SIEMENS
Ingenuity for life

SiPass integrated MP2.95

Software Installation & Update V1.1

www.siemens.com/buildingtechnologies

SiPass integrated MP2.95

Software Installation & Update V1.1

Inhalt

1. PC Anforderungen 3
2. Datenbank Informationen 4
3. SQL / SQL Express Datenbank Installation 5
4. Java Runtime Installation 5
5. IIS Installation 5
6. SiPass Lizenz 6
7. Engineer License 7
8. SiPass integrated Server/Client Installation 8
9. Zertifikate erneuern 22
   9.1 Selbstsigniertes Server Zertifikat erneuern 22
   9.2 Remote Client Zertifikat erneuern (auf Basis des Selbst signierten Server Zertifikats) 23
   9.3 Maschinenzertifikate Erneuern 25
10. Verwaltung der SiPass Zertifikate 26
11. DEMO Installation 29
   11.1 DEMO Features 29
12. SiPass integrated Login 30
13. SiPass Client Installation 31
   13.1. Client Connectivity Tool 31
   13.2 Remote Client setup 33
   13.3 Client Zertifikat falsch/abgelaufen 38
14. Update der SiPass Funktionen 40
15. SiPass integrated Upgrade Pfad 40
   15.1 SiPass Versions Upgrade – Schritt für Schritt: 41
16. SiPass integrated Web Client 44
17. Empfohlene SQL Datenbank Einstellungen 47

1. PC Anforderungen

SiPass Server / Client Systemanforderungen:

Operation System	Windows 10 /11 Prof. / Ent. (64-bit)	Windows Server 2019 / 2022
SiPass MP 2.95	✓	✓

Wichtig:
Ab SiPass 2.80 werden nur noch 64 Bit Betriebssysteme unterstützt.

Microsoft SQL	SQL 2019 Express, Standard, Enterprise	SQL 2022 Express, Standard, Enterprise
SiPass MP 2.95	✓	✓

- Arbeitsspeicher: 8 GB (Minimum), 16 GB empfohlen
- Festplattenspeicher: 1 TB oder mehr empfohlen
- Ethernet Ports: 100 Mbit / 1000 Mbit (1000 Mbit empfohlen)
- Intel Core i5 oder höher (5. Generation oder höher)

Bitte beachten:
In den Dokumenten „*Release notes*“ und „*System limits*“ der entsprechend verwendeten Version von SiPass integrated sind die Angaben zu aktuell kompatiblen Betriebssystemen und Service Packs zu finden.

2. Datenbank Informationen

SiPass kann einen Lizenzierten SQL-Server oder die kostenfreie SQL Express variante verwenden. (siehe auch Seite 12)
Entsprechend der Anlagengröße ist die entsprechende SQL-Variante einzusetzen.

Die MSSQL Express Editionen der Datenbank Anwendungen wurden von Microsoft eingeschränkt. Bei erhöhten Datenbankzugriffen nimmt die Leistung der Datenbank Anwendung ab. Als Faustregel lässt sich festhalten, dass der SiPass integrated Server, welcher SQL Express verwendet, nicht mehr als
10.000 Personen oder **100** Türen oder **5** Client-Workstations haben sollten.

Obwohl es durch Abwägung dieser Zahlen und Grenzwerte möglich ist Kompromisse zu finden und Anlagen mit geringer Netz Last existieren können, wird für größere Installationen empfohlen eine SQL Server Datenbank Lizenz zu erwerben. Dies gewährleistet die dauerhafte Integrität der Anlage.

(Dies ist ein Auszug aus dem Dokument: „*System Limits*“)

Zu beachten:
Wird die SQL Datenbank manuell installiert, ist es zwingen notwendig der „SiPass integrated Installation Guide“ zu folgen.
Dieser befindet sich auf jeder SiPass DVD unter \Documentation\Installation and User Information.

3. SQL / SQL Express Datenbank Installation

Manuelle SQL-Installation:
Während der manuellen Installation der SQL Datenbank müssen einige Punkte berücksichtigt werden!
Siehe => SiPass integrated Installation Guide.pdf

Automatische SQL Express-Installation:
Sollte auf dem SiPass Server kein SQL-Server vorinstalliert sein, kann das SiPass Setup automatisch SQL Express installieren.

Achtung:

Ab der SiPass Version 2.90 muss der SQL Server nicht mehr auf dem SiPass Server installiert sein! (Siehe Kursunterlagen „SiPass with remote SQL“)

4. Java Runtime Installation

Die SiPass Version 2.95 benötigt kein Java Runtime, muss also nicht installiert werden.

5. IIS Installation

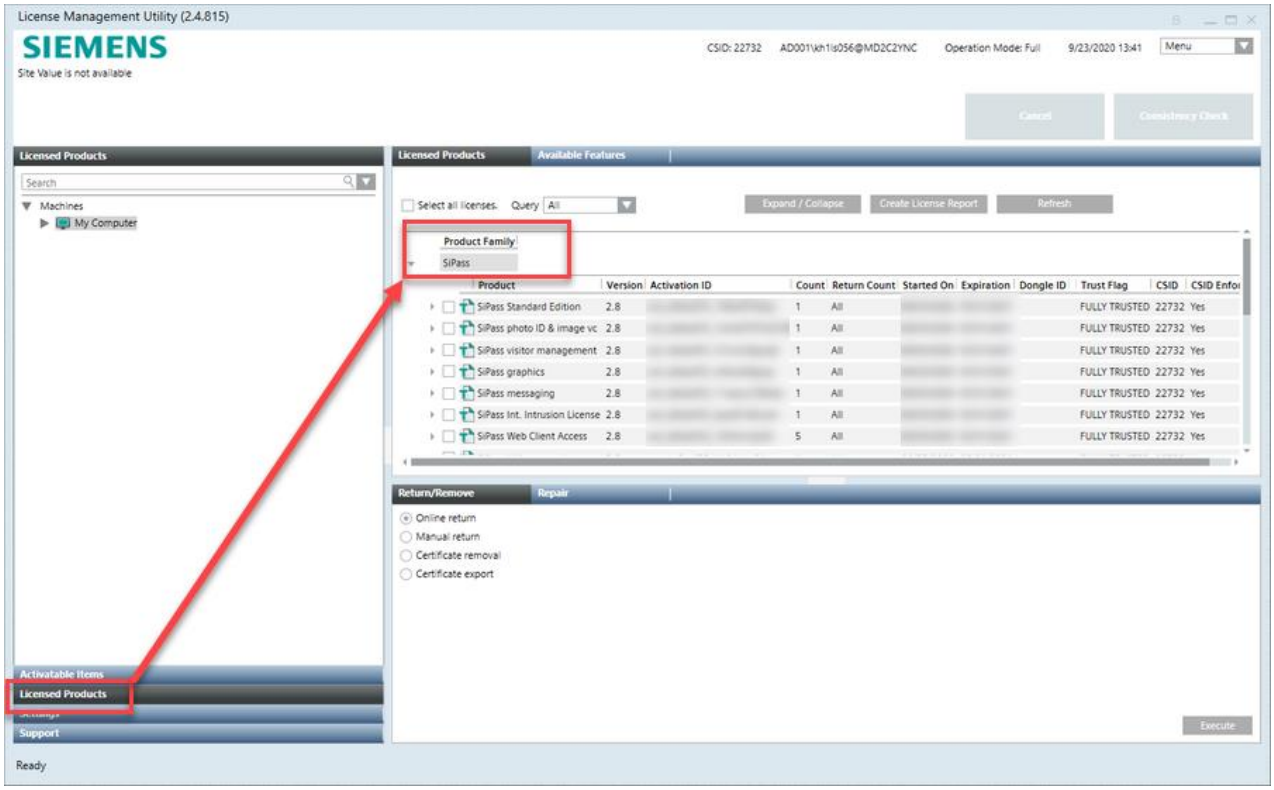
Der Internet Information Service (IIS) wird für die SiPass Web-Clients benötigt.
Ab SiPass 2.80 wird IIS mit den notwendigen Einstellungen automatisch aktiviert.
Es sind also keine weiteren Einstellungen, wie in den Vorgängerversionen, notwendig.

6. SiPass Lizenz

Mit SiPass 2.80 wurde die Lizenzierung über das „Lizenz Management Utility“ (LMU) eingeführt. Die LMU-Installation ist nicht Bestandteil der SiPass-Installation. Empfohlen wird, die LMU-Installation und die SiPass Lizenzierung vor der SiPass-Installation durchzuführen. (SiPass 2.90 benötigt die LMU Version 2.6)

Das LMU-eLearning findet man unter folgendem Link: https://siemens-learning-sipartnerportal.sabacloud.com/Saba/Web_spf/EU2PRD0112/common/ledetail/AAA-00005041/latestversion
(Falls der Link nicht funktionieren sollte, auf „MyLearning“ nach LMU suchen.)

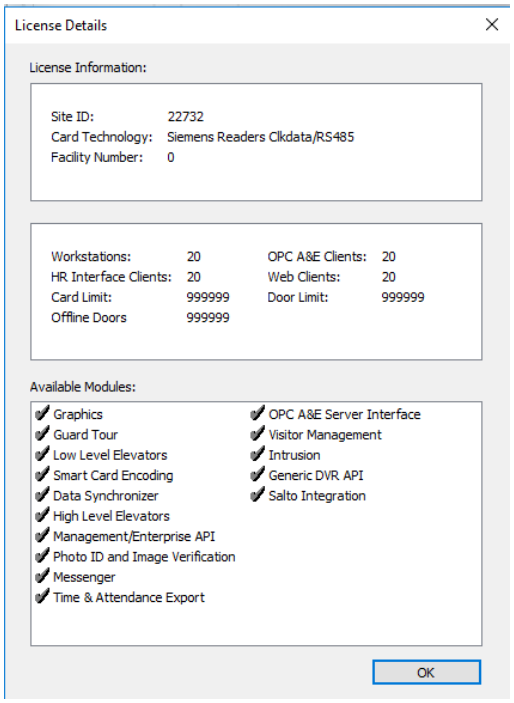
Für die SiPass Installation ist die DVD ISO „Bereitzustellen“/ zu „Mounten“.
Da LMU bei der Installation ein Log-File in das Verzeichnis von dem installiert wurde schreiben will, funktioniert dies bei dem „Mounted“ ISO-File nicht.
Aus diesem Grund muss das LMU-Setup File auf die Festplatte kopiert werden, damit ein Schreiben möglich ist.
Das LMU-Setup File ist auf der SiPass DVD im Verzeichnis: \Prerequisites.



Hotline für LMU, wird genauso wie bei SiPass gehandhabt.

How to order / upgrade guide: SiPass how to order and Upgrade Guide - ID: 109784510 - Industry Support Siemens

7. Engineer License



Die neue „SiPass Engineering Lizenz" ist mit LMU-Lizenzierung eingeführt worden.
In welchen Fällen, kann diese Dongle-basierende Lizenz, verwendet werden?

F: Wird die „Engineering Lizenz" benötigt,
um eine Kundenanlage aufzubauen?
A: Nein

F: Hat die „Engineering Lizenz" zusätzliche Funktionen?
A: Nein

F: Ist es notwendig einen HW-Dongle zu bestellen?
A: Ja, die „Engineering Lizenz" funktioniert nur
mit einem Dongle! Bestellnummer: S55802-Y148

F: Hat die „Engineering Lizenz" ein Ablaufdatum?
A: Ja, nach Aktivierung kann die „Engineering Lizenz"
12 Monate verwendet werden.

F: Kann die SiPass „Engineering Lizenz" über eine SUR Bestellung erweitert werden.
A: Nein, eine neue SAP Bestellung ist notwendig (P54511-P110-A1-L).

Wofür kann ich die SiPass „Engineering Lizenz" verwenden?

- Test / Lab Systeme (falls der forhanden SiPass DEMO Mode nicht ausreichend ist)
- Um die Kundenanlage aufzubauen => Ist die Anlage aufgebaut, kann der Engineering-Dongle entfernt werden und die Kundenlizenz aktiviert werden, dadurch hat der Kunde noch volle 12 Monate Software Subscription.
- Kunden Demos (falls der forhanden SiPass DEMO Mode nicht ausreichend ist)
- POC
- API Entwicklung

Der Dongle wird auch für Desigo-CC verwendet. (CMD.04 LMS Micro Dongle)
Generell handelt es sich hier um einen LMS-Dongle (Lizenz Management System) und jedes System, das über LMU Lizenziert wird, kann den Dongle verwenden.

- Jede SiPass Lizenz Option kann aktiviert werden: online (trusted store)
- Dongle (falls die vom Kunden benötigt oder gefordert wird)

Die SiPass Engineering Lizenz kann nur über einen Dongle aktiviert werden!
(keine online Trusted Store Aktivierung möglich)

8. SiPass integrated Server/Client Installation

Ab SiPass 2.80 wurde die Installation um folgende Punkte vereinfacht:

- Keine Eingabe der Lizenz-details mehr.
- Card Technology, Facility und Site code können individuell bei der Installation ausgewählt werden. (Dies ist nicht mehr Bestandteil der Lizenz)
  Änderungen sind über das „Identifikationsprofil“ möglich, solange noch keine Karten zugewiesen wurden.
- IIS wird automatisch installiert und konfiguriert.
- Ab SiPass Version 2.95 wird kein Java Runtime mehr benötigt.

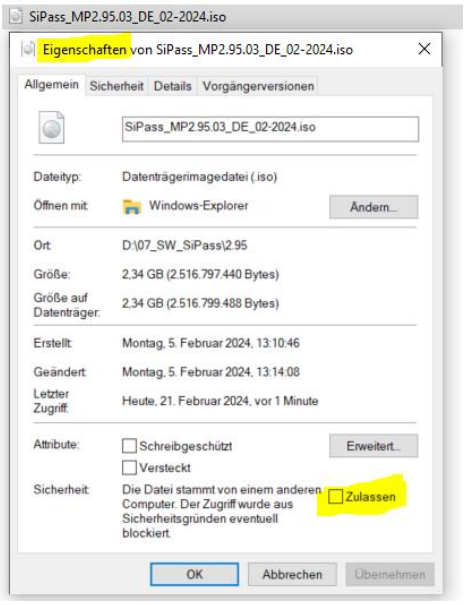
Während der SiPass Installation werden alle Optionen installiert, auch wenn eine Lizenz mit geringeren Optionen zuvor schon aktiviert wurde.
Wenn z.B. die HR-API nicht in der Lizenz vorhanden ist, kann der entsprechende Dienst nicht gestartet werden.

Bei der Installation können ein bis zwei Neustarts notwendig werden.
Fall die Installation, nach Neustart, nicht weitermacht, die Installation erneut starten.

Vorbereitung: „SiPass Service User“ anlegen:

Die SiPass-Dienste werden mit einem Standard Windows-User gestartet.
Dieser Standard Windows-User wird SiPass-Service-User genannt.
Der für diesen Zweck angelegte Standard Windows-User sollte auch entsprechend benannt werden.
Vor dem Start der SiPass Installation kann der SiPass-Service-User als Vorbereitung schon angelegt werden. Dieser muss, während der SiPass Installation dann ausgewählt werden-
(Siehe dazu auch Seite 14)

Beachten vor der Installation vom ISO-File!



Das ISO-File **muss** entsperrt werden oder entsperrt sein!
Wird nach dem Aufruf der ISO-File Eigenschaften, im unteren Teil der Maske „Zulassen“ („Unblock“) angezeigt, ist das ISO-File noch gesperrt.
Dann „Zulassen“ anhaken und „Übernehmen“!

Wird mit einem gesperrten ISO-File installiert kann am Ende der Installation meist der SiPass-Server-Service nicht gestartet werden!

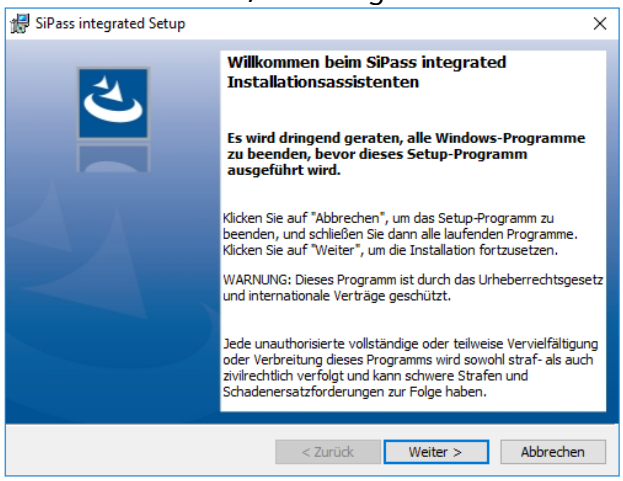
Unbedingt beachten!

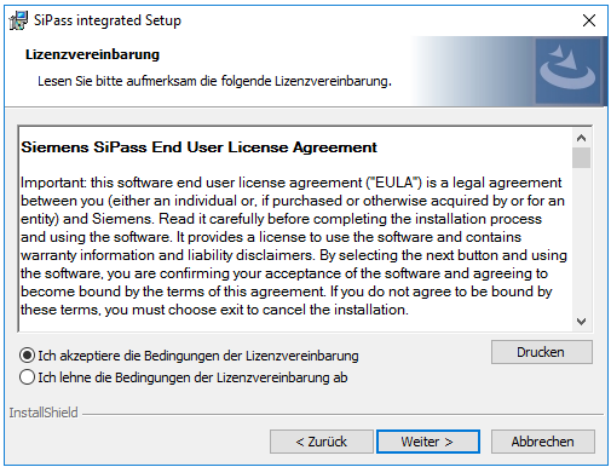
Am besten ist es, das SiPass DVD ISO-File zu “Mounten”, oder die komplette DVD auf die Festplatte zu kopieren und von dort die SiPass Installation zu starten.

