

Product Report: Imprivata OneSign

Imprivata OneSign 4.0

Product Report

© Kuppinger Cole + Partner, Digital ID Analysis + Evaluation, 2007

Autor: Martin Kuppinger

Executive Summary

Imprivata OneSign ist eine auf einer Hardware-Appliance basierende Lösung für Enterprise Single Sign-On, die Mechanismen für die starke Authentifizierung und die Konvergenz zu physischen Zugangskontrollsystemen unterstützt. Durch den gewählten Appliance-Ansatz nimmt das Produkt eine Sonderstellung in diesem Marktsegment ein.

Das Produkt weist eine umfassende Funktionalität auf. Die Definition von Anwendungen für das Single Sign-On ist einfach möglich. Im Bereich der starken (und spezialisierten) Authentifizierung werden vielfältige Mechanismen unterstützt. Damit kann Imprivata OneSign auch in spezialisierten Einsatzfeldern wie Krankenhäusern genutzt werden. Zudem unterstützt das Produkt auch die Anforderung zusätzlicher starker Authentifizierungen für definierte Anwendungen oder Teilfunktionen von Anwendungen.

Die Appliance-Lösung macht die Einrichtung und Nutzung des Produkts sehr einfach. Das gilt auch für die einfach zu bedienenden grafischen Benutzerschnittstellen. In der Version 4.0 wurde das Management verteilter Appliances signifikant verbessert.

Im Vergleich mit den anderen Anbietern in diesem Marktsegment ist die Lösung von Imprivata als voll konkurrenzfähig einzuschätzen, auch wenn es einzelne Kritikpunkte gibt wie das weiterhin nicht optimale Konzept von Anwendungsrichtlinien. Dennoch zählen wir Imprivata OneSign zu den führenden Lösungen im Segment der Enterprise Single Sign-On-Produkte.

Kernpunkte der Analyse

Breite Unterstützung der Konvergenz mit physischen Zugangskontrollsystemen.	Unterstützung mehrerer Konten in einer Anwendung pro Benutzer.
Integrierte Failover, Auslieferung der Appliance nur paarweise.	Spezialisierte Modi für Kiosk- und Mehrbenutzer-Umgebungen.
⌘ Unterstützung nur von Windows-Clients.	Breite Zahl an vordefinierten Reports und konfigurierbare anwendungsspezifische Reports.
Breite Unterstützung von Authentifizierungsmechanismen, auch situative Nutzung.	Stark verbesserte Management-Funktionen.
Unterstützung von Windows Vista, auch in der 64-Bit-Version	⌘ Informationen aus dem Active Directory und anderen Systemen müssen synchronisiert werden.
⌘ GINA-Erweiterung für Windows 2000 und Windows XP erforderlich.	Hohe Systemsicherheit durch Compliance-Ansatz.
Unterstützung auch von mobilen Benutzern.	Kein Repository mit vordefinierten Anwendungsprofilen.

Product Report: Imprivata OneSign

Keine Unterstützung von Anwendungsrichtlinien.

⌘ Relativ wenige (meist kleinere) Partner im D-A-CH-Raum, allerdings in steigender Zahl.

⌘ Eingeschränkte APIs.

Produktkategorie

Imprivata OneSign ist eine Hardware-Appliance, die im Marktsegment Enterprise Single Sign-On einzuordnen ist. Das Produkt unterstützt dabei integriert verschiedene Ansätze für die starke Authentifizierung.

Enterprise Single Sign-On (E-SSO) bezeichnet in der Definition von Kuppinger Cole + Partner (KCP) die Technologien, mit denen Single Sign-On für bestehende Anwendungen ohne Anpassung der Anwendungen, mit zentralem Management und zentraler Speicherung der Credentials (Authentifizierungsinformationen) realisiert wird. E-SSO ist davon gekennzeichnet, dass eine Client-Anwendung sich gegenüber einem E-SSO-Serversystem authentifiziert und damit Zugriff auf gespeicherte Credentials erhält. Beim Zugriff auf eine Anwendung, die eine Authentifizierung erfordert, wird dies von der Client-Anwendung erkannt. Diese holt die erforderlichen Credentials aus dem zentralen Credential-Speicher und übergibt sie transparent im Hintergrund an die Anwendung. Aus Sicht des Benutzers erfolgt damit ein Single Sign-On, auch wenn es auf der Ebene der Anwendungen kein echtes Single Sign-On gibt.

