# Hierodiction Software

## Secure Key Manager (SKM)

## Verifier (VFY), Base System Security (BSS)

### Was ist Hierodiction SKM 2.0?

Hierodiction Secure Key Manager 2.0 bietet die sichere Bildung, Speicherung und Wiedergewinnung kryptographischer Schlüssel und besteht aus: (a) dem SKM Server, der als Web Service implementiert ist und (b) dem SKM Requestor als Client. Dieser enthält eine Reihe von Bibliotheksfunktionen, mit denen der SKM Server aufgerufen werden kann für die Integration in Ihre eigenen .net Applikationen. Zusätzlich umfasst der Requestor eine mächtige Krypto-Bibliothek, mit der Ihrer Applikationsentwicklung auch komplexe kryptographische Funktionen einfach zugänglich sind.

Der SKM Server bietet die folgenden Web-Dienste:

(a) RequestKey() bildet kryptographische Schlüsselpaare im Sicheren Key Server, wobei der öffentliche Schlüssel an den Requestor ausgegeben wird, der private Schlüssel bleibt unbekannt, da er nirgendwo gespeichert wird. Er wird gleichsam „vergessen“ und kann nur vom autorisierten Requestor wiederhergestellt werden. Sogar die vollständige Kontrolle über den Key Server erlaubt es nicht, die privaten Schlüssel auszulesen.

(b) ActivateKey() stellt die privaten Schlüssel wieder her und gibt sie an den Requestor aus.

Verifier (VFY):

Dies ist eine Erweiterung des SKM, die zusätzlich zum Wahlserver eine zweite digitale Signatur auf elektronische Wahlkarten aufbringt. Dies unterstützt die Wahlbeobachtung durch eine unabhängige Instanz.

### Nutzen

**Hohe Sicherheit:** Aufgrund der Tatsache, dass die Schlüssel als solche nirgends gespeichert werden, ermöglicht auch bei vollständiger Kontrolle über den SKM Server nicht das Auslesen der privaten Schlüssel.

**Flexibel:** Der SKM unterstützt derzeit Schlüssellängen zwischen 512 und 2048 bit. Zukünftige Upgrades werden auch Schlüssellängen darüber hinaus unterstützen. Die Länge jedes Schlüssels kann flexibel gewählt werden, womit der SKM auch problemlos inkrementelle Verschlüsselung in Teams unterstützt. Auch der Port, über den der SKM Web Service angesprochen wird, kann flexibel eingestellt werden.

**Plattformunabhängigkeit:** Schlüssel werden im Microsoft Crypto Provider oder in Java Big Integer Format unterstützt.

**Einfache Verwaltung:** Einfache Customizing-menüs zur Parametrierung von SKM Server und Requestor.

**Robust:** Wiederherstellungsprozedere im Notfall.

**Auditierbar:** Manipulationsgesichertes, verschlüsseltes Logging in Server und Requestor.

**Skalierbar:** AES 256 bit Verschlüsselung der SKM Serverdaten zur SAN-Unterstützung.

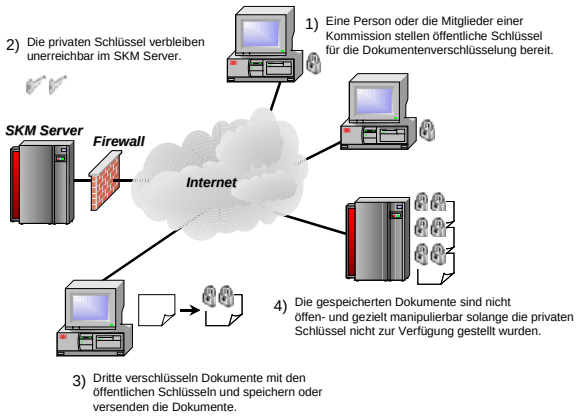
**Sichere Kommunikation:** 1024 bit RSA authentisierter und verschlüsselter Datenaustausch zwischen SKM Server und Requestor. Nur der ursprünglich den Schlüssel anfordernde Requestor kann seinen privaten Schlüssel wiedererlangen.

**Produktivität:** Der SKM ist mehr als nur ein Key Server. Der Requestor wird mit einer dokumentierten und mächtigen Kryptobibliothek geliefert, die Programmentwicklern ermöglicht, rasch stabile und sichere kryptographische Funktionen zu entwickeln. Die Funktionalitäten umfassen u.a. RSA für Verschlüsselung und Signatur, blinde Signatur, Zero-Knowledge Proof, AES, hexadezimale und Big Integer Umsetzung, Generierung/Verifikation zufälliger Primzahlen, SHA-1, Konvertierung zwischen Microsoft Crypto Provider und Java Big Integer, Formatkonvertierungen hex – Big Integer – String u.v.a.m.