Um die SiPass Installation zu starten, ist das **„Install.exe“** von der DVD „als Administrator“ zu starten. (rechte-Maus -> Starten als Administrator)

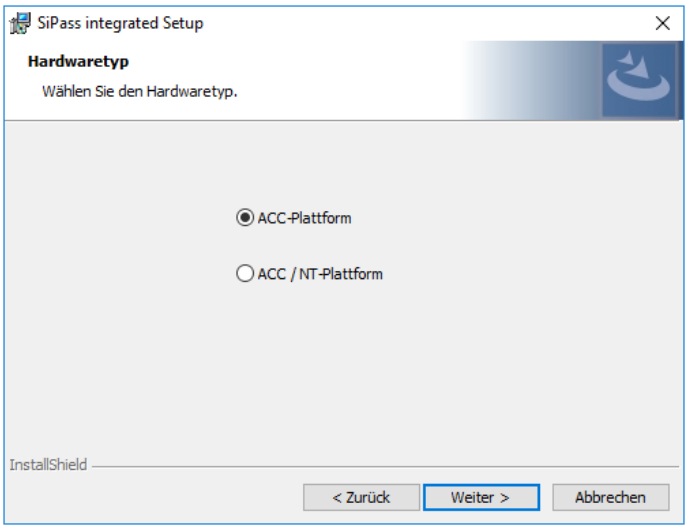
Benötigte Anwendungen werden vom Setup überprüft und gegebenenfalls installiert. Ein Neustart des PCs während des Pre-Setups von SiPass könnte erforderlich sein. Microsoft erlaubt es nicht, die Installation bestimmter Applikationen zu verstecken, daher ist es notwendig, die einzelnen Installationsvorgänge zu bestätigen.

Nach der Installation der Systemanwendungen, startet das SiPass integrated Setup mit dem „*Willkommen*“-Dialogfenster. Auf der nächsten Seite befindet sich dann das Lizenzabkommen, dem zugestimmt werden muss.





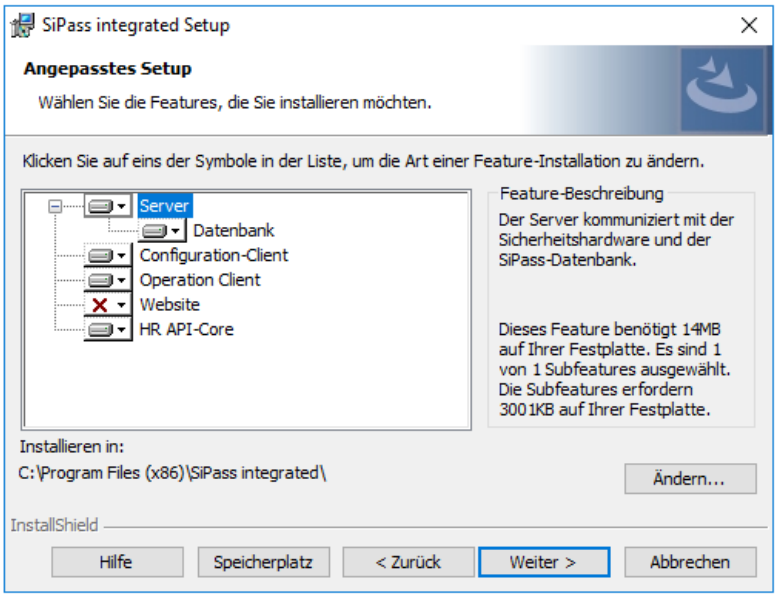
Das nächste Dialogfenster definiert die Hardware Plattform.



Die „**ACC-Plattform**“ wird verwendet für SiPass integrated in Verbindung mit ACC-Controllern: AC5102, ACC-AP, AC5200, AC5100 oder Granta Kontroller.

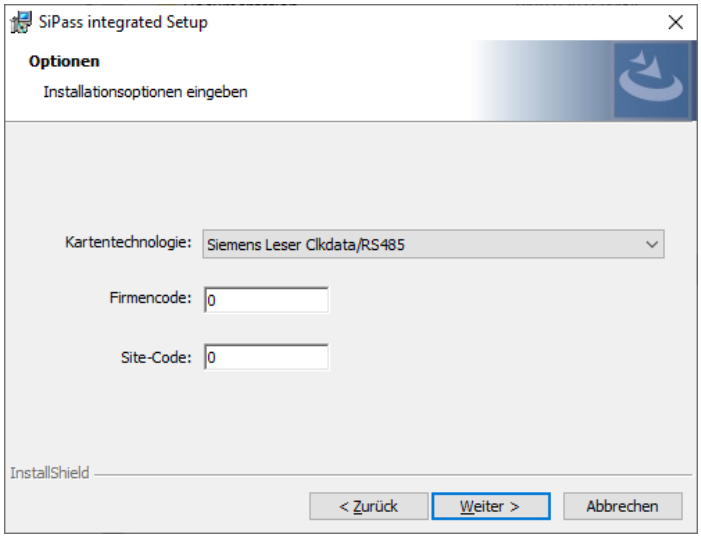
Die „**ACC/NT-Plattform**“ ist für SiPass in Verbindung mit dem älteren *Advantage NT* System und ACC- Controllern gedacht.

Nun können die zu installierenden Features ausgewählt werden.
Ab der SiPass Version 2.90 kann die Web-Server „Website“ Installation deaktiviert werden. Sollten zu einem späteren Zeitpunkt doch Web-Clients benötigt werden, kann der Web-Server nachinstalliert werden.



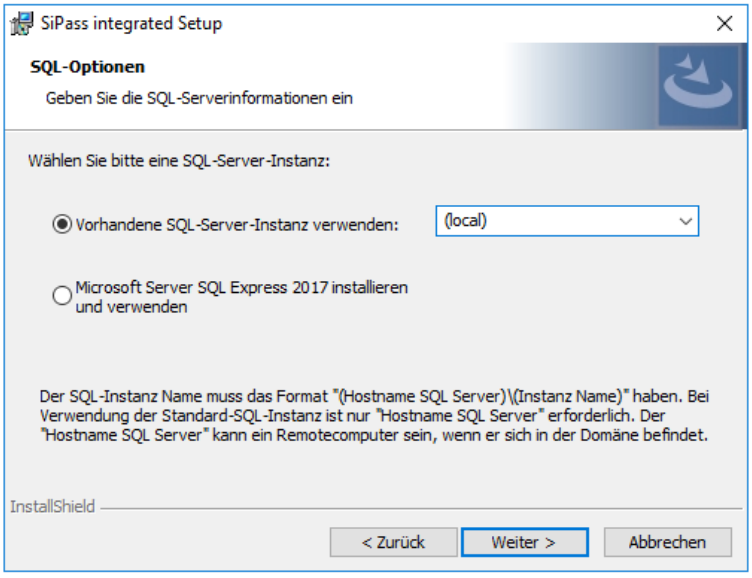
Der Installationspfad kann über „Ändern“ definiert werden, dazu muss der Punkt „*Server*“ auswählt sein.

Seit Einführung der LMS-Lizenzierung kann die Kartentechnologie, Facility und Site Code frei definierbar eingegeben werden.

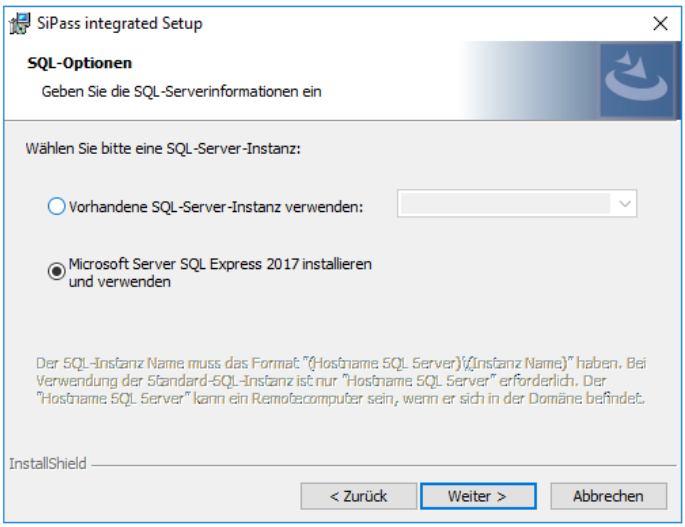


Falls die falsche Kartentechnologie ausgewählt wurde, kann dies nachträglich korrigiert werden, wenn noch keine Ausweiskarten zugewiesen wurden.
Die Änderung kann im Operation Client bei „Identifikationsprofil" durchgeführt werden.

Klicken Sie auf *Weiter* und wählen Sie die SQL Instanz, welche für das SiPass integrated System verwenden wollen.
Ab SiPass 2.90 muss der SQL-Server nicht mehr auf dem gleichen PC sein wie der SiPass-Server! (Bei einem externen SQL-Server siehe Kursunterlagen „SiPass with remote SQL")

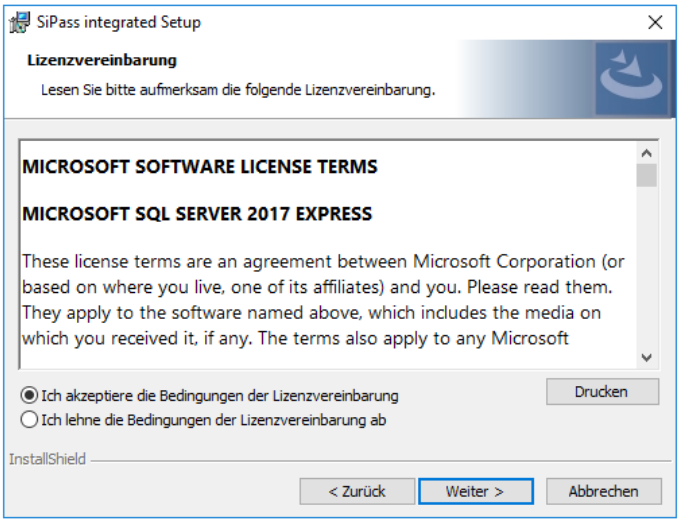


Sollte keine SQL Instanz auf dem SiPass Server PC verfügbar sein oder sollte die existierende SQL Instanz nicht mit SiPass integrated kompatibel sein, kann das SiPass Setup automatisch die entsprechende SQL Express Version installieren.



Jede SQL Datenbank Installation benötigt einen „*SA*“ Administrator.
Die SiPass integrated Installation legt im Hintergrund das SA-Passwort an.
Dieses Passwort muss nicht bekannt sein und kann vom Kunden, wenn gewünscht, über das SQL Management Studio geändert werden.

Die Lizenzbedingungen für die SQL Express Installation müssen akzeptiert werden.



Info zum „SiPass Service User": ----------
Der SiPass Server Service muss mit einen **eignen Windows Konto** gestartet werden. [Windows Standard Konto, keine administrativen Rechte notwendig.] Für manche Host Ereignissteuerungen werden Administratorrechte für den SiPass Service User benötigt (z.B. um ein automatisches Datenbankbackup über eine Host Ereignissteuerung zu erstellen).

Achtung: Als „SiPass Service User" nicht den User verwenden, mit dem man gerade am Window PC angemeldet ist! Dies wird mit einer Fehlermeldung abgewiesen.

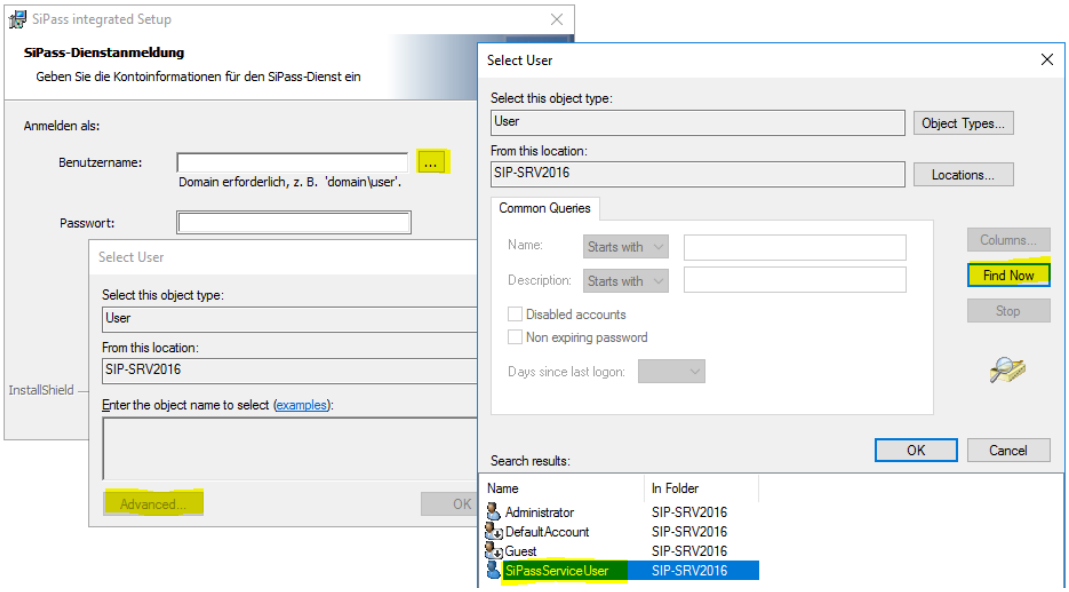
Hinweis: Es ist **nicht** möglich den SiPass Service User nachträglich zu ändern.
Ist dies notwendig, muss SiPass deinstalliert und mit dem neuen Windows-User neu installiert werden (bitte vor der Deinstallation ein aktuelles Datenbank Backup erstellen).

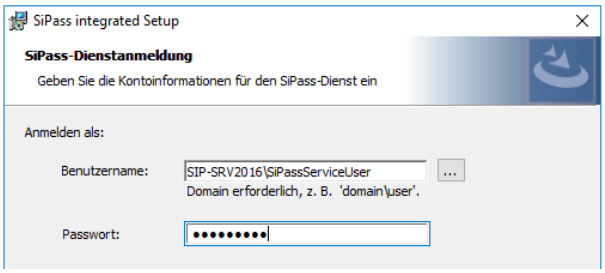
Ab SiPass Version 2.95 ist es möglich das **Passwort** des SiPass Service User nachträglich zu ändern. Dazu sind folgende Schritte notwendig:

- SiPass Dienste stoppen.
- SSU Passwort im AD oder Lokal ändern
- Das Passwort bei allen SiPass Dienste ändern (Properties \ Log On).
- SiPass Dienste starten.

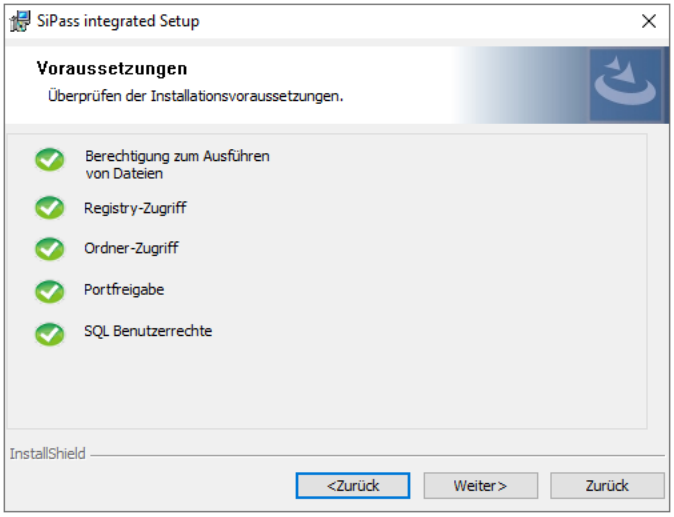
Tipp zum Anlegen des SiPass Service User:
Öffne den „Ausführen" Dialog mit der Tastenkombination Win + R und suche nach „LUSRMGR.msc" um den Benutzer anzulegen (wenn sich der Rechner in einer Domäne befindet, muss ein Domain-User vom Domain-Admin angelegt werden).

Klicken Sie auf  und Windows öffnet ein Fenster zur Benutzerauswahl. Klicken Sie auf die *Erweitert* Option und wählen Sie den Standardbenutzer (SiPass Service User) aus. Dann mit OK bestätigen und das Passwort eingeben.

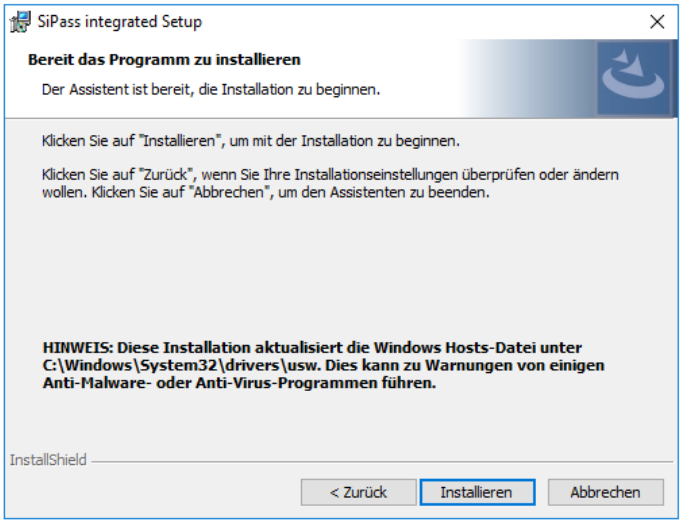




Ab Version 2.95 werden die Installationsvoraussetzungen überprüft.

