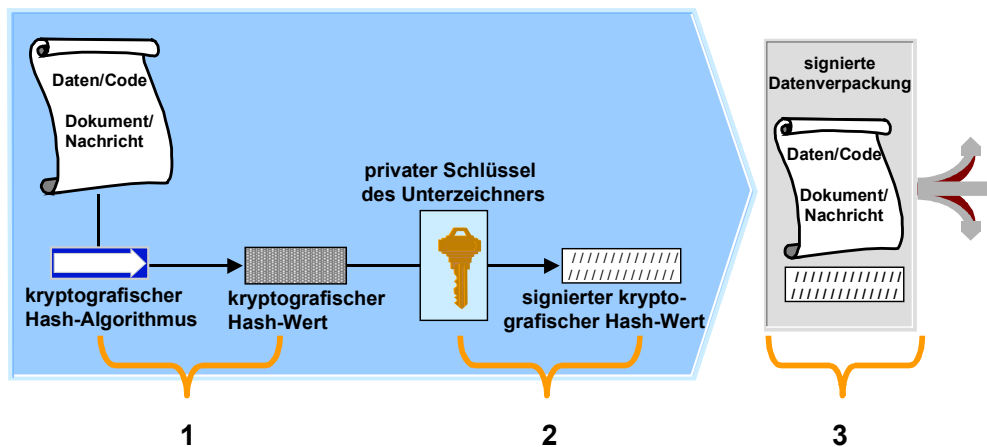


Dieser Schritt kann auch einen Teil eines Business Workflow enthalten, für den das System eine digitale Unterschrift fordert, bevor Sie fortfahren können. Sie müssen dem System ausdrücklich Zugriff auf Ihren privaten Schlüssel einräumen, beispielsweise über eine PIN oder eine Kennphrase, mit der das System auf die Smartcard oder Datei zugreifen kann, die Ihren geheimen Schlüssel enthält.

Folgende Grafik zeigt, was passiert, wenn Sie ein Dokument digital signieren.

Ein digitales Dokument digital signieren

Ein digitales Dokument digital signieren



Im folgenden wird jeder Schritt beschrieben:

1. Ein Hash-Algorithmus wird auf das Dokument bzw. die Nachricht angewandt, um für das Dokument einen kryptografischen Hash-Wert zu erstellen.
Der so erstellte kryptografische Hash-Wert ist ein eindeutiger Fingerabdruck des Dokuments. Mit einem kryptografischen Hash-Algorithmus sollte es nicht möglich sein, eine andere sinnvolle Eingabenachricht zu berechnen, die denselben kryptografischen Hash-Wert erzeugt.
2. Der private Schlüssel des Unterzeichners wird auf den kryptografischen Hash-Wert angewandt, um einen signierten kryptografischen Hash-Wert zu erzeugen.
3. Das Dokument (in Klartext) wird mit dem signierten kryptografischen Hash-Wert zu einem digital signierten Dokument zusammengepackt.

Ergebnis

Sie erhalten ein digital signiertes Dokument, das Sie genau wie jedes andere Dokument auch bearbeiten können (beispielsweise versenden, sichern oder archivieren.) Durch Prüfen der digitalen Signatur (siehe: [Eine digitale Signatur prüfen \[Seite 11\]](#)) können Sie dann beweisen, wer der Unterzeichner des Dokuments war und ob die Integrität des Dokuments noch gegeben ist.

Eine digitale Signatur prüfen

Einsatzmöglichkeiten

Sie könnten aus verschiedenen Gründen eine digitale Signatur prüfen wollen. Zum Beispiel:

- Sie haben ein digital signiertes Dokument erhalten und wollen die Identität des Absenders prüfen.
- Sie wollen die Integrität eines signierten Dokuments prüfen (z. B. beim Auditing von Archiven).

Voraussetzungen

Bevor Sie eine digitale Signatur prüfen können,

- benötigen Sie ein signiertes Dokument, das Sie prüfen wollen
- müssen Sie den Hash-Algorithmus kennen, den der Unterzeichner für seine Signatur verwendete.
- benötigen Sie Zugriff auf den öffentlichen Schlüssel des Unterzeichners.

