Kundeninfo zu den SV Zertifikaten

Wir stellen Ihnen hier einen Auszug aus unserer Kundeninformation vor.
Diesen erhalten unsere Bestandskunden regulär monatlich.

Bei weiterem Interesse Ihrerseits kontaktieren Sie uns bitte über unser Kontaktformular http://abresa.de/kontakt/ oder unter der Telefonnummer: +49 6196 - 969 58 0

Anke Schönwald

abresa GmbH

03.11.2014

Sehr geehrte Damen und Herren,

anbei erhalten Sie die Kundeninfo zum Thema SV-Zertifikate.

- Die aktuelle Gültigkeit Ihrer Zertifikate können Sie mit dem Report RPUSVHD0 (Testreport) überprüfen.
  - Gehen Sie in Ihr produktives HR System
  - Starten Sie den Report RPUSVHD0
  - Suchen Sie im Protokoll nach dem Wort ‚Gültigkeit'; dort sollte abhängig von Ihrer Betriebsnummer die Gültigkeit des aktuellen Zertifikates stehen
- Ein neues Zertifikat für SV beantragen die mit dem Report RPUSVKD0 (s.u.)!

Sachgebiet	**PY-DE-BA Behördenkommunikation**
Hinweis	**1943292 - SV: SHA256 Verbesserungen und Prüfungen** **1528670: SV Verlängerung_Folgeantrag der Zertifikate** **1930290: - SV SHA256 Verschlüsselung für Kommunikation Krankenkassen** **1994240: Zertifikat erstellen mit SHA256** **1967769 - SV: Verschlüsselung SHA256 - Ablehnung der Daten**
Inhalt	Vorgaben zur Beantragung eines neuen SV-Zertifikats bei der ITSG
Kunden-Aktion	! Bitte beachten Sie bei der Verlängerung der SV-Zertifikate die Verschlüsselung. Hinweis: eine Verlängerung von der Verschlüsselung SHA1 wird nur bis 20.12.2013 akzeptiert, danach muss ein neues Zertifikat beantragt werden. Dieses neue Zertifikat sollte die Verschlüsselung SHA256 beinhalten und hat unabdingbare die Zusammenhänge mit dem SAP Kernel!

	Auflistung der einzelnen Hinweise
Hinweis	**1943292 - SV: SHA256 Verbesserungen und Prüfungen**
Inhalt	Für die Nutzung von Zertifikaten mit SHA256 werden zusätzliche Funktionen und Prüfungen bereitgestellt. Beachten Sie in diesem Zusammenhang Hinweis 1930290 und die dort aufgeführten Voraussetzungen bzgl. der SAP-Cryptolib bzw. CommonCryptoLib.
Kunden-Aktion	! Release 600 SAPK-600A3INSAPHRCDE, Release 604 SAPK-60469INSAPHRCDE
Hinweis	**1528670: SV Verlängerung, Folgeantrag der Zertifikate**
Inhalt	Ab dem 20.12.2013 sind nur noch Zertifikate mit dem Signaturalgorithmus SHA-256 zulässig. Aus diesem Grund können Zertifikates(PSE-Datei), die vor diesem Datum mit SHA-1 angelegt wurden, nicht verlängert werden. Ein neues Zertifikat (neue PSE-Datei) muss angelegt werden. Im Zertifikat steht ein Sachbearbeiter als Ansprechpartner und der Firmenname eingetragen. Wenn sich der Ansprechpartner oder der Firmenname ändert, kann man das nur durch ein neues Zertifikat berücksichtigen. Die Beantragung eines neuen Zertifikates beim Trustcenter der ITSG sollte in der Regel innerhalb einiger Werktage abgeschlossen sein. Wird ein neues Zertifikat im System erzeugt, so wird das bisherige Zertifikat(PSE-Datei) überschrieben!