Wichtig für E-SSO-Lösungen sind Funktionen wie die zentrale Steuerung der Richtlinien, die Erkennung auch von Anforderungen für die Änderung von Kennwörtern und eine breite Unterstützung von Anwendungen mit einfachen Werkzeugen für die Definition der Authentifizierungsdialoge.

Neben dem E-SSO-Segment gibt es im Bereich des Single Sign-Ons noch verschiedene andere Ansätze. Diese sind im *Single Sign-On Report 2008* von Kuppinger Cole + Partner (Januar 2008) beschrieben.

E-SSO hat aus Sicht von KCP den Vorteil, dass die Lösungen mit einer hohen Abdeckung von bestehenden Anwendungen in relativ kurzer Zeit zu implementieren sind, da sie eben keine Eingriffe in die Anwendung erfordern. Es handelt sich aber um kein echtes Single Sign-On. Dennoch werden diese „taktischen“ Lösungen schon aufgrund der hohen Zahl bestehender Anwendungen nach Einschätzung von Kuppinger Cole + Partner auch auf lange Sicht ihre Relevanz im Markt haben.

Produktbeschreibung

Im Gegensatz zu den anderen Produkten im E-SSO-Marktsegment ist Imprivata OneSign als Hardware-Appliance realisiert worden. Das Gerät wird grundsätzlich als Paar ausgeliefert, um einen Failover zu ermöglichen. Die technische Basis ist Novell SuSE Linux in Kombination mit einer Oracle-Datenbank. Imprivata hat in der Version 4 den Wechsel von MySQL zu Oracle aufgrund der höheren Leistungsfähigkeit und der granulareren Steuerung von Zugriffsberechtigungen für das erweiterte Sicherheitskonzept vollzogen. Allerdings sind das Betriebssystem und die Datenbank vollständig verborgen, da eine Administration ausschließlich über zwei web-basierende Schnittstellen erfolgt. Der einzige geöffnete Port des Systems ist auch der Port 443. Alle anderen Ports sind, wie ein Test ergab, geschlossen.

Die Funktionalität des Produkts lässt sich in drei Bereiche gliedern:

- Single Sign-On: Speicherung und Bereitstellung von Credentials für den Anwendungszugriff.

Product Report: Imprivata OneSign

- Integrierte Unterstützung für starke Authentifizierung: Mechanismen für die starke Authentifizierung von Benutzern werden integriert unterstützt. Damit lassen sich solche Lösungen einfach im Rahmen eines Single Sign-On-Projekts einführen.
- Integration mit physischen Zugangskontrollsystemen: Es gibt eine Integration mit physischen Zugangskontrollsystemen, um Ereignisse bei diesen Systemen wie den Zutritt zu einem Gebäude erkennen zu können. Diese Ereignisse können in Richtlinien mit anderen Ereignissen wie einer erfolgreichen starken Authentifizierung verknüpft werden. Die Zahl der unterstützten Ereignisse und der direkt unterstützten physischen Zugangskontrollsysteme wurden in der Version 4 erhöht.

Das generelle Konzept des Produkts sieht eine richtlinien-basierende Administration vor. Die Richtlinien werden zentral auf dem Server definiert und von dort verteilt. Gleiches gilt für die Beschreibungen der Anwendungen, die beim Single Sign-On unterstützt werden. Es gibt also eine vollständig zentrale Administration. Diese unterstützt ab der Version 4 nicht mehr nur das Management eines Paares von Appliances, sondern ein verteiltes Management-Konzept für alle Appliances im Netzwerk mit der Unterstützung für ein granulares Modell der delegierten Administration.

Imprivata hat sich bei der Implementierung des OneSign-Konzepts dafür entschieden, Benutzerinformationen lokal auf dem System zu verwalten. Entsprechend müssen die Benutzer auf dem System angelegt werden. Das kann einerseits durch die Synchronisation aus gängigen Verzeichnissen, darunter dem Microsoft Active Directory, und andererseits über SPML erfolgen. Über SPML kann grundsätzlich eine Anbindung an Provisioning-Systeme erfolgen. Diese Funktion ist positiv zu bewerten. Eine formale Unterstützung gibt es aktuell aber nur für die Provisioning-Systeme von Fischer International und Courion. Eine Integration mit weiteren Lösungen sollte aber keinen hohen Projektaufwand versuchen.