Ablauf

Üblicherweise geben Sie nur an, daß Sie ein Dokument "prüfen" wollen und das System erledigt alles Weitere.

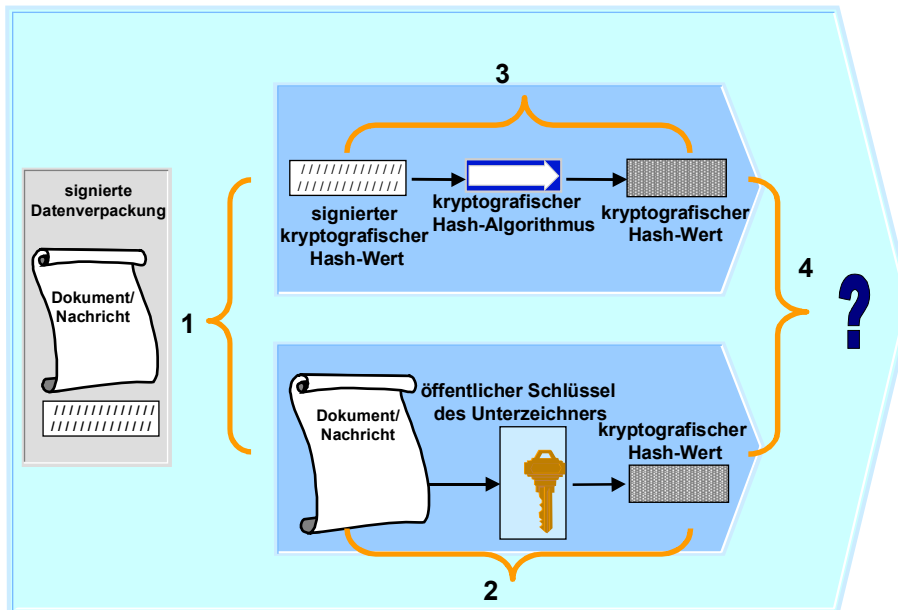


Dieser Schritt kann auch einen Teil eines automatischen Arbeitsablaufes enthalten, für den das System vor der Verarbeitung die Prüfung einer digitalen Signatur verlangt.

Folgende Grafik zeigt, was passiert, wenn Sie eine digitale Signatur prüfen:

Eine digitale Signatur prüfen

Eine digitale Signatur prüfen



Im folgenden wird jeder Schritt beschrieben:

1. Das digital signierte Dokument wird in seine Komponenten unterteilt: der signierte kryptografische Hash-Wert und das eigentliche Dokument.
2. Der öffentliche Schlüssel wird auf den signierten kryptografischen Hash-Wert angewandt.
Das Ergebnis ist der kryptografische Hash-Wert des Originaldokuments.
3. Dann wird derselbe Hash-Algorithmus auf das zu prüfende Dokument angewandt, der für den Signiervorgang verwendet wurde.
Das Ergebnis ist der kryptografische Hash-Wert des signierten Dokuments.
4. Die beiden kryptografischen Hash-Werte werden verglichen.

Ergebnis

Auf der Grundlage der folgenden Schlußfolgerungen wird die digitale Signatur entweder akzeptiert oder abgelehnt.

- Sind die kryptografischen Hash-Werte identisch,
 - ist der Unterzeichner der, den Sie erwartet haben (d. h. der Unterzeichner ist der Besitzer des privaten Schlüssels, der zu dem öffentlichen Schlüssel gehört, mit dem Sie die Signatur geprüft haben)
 - wurde das Dokument nach der Unterzeichnung nicht geändert
- Sind die kryptografischen Hash-Werte nicht identisch,
 - wurde das Dokument entweder verändert oder

Eine digitale Signatur prüfen

- der Unterzeichner ist nicht der, den Sie erwartet haben (d. h. die Nachricht wurde mit einem anderen als dem privaten Schlüssel unterzeichnet, der zu dem öffentlichen Schlüssel gehört, den Sie zur Prüfung verwendeten).