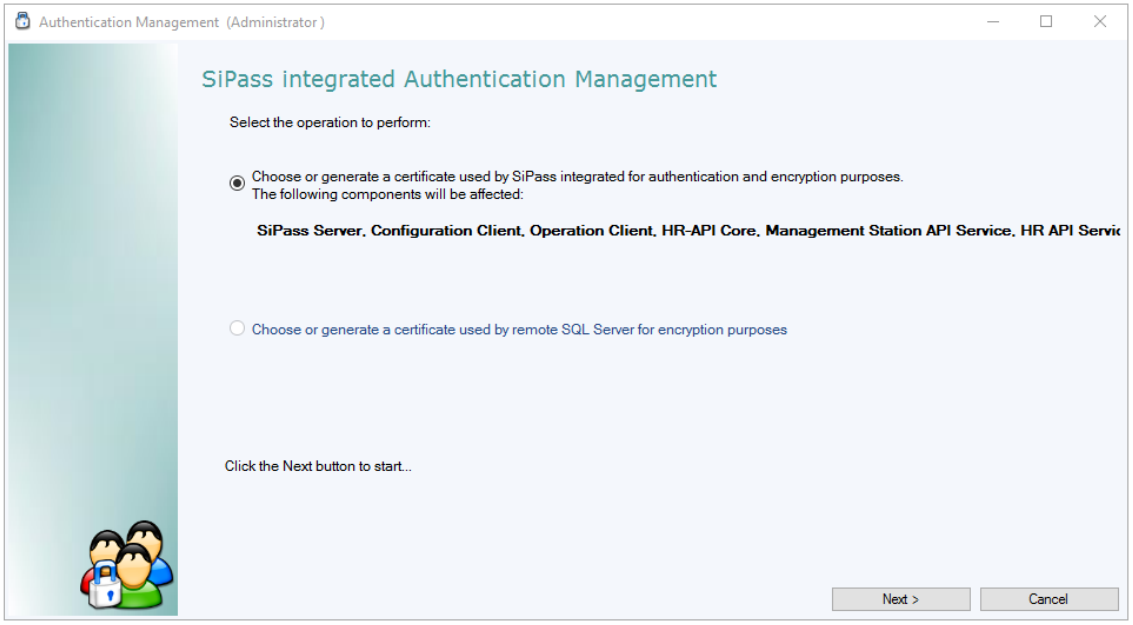


Die SiPass installation kann nun gestartet werden.



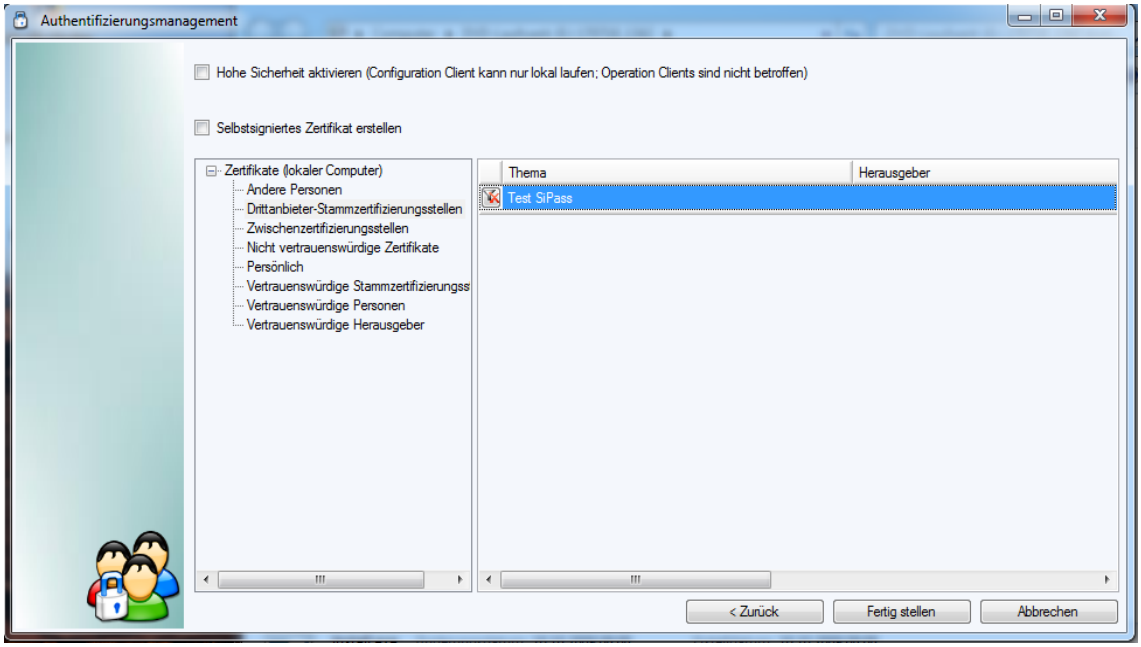
Die SiPass Installation wird nun die benötigten Programme installieren, dies kann einige Minuten dauern.

Über das SiPass Authentifizierungsmanagement können die Server-Zertifikate erstellt werden.
Das SiPass Authentifizierungsmanagement kann auch separat geöffnet werden, falls für eine Remote SQL Verbindung Zertifikate benötigt werden sollten.
(Bei einem externen SQL-Server siehe Kursunterlagen „SiPass with remote SQL“)



Auf den nächsten Seiten beschreiben wir zwei Zertifikat-Optionen:

1. Anwendung eines existierenden Maschinenzertifikats.
2. Generierung und Anwendung eines selbstsignierten Zertifikats.



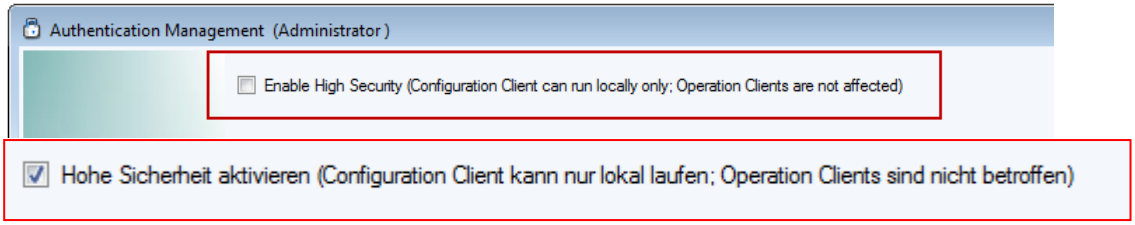
Sie können den SiPass integrated Server und die Remote Clients über ein Maschinenzertifikat oder ein selbstsigniertes Zertifikat installieren. Der grundlegende Prozess ist in beiden Fällen der Gleiche. Der Unterschied liegt in der Prüfung der Übereinstimmung der Zertifikate bei Server und Client-Computer.

Selbstsigniertes Zertifikat (s. Seite 18)
Diese können über verschiedene Tools installiert werden. Wir empfehlen den *SiPass integrated Authentifizierungsmanagement* Assistenten.

Bitte beachten: Die CA (Certification Authority) Signatur ermöglicht nicht die maximale Sicherheit. Die Methode ermöglicht allerdings die automatische Generierung und Zuweisung für Server und Clients mit minimalem Aufwand.

Maschinenzertifikate (s. Seite 19)
In der Windows Domäne einer Organisation wird jedem Computer von einer Zertifizierungsstelle ein eigenes Maschinenzertifikat zugewiesen und installiert. Dies gewährleistet maximale Sicherheit auf jeder Ebene.

Bitte beachten: Diese Methode wird empfohlen um ein Maximum an Sicherheit zu gewährleisten. Es erfordert zusätzlichen Aufwand des Benutzers das installierte Maschinenzertifikat im *Windows Certificate Store* zu suchen, den *Certificate Thumbprint* zu kopieren und diesen manuell im Authentifizierungsprozess bereit zu stellen.

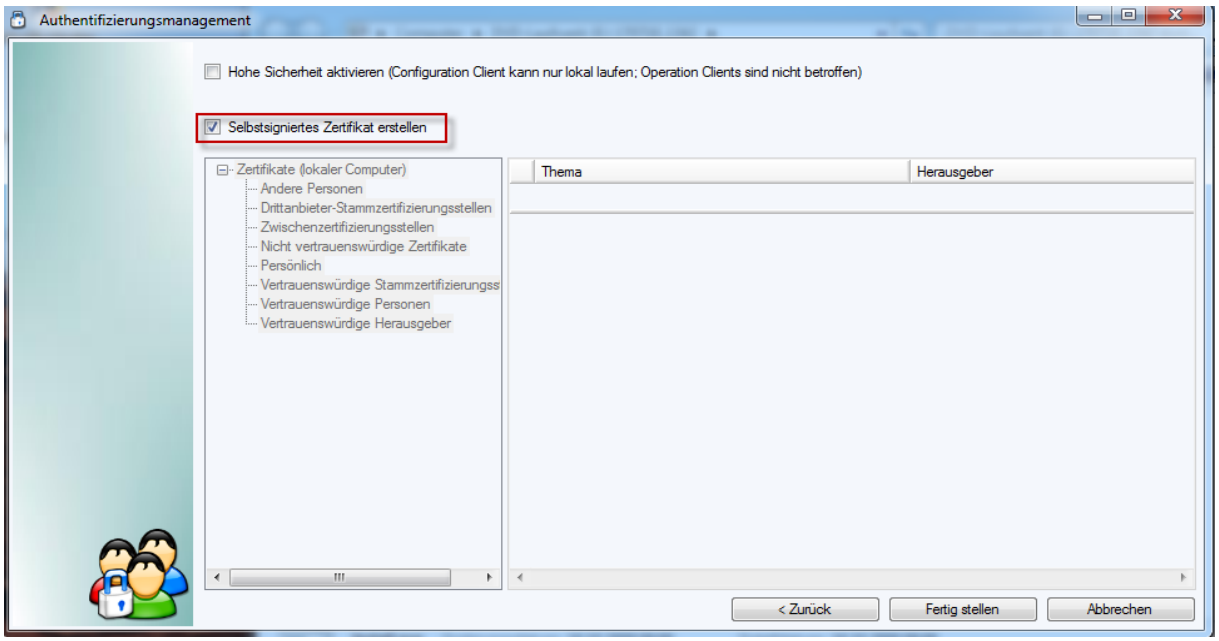


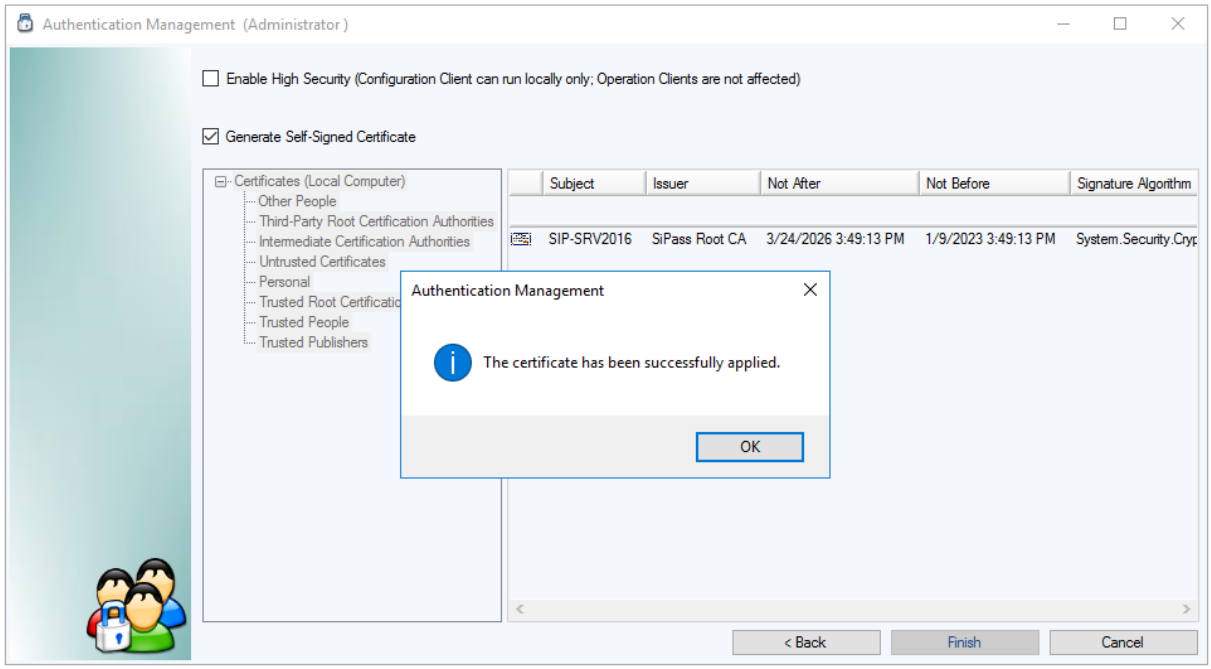
Wenn Sie *Hohe Sicherheit* aktivieren, kann der *Configuration Client* nur auf dem SiPass Server PC selbst betrieben werden und nicht auf einen Remote Client.

Verwendung von selbstsignierten Zertifikaten

Wählen Sie *Selbstsigniertes Zertifikat erstellen* und klicken Sie auf *„Fertig stellen“*. Die Installation startet, kann einen Moment dauern.

Ein neues Zertifikat wird generiert und für den SiPass Server und lokale Clients verwendet. Das in diesem Schritt generierte Zertifikat wird den vollständigen Computernamen in seinem Betreff enthalten.
Für die Remote Clients werden später Zertifikate auf Basis des selbstsignierten Zertifikats erstellt.



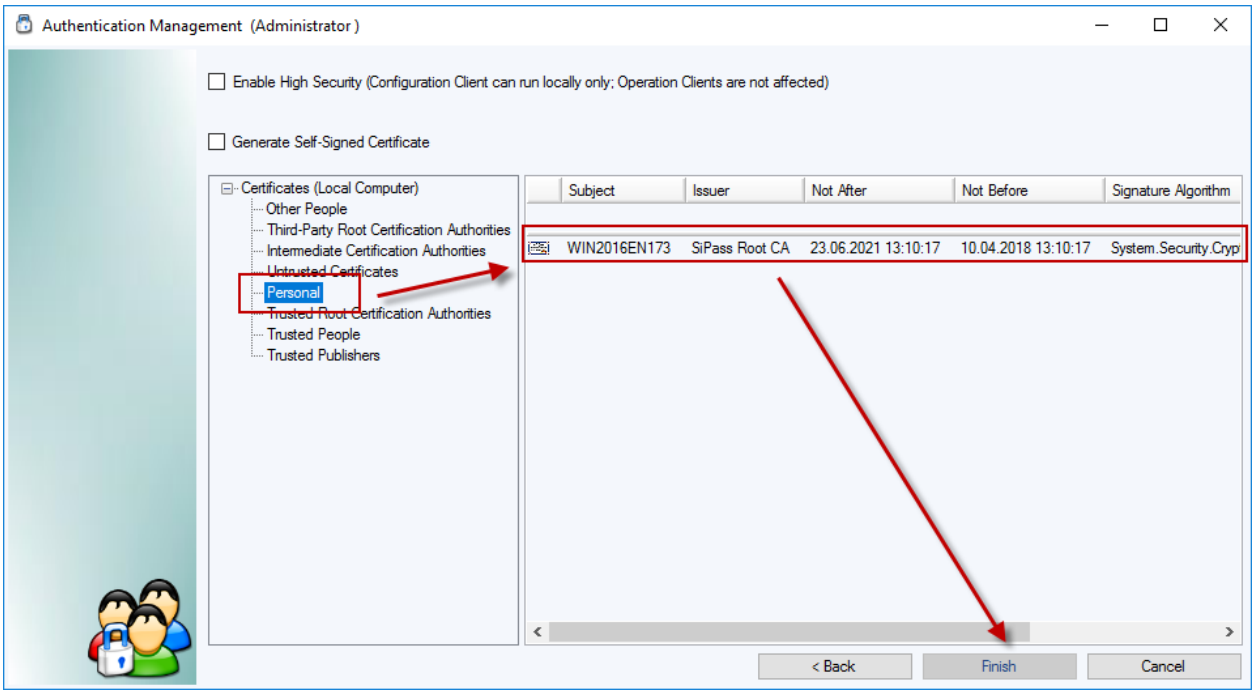


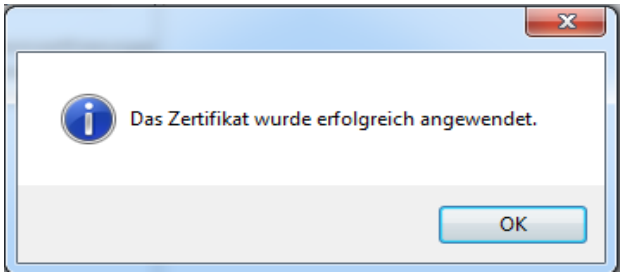
Verwendung von Maschinenzertifikaten

Die Baumstruktur auf der Liste im linken Fenster zeigt alle für Sie verfügbaren *Certificate Stores* an. Wählen Sie einen *Certificate Store* (Persönlich) im linken Fenster und anschließend das gewünschte Zertifikat im rechten Fenster aus.
(Das rechte Fenster zeigt alle Zertifikate, die im ausgewählten Store eingetragen sind.)