Im Vergleich mit anderen Lösungen im Bereich E-SSO fällt bei Imprivata OneSign insbesondere die Unterstützung der Konvergenz zu physischen Zugangskontrollsystemen, also die Kontrolle des Zugangs zu Gebäuden auf. Dabei handelt es sich aktuell um eine unidirektionale Unterstützung, bei der Imprivata OneSign Ereignisse von einigen solcher Systeme empfangen kann, aber keine Informationen an diese senden kann. Dennoch ergeben sich daraus in Verbindung mit den Richtlinien von Imprivata OneSign einige interessante Einsatzmöglichkeiten, auf die weiter unten noch eingegangen wird.

Single Sign-On

Die Kernfunktion des Produkts ist das Single Sign-On. Dazu muss auf den Client- und Administrations-Systemen der *OneSign Agent* installiert werden. Die Anwendungen werden in so genannten *application profiles* oder Anwendungsprofilen beschrieben. Diese Profile können mit dem *application profile generator (APG)* erzeugt werden. Dabei handelt es sich um eine Assistenten-basierte Web-Anwendung, mit der die Login-Schnittstellen von Anwendungen analysiert und in die von Imprivata OneSign benötigten Anwendungsprofile umgesetzt werden können.

Wenn ein Benutzer sich an einer durch ein solches Profil beschriebenen Anwendungen authentifiziert, arbeitet der OneSign Agent als Proxy, der die Credentials aus dem Speicher an diese Anwendung übergibt. Anwendungsprofile können gezielt für ausgewählte Benutzergruppen und Benutzer bereitgestellt werden.

Auf dem Client muss der Imprivata OneSign Agent eingerichtet werden. Das Deployment erfolgt über das Netzwerk, wobei für neue Benutzer ein Link in einer eMail geliefert wird. Alternativ kann das Deployment auch auf anderen Wegen erfolgen, da der Agent in Form einer MSI-

Product Report: Imprivata OneSign

Datei bereitgestellt wird. Der Agent kommuniziert mit dem Server und ist daher unter anderem über die verfügbaren Profile informiert.

Der Agent erfordert, durch die Integration auch mit starken Authentifizierungsmechanismen, zwingend eine erweiterte GINA (grafische Anmeldeschnittstelle in Windows-Systemen) bei Windows 2000 und Windows 2000. Das macht auch einen Neustart bei der Installation zwingend. Imprivata verweist aber darauf, dass mit einer Erweiterung der GINA gearbeitet wird, statt diese zu ersetzen. Die Standard-GINA bleibt damit unverändert auf dem System vorhanden. Hinzuweisen ist darauf, dass die Schwächen dieser Lösung im Konzept der GINA liegen und bei dem von Imprivata gewählten Ansatz nicht zu umgehen sind. Bei Windows Vista werden die neuen Konzepte der modularen Authentifizierung unterstützt.

Für Systeme, die im *Shared Workstation*- oder *Kiosk*-Modus betrieben werden, ist (bei Windows 2000 und Windows XP) eine eigene GINA erforderlich. Diese Modi sind wichtig, um spezielle Einsatzszenarien beispielsweise in Krankenhäusern mit wechselnden Benutzern an einem System zu unterstützen. In diesem Bereich profitiert Imprivata Single Sign-On auch von der engen Integration mit speziellen Authentifizierungsmechanismen wie Proximity-Cards.

Außerdem gibt es einen Agent für Citrix-Systeme, um die Imprivata-Lösung auch in Verbindung mit Terminalservern einsetzen zu können.

Derzeit gibt es noch keine Unterstützung für andere Client-Plattformen als Windows. Diese sind – trotz deren noch geringer Relevanz beim Client – auch nicht ohne grundlegende konzeptionelle Änderungen zu realisieren.