Digitaler Umschlag

Digitaler Umschlag

Definition

Ein digitaler Umschlag ist eine sichere "Datenverpackung", der die Vertraulichkeit des Datenpakets schützt. Er schützt den Inhalt des Datenpakets davor, von anderen als dem rechtmäßigen Empfänger eingesehen zu werden.

Verwendung

Digitale Umschläge können Sie zum Ablegen oder Versenden vertraulicher Daten verwenden.

Integration

Sie benötigen ein externes Sicherheitsprodukt in Verbindung mit dem SAP-System, um digitale Umschläge einsetzen zu können. Das Sicherheitsprodukt muß von SAP zertifiziert werden und das Standarddatenformat PKCS#7 sowie die Public-Key-Zertifikate X.509 unterstützen.

Einen digitalen Umschlag erstellen

Einsatzmöglichkeiten

Mit einem digitalen Umschlag schützen Sie ein digitales Dokument davor, von anderen als dem rechtmäßigen Empfänger eingesehen zu werden.

Hier einige mögliche Gründe für den Einsatz digitaler Umschläge:

- Versenden vertraulicher Daten oder Dokumente über (möglicherweise) unsichere Kommunikationsverbindungen.
- Ablegen vertraulicher Daten oder Dokumente (z. B. firmeninterne Berichte)

Voraussetzungen

Zum Erstellen eines digitalen Umschlags müssen Sie auf den öffentlichen Schlüssel des Empfängers zugreifen können. Wie Sie Zugriff auf den öffentlichen Schlüssel erhalten, hängt von der Public-Key-Infrastruktur Ihres Unternehmens ab.

Sie benötigen ebenfalls das zu schützende digitale Dokument.

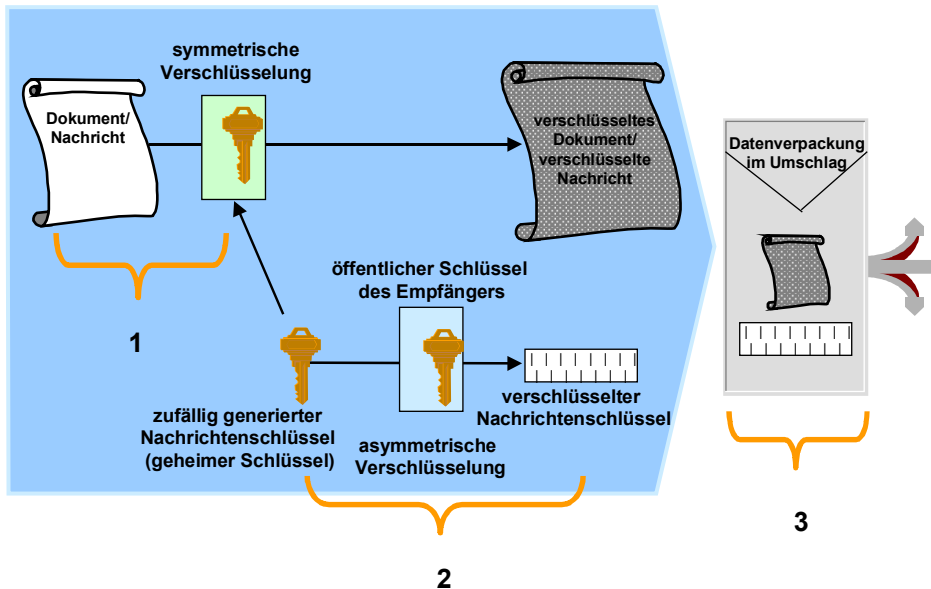
Ablauf

Als Endanwender geben Sie normalerweise nur an, daß Sie einen digitalen Umschlag für ein Dokument erstellen wollen und das System erledigt alles Weitere.

Folgende Grafik zeigt, was passiert, wenn Sie einen digitalen Umschlag erstellen.

Einen digitalen Umschlag erstellen

Einen digitalen Umschlag erstellen



Im folgenden wird jeder Schritt beschrieben:

- Die Nachricht wird mittels symmetrischer Verschlüsselung verschlüsselt. Normalerweise wird ein neuer zufällig generierter Nachrichtenschlüssel (geheimer Schlüssel) zur Verschlüsselung verwendet.