Bitte beachten: Nur Zertifikate mit einem privaten Schlüssel werden hier angezeigt.

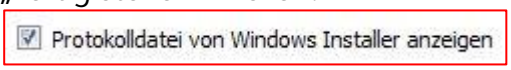
Klicken Sie auf *Fertig stellen* um das gewählte Zertifikat anzuwenden und mit der Installation zu beginnen. Das ausgewählte Maschinenzertifikat wird für die Installation auf den SiPass integrated Server und allen ausgewählten lokalen Clients angewendet.



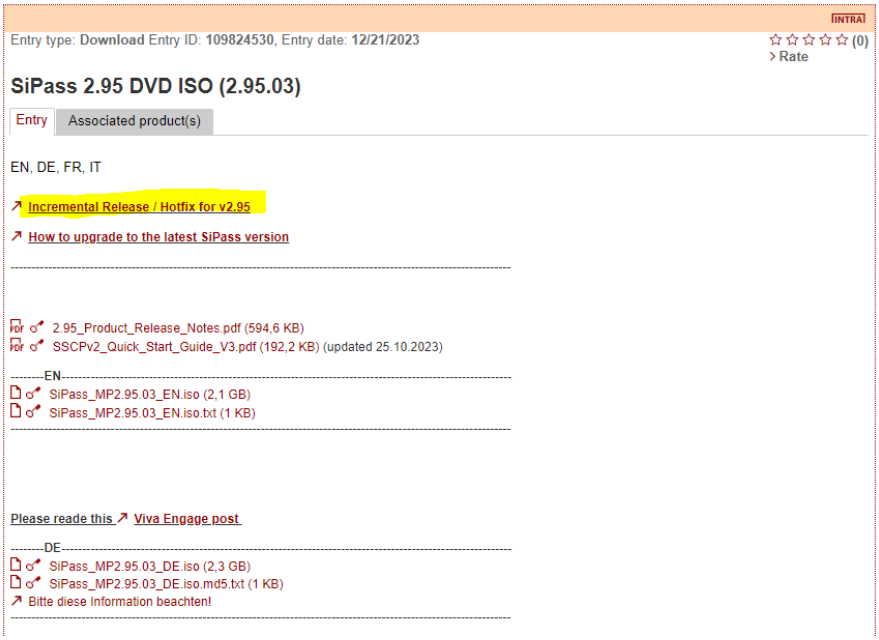


Das Setup von SiPass integrated wurde erfolgreich abgeschlossen.

Zur Anzeige der Log-Datei der Installation setzen Sie den Haken bevor Sie auf *„Fertig stellen“* klicken.



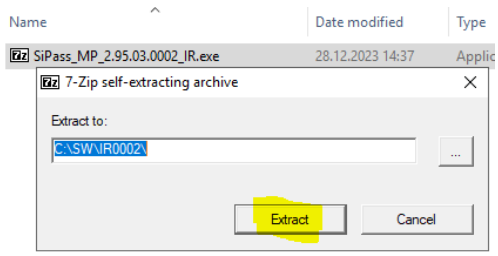
Wichtig:
Nicht vergessen, das letzte Patch zu installieren, bevor mit der Systemkonfiguration begonnen wird. Die Patches sind über SIOS, im SiPass 2.95 Kontainer, ladbar.
SiPass 2.95 DVD ISO (2.95.03) - ID: 109824530 - Industry Support Siemens

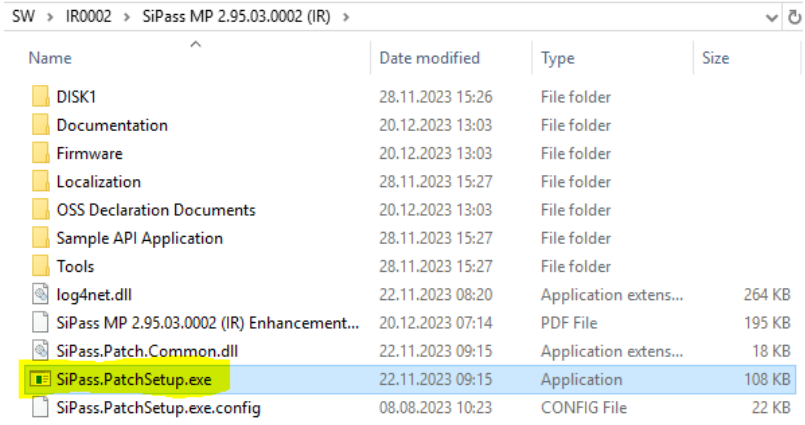


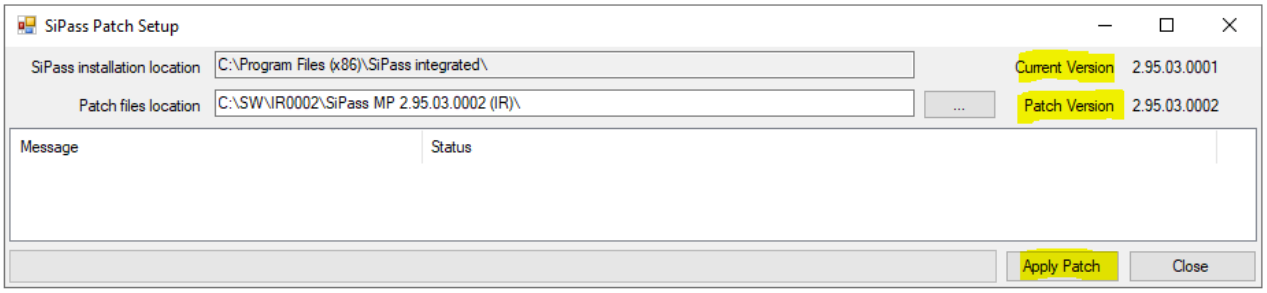
➔ Weiter mit Login, siehe Kapitel 12.

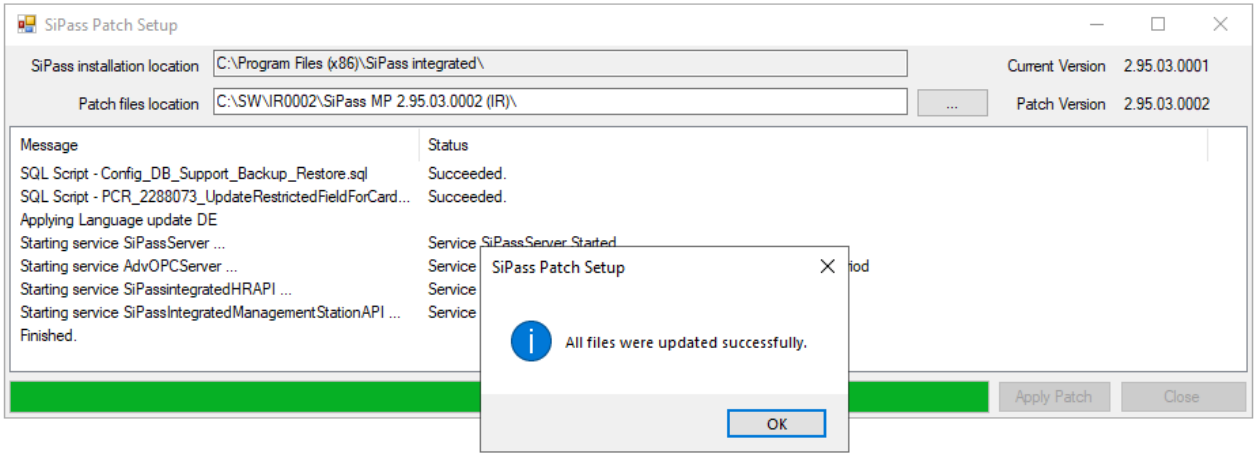
Beispiel: SiPass 2.95.03, Incremental Release 0002.

IR=Incremental Release; HF=Hotfix
Immer das letzte Release installieren, egal ob die letzte Version ein IR oder HF ist.









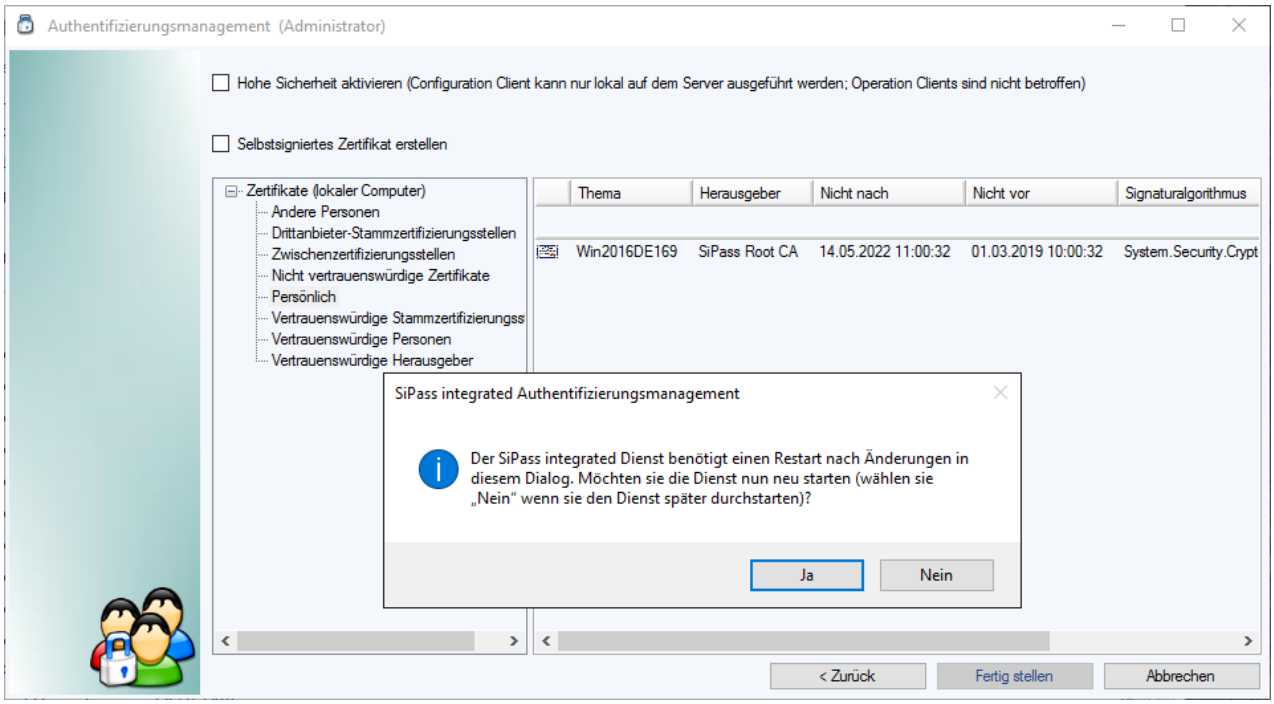
9. Zertifikate erneuern

Das Selbst signierte SiPass Zertifikat ist 1170 Tage gültig. 30 Tage vor Ablauf erhält der Benutzer beim Einloggen einen entsprechenden Hinweis, dass das/die Zertifikate erneuert werden müssen.

Dies wird mit Hilfe des *SiPass.CertificatePicker.exe* durchgeführt, dieses Tool befindet sich im SiPass integarted Installationsordner (C:\Program Files (x86)\SiPass integrated).

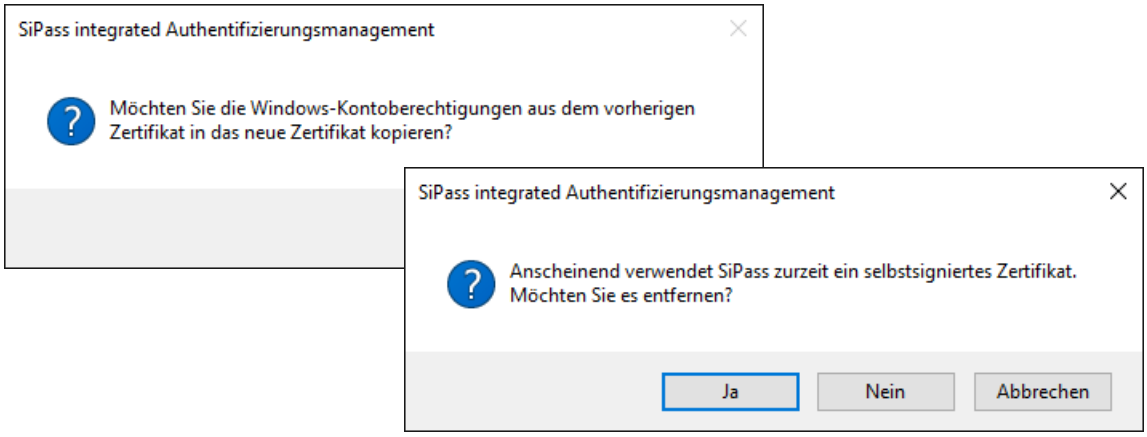
9.1 Selbstsigniertes Server Zertifikat erneuern

Starten sie das Tool mit rechts klick => als Administrator ausführen und klicken sie auf weiter.
Folgender Dialog erscheint.

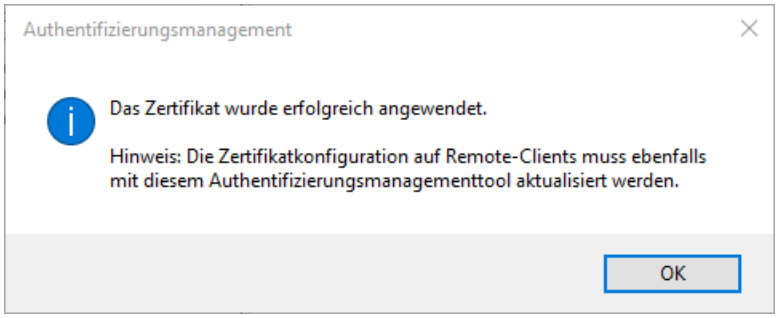


Empfohlen wird den SiPass Dienst zuvor zu stoppen.
Aktivieren sie danach die Option „Selbstsigniertes Zertifikat erstellen"

Folgende Options ist empfohlen mit ja zu bestätigen:



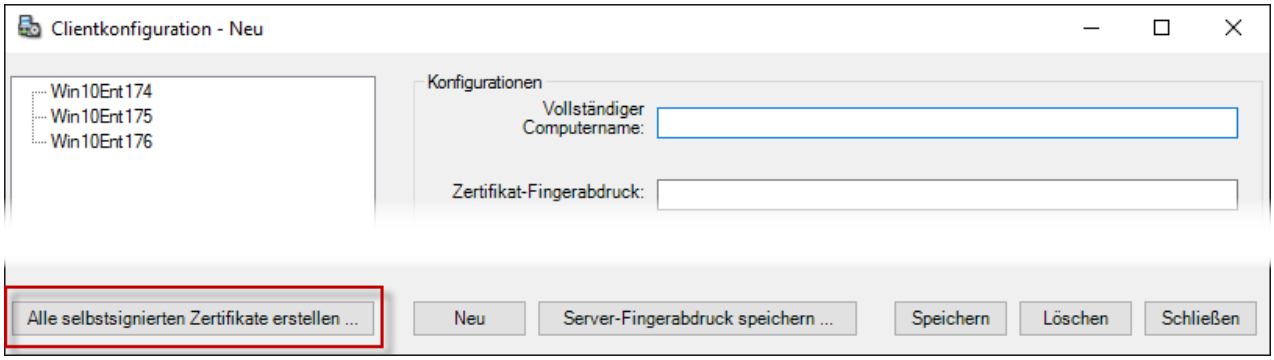
Ist der Vorgang erfolgreich wird dies mit folgendem Dialog bestätigt.



Ab diesem Zeitpunkt kann sie kein Remote Client mehr mit dem SiPass Service verbinden.
So seht als nächstes das Erneuern des Remote Client Zertifikates an.