Der APG ist eine erfreulich einfach zu nutzende Anwendung. Anwendungsprofile können in einfacher Weise benutzerdefiniert erstellt werden, wobei auch die spezifischen Besonderheiten wie Dialoge für eine regelmäßige Kennwortänderung abgefangen werden können. Die Kennwortänderungen können von Imprivata OneSign automatisch durchgeführt werden.

Im Gegensatz zu vielen anderen Anbietern stellt Imprivata keine vordefinierten Anwendungsprofile bereit. Der Hersteller begründet das damit, dass die Neuerstellung erfahrungsgemäß einfacher als die Modifikation von Profilen ist. Diese Einschätzung wird von KCP in dieser Form nicht geteilt. Wir halten es für sinnvoll, dass man ein solches Repository bereitstellt und dem Kunden diese Entscheidung überlässt.

Trotz des gewählten Appliance-Ansatzes werden beim Single Sign-On auch mobile Benutzer unterstützt. Diese Einstellung kann in den Benutzerprofilen vorgenommen werden. Dabei ist auch die Lebensdauer des Caches konfigurierbar. Die Credentials werden auf dem lokalen System verschlüsselt gespeichert. Das lokale Caching ist für Benutzer von Notebooks, die nicht immer mit dem Unternehmensnetzwerk verbunden sind, unverzichtbar.

Positiv ist die Unterstützung von so genannten Shared Credentials zu bewerten. Dabei handelt es sich um Credentials, die von mehreren Anwendungen gemeinsam verwendet werden. Diese können über die Verwaltungsschnittstelle einfach konfiguriert werden.

Trotz der genannten Einschränkungen ist der Bereich Single Sign-On bei Imprivata OneSign insgesamt positiv zu bewerten. Je nach geplantem Einsatzbereich gibt es aber Kriterien, die einen Einsatz der Appliance ausschließen. Hier sind insbesondere heterogene Client-Plattformen sowie die eingeschränkte Unterstützung für mobile Benutzer zu nennen.

Starke Authentifizierung und Konvergenz

Die OneSign-Appliance wird mit einer integrierten Unterstützung für starke (und spezialisierte) Authentifizierungsmechanismen ausgeliefert. Benutzer können sich zwar weiterhin mit Benut-

Product Report: Imprivata OneSign

zername und Kennwort an ihren Windows-Clients authentifizieren. Alternativ wird aber eine Reihe weiterer Mechanismen unterstützt:

- Fingerabdruck-Leser
- Proximity-Cards, also Karten, die in der Nähe eines Lesegeräts sein müssen (RFID-basierend)
- XyLoc-Schlüsselkarten
- Smartcards und USB-Tokens mit digitalen Zertifikaten
- RSA SecurID-Tokens
- SafeWord ID Token
- Vasco Digipass Token

Damit ist eine große Bandbreite an Möglichkeiten gegeben. Der Vorteil der von Imprivata gewählten Integration dieser Mechanismen mit der Windows-Authentifizierung ist, dass Benutzer sich in jedem Fall nur einmal authentifizieren müssen. Eine gesonderte, zusätzliche Authentifizierung gegenüber Imprivata OneSign ist nicht erforderlich. Auf die Nachteile des Konzepts wurde bereits weiter oben eingegangen.

Mit dem *emergency access privilege* kann Benutzern auch durch die Bearbeitung von vorgegebenen Fragen der Zugang erlaubt werden, auch wenn sie ihr Kennwort vergessen oder ihren Token nicht verfügbar haben. Diese Fragen können zentral vorgegeben werden. Das System zeigt in diesem Bereich eine hohe Flexibilität auch in Bezug auf die Anzahl der angezeigten und zu beantwortenden Fragen. Außerdem kann die mehrmalige Nutzung dieser Funktion innerhalb eines Monats eingeschränkt werden.

Interessant ist, dass für definierte Bildschirme in Anwendungen – und damit auch ausgewählte Anwendungen insgesamt – eine stärkere Authentifizierung angefordert werden kann. Das ist insbesondere in sicherheitskritischen Umgebungen von Bedeutung.