Symmetrische Verschlüsselung bedeutet, daß für die Ver- und Entschlüsselung derselbe (geheime) Schlüssel verwendet wird. Jeder, der die Nachricht entschlüsseln will, muß Zugriff auf diesen Schlüssel haben.
- Um die geheime Nachricht zwischen Sender und Empfänger zu übertragen, wird der geheime Schlüssel mit dem öffentlichen Schlüssel des Empfängers verschlüsselt.
- Das verschlüsselte Dokument wird zum Sichern oder zum Versenden an den rechtmäßigen Empfänger zusammen mit dem verschlüsselten Nachrichtenschlüssel in dasselbe Datenpaket gepackt.

Ergebnis

Sie erhalten ein gesichertes digitales Dokument, das nur der Besitzer des entsprechenden privaten Schlüssels einsehen kann (siehe [Einen digitalen Umschlag "öffnen" \[Seite 17\]](#)).

Einen digitalen Umschlag "öffnen" (entschlüsseln)

Einsatzmöglichkeiten

Sie "öffnen" einen digitalen Umschlag, wenn Sie der rechtmäßige Empfänger oder Betrachter eines digitalen Dokuments sind, das mit einem digitalen Umschlag gesichert wurde.

Voraussetzungen

- der zu öffnende digitale Umschlag
- Ihr privater Schlüssel

Ablauf

Als Endanwender geben Sie normalerweise nur an, daß Sie einen digitalen Umschlag öffnen wollen, und das System erledigt alles Weitere.

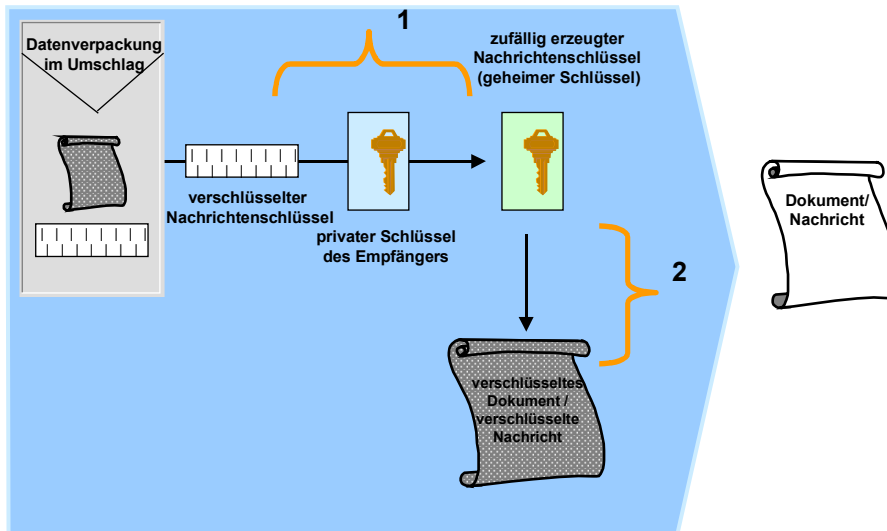


Dieser Schritt kann auch einen Teil eines Business Workflow enthalten, für den das System das Öffnen eines digitalen Umschlags fordert, bevor Sie fortfahren können. Sie müssen dem System ausdrücklich Zugriff auf Ihren privaten Schlüssel einräumen beispielsweise über eine PIN oder eine Kennphrase, mit der das System auf die Smartcard oder Datei zugreifen kann, die Ihren geheimen Schlüssel enthält.

Folgende Grafik zeigt, was passiert, wenn Sie einen digitalen Umschlag "öffnen".

Einen digitalen Umschlag "öffnen"

Einen digitalen Umschlag "öffnen" (entschlüsseln)



Im folgenden wird jeder Schritt beschrieben:

5. Der Empfänger wendet seinen privaten Schlüssel auf den verschlüsselten Nachrichtenschlüssel an.

Das Ergebnis ist der geheime Schlüssel, der ursprünglich zum Verschlüsseln des digitalen Dokuments benutzt wurde.