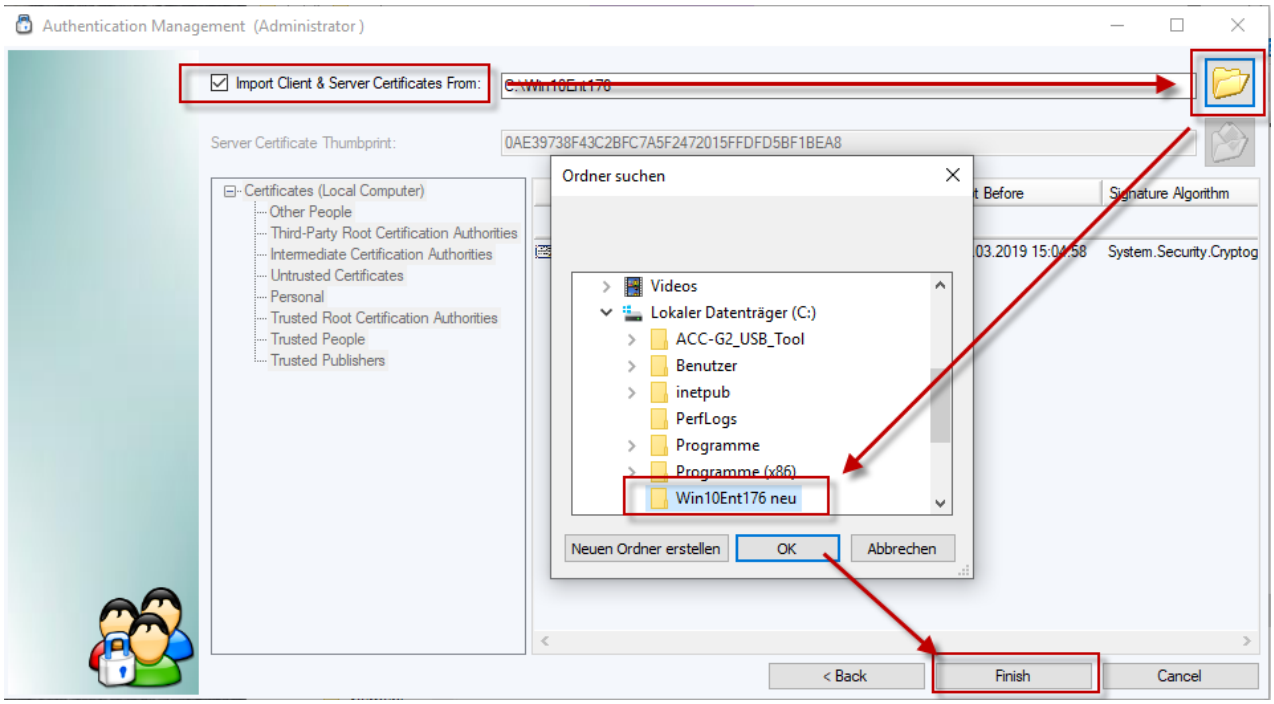
9.2 Remote Client Zertifikat erneuern (auf Basis des Selbst signierten Server Zertifikats)

Starten sie den „Configuration Client“ und öffnen sie den „Clientkonfiguration“ Dialog.
Es können für alle Clients auf einmal die neuen Zertifikate erstellt werden.

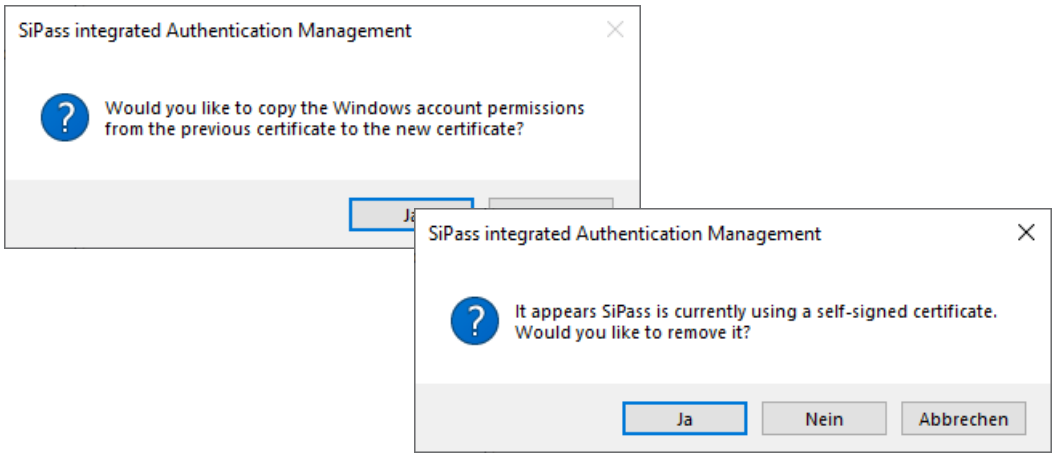


Wählen sie „Alle selbstsignierten Zertifikate erstellen...“ und erstellen sie einen neuen Ordner.
In diesem Ordner wird für jeden Remote Client ein weiterer Ordner angelegt.
Kopieren sie die neu Erstellten Remote Client Zertifikate auf die entsprechenden Remote Clients.

Starten sie nun auf dem Remote Client den SiPass.CertificatePicker.exe mit rechts klick => als Administrator ausführen und klicken sie auf weiter.



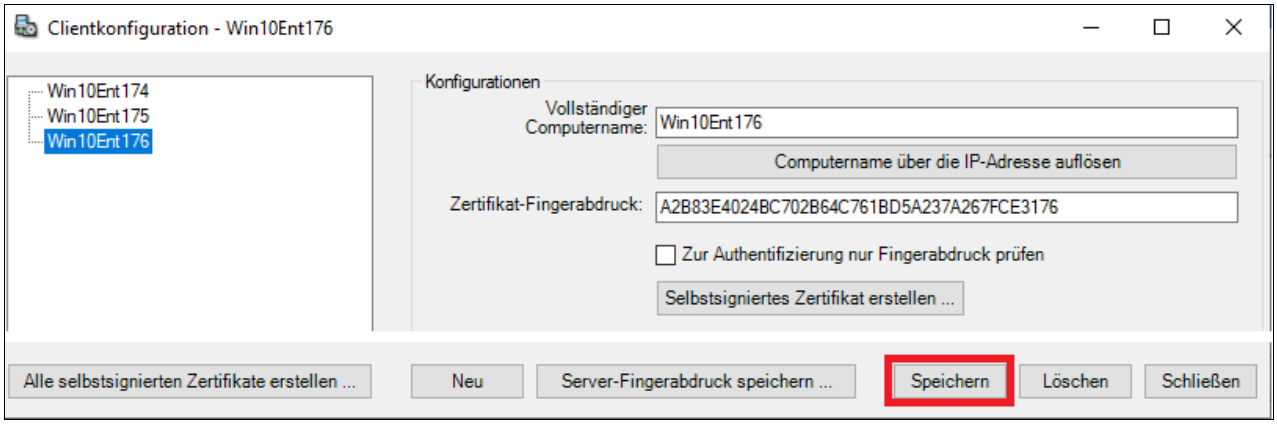
Nun muss lediglich das gerade kopierte Zertifikat ausgewählt werden und zwei mal mit Ja bestätigt werden.



Der danach angezeigte Zertifikat Fingerabdruck dient nur der Information, keine weitere Aktion notwendig bei Verwendung der selbst signierten Zertifikate.

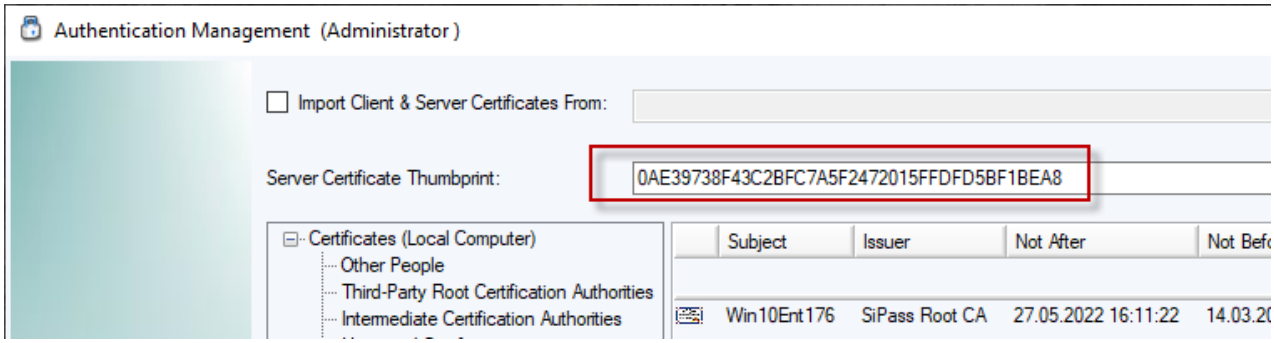
9.3 Maschinenzertifikate Erneuern

SiPass-Server seitig:
Auch hier wird der *SiPass.CertificatePicker.exe* verwendet, wie oben beschrieben.
Anstatt ein neues Zertifikat zu erzeugen oder zu importieren wird lediglich ein neues Zertifikat ausgewählt, das schon im Microsoft Zertifikat Store vorhanden ist.
Für den SiPass-Server ist das SiPass Server Zertifikat damit geändert.
Sind Remote-Clients vorhanden, muss für jeden Client in der „Client Konfiguration" der Fingerabdruck des neuen Client-Zertifikates eingetragen werden.



Remote Client seitig:
Auf der Remote Client Seite, ist das Auswählen des neuen Client-Zertifikates und das Hinterlegen, des neunen Server Zertifikat Fingerabdrucks, in einem Dialog zu finden.

SiPass.CertificatePicker.exe starten und das neue Client-Zertifikat auswählen und den Server Zertifikat Fingerabdruck eingeben. (siehe Bild unten)



Sollte der Server-Fingerabdruck (Thumbprint) nicht bekannt sein, kann dieser über die Clientkonfiguration auf dem Server, über die Taste „Server-Fingerabdruck speichern" in eine Datei gespeichert werden.

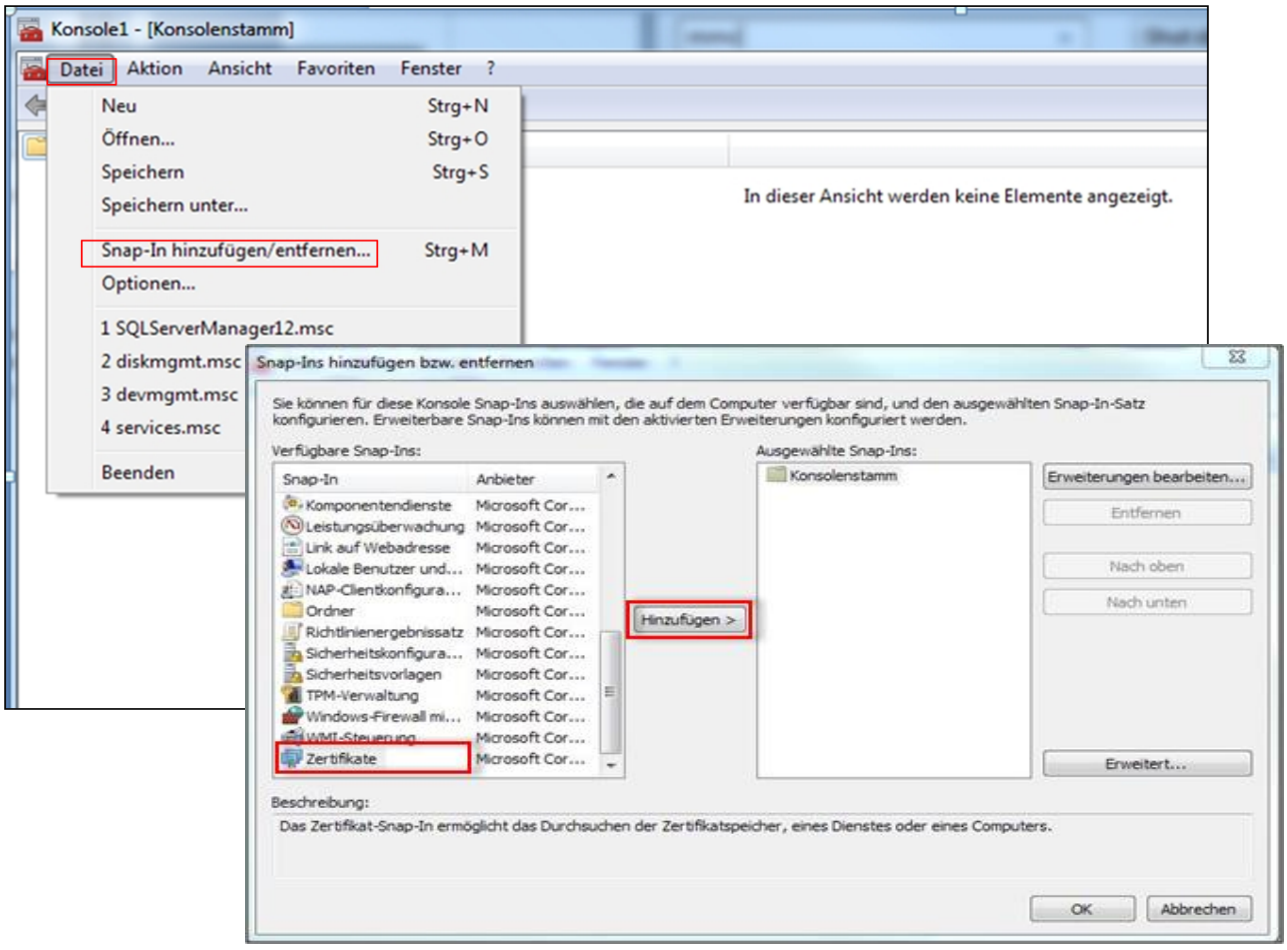
10. Verwaltung der SiPass Zertifikate

Für die nachfolgenden Schritte muss ein Windows Administrator Konto verwendet werden.

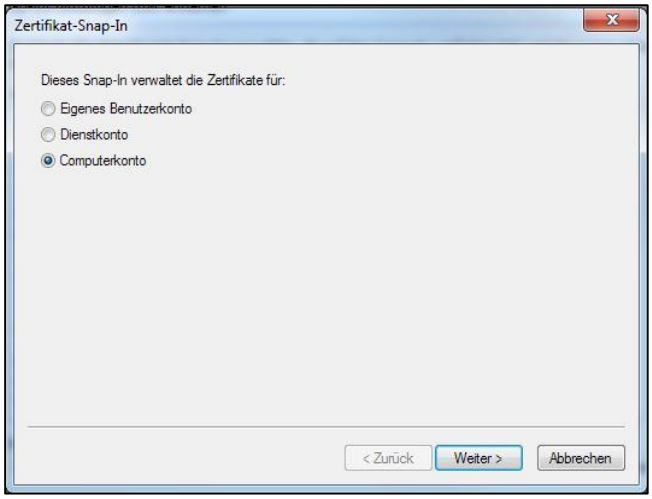
Um die SiPass Zertifikate zu verwalten, müssen Sie die MMC Konsole öffnen.

Über Ausführen (Windows-Taste + R) „mmc" eingeben und Return drücken.
Die „*mmc.exe*" Anwendung „Microsoft Management Console" wird geöffnet.

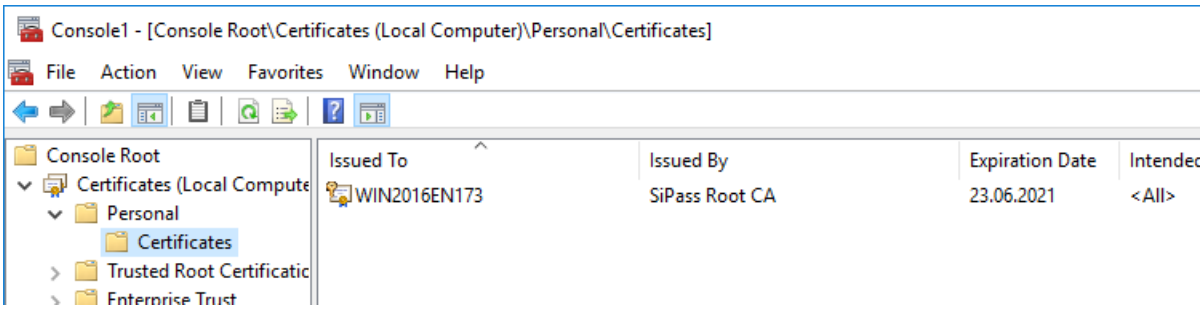
Klicken Sie auf Datei → Snap-In hinzufügen/ entfernen
→Wählen Sie *Zertifikate* und klicken Sie auf *Hinzufügen*.



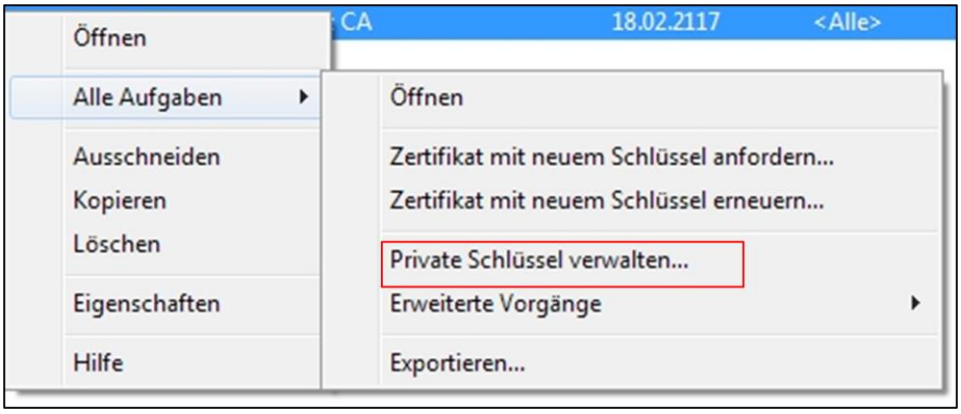
Wählen Sie im neuen Fenster ***Computerkonto*** aus und klicken Sie auf *Weiter*.
Wählen Sie ***Lokalen Computer*** und klicken Sie auf ***Fertig stellen***.



Im Konsolenstamm finden Sie unter ***Eigene Zertifikate*** alle persönlichen Zertifikate sowie die Zertifikate, die durch SiPass (*SiPass Root CA*) generiert wurden.