Neben einer umfangreichen Dokumentation der Schnittstellen werden Beispiele für die Verwendung in Standard-Szenarios gegeben.

Kontakt: Hierodiction Software GmbH, Rabengasse 6, A-2230 Gänserndorf. http://www.hierodiction.at

## Applikationsszenario I: Dokumentenmanagement in Organisationen

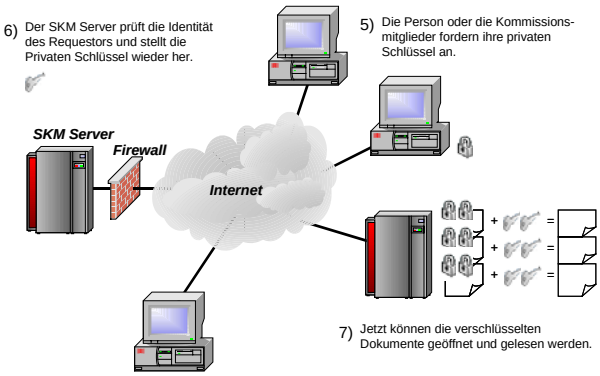



Dies ist ein Standardszenario in vielen Geschäftsprozessen in den Bereichen Öffentlicher Sektor, Banken und Rechtsinformatik. Als Beispiel dient im folgenden die elektronische Angebotsabgabe im öffentlichen Bereich (offenes Verfahren).

Die Mitglieder der Vergabekommission generieren Schlüsselpaare im SKM Server, wobei der öffentliche Schlüssel den Bietern zur Verschlüsselung der Angebote zur Verfügung gestellt wird. Die privaten Schlüssel verbleiben im SKM und können von niemandem außer dem jeweiligen Kommissionsmitglied ausgelesen werden (Schnitte 1 und 2).

Anmerkung: Die Verschlüsselung der Angebotsunterlagen und die sichere Verkettung von Beilagen mit SHA-1 kann einfach und rasch mit der Kryptobibliothek des Requestors entwickelt werden (Schritte 3 und 4).

Nach Ende der Frist für die Angebotsabgabe stellen die einzelnen Kommissionsmitglieder ihre privaten Schlüssel wieder her (Schritte 5 und 6), mit denen nun die Angebote geöffnet werden können (Schritt 7).




## Applikationsszenario II: Elektronische Stimmabgabe

Ein ähnliches Szenario wird für e-Voting eingesetzt:

Eines der wesentlichen Probleme eines jeden e-Voting-Systems ist die mögliche Manipulation der Stimmen durch die Administration der elektronischen Wahlurne. Eine anerkannte Sicherungsmaßnahme dagegen ist die Verschlüsselung der Stimmzettel mit den öffentlichen Schlüsseln der Wahlkommissionsmitglieder dezentral am PC des Wählers vor Absenden an die Wahlurne (Schritte 3 und 4).

Damit ist weder die Administration des Wahlsystems noch ein einzelnes Kommissionsmitglied in der Lage, die Stimmen vor der Zeit einzusehen oder diese zu manipulieren. Die privaten Schlüssel der Kommissionsmitglieder verblieben im SKM und nur das jeweilige Kommissionsmitglied kann die Wiederherstellung des Schlüssels verlagen. Nach Ende der Stimmabgabe tritt die Kommission zusammen und jedes Mitglied stellte seinen privaten Schlüssel aus dem SKM Server wieder her, worauf die Stimmen geöffnet und gezählt werden könnten (Schritte 5-7 oben).

## Mehrheitsentscheidungen

In beiden Szenarien ist die Abbildung von Mehrheitsentscheidungen möglich. So können beispielsweise 3 von 5 Mitgliedern der Kommission ein Dokument einsehen oder eine Wahlurne öffnen.

Das dabei ex ante definierte Mehrheitsquorum ist nachträglich nicht mehr änderbar und kann auch nicht (z.B. durch Ändern von Feldern in der Datenbank durch einen Administrator) manipuliert werden.

