

Link: <https://www.computerwoche.de/a/avocent-erweitert-unterstuetzung-fuer-smartcard-und-cac-technologie,1887088>

User-Identifikation

## Avocent erweitert Unterstützung für SmartCard- und CAC-Technologie

Datum: 13.02.2009  
Autor(en):Uli Ries

Avocent erweitert den Support für die Benutzeridentifikation via SmartCard und Common Access Card (CAC). Avocents Management-Software DSView 3 sowie die DSR-Switch-Appliances unterstützen im Rechenzentrum ab sofort SmartCard/CAC-kompatible Leser.



Der SmartCard/CAC-kompatible KVM-Switch Avocent DSR8035 bietet 32 Ports, eine doppelte Stromversorgung und unterstützt einen lokalen und acht digitale User.

Foto: Avocent

**Avocent**<sup>1</sup> beschreibt dies als wichtigen Schritt um zu überwachen, wer Zugang zu welchen IT-Systemen und Daten besitzt. Die Identifikation via SmartCard/CAC sei auch zum Einhalten von **Compliance**<sup>2</sup>-Anforderungen wie der US-amerikanischen Heimschutzdirektive 12 nötig. Die **HSPD 12**<sup>3</sup> (Homeland Security Presidential Directive) schreibt Bundesstellen und ihren Auftragsnehmern aus Sicherheitsgründen einen einheitlichen Identifikationsprozess für Mitarbeiter vor.

Im Rechenzentrum werden SmartCard/CAC-kompatible Lesegeräte von Avocents Management-Software **DSView 3**<sup>4</sup> sowie den **DSR-Switch-Appliances**<sup>5</sup> unterstützt. Über die Zugangskarten lässt sich neben der reinen Überwachung von Zugriffen auch definieren, wer welche Rechte im Rechenzentrum hat und welchen Grad an Kontrolle diese Person ausüben darf. Wegen der Unterstützung im Rechenzentrum durch die Soft- und Hardware von Avocent sollen sich SmartCard/CAC-kompatible Lesegeräte auch entfernt vom Rechenzentrum aufstellen lassen, ohne die **Sicherheit**<sup>6</sup> der Datenverbindungen zu gefährden.

DSView 3 erlaubt den lokalen oder Fernzugriff auf **Server**<sup>7</sup> und Ausrüstung zur Beurteilung des Betriebszustands des Rechenzentrums. Über die Software kann die IT-Abteilung durch Fernzugriff Wartungsarbeiten am Betriebssystem und anderer Software ausführen sowie die Energiezufuhr kontrollieren und überwachen. Die Unterstützung von SmartCard/CAC-Lesegeräten ermöglicht die Standardisierung aller Einrichtungen von Desktops bis zum Rechenzentrum.

Auf der **Desktop**<sup>8</sup>-Ebene wurde Avocents Switch-Familie **SwitchView SC**<sup>9</sup> von der National **Information Assurance Partnership**<sup>10</sup> (NIAP) geprüft und mit **EAL4+**<sup>11</sup> bewertet worden. Die Switch-Familie umfasst zusätzliche Merkmale zur Sicherstellung des Datenschutzes in sicheren Umgebungen, ohne dass dabei die Arbeit am Rechner beeinträchtigt wird. Mit diesen Switches sollen beispielsweise Sicherheitsexperten von nur einer Konsole sicheren Zugang zu Daten erhalten, die sich auf mehreren Rechnern befinden. Ein einziges SmartCard/CAC-Lesegerät ermöglicht in diesem Szenario den Fernzugriff auf alle angebotenen Desktops. So soll Zeit gespart und die Komplexität des Systems verringert werden.

**Gartner**<sup>12</sup> kommentiert die CAC-Technologie in der Studie **Using One Card for Access Control**<sup>13</sup> (3.März 2008, ID-Nummer: G00155502) wie folgt: "Der Einsatz eines Systems, das auf einer einzigen CAC beruht und die physische und logische Sicherheit in einem Unternehmen garantiert, wird im Laufe der Zeit die Sicherheit erhöhen, den Missbrauch von Karten reduzieren und zu Kosteneinsparungen führen. Und wenn das CAC-System richtig implementiert wird, trägt es dazu bei, das gesamte Unternehmen besser zu schützen, also Menschen, Technologien und Prozesse. Bis 2011 werden etwa 70 Prozent der Unternehmen, die jetzt SmartCards für die Netzwerkauthentifizierung einsetzen, auch CAC einsetzen."

## Links im Artikel:

<sup>1</sup> <http://www.avocent.com/>

<sup>2</sup> [https://www.computerwoche.de/knowledge\\_center/compliance\\_recht/](https://www.computerwoche.de/knowledge_center/compliance_recht/)

<sup>3</sup> [http://www.wfm.noaa.gov/pdfs/WFM\\_HSPD12.pdf](http://www.wfm.noaa.gov/pdfs/WFM_HSPD12.pdf)

<sup>4</sup> <http://www.avocent.com/DSView3.aspx>

<sup>5</sup> [http://www.avocent.com/DSR\\_Switches.aspx](http://www.avocent.com/DSR_Switches.aspx)

<sup>6</sup> <https://www.computerwoche.de/schwerpunkt/s/Security.html>

<sup>7</sup> <https://www.computerwoche.de/schwerpunkt/s/Server.html>

<sup>8</sup> [https://www.computerwoche.de/knowledge\\_center/virtualisierung/1881989/](https://www.computerwoche.de/knowledge_center/virtualisierung/1881989/)

<sup>9</sup> [http://www.avocent.com/Secure\\_KVM\\_Switching.aspx](http://www.avocent.com/Secure_KVM_Switching.aspx)

<sup>10</sup> <http://www.niap-ccevs.org/>

<sup>11</sup> [http://en.wikipedia.org/wiki/Evaluation\\_Assurance\\_Level](http://en.wikipedia.org/wiki/Evaluation_Assurance_Level)

<sup>12</sup> <http://www.gartner.com/>

<sup>13</sup> [http://www.gartner.com/DisplayDocument?doc\\_cd=155502&ref=g\\_rss](http://www.gartner.com/DisplayDocument?doc_cd=155502&ref=g_rss)

---

IDG Tech Media GmbH

Alle Rechte vorbehalten. Jegliche Vervielfältigung oder Weiterverbreitung in jedem Medium in Teilen oder als Ganzes bedarf der schriftlichen Zustimmung der IDG Tech Media GmbH. dpa-Texte und Bilder sind urheberrechtlich geschützt und dürfen weder reproduziert noch wiederverwendet oder für gewerbliche Zwecke verwendet werden. Für den Fall, dass auf dieser Webseite unzutreffende Informationen veröffentlicht oder in Programmen oder Datenbanken Fehler enthalten sein sollten, kommt eine Haftung nur bei grober Fahrlässigkeit des Verlages oder seiner Mitarbeiter in Betracht. Die Redaktion übernimmt keine Haftung für unverlangt eingesandte Manuskripte, Fotos und Illustrationen. Für Inhalte externer Seiten, auf die von dieser Webseite aus gelinkt wird, übernimmt die IDG Tech Media GmbH keine Verantwortung.