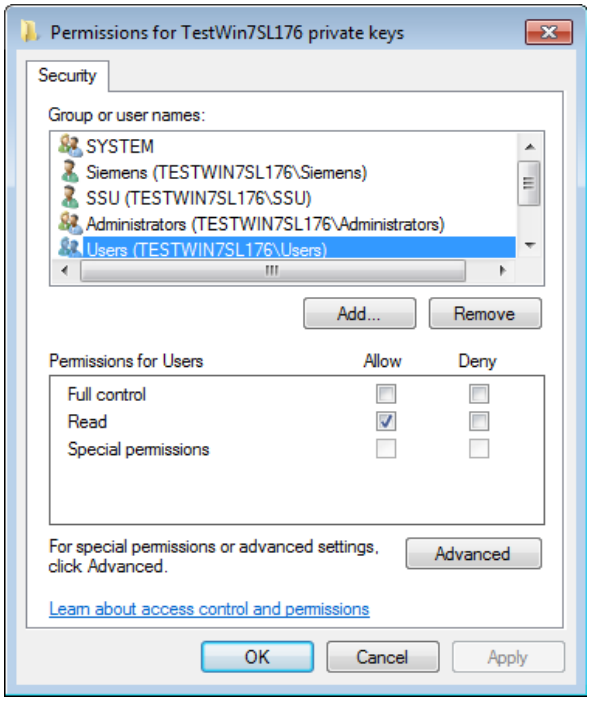
Um die Zugriffsrechte für die Benutzer auf die Zertifikate zu verändern, machen Sie einen Rechtsklick auf das entsprechende Zertifikat und wählen Sie *Alle Aufgaben → Private Schlüssel verwalten*...



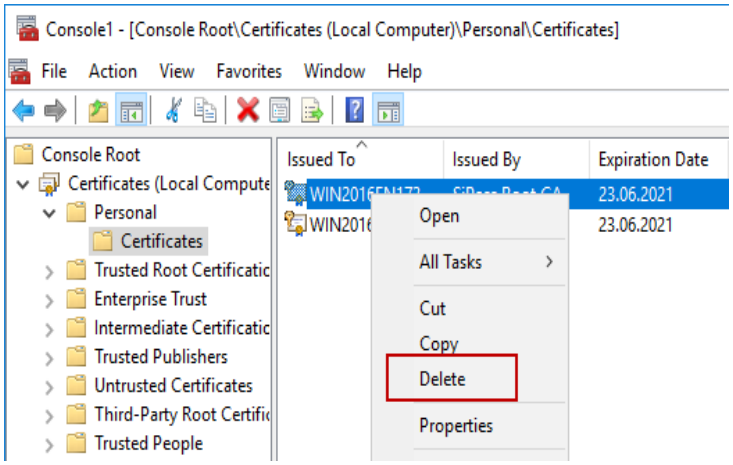
Im nächsten Fenster können Sie Benutzer / Benutzergruppen hinzufügen.

Es sind nur Leserechte erforderlich!

Mit diesem Schritt wird ein Benutzer hinzugefügt, der kein Mitglied einer vorhandenen Benutzergruppe oder kein Administrator ist.



Wenn die SiPass Installation scheitert, könnten mehrere SiPass Root Zertifikate in der *mmc*-Konsole aufgelistet sein. Sie können die nicht verwendeten Zertifikate mit einem Rechtsklick auf das Zertifikat löschen. Behalten Sie das aktuelle Zertifikat.

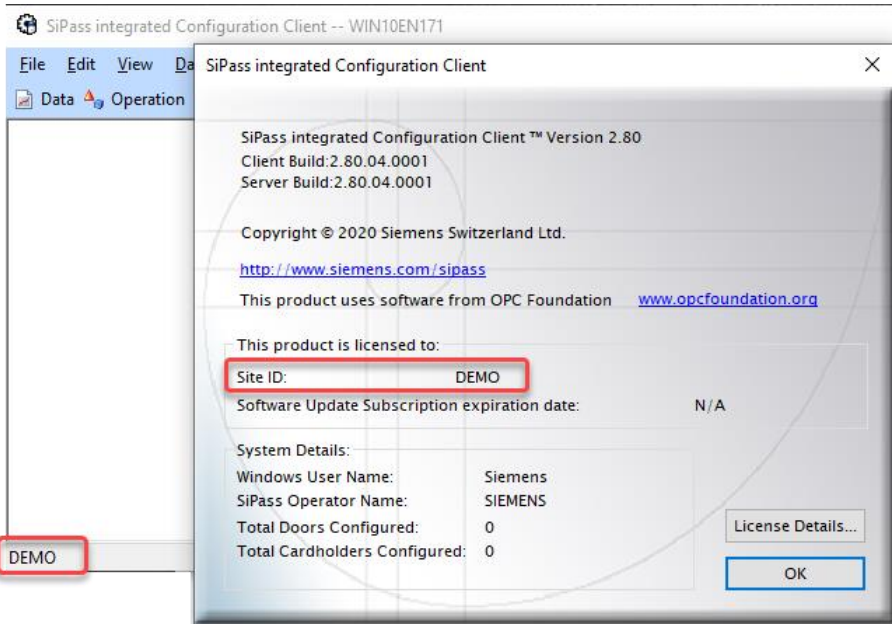


11. DEMO Installation

Jede SiPass integrated Installation, ist eine DEMO Installation.
Wurde LMU installiert und darüber die Lizenz aktiviert, verwendet SiPass die Funktionen entsprechend der Lizenz.

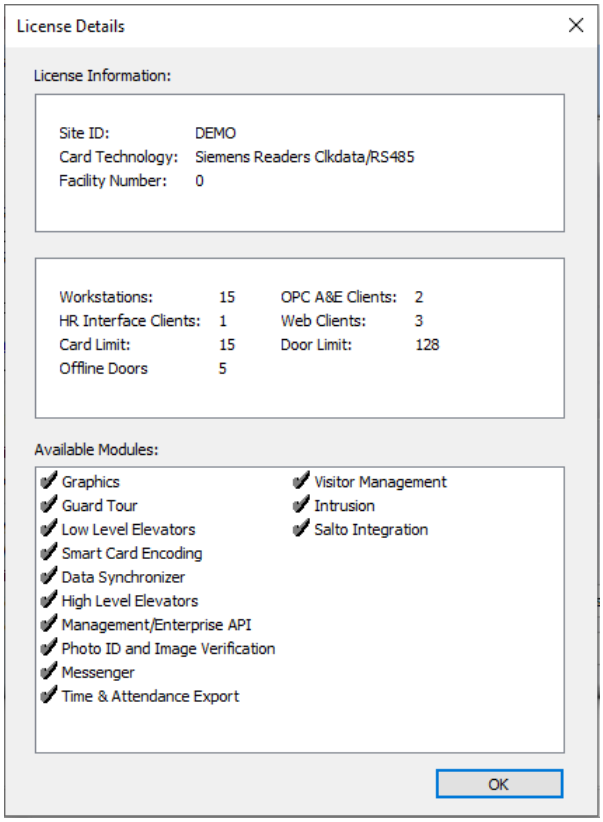
Im SiPass Configuration und Operation Client steht solange "DEMO", bis über LMU die CSID Lizenz aktiviert wurde.

SiPass kontaktiert LMU alle 10 Minuten ob Lizenzupdates Vorhanden sind.



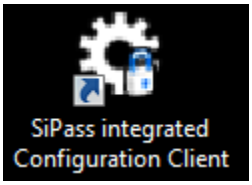
11.1 DEMO Features

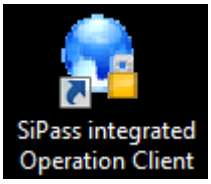
Dies sind die 2.80 DEMO Features (Hilfe -> Über -> Lizenz Details)



12. SiPass integrated Login

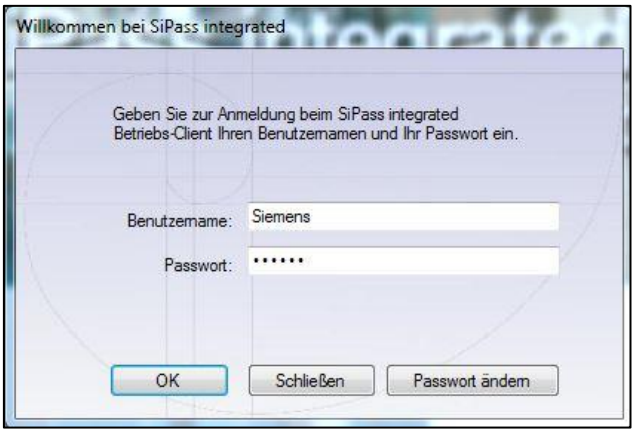
Seit MP 2.70 ist SiPass integrated in den *Configuration* und den *Operation Client* aufgegliedert.





Standard Benutzername und Passwort lauten:
Benutzername: *Siemens*
Passwort: *spirit*

Configuration Client Login



Operation Client Login

<u>Beachten Sie:</u>

Beim ersten Login am Operation Client **oder** Configuration Client (s. oben) muss das Passwort zwingend geändert werden.

Bitte erstellen Sie einen neuen SiPass Benutzer (Administrator) für den Kunden.

Geben Sie den Standard Login **nicht** an den Kunden weiter!

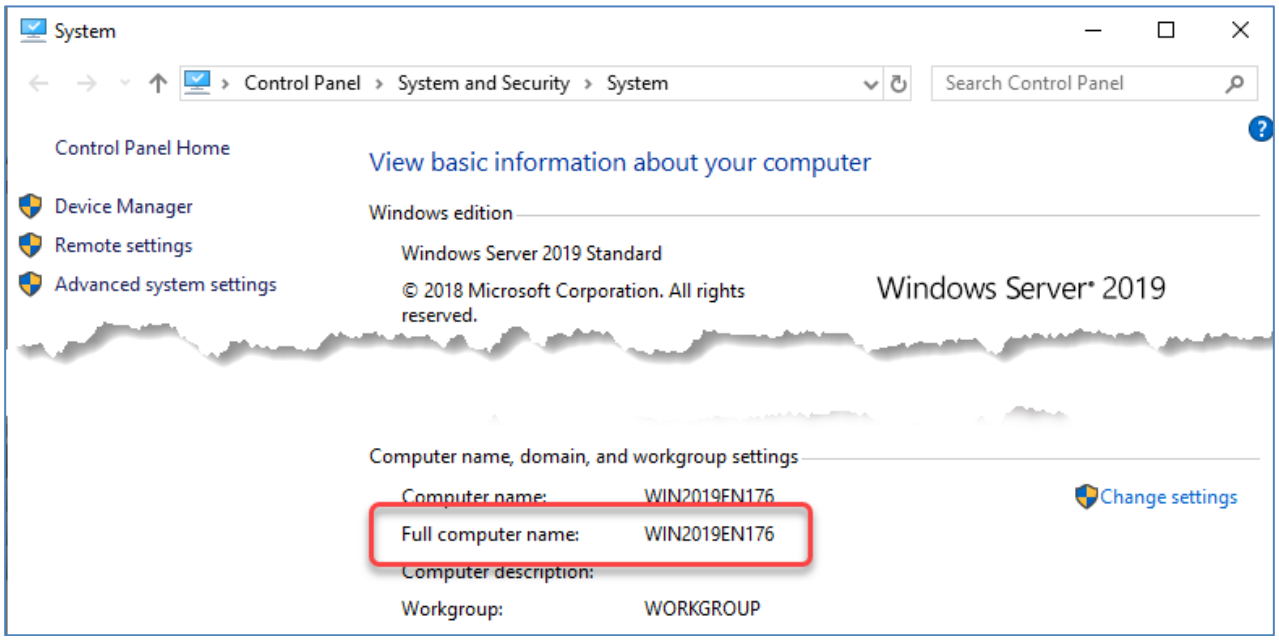
13. SiPass Client Installation

Die SiPass Remote Client Installation ist oft nicht so einfach.
Mit den Verbesserungen, in der Version 2.80, wie dem “Client Connectivity Tool”, werden unter anderem Fehleingaben bei der Verbindungseinstellung vermieden.

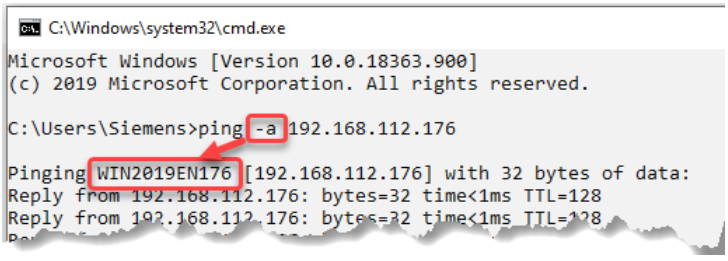
13.1. Client Connectivity Tool

Das neue Client Connectivity Tool befindet sich im Tools-Ordner jeder SiPass DVD.
Das Tool wird verwendet, um die Verbindung zwischen Remote Client und SiPass Server zu überprüfen. Das Tool sollte also vor der Remote Client Installation verwendet werden.
“SiPass.ConnectivityTool.exe” ist dazu auf den zukünftigen Remote Client zu kopieren und als Administrator zu starten.

Im Tool ist der volle Computername des SiPass Server PC einzutragen. Den Namen kann man sich über den Windows System Dialog anzeigen lassen. (Windows Taste + Pause).



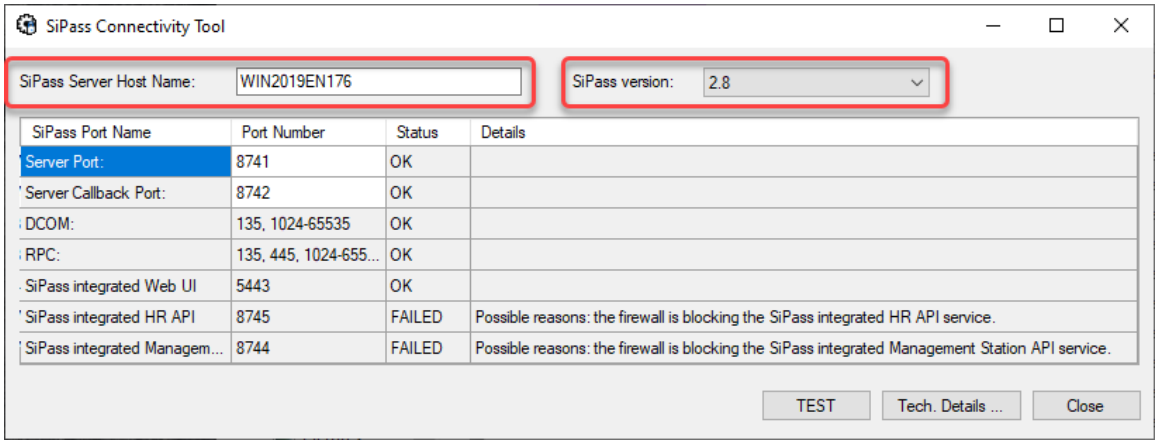
Alternativ über CMD Befehl: ping -a [server IP address]
Der korrekte SiPass Server name, muss im Client Connectivity Tool, für den Test eingetragen werden und natürlich dann, bei der tatsächlichen Remote Client Installation.



Arbeitsgruppen-Umgebung mit DNS-Funktion:

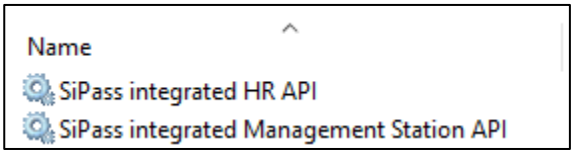
Falls die Bedienplätze über einen Internet-Router angeschlossen sind könnte der Computer Name und die Router ID verdreht sein.

Eingabe des SiPass Server PC Namen, Auswahl der korrekten SiPass Version und den „TEST“ starten.



Das Testergebnis oben zeigt einen nicht gestarteten HR und MS API Service.
Falls diese 2 Funktionen nicht Bestandteil der Lizenz sind ist das Ergebnis OK.

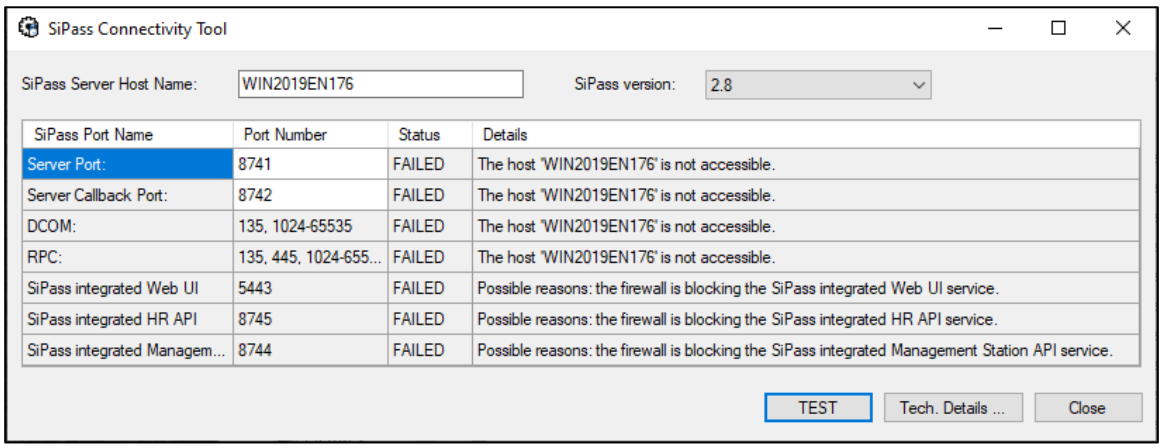
Falls HR und MS API Bestandteil der Lizenz sind, überprüfen ob die Dienste laufen und den Test wiederholen.