Imprivata ermöglicht mit dem gewählten Modell im Bereich der Authentifizierung eine schnelle Umsetzung von Projekten, bei denen die Single Sign-On-Lösung gemeinsam mit einem Verfahren für die starke Authentifizierung eingeführt wird. Das ist aus Sicht von KCP positiv zu bewerten, da Single Sign-On-Lösungen dauerhaft nur in Verbindung mit starker Authentifizierung – und das bedeutet, in jedem Fall mit einem anderen Mechanismus als nur Kennwörtern – betrieben werden sollten.

Eine Schwachstelle ist nach Ansicht von KCP, dass es nicht möglich ist, für bestimmte Anwendungen spezifische Richtlinien zu konfigurieren, die ein bestimmtes Niveau der Authentifizierung voraussetzen. Richtlinien werden nur Benutzern oder Computern zugeordnet. Für einen Benutzer können zwar unterschiedliche Authentifizierungsverfahren freigegeben werden. Es ist aber weder möglich, bestimmte Kombinationen solcher Verfahren für eine Mehr-Faktor-Authentifizierung zu erzwingen noch das zu verwendende Verfahren in Abhängigkeit von Anwendungen zu konfigurieren. Allerdings ist anzumerken, dass solche Funktionen auch bei Mitbewerbern von Imprivata nicht die Regel sind.

Ein Alleinstellungsmerkmal von Imprivata OneSign ist die Unterstützung von physischen Zugangskontrollsystemen. Diese liefern Ereignisse dazu, ob ein Benutzer bereits bei einem solchen System authentifiziert ist. Abhängig davon kann ein Zugriff eines Benutzers blockiert werden.

Product Report: Imprivata OneSign

Diese grundsätzlich gute Idee erlaubt es beispielsweise, dass ein Benutzer nur auf Anwendungen zugreifen darf, wenn er sich auch in einem bestimmten Gebäude befindet. Sie hat aber zwei Schwachstellen:

- Auch hier fehlen Richtlinien in Abhängigkeit von Anwendungen, so dass man sensitive Anwendungen beispielsweise nur in einem bestimmten Gebäude nutzen darf, weniger kritische Applikationen dagegen beispielsweise auch bei einer Einwahl.
- Die Unterstützung ist derzeit nur unidirektional. Es ist also beispielsweise nicht möglich, durch das De-Provisioning eines Benutzers in Imprivata OneSign auch eine direkte Zugangssperre für einen Benutzer im physischen Zugangskontrollsystem zu erwirken.

Die Unterstützung von Systemen für die physische Zugangskontrolle wurde in der aktuellen Version deutlich ausgebaut. Außerdem gibt es eine standardisierte API für die Integration solcher Anwendungen.

Benutzerschnittstellen

Wie schon kurz angesprochen verfügt Imprivata OneSign über zwei Benutzerschnittstellen, neben dem nur wenig sichtbaren OneSign Agent. Über den *OneSign Administrator* erfolgt die Administration der eigentlichen OneSign-Funktionen. Mit dem *Appliance Administrator* können dagegen administrative Aufgaben auf der Ebene der Appliance selbst durchgeführt werden. Wie angesprochen handelt es sich bei beiden Schnittstellen um Web-Schnittstellen, die nur über SSL und den Port 443 genutzt werden können. Andere Ports sind – nach der Erstkonfiguration über Port 81 – nicht geöffnet.

Die Authentifizierung an den Administrationsschnittstellen kann über Kennwörter, Digipass-Tokens oder optional, nach Einrichtung des Single Sign-Ons, auch andere Authentifizierungsmechanismen gesichert werden.

Die Schnittstellen sind, wie auch der bereits angesprochen APG, einfach und intuitiv zu bedienen. Dementsprechend ist die Einrichtung des Produkts einfach. Bei der Administration wird nur eine englische Sprachversion unterstützt.

Positiv ist die bereits angesprochene Erweiterung der Administration auf mehrere Appliances und das umgesetzte Konzept einer granularen, delegierten Administration zu beurteilen.

Schnittstellen

Durch das Appliance-Konzept sind flexible Schnittstellen bei einem Produkt wie Imprivata OneSign von besonderer Bedeutung. Imprivata ist eine der ersten Anbieter, die SPML als „Konsument“ unterstützen, also SPML-Dokumente von Provisioning-Systemen empfangen können. Auch wenn sich die standardmäßige Unterstützung derzeit noch auf die kleineren Hersteller Fischer International und Courion beschränkt, ist dieser Ansatz doch positiv, weil er eine einfache Übernahme von Benutzerinformationen ermöglicht. SPML als Standardschnittstelle kann einfach auch von anderen Herstellern genutzt werden. Derzeit wird SPML v1.0 unterstützt.