	Weiter kann dieses Zertifikat erst nach dem Einspielen der Zertifikatsantwort des Trustcenters für die Kommunikation mit den Krankenkassen verwendet werden. Zuvor führt die Verwendung eines solchen Zertifikates zu Fehlern im Prozess. Um eine Unterbrechung der Kommunikation mit den Krankenkassen für die Dauer der Beantragung zu verhindern, kann das Zertifikat z.B. aus dem Test-/Konsolidierungssystem beantragt werden und nach Abschluss der Beantragung ins Produktivsystem übernommen werden. Bei der Bereitstellung der Antworten und Meldungen der Krankenkassen an den Arbeitgeber werden diese auf dem Kommunikationsserver ebenfalls mit dem jeweils aktuellen Zertifikat des Arbeitgebers, Ordnungskriterium Betriebsnummer, verschlüsselt abgelegt. Bei noch nicht abgeholte und nach einem Zertifikatswechsel mit dem alten Zertifikat verschlüsselte Antworten wird dies automatisch erkannt. Es erfolgt eine Neuverschlüsselung und die Meldungen können mit einem zeitlichen Versatz, i.d.R. 24 Stunden, abgeholt werden. Abfolge beim Beantragen neuer Zertifikate: 1: Es ist sicher nicht verkehrt, wenn Sie sich zuerst die bisherige PSE-Datei (vom Applikationsserver, Verzeichnis DIR_INSTANCE\sec) kopieren/sichern. 2: Dann löschen Sie alle Dateien BN<Betriebsnummer>*.* die mit der vorherigen Zertifikatserzeugung zusammenhängen. (Je nach den Einstellungen der logischen Pfadnamen HR_DE_B2A_KK* in der Transaktion FILE.) 3: Im Report RPUSVKD0 tragen Sie dann die Betriebsnummer ein und im Kommandofeld die Zeichen 'CR' (ohne Anführungszeichen). Nach der Datenfreigabe ist im Selektionsbild der Abschnitt 1 (Zertifikat erzeugen) wieder eingabebereit. Hier können Sie dann den Namen des Sachbearbeiters ändern. Der Rest läuft dann, wie in der Report-Dokumentation beschrieben.
Kunden-Aktion	Release 600 SAPK-60063INSAPHRCDE, Release 604 SAPK-60429INSAPHRCDE
Hinweis	**1930290: - SV SHA256 Verschlüsselung für Kommunikation Krankenkassen**
Inhalt	Zum 01.01.2014 wird SHA256 den bis dahin geltenden Algorithmus SHA1 komplett ablösen. Ab dem 20.12.2013 werden neue Zertifikate nur noch mit SHA256 vom Trustcenter der ITSG ausgegeben. Zertifikate die vor dem 20.12.2013 noch mit SHA1 beantragt wurden, können bis zu deren Gültigkeitsende verwendet werden. D.h. noch maximal drei Jahre. Voraussetzung für die Nutzung der Funktionalität ist, daß die aktuelle SAP-Cryptolib Version 5.5.5pl36 (Hinweis 1841573 und 45503) oder höher bzw. die aktuelle CommonCryptoLib 8.4.13 (Hinweis 1963136) oder höher installiert ist.
Kunden-Aktion	Release 600 SAPK-600A2INSAPHRCDE, Release 604 SAPK-60468INSAPHRCDE
Hinweis	**1994240: Zertifikat erstellen mit SHA256**
Inhalt	Zusammenfassung aller relevanten Hinweise! Sowie Verweis auf Hinweis 1958737 „SV: Laufzeitfehler RPUSVKD0“ (Release 600 SAPK-600A4INSAPHRCDE, Release 604 SAPK-60470INSAPHRCDE) und Hinweis 1970145 „SV: Korrektur zu 1958737 - SV: Laufzeitfehler RPUSVKD0“ (Release 600 SAPK-600A6INSAPHRCDE, Release 604 SAPK-60472INSAPHRCDE)
Kunden-Aktion	Information

Hinweis	1967769 - SV: Verschlüsselung SHA256 - Ablehnung der Daten
Inhalt	Bei der Verschickung der SV-Daten kommt es zu einer Ablehnung. Verwendung von Zertifikaten mit SHA256 Signatur. Beim Versenden wurde der Parameter für die Signatur nicht richtig übergeben.
Kunden-Aktion	! Prüfen Sie auch diesen Hinweis (Release 600 SAPK-600A5INSAPHRCDE, Release 604 SAPK-60471INSAPHRCDE).

