Support
signatures-support@infotech.de

Infotech
Gesellschaft für Informations- und Datentechnik mbH

Holthoffstr. 122a
45659 Recklinghausen

Telefon 02361-9130-0
Telefax 02361-9130-105
eMail info@infotech.de
Website www.infotech.de

Stand: 10.07.2014

Signatures

Hinweise zur Ersteinrichtung

- Windows-Server
- Windows-Client
- iOS-Client
- Android-Client

Einrichten des Servers

Damit der Serverdienst für die Clients erreichbar ist muss sichergestellt sein, dass alle zwischen den beiden Stationen liegenden Firewalls und Router die Verbindung zulassen. Standardmäßig wird hierfür der TCP-Port 8022 auf dem Server geöffnet. Insbesondere für Mobilfunk-Clients kann eine Verbindung auch direkt aus dem Internet, z.B. durch entspr. Weiterleitungen, erforderlich sein. Der Server muss außerdem in der Lage sein den Host „ca.infotech.de“ auf TCP-Port 25050 zu erreichen um sich aktivieren zu können.

- Falls die Remote-Signatur genutzt werden soll: Alle zu verwendenden Kartenlesegeräte samt Treiber auf Betriebssystemebene installieren
- Das Signatures-Setup starten und die Komponente „Server“ entsprechend der Vorgaben des Setup-Assistenten installieren. Das Setup startet die Serverkomponente nach Abschluss der Installation auf Wunsch automatisch
- Ggf. auftretende Meldung der Windows-Firewall mit „Zugriff Zulassen“ bestätigen. Der Signatures-Server muss einen Netzwerkanschluss für die Verbindung zu den Clients bereitstellen können
- Der Signatures-Server registriert sich nun vollautomatisch und anonym bei Infotech.
- Die Systemstatusübersicht wird angezeigt. Hier sind Karten- und Dienststati auf einen Blick ersichtlich (Abb.1)

Abb.1

- Die vom Administrator erhaltenen Verbindungsinformationen (Benutzername [Groß-/Kleinschreibung wird unterschieden], numerisches Erstkennwort [ohne trennende Leerzeichen], Servername, ggf. Port falls vom Standard 8022 abweichend) in die entspr. Felder eintragen. „Timeout“ zunächst bei 10 Sekunden belassen. Sollten bei der späteren Benutzung häufiger Verbindungsabbrüche auftreten kann dieser Wert erhöht werden (Abb.8).

Abb.7

Abb.8

- „Gerätezertifikat“ antippen und das Speichern der Einstellungen sowie die Meldung zum fehlenden Gerätezertifikat bestätigen. In der erscheinenden Maske unten auf „Zertifikat anfordern“ tippen.
- Die ebenfalls vom Administrator erhaltene Freigabe-TAN (ohne trennende Leerzeichen) eingeben und „Ok“ tippen. Es folgt eine Bestätigungsmeldung.
- Es wird nun zur Änderung des Erstkennworts aufgefordert. Ein neues Kennwort festlegen, die Eingabe im zweiten Feld wiederholen und „Ändern“ antippen. Die erfolgreiche Änderung wird daraufhin bestätigt.
- „Signaturzertifikate“ antippen und das zu verwendende Zertifikat auswählen. Falls gewünscht die RemotePIN hinterlegen, ansonsten leer lassen (es wird dann bei der Signatur erneut danach gefragt).
- Mit dem Zurück-Button ins Hauptmenü wechseln. Die App ist nun betriebsbereit.

Abb.5

Abb.6

- „Gerätezertifikat“ antippen und das Speichern der Einstellungen sowie die Meldung zum noch fehlenden Gerätezertifikat bestätigen. In der erscheinenden Maske unten auf „Zertifikat anfordern“ tippen.
- Die ebenfalls vom Administrator erhaltene Freigabe-TAN (ohne trennende Leerzeichen) eingeben und „Ok“ tippen. Es folgt eine Bestätigungsmeldung.
- Es wird nun zur Änderung des Erstkennworts aufgefordert. Ein neues Kennwort festlegen, die Eingabe im zweiten Feld wiederholen und „Ok“ klicken. Auf die erfolgreiche Änderung wird daraufhin nach dem Hinterlegen des neuen Kennworts in der Konfiguration gefragt. Mit „Ja“ bestätigen.
- „Signaturzertifikat“ antippen und das zu verwendende Zertifikat auswählen.
- Falls gewünscht die RemotePIN hinterlegen, ansonsten leer lassen (es wird dann bei der Signatur erneut danach gefragt). „zurück“ antippen.
- Mit „zurück“ ins Hauptmenü wechseln. Die App ist nun betriebsbereit.