Falls man mit Verzeichnisdiensten für das Benutzermanagement arbeiten möchte, gibt es einige standardisierte Schnittstellen, unter anderem zum Active Directory. Hier ist aber ein regelmäßiger Abgleich der Benutzerinformationen erforderlich. Diese Synchronisation erfolgt pro Verzeichnisdienst, so dass die Informationen in Imprivata OneSign faktisch eine Spiegelung darstellen. Das verursacht zwar einen etwas erhöhten Administrationsaufwand, ist in der Praxis aber durchaus handhabbar.

Product Report: Imprivata OneSign

Problematischer ist es, wenn Benutzer aus verschiedenen Quellen stammen. Allerdings wird hier immerhin ein manuelles Mapping über die Benutzerschnittstelle durchführbar, indem zwei oder mehr Benutzerkonten ausgewählt und miteinander verknüpft werden.

Eine interessante Schnittstelle ist die zu RADIUS (Remote Authentication Dial-In User Service). RADIUS kann für eine Authentifizierung von Remote-Benutzern an Imprivata OneSign genutzt werden. Zudem kann Imprivata OneSign aber auch als Proxy arbeiten und die Authentifizierung weiterleiten.

Eine Lücke ist bei dem Produkt allerdings die noch fehlende Unterstützung für Federation-Standards. Eine Authentifizierung über diese wäre insbesondere für die Zugangskontrolle von externen Benutzern über das Web und den Zugriff auf spezifische Anwendungen eine interessante Option. Derzeit hat im E-SSO-Markt allerdings nur Citrix eine solche Unterstützung realisiert.

Zudem sind auch andere Schnittstellen wie Web Services für die Einbindung in externe Administrationsanwendungen noch nicht vorhanden. Auch die Logs können noch nicht in einfacher Weise mit anderen, externen Applikationen für das Historien- oder Real Time-Monitoring verarbeitet werden.

Auditing

Im Bereich des Auditing kann Imprivata OneSign nicht überraschen. Die internen Auditing-Funktionen sind gut gelöst. Es gibt eine Reihe vordefinierter Reports, die genutzt werden können. Außerdem lassen sich auch anwendungsspezifische Reports erstellen. Interessant ist, dass auch Benachrichtigungen pro Anwendung definiert werden können, um Administratoren in kritischen Situationen direkt zu informieren.

Diese Audit-Reports sind aber eine rein interne Lösung. Sie können zwar in Form von CSV-Dateien exportiert werden. Es gibt aber keine externe Schnittstelle, um diese beispielsweise in Realtime-Monitoring-Lösungen integrieren zu können.

Partner-Infrastruktur

Nachdem sich mit NEC der bisher wichtigste Partner von Imprivata aus dem deutschen Markt zurück gezogen hat, ist das Unternehmen im D-A-CH-Raum nur über – zumindest in Bezug auf die Marktpräsenz – Partner vertreten. In der Schweiz und in Österreich gibt es aktuell jeweils nur einzelne Reseller. Positiv zu bewerten ist dagegen, dass das Unternehmen in allen Ländern mit Spezialisten aus dem Bereich der Sicherheit kooperiert. Zudem hat Imprivata aktuell mit dem Aufbau einer europäischen Präsenz begonnen.

Dennoch ist es aus unserer Sicht weiterhin zwingend, dass Imprivata in diesem Bereich deutlich mehr Partner gewinnt und auch mit eigenen Ressourcen insbesondere im Bereich der Professional Services präsent ist, um spezifische Anpassungen und Erweiterungen durchführen zu können. Imprivata befindet sich in diesem Prozess.