Sachgebiet	BC-SEC-SSF Sicheres 'Store and Forward'	
Hinweise		
Inhalt	Basisseitig prüfen Sie bei Problemen bitte auch die folgenden Hinweise:	
Kunden-Aktion	! 1739681 Kernel: Unterstützung Anlegen von RSA-PSEs mit SHA-256 1740744 SSFPSE_CREATE: Anlegen von RSA-PSEs mit SHA-256 unterstützen 1856192 Anlegen von RSA PSEs größer als 2048 Bit in STRUST	
Inhalt	SECURITY NOTE: bitte unbedingt folgenden Basis-Hinweise umsetzen! s.a. https://websmp109.sap-ag.de/securitynotes?lf1=8361038169d525716883439e30901056	
2068693	Änderungen CommonCryptoLib, CCL, SAPcryptolib, SAPseculib durch (externe) Anforderungen	
2067859	Ein Angreifer kann Versionen der SAP Cryptographic Libraries, die vom SAP NetWeaver Application Server (SAP NetWeaver AS) für ABAP- und SAP-HANA-Anwendungen verwendet werden, für eine Spoofing-Attacke auf digitale Signaturen einsetzen. In Versionen der Komponenten SAPCRYPTOLIB, SAPSECULIB und CommonCryptoLib des SAP NetWeaver AS für ABAP- und SAP-HANA-Anwendungen gibt es eine kritische Sicherheitsschwachstelle. Dieses Problem betrifft Anmeldetickets, Authentifizierungszusicherungstickets sowie weitere Anwendungen, die SAP NetWeaver AS für vom ABAP und SAP-HANA-System generierte digitale Signaturen verwenden. Ersetzen Sie die betroffenen Bibliotheken. •Wenn Sie SAPCRYPTOLIB verwenden, führen Sie ein Upgrade auf die Version 5.555.38 oder höher durch. •Wenn Sie SAPSECULIB verwenden, führen Sie ein Upgrade auf SAPCRYPTOLIB in der Version 5.555.38 oder höher durch. •Wenn Sie CommonCryptoLib verwenden, führen Sie ein Upgrade auf Version 8.4.30 oder höher durch. Option 1: Manuelles Ersetzen (siehe Infodatei „Instructions for SAP Security Note 2067859") Option 2: Automatisches Ersetzen per Kernel-Update	
Kunden-Aktion	! 2068693 Replacing Key Pairs in SAP NetWeaver Application Server for ABAP and SAP HANA Platform Systems 2067859 Gefahr eines möglichen Spoofing-Angriffs auf digitale Signaturen	

Update Oktober 2014:

- **Fehler im Report RPUSVKD0 mit Verweis auf den SAP Kernel** (SSF Kernel Fehler: ungültiger Parameter)

Sachgebiet	PY-DE	
Hinweise		
Inhalt	Bitte prüfen Sie Ihren aktuellen Systemstand und spielen Sie die folgenden Hinweise ein:	
Kunden-Aktion	 2049898 SV: Sammelhinweis Datenaustausch 4/2014 Dieser setzt viele Hinweise voraus, dieses sind die relevanten Hinweise: 2036330 SV: Sammelhinweis Datenaustausch 3/2014 (vom 22.7.14) 1981825 Zertifizierungsantrag ITSG: Formular HR_DE_SV_ZERTR wurde angepasst 2063990 SV: Sammelhinweis Datenaustausch 5/2014	
Inhalt		
2049898	Neben den zwei nachfolgenden Hinweisen müssen Reporttexte eingepflegt werden (Bitte beachten, dass dies ggf. nur über die Funktion ‚abgleichen' funktioniert). Dieser Hinweis beinhaltet die Korrektur, die beim Starten des Report RPUSVKD0 zum Fehler „SSF Kernel Fehler: ungültiger Parameter" führt. (6.00 in Patch B2, 6.04 in Patch 78, 6.08 in Patch 06)	
2036330	Nach dem Einspielen muss die Nachrichtenpflege muss noch erfolgen. Der Hinweis beinhaltet u.a. auch die Meldung vom Kommunikationsserver bei einer erneuten Anfrage nach 15 Minuten. (6.00 in Patch B1, 6.04 in Patch 77, 6.08 in Patch 05)	
1981825	Das SAPScript Formular HR_DE_SV_ZERTR stimmt nicht mehr mit der Vorlage der ITSG überein, es muss in das System manuell implementiert werden. (6.00 in Patch B1, 6.04 in Patch 77, 6.08 in Patch 05)	
2063990	Warnung bei Zertifikaterzeugung: "SSF Kernel Fehler: ungültiger Parameter" wird deaktiviert! (Dieses Patch wird erst zum 13.11. von SAP freigegeben! Der Hinweis wird ausgeliefert mit 6.00 in Patch B4, 6.04 in Patch 80, 6.08 in Patch 08)	
Kunden-Aktion	 s.o. bitte prüfen Sie die aufgeführten Hinweise!	