Kontakt: Hierodiction Software GmbH, Rabengasse 6, A-2230 Gänserndorf. http://www.hierodiction.at

## Der Verifier (VFY)

Ein wesentliches Problem bei e-Voting ist die Beobachtbarkeit des Wahlvorganges durch unabhängige Stellen. **EVOTE unterstützt unabhängige Wahlbeobachtung** durch zahlreiche Systemfunktionen. Unter anderem kann das elektronische Wahltoken (=der elektronische Stimmrechtsausweis), auf das hin die Wählenden ihre Stimme abgeben, mit einer zweiten digitalen Signatur versehen werden. Dies ist die Aufgabe des Verifiers.

**Dies ermöglicht es einer Kontrollinstanz die Arbeit des eigentlichen Wahlservers zu kontrollieren**, da am Ende der Wahl nur Stimmen vorhanden sein (und gezählt werden) dürfen, die mit einem Token verknüpft sind, das von dieser Kontrollinstanz signiert wurde.

Außerdem muss die Liste der Wählenden, für die die Kontrollinstanz einen solchen elektronischen Stimmrechtsausweis signiert hat, mit der entsprechenden Liste des Wahlservers vollkommen ident sein.

Diese Verifizierer-Funktionalität wurde in den SKM integriert, allerdings können aufgrund des modularen, Web-Service-basierten Konzepts aller Hierodiction-Systeme SKM und Verifizierer auch getrennt betrieben werden.

Die Möglichkeit zur unabhängigen Wahl-beobachtung schafft Vertrauen und Auditierbarkeit und sie erhöht die Kontrolle des elektronischen Wahlsystems durch die für eine Wahl politisch und rechtlich verantwortlichen Stellen.

## Base System Security (BSS)

„Ist das tatsächlich der Wahlserver?"

„Wurde während der Wahl die Softwarekonfiguration des Servers geändert?"

Fragen, die regelmäßig im Zusammenhang mit elektronischen Wahlen gestellt werden (und die vollkommen berechtigt sind!). Schließlich sind die Server eines Wahlsystem per se unbeobachtbar. Hier **Vertrauen** und Sicherheit zu schaffen, ist eine der wesentlichen Aufgaben im Bereich elektronischer Wahlen.

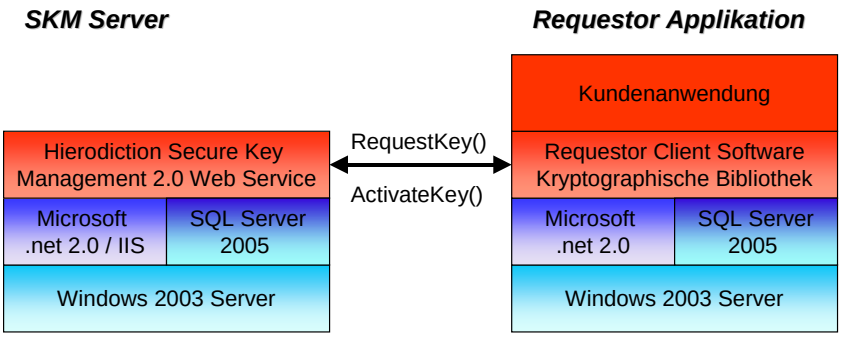
BSS bietet die Möglichkeit von einem sicheren Server aus, der nicht der Kontrolle der Systemadministration des Wahlsystems unterliegt, dieses zu überprüfen. Dabei wird **laufend die softwareseitige Integrität des Wahlsystems geprüft**. Manipulationen an den eingesetzten Systemen werden erkannt und gemeldet, worauf die unabhängige Kontrollinstanz entsprechende Maßnahmen einleiten kann.

Selbstverständlich kann auch eine SKM/VFY-Installation (bzw. jedes beliebige Drittprodukt) einer solchen Kontrolle unterzogen werden.

## Systemumgebung

Der SKM/VFY sowie der BSS Dienst basieren auf Industriestandards, die breite Unter-stützung von Providern haben und für die ausreichend qualifiziertes Personal zur Verfügung steht.

Aufgrund seiner Web-basierten Architektur passt sich der SKM-Service aber auch leicht in jede beliebige Applikationslandschaft an, solange der SOAP Standard für Web Services unterstützt wird. Die SKM Kryptobibliothek unterstützt darüber hinaus die einfache Konversion kryptographischer Schlüssel wie sie in Java verwendet werden, in die Formate der .net Welt und umgekehrt.






Kontakt: Hierodiction Software GmbH, Rabengasse 6, A-2230 Gänserndorf. http://www.hierodiction.at