Wenn das Testergebnis in Ordnung ist kann mit der SiPass Remote Client Installation begonnen werden.

Test-Beispiel mit aktiver Firewall am SiPass Server:

An der Firewall wurden noch keine Regeln für SiPass hinterlegt. Wie das Testergebnis zeigt wird eine Verbindung zwischen Server und Client nicht möglich sein.
In diesem Fall am besten einen Ausdruck machen und mit der Kunden-IT besprechen.

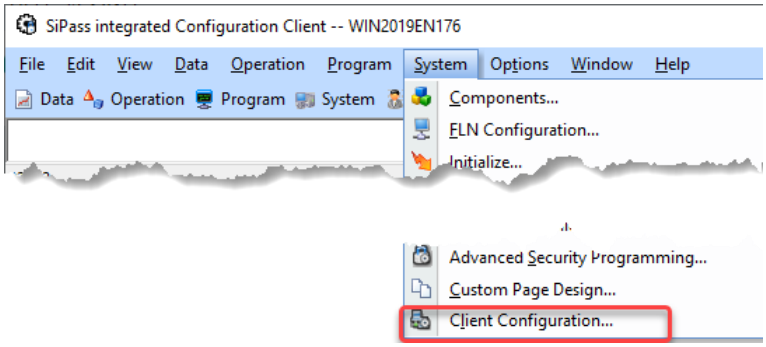


13.2 Remote Client setup

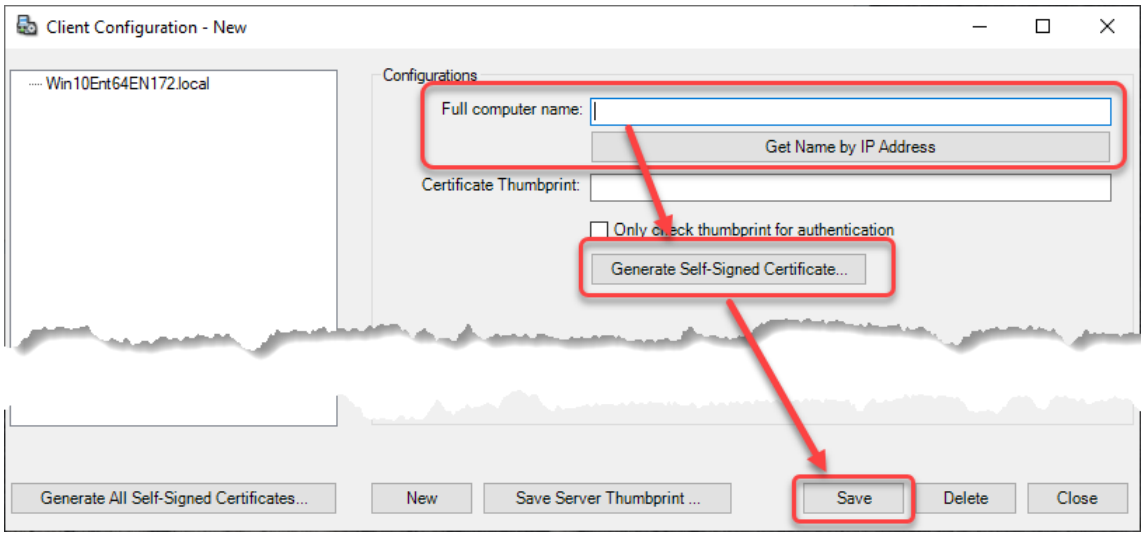
Hier beschreiben wir die Installation des Clients mit selbstsigniertem Zertifikat.
Die Zertifikate für die SiPass Remote Clients werden am SiPass Server erstellt.
Diese Zertifikate werden dann bei der Remote Client Installation verwendet / benötigt.

Nähere Informationen zur Verwendung von Maschinenzertifikaten entnehmen Sie bitte den Kapiteln 9 und 10, sowie dem Installations Manual auf der Produkt DVD.

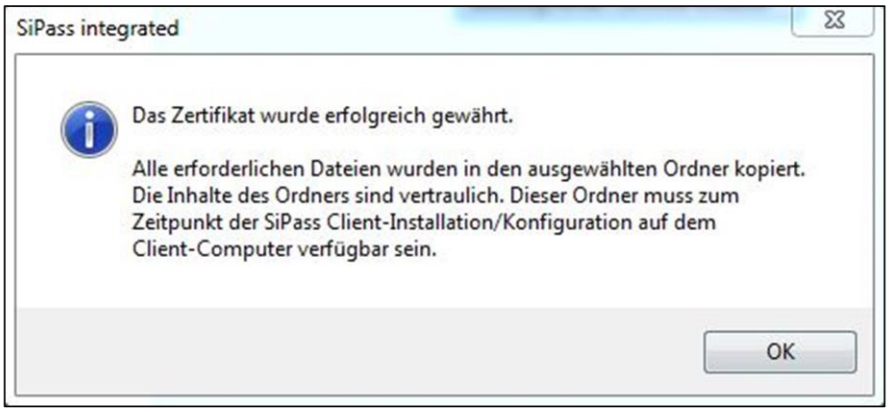
Öffnen Sie den *Configuration Client* auf dem SiPass Server und navigieren Sie im Menü System zu *Clientkonfiguration*.

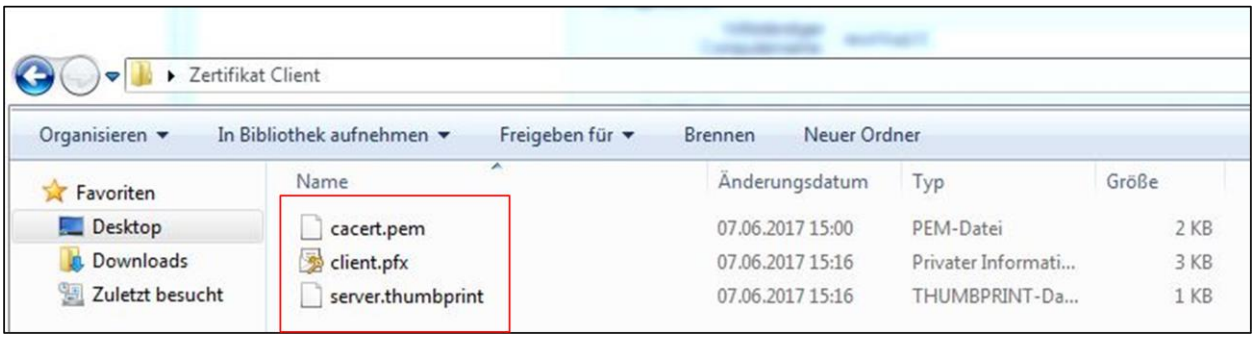


Seit der Version 2.80 ist es möglich die IP-Adresse des Client PC einzugeben.
Die SiPass Client Konfiguration, sucht über die IP, den richtigen Computernamen.
Danach auf *Selbstsigniertes Zertifikat erstellen klicken*.
Alternativ kann der Computernamen des SiPass Client PC auch manuell eingetragen werden und danach auf *Selbstsigniertes Zertifikat erstellen geklickt* werden.
Danach auf „Sichern" drücken und einen leeren Ordner auswählen, in dem die Zertifikate abgelegt werden sollen. (immer eigenen neuen Ordner anlegen für jeden Client).

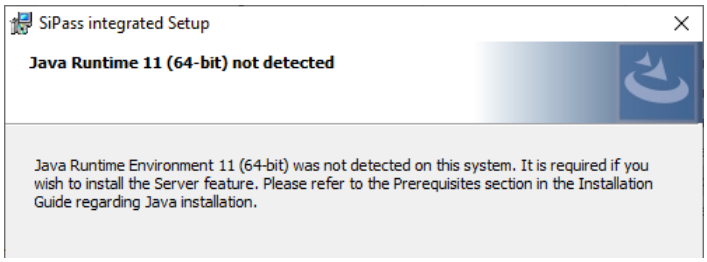


SiPass erstellt das Client Zertifikat sowie den *Server Thumbprint* in dem von Ihnen ausgewählten Ordner.
Dieser Ordner muss vom Remote Client Computer aus erreichbar sein.
Sie können den Ordner entweder manuell auf den Client Computer kopieren, ihn über ein Netzlaufwerk teilen oder über Remotezugriff vom Server Computer aus auf den Client Computer zugreifen.
Nachdem Sie das Zertifikat genutzt haben, stellen Sie sicher, den Ordner dauerhaft zu löschen. Dieser Schritt dient der Informationssicherheit.

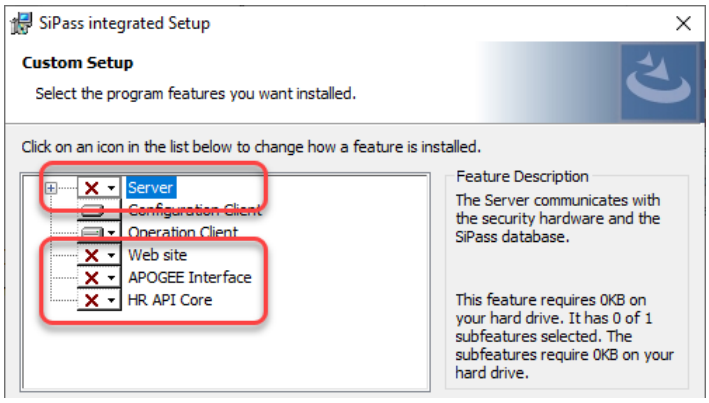




Installieren Sie den SiPass Client auf die gleiche Weise wie den SiPass Server, mit der gleichen Installationsdatei.
LMU und Java Runtime wird nicht benötigt am SiPass Client PC.
Die Java-Information unten kann also ignoriert werden.

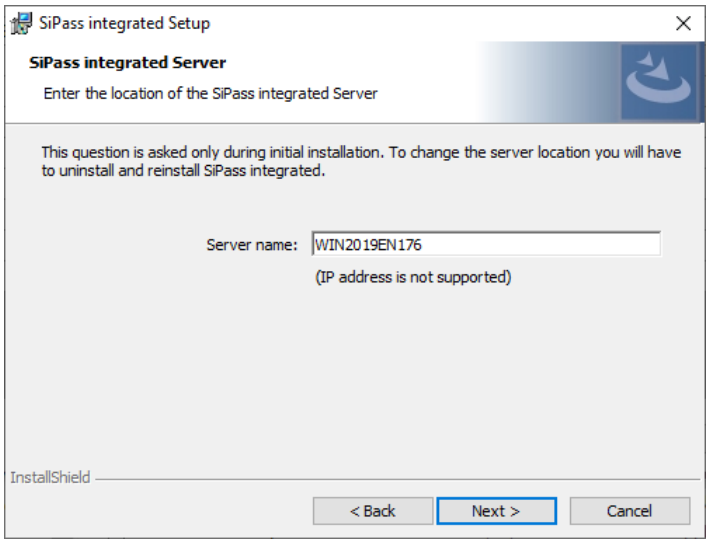


Damit keine SiPass Server, sondern eine SiPass Client Installation durchgeführt wird, **muss** der „*Server*“, „*Webseite*“ und „HR API Core“ deaktiviert werden.
Es sind also nur noch die Clients für die Installation aktiv.



Achtung:

Im “Server name” Feld ist der komplette name des SiPass Server PC einzutragen.
(siehe 13.1. Client Connectivity Tool)

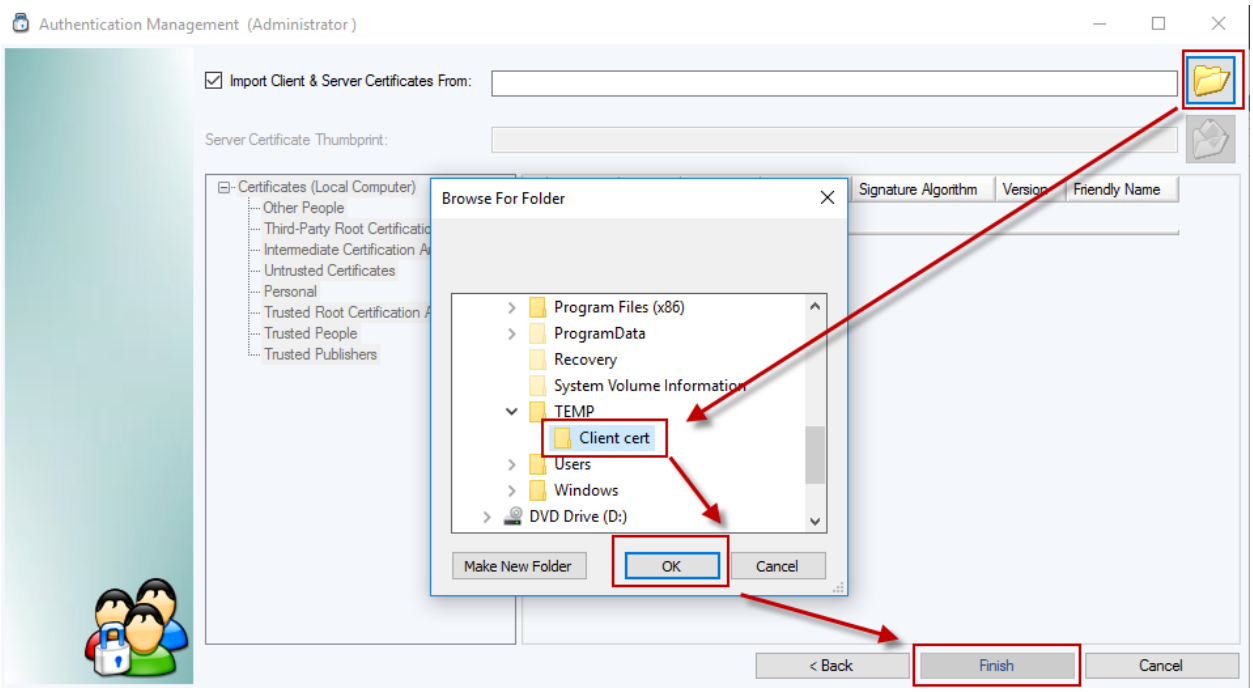


SiPass Client Installation in einer Arbeitsgruppen Umgebung:
Alle Windows Benutzer des Client PCs müssen innerhalb des SiPass Server PCs als Windows Benutzer existieren. (Das Passwort für den Windows Benutzer muss gesetzt sein.)
Info: Wenn der Windows Benutzer dem SiPass Server PC nicht bekannt ist, startet der SiPass Client nicht. (Folgende Fehlermeldung erscheint: „*Der Server startet noch oder ist nicht verfügbar.*“)

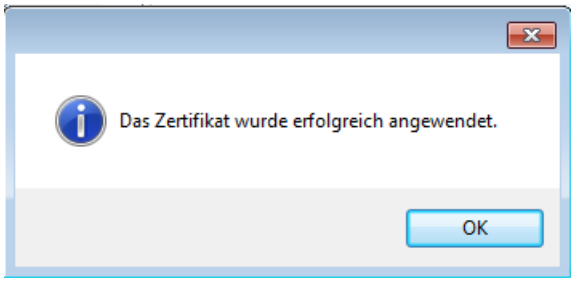
Wenn der SiPass Client innerhalb einer Domäne installiert wird:
Der Windows Benutzer des SiPass Client PCs muss mindestens lokale Benutzerrechte auf dem Windows SiPass Server PC haben.

Das *SiPass integrated Authentifizierungsmanagement* wird angezeigt.

Wählen Sie im *Authentifizierungsmanagement* den Ordner, der das Client Zertifikat beinhaltet und drücken Sie auf *Fertig stellen*.
(Das Zertifikat wurde zuvor am SiPass Server erstellt, siehe 13.2)



Das Zertifikat ist nun dem SiPass Client zugewiesen.

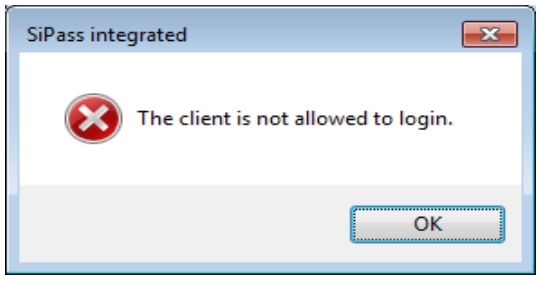


Das Setup des SiPass integrated Client wurde erfolgreich abgeschlossen.