Einrichten von Android Clients

- Signatures kostenlos aus dem Google Play Store laden.
- Die App starten. Es wird gefragt, ob jetzt ein Zertifikat für das Mobilgerät angefragt werden soll. Mit „Ja“ beantworten. Es wird in die Einstellungsmaske weitergeleitet (Abb.7).

- Mindestens einen Benutzer anlegen:
  - Auf den Hauptreiter „Benutzer“ wechseln und „Neu“ klicken
  - Anmeldenamen eintragen (das Erstanmeldekennwort wird automatisch erzeugt) und den Haken für die automatische Vergabe einer Freigabe-TAN setzen
  - Benutzeranlage mit „Ok“ abschließen (Abb.2)

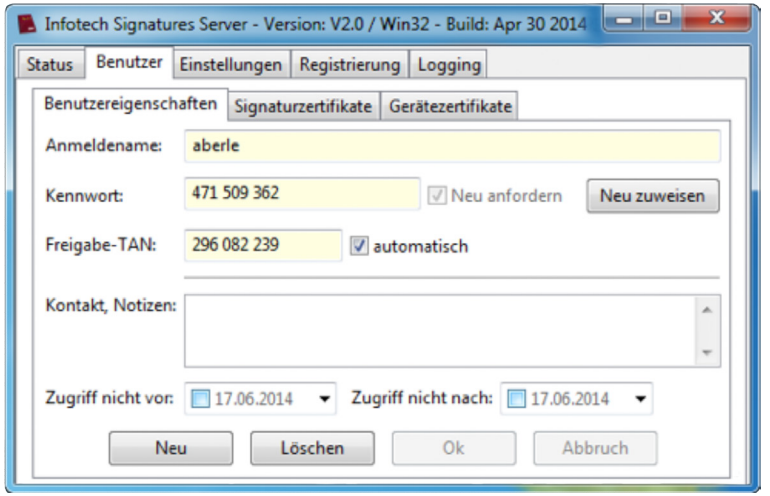

Abb.2

- Bei Benutzern, welche die Remote-Signatur nutzen sollen (Anwesenheit des Karteninhabers ist erforderlich):
  - Die Smartcard des Benutzers in einen angeschlossenen Kartenleser einlegen und in der anschließenden Meldung der Verwendung der Fernsignaturkomponente zustimmen
  - Die ausgegebene RemotePIN durch den Karteninhaber notieren lassen (diese ist später am Client zur Nutzung der Karte erforderlich) und mit „Ja“ bestätigen. Im folgenden Dialog die Option „Zulassen, solange die Karte gesteckt ist“ wählen und erneut bestätigen. Anschließend wird die Signatur-PIN am Kartenleser eingegeben. Die Karte ist daraufhin für die Remote-Signatur nutzbar.
  - Das Kartenzertifikat über die Benutzerverwaltung des Servers auslesen und einem Benutzer zuweisen (Abb.3)