Die Sicht von Kuppinger Cole + Partner

Trotz einiger Kritikpunkte ist Imprivata OneSign ein nach Einschätzung von KCP sehr interessantes Produkt, das in Evaluationsprozesse im Bereich des Single Sign-On einbezogen werden sollte. Es gibt allerdings mit der fehlenden Unterstützung von Anwendungsprofilen einen Bereich, der einen Einsatz des Produkts ausschließen kann. Die wichtigsten Kritikpunkte sind hier:

Product Report: Imprivata OneSign

- Richtlinien werden nur für Benutzer und Computer, aber nicht für individuelle Anwendungen unterstützt. Wenn Anwendungen spezifische Anforderungen an eine starke Authentifizierung haben, kann dies nicht konfiguriert werden.
- Kein Repository mit vordefinierten Anwendungsprofilen.
- Keine externen Schnittstellen für das Auditing, Export nur manuell als CSV-Datei.

Neutral betrachten wir folgende Funktionen, die in bestimmten Situationen zu Problemen führen können:

- Nur Unterstützung von Windows-Clients, Windows 2000 und höher.
- Produkt erfordert bis Windows XP eine GINA-Erweiterung, für Windows Vista gibt es die Unterstützung eines Credential Providers.
- Die physische Konvergenz wird nur unidirektional und für eine relativ kleine Zahl an Systemen unterstützt.
- Informationen aus Verzeichnissen wie dem Active Directory müssen synchronisiert werden, statt online auf diese Verzeichnisse zuzugreifen.
- Die Partner-Infrastruktur im D-A-CH-Raum ist noch nicht ausreichend. Sie wird derzeit allerdings ausgebaut.

Positiv bewerten wir dagegen folgende Funktionen:

- Die generelle Unterstützung physischer Konvergenz wird positiv bewertet.
- Breite Unterstützung von Authentifizierungsmechanismen für starke Authentifizierung und spezielle Anforderungen beispielsweise im Mehrbenutzer-Betrieb und die daraus resultierende einfache Umsetzung von Projekten.
- Integriertes Failover, Auslieferung der Appliance nur im Paar.
- Hohe Systemsicherheit durch Appliance-Ansatz, keine offenen Angriffspunkte.
- Konfigurierbare Unterstützung mobiler Benutzer, Speicherung verschlüsselter Credentials auf den lokalen Systemen.
- Unterstützung von Kiosk-Modus und Mehrbenutzer-Modus (Shared workstation mode).
- Relativ große Zahl vordefinierter Reports, Möglichkeit zur Konfiguration anwendungsspezifischer Reports.
- Stark verbesserte Administrationsfunktionen.
- Unterstützung mehrerer Konten eines Benutzers für eine Anwendung.

In der Summe erhält das Produkt trotz der genannten Einschränkungen und Schwachstellen von KCP ein sehr positives Rating und wird zu den führenden Lösungen im Enterprise Single Sign-On-Markt gezählt. Das gilt insbesondere, weil die genannten Schwachstellen und neutral bewerteten Aspekte teilweise ohnehin bereits spezielle Funktionen darstellen, die bei anderen Produkten in diesem Marktsegment überhaupt nicht zu finden sind oder weil diese bei den Wettbewerbsprodukten in vielen Fällen und für die meisten Punkte nicht besser gelöst sind.

Zitieren von Informationen und Daten von Kuppinger Cole + Partner: In internen Dokumenten und Präsentationen dürfen einzelne Sätze und Abschnitte für die ausschließlich interne Kommunikation in Unternehmen ohne explizite Erlaubnis von Kuppinger Cole + Partner verwendet werden. Die Verwendung großer Abschnitte oder des vollständigen Dokuments setzt die vorherige schriftliche Zustimmung von Kuppinger Cole + Partner voraus und kann die Zahlung von Lizenzgebühren einschließen. Die externe Pub-

Product Report: Imprivata OneSign

likation von Dokumenten und Informationen von Kuppinger Cole + Partner in der Werbung, Pressemeldungen oder anderen Marketing-Materialien erfordert generell eine vorherige schriftliche Zustimmung von Kuppinger Cole + Partner. Ein Entwurf des entsprechenden Dokuments sollte vorgelegt werden. Kuppinger Cole + Partner behalten sich das Recht vor, die externe Verwendung aus jedwedem Grund zu untersagen. © Kuppinger Cole + Partner 2004-2007. Vervielfältigung verboten, falls nicht autorisiert. Für zusätzliche Kopien kontaktieren Sie bitte service@kuppingercole.de.