6. Der geheime Schlüssel, der im vorigen Schritt aufgefunden wurde, wird zum Entschlüsseln des digitalen Dokuments eingesetzt.

Ergebnis

Der rechtmäßige Empfänger (Eigentümer des entsprechenden privaten Schlüssels) kann den Inhalt des digitalen Dokuments einsehen.

Persönliche Sicherheitsumgebung (Personal Security Environment) (PSE)

Definition

Sicherer Ort, an dem die Public-Key-Informationen eines Benutzers oder einer Komponente abgelegt werden. Die PSE eines Benutzers oder einer Komponente befindet sich normalerweise in einem geschützten Verzeichnis im Dateisystem oder auf einer Smartcard. Sie enthält sowohl die öffentlichen Informationen (Public-Key-Zertifikat und privates Adreßbuch) als auch die privaten Informationen (privater Schlüssel) des Besitzers. Daher sollte nur der Besitzer der Informationen auf seine PSE Zugriff haben.



Beispielsweise legt die SAP Security Library (SAPSECULIB) die Informationen des Anwendungsservers in einer PSE ab. In diesem Fall enthält die PSE sowohl das [private Adreßbuch \[Extern\]](#) für das SAP-System als auch das [SSF-Profil \[Extern\]](#).

Verwendung

Die PSE des Benutzers oder der Komponente enthält die Informationen, die für das Erstellen und Prüfen digitaler Signaturen sowie zum Erstellen oder "Öffnen" digitaler Umschläge benötigt werden. Als Teil eines System-Workflow, wenn das System für einen Benutzer eine digitale Signatur erstellt, muß der Benutzer normalerweise dem System den Zugriff auf die Informationen in seiner PSE ausdrücklich gestatten. Er muß beispielsweise seine PIN (Personal Identification Number) oder Kennphrase eingeben, die die PSE schützt.

Struktur

Die exakte Struktur und der Inhalt der PSE wird durch das von Ihnen verwendete Produkt bestimmt. Normalerweise enthält die PSE das [Public-Key-Zertifikat \[Seite 20\]](#), das private Adreßbuch und den privaten Schlüssel des Benutzers.

Das Public-Key-Zertifikat

Das Public-Key-Zertifikat

Definition

Das Public-Key-Zertifikat fungiert als digitaler Ausweis, der eine Person oder Komponente identifiziert.

Verwendung

Sie verwenden Ihr Public-Key-Zertifikat, um sich gegenüber anderen zu identifizieren.

Sie können das Public-Key-Zertifikat eines anderen zur Prüfung von dessen digitaler Unterschrift benutzen.

Struktur

Das Public-Key-Zertifikat eines Unterzeichners enthält die für Sie zur Prüfung seiner digitalen Unterschrift notwendigen Informationen, insbesondere den öffentlichen Schlüssel und die Angabe des verwendeten Algorithmus. Darin sind auch Zusatzinformationen enthalten, so daß Sie wissen, daß dieser öffentliche Schlüssel tatsächlich zu der Person oder Komponente gehört.

Zur Ablage dieser Informationen gibt es verschiedene Formate; ein üblicher Standard ist das X.509-Zertifikat, das folgende Informationen enthält:

- **Allgemeine Informationen**
 - Version
 - Seriennummer
 - Gültigkeitsdauer
- **Information über den Zertifikatausteller**
 - Distinguished Name der CA
- **Informationen über den Zertifikatbesitzer**
 - Distinguished Name des Besitzers
 - öffentlicher Schlüssel des Besitzers
 - verwendeter asymmetrischer, kryptografischer Algorithmus
- **digitale Signatur der CA**
 - verwendeter asymmetrischer, kryptografischer Algorithmus
 - digitale Signatur der CA



Beachten Sie, daß die Signatur der CA auch in dem Public-Key-Zertifikat als zusätzliche (und notwendige) Maßnahme enthalten ist, um die Authentizität des Zertifikats, des öffentlichen Schlüssels und somit der digitalen Signatur nachzuweisen.