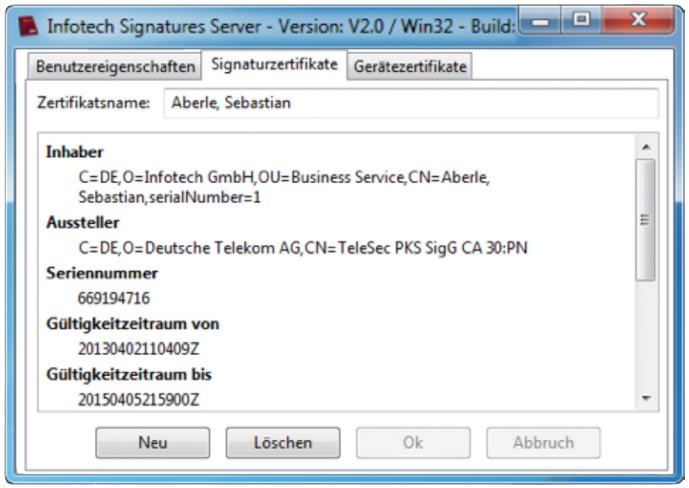

Abb.3

- Die für die Anmeldung am Server erforderlichen Informationen (Servername, Benutzername, Kennwort, Freigabe-TAN) zur Einrichtung der Clients an die Benutzer übergeben (zB. per E-Mail). Dabei darauf hinweisen, dass die Leerzeichen, welche die drei Zifferngruppen voneinander trennen, nur zur besseren Lesbarkeit eingefügt sind und bei Verwendung nicht mit eingegeben werden dürfen, sowie dass im Benutzernamen Groß- und Kleinschreibung unterschieden wird
- Weitere Einstellungen, zB. zur Nutzung eines HTTP-Proxies oder Vergabe eines Kennworts zur Absicherung der Serverkonfiguration können im Reiter „Einstellungen“ vorgenommen werden.

Einrichten von Windows-Clients

- Falls die lokale Signatur genutzt werden soll: Alle zu verwendenden Kartenlesegeräte samt Treiber auf Betriebssystemebene installieren
- Das Signatures-Setup starten und die Komponente „Client“ entsprechend der Vorgaben des Setup-Assistenten installieren. Das Setup startet den Client nach Abschluss der Installation auf Wunsch automatisch
- Die vom Administrator erhaltenen Verbindungsinformationen (Servername, Benutzername [Groß-/Kleinschreibung wird unterschieden], numerisches Erstkennwort [ohne trennende Leerzeichen]) in die Anmeldemaske eintragen und „Anmelden“ klicken
- Die ebenfalls vom Administrator erhaltene Freigabe-TAN (ohne trennende Leerzeichen) in den nun folgenden Dialog eintragen und „Zertifikat beantragen“ klicken. Es folgt eine Bestätigungsmeldung. (Abb.4)

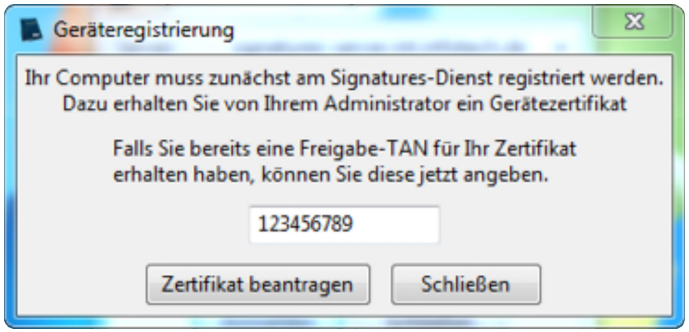

Abb.4

- Es wird nun zur Änderung des Erstkennworts aufgefordert. Ein neues Kennwort festlegen, die Eingabe im zweiten Feld wiederholen und „Wählen“ klicken. Die erfolgreiche Änderung wird daraufhin bestätigt.
- Die zum Nutzungsprofil am besten passende Rolle wählen. Die Auswahl legt lediglich die erste Fensteranordnung fest. Diese kann jederzeit beliebig geändert werden.

Einrichten von iOS Clients

- Die App starten. Es wird gefragt, ob zunächst die Einstellungen vorgenommen werden sollen. Mit „Ja“ beantworten. Es wird in die Einstellungsmaske weitergeleitet (Abb.5).
- Die vom Administrator erhaltenen Verbindungsinformationen (Benutzername [Groß-/Kleinschreibung wird unterschieden], numerisches Erstkennwort [ohne trennende Leerzeichen], Servername, ggf. Port falls vom Standard 8022 abweichend) in die entspr. Felder eintragen. „Timeout“ zunächst bei 20 Sekunden belassen. Sollten bei der späteren Benutzung häufiger Verbindungsabbrüche auftreten kann dieser Wert erhöht werden (Abb.6).