

Digitalzertifikate von SSH Server sichern Datensammlungsgeräte

DAWSONVILLE, Georgia, 20. Sept 2011 /PRNewswire/ -- [SSH Server](#) von Georgia SoftWorks verbessert die Sicherheit mittels der Authentifizierung mit Digitalzertifikaten. Es wird eine Option mit einfacherer Einrichtung und besserer Verwaltung geboten als schlichte öffentliche Schlüssel. Ein neues Niveau der [Sicherheit für SAP](#) und für Nutzer von ERP-Mobilgeräten in Datensammlung, Lagerhaltung, Vertrieb, Logistik und Herstellung wird definiert.

(Logo: <http://photos.prnewswire.com/prnh/20110920/CL71065LOGO>)

Die Authentifizierung mittels Digitalzertifikaten ist der Authentifizierung mittels Nutzernamen und Passwort überlegen und zudem deutlich einfacher zu konfigurieren und zu verwalten als einfache öffentliche Schlüssel. Zudem werden zusätzliche Sicherheitsleistungen bereitgestellt wie Nicht-Zurückweisung, Schutz gegen den ‚Agenten in der Mitte‘ und Attacken mittels Serviceverweigerung.

„Die Sicherheit mittels öffentlicher Schlüsselinfrastruktur (Public Key Infrastructure – PKI) ist unter Nutzung von SSH Server für Windows von Georgia SoftWorks jetzt problemlos realisierbar“, sagte Brian Butler von Georgia SoftWorks. „Digitalzertifikate ermöglichen etwas, das zuvor für Branchen nicht realisierbar war, die Barcodescanner, Datensammlung, RFID und Mobilgeräte in SAP-Umgebungen und sonstigen ERP-Umgebungen nutzen.“

Die Bereitstellung und Wartung schlichter öffentlicher Schlüssel ist derart komplex und arbeitsaufwendig, dass viele Unternehmen nicht Willens oder in der Lage sind, die nötigen Mittel für eine Implementierung aufzubringen. Bei der Nutzung schlichter öffentlicher Schlüssel ist z. B. für jeden Nutzer die Bearbeitung einer textbasierten Konfigurationsdatei von Hand erforderlich. Hat man Dutzende oder Hunderte von Nutzern, ist der Zeitaufwand für die richtige Wartung des Systems nicht mehr zu leisten.

SSH Server von GSW authentifiziert dagegen die Nutzer durch Mapping des [Digitalzertifikats](#) des Klienten an einen Windows-Nutzeraccount. Mittels einer grafischen Benutzerschnittstelle ähnlich Windows IIS sind Mappings der Typen ‚Eineindeutig‘ und ‚Mehreindeutig‘ konfigurierbar, was den Bereitstellungsprozess deutlich *vereinfacht*.

„Die Komplexität der Bereitstellung und Wartung schlichter öffentlicher Schlüssel stellt mit SSH Server von GSW und seiner Authentifizierung mit Digitalzertifikaten keine hohe Hürde für eine starke PKI mehr dar“, sagte Luke Batko, Chief Engineer bei GSW. „Es wird unmittelbar machbar, die Sicherheit auf ein neues Niveau zu bringen.“

Die SSH-Authentifizierungsstandards ‚x509v3-sign-rsa‘ und ‚x509v3-sign-dss‘ nutzen Digitalzertifikate und geben GSW die Protokollbasis, um viele Probleme schlichter öffentlicher Schlüssel anzugehen.

Mobil-SSH-Clients von GSW unterstützen mittels NTLM über GSSAPI (‚gssapi-with-mic‘) Single Sign On (SSO). Die SSH-Desktopclients unterstützen SSO mit NTLM und Kerberos über GSSAPI.

Die Hinzunahme der x509v3-Konformität ist eine logische Ergänzung der SSH-Option von GSW, die konform mit FIPS 140-2 ist.

[Georgia SoftWorks](#) wurde 1991 gegründet. Es handelt sich um ein Softwareentwicklungsunternehmen in privater Hand, das bekannt dafür ist, Hochleistungsanwendungen in den Bereichen Datenkommunikation, System und Telekommunikation zu kreieren.

Georgia SoftWorks hat mit seinem industriellen SSH-/Telnet-Server für Microsoft Windows weltweite Präsenz erreicht.

Doug Hitchcock
Georgia SoftWorks
+1-(706)-265-1018
doug@georgiasoftworks.com

QUELLE Georgia SoftWorks