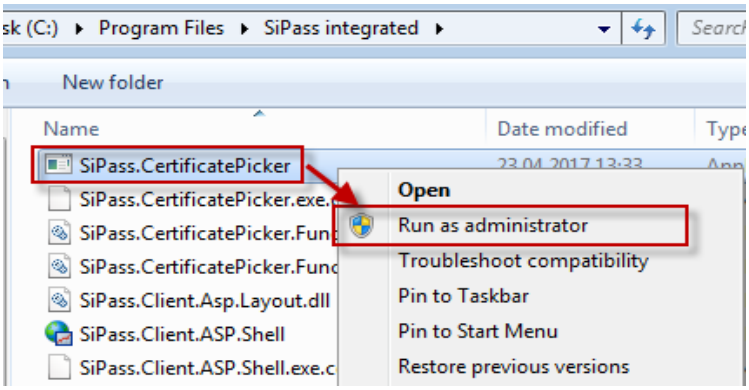
Der Client benötigt die gleich Patch Version wie der Server.
Der Client kann ansonsten nicht verwendet werden.

13.3 Client Zertifikat falsch/abgelaufen

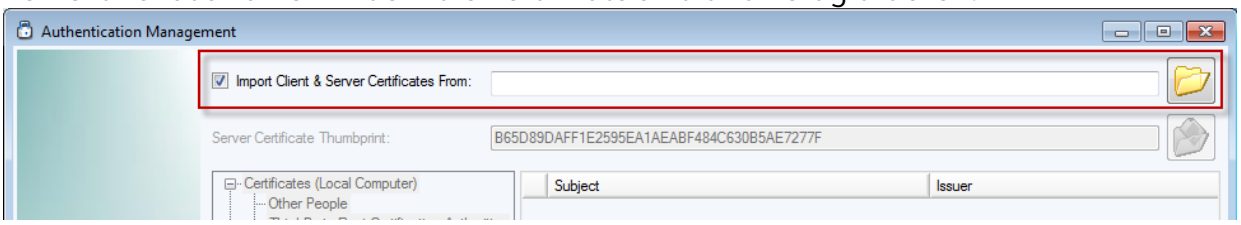
Falls das Zertifikat nicht zum Server Zertifikat passt, wird die folgende Fehlermeldung ausgegeben.



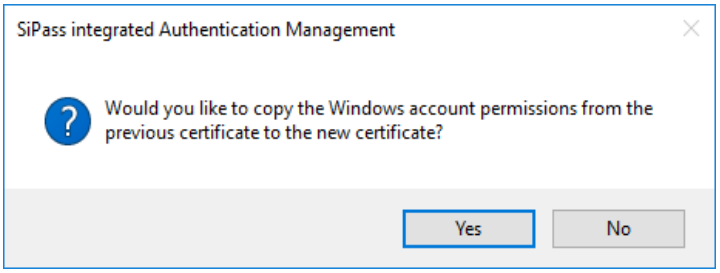
In diesem Fall ist der SiPass.CertificatePicker.exe “als Administrator” zu starten und das korrekte Zertifikat auszuwählen.
Der SiPass.CertificatePicker.exe befindet sich im SiPass integrated Ordner.



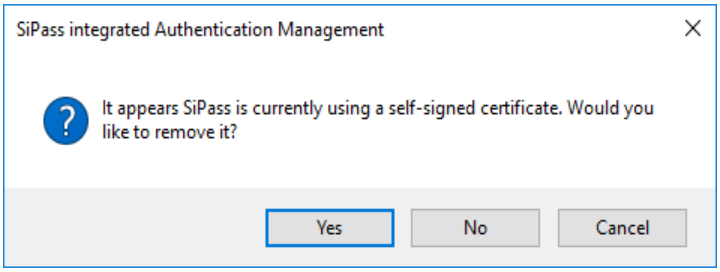
Den Ordner auswählen in dem die Zertifikate sind und Fertig drücken.



Die Windows account Einstellungen sind vom alten in das neue Zertifikat zu übernehmen / kopieren.

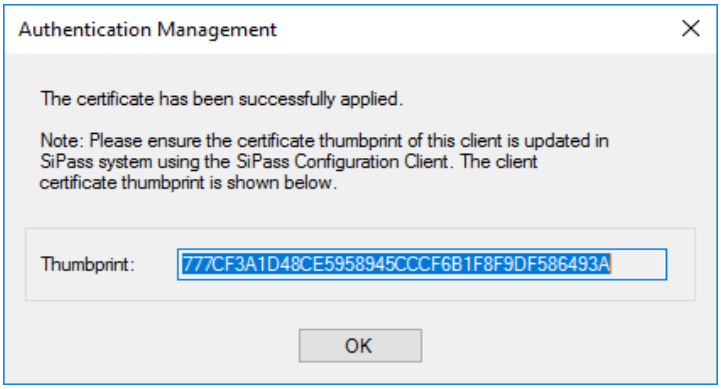


Das alte Zertifikat (wird ja nicht mehr benötigt) Ist zu löschen.



Der Client Zertifikat Thumbprint wird nur bei Verwendung von Maschinenzertifikaten benötigt. (wird immer angezeigt)

Wenn das neue Zertifikat von SiPass generiert wurde, ist keine weitere Aktion mit dem Client Thumbprint notwendig!



14. Update der SiPass Funktionen

Bis zur Version 2.76 war es nötig eine neue Lizenz zu bestellen und diese über den SiPass Setup über „Programm ändern" einzugeben.

Seit der Version 2.80 verwendet SiPass das LMU und der Lizenzupdate ist einfacher. Wurde die Bestellung durchgeführt, kann die neue Lizenz über das LMU aktiviert werden. Nach 10 Minten ist die neue Funktion oder Erweiterung automatisch in SiPass aktiv.

15. SiPass integrated Upgrade Pfad

Ein Upgrade von älteren SiPass integrated Version auf die 2.90 ist möglich.

Welche Versionen direkt aktualisiert werden können und bei welchen Versionen zusätzliche Schritte notwendig sind, kann im „*SiPass integrated Installation Guide*" der offiziellen DVD eingesehen werden.

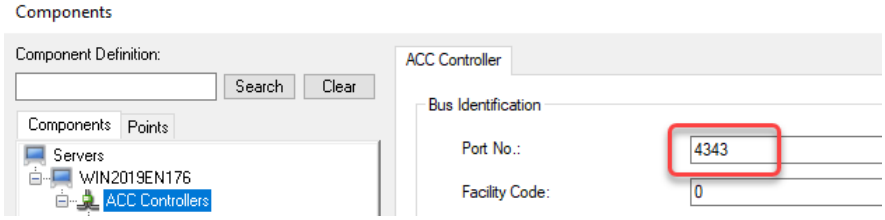
	TARGETTES UPGRADE VERSION											
Current Version	**SiPass integrated Version**	**MP 2.40 2.50**	**MP 2.60**	**MP 2.65**	**MP 2.70**	**MP 2.75**	**MP 2.76**	**MP 2.80**	**MP 2.85**	**MP 2.90**	**MP 2.95**	**MP x.xx**
	MP 2.35	✓	X	X	X	X	X	X	X	X	X	X
	MP 2.40	✓	X	X	X	X	X	X	X	X	X	X
	MP 2.50		✓	✓	X	X	X	X	X	X	X	X
	MP 2.60			✓	✓	✓	X	X	X	X	X	X
	MP 2.65 SP4				✓	✓	✓	✓	✓	✓	✓	✓
	MP 2.70					✓	✓	✓	✓	✓	✓	✓
	MP 2.75						✓	✓	✓	✓	✓	✓
	MP 2.76							✓	✓	✓	✓	✓
	MP 2.80								✓	✓	✓	✓
	MP 2.85									✓	✓	✓
	MP 2.90										✓	✓

Das Support Center bietet auch einen "**Database Upgrade Service**" an.
Besonders wenn ältere Systeme einen Upgrade bnötigen ist dies sinnvoll.
SAP Bestellnummer P54511-P200-A10 "SiPass Uprade Service".

15.1 SiPass Versions Upgrade – Schritt für Schritt:

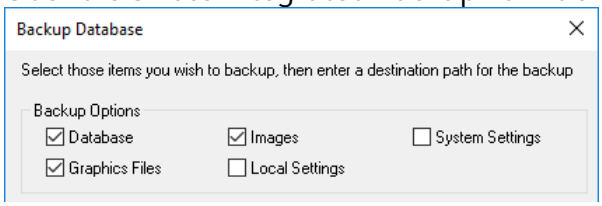
Eine neue SiPass Version benötigt eine neue Lizenz.
Die Lizenz-Bestellung ist ab der Version 2.80 allerdings ohne Order-Form.
Zuerst muss eine CSID (Nummer) generiert werden. Dies geschieht über das LMS Cockpit (https://lmscockpit.bt.siemens.com).
Danach kann der Upgrade auf z.B. SiPass 2.90 über SAP bestellt werden.
Damit die richtigen Positionen bestellt werden, steht als Hilfe ist ein Excel-Migrationstool zur Verfügung.
Nach manueller Überprüfung durch die HQ-Logistik sendet das LMS-Tool eine eMail an den Besteller. Auf der Anlage kann die Lizenz dann über LMU aktiviert werden.
Falls Zwischenlizenzen für die Migration benötigt werden, weil ein direktes Upgrade nicht möglich ist, werden diese separat an den Besteller gesendet.

1. Kommunikation zu den ACC's unterbrechen. ACC Port ändern => alle ACCs offline

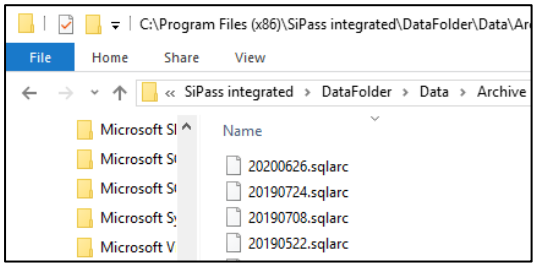


Dies ist notwendig da die ACC's ansonsten weiterhin Systemereignisse an den Server senden, die dann bei der Migration verloren gehen würden.
Die ACC's speichern nun alle Ereignisse, bis der Upgrade erfolgreich beendet ist.

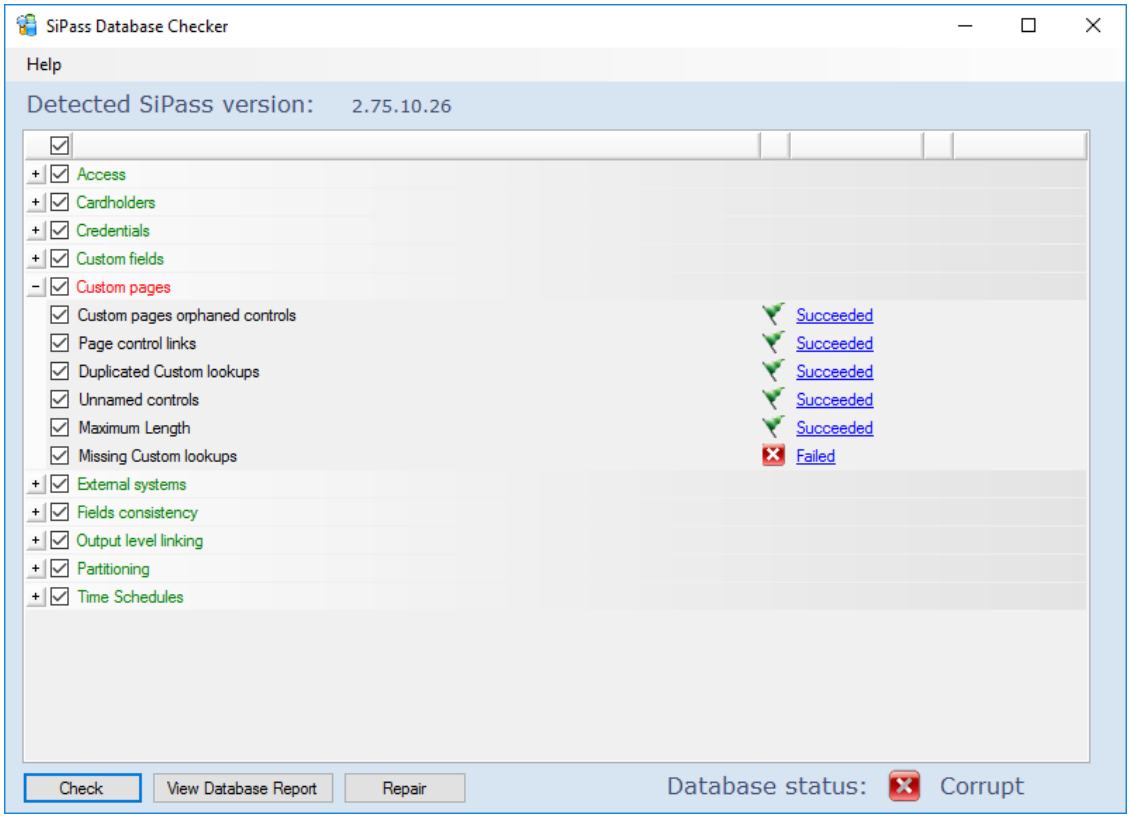
2. Über die SiPass integrated Backup Funktion, ist ein Backup zu erstellen.



Dieser Backup wird später benötigt um alle Daten wieder herzustellen.
Immer einen neuen leeren Backup-Ordner verwenden, keinen existierenden verwenden, da dieser überschrieben wird.
Die Ereignisanzeige (*Audit Trail)* ist im Datenbank Backup nicht enthalten.
Daher sind die SQL archive files (date.sqlarc) an einen sicheren Platz zu schieben oder kopieren, außerhalb des SiPass integrated Ordners. Der Standardspeicherort dieser Dateien lautet: C:\Program Files\SiPass integrated\DataFolder\Data\Archive



3. Über das DB check tool ist die Datebank zu überprüfen und falls notwedig zu reparieren. Das DB check tool findet man im Tools Ordner jedes SiPass DVD image. Falls der Check einen Fehler anzeigt kann die Repair Option verwendet werden.

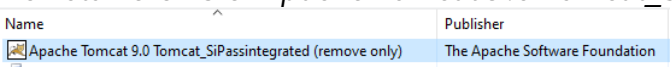


Nach dem "Repair" einen neuen DB backup erstellen (in neuem Ordner)
Falls der Fehler nicht behoben werden kann, ist die Hotline zu kontaktieren und das DB check File und falls möglich, den DB Backup zur Verfügung zu stellen.

4. Schließen Sie alle laufenden Programme.

5. Deinstallieren Sie die aktuell installierte SiPass Version über die SiPass Installation und der Option „*Entfernen*". (als Administrator ausführen)

6. Deinstallieren Sie "*Apache Tomcat 9.0 Tomcat_SiPassintegrated*"



Wird die Applikation nicht gelöscht, funktioniert der Web-Client Activity Feed und die Area Monitoring Anzeige nach der SiPass Installation nicht.

7. Überprüfen Sie, ob das Betriebssystem, die installierte SQL Version und das Service Pack mit der SiPass Version kompatibel sind.

8. LMU auf dem SiPass Server Installieren und die Lizenz aktivieren.

9. Neue SiPass Version installieren. (Als Administrator ausführen)

10. Falls SiPass Patches verfügbar sind, diese jetzt installieren.

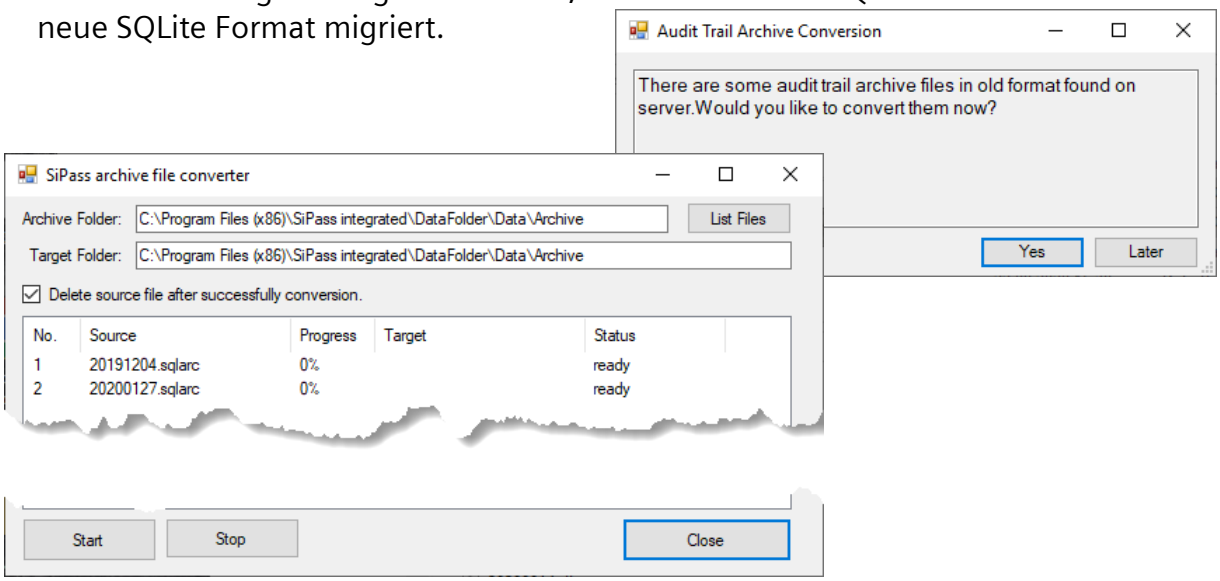
11. SiPass integrated Configuration client starten und den zuvor erstellten Backup jetzt wieder herstellen. (Restore)

12. Nach der Datenbank Wiederherstellung ist der PC neu zu starten.

13. Anmelden und die Daten mit dem Kunden überprüfen.

14. Einen neuen Datenbank-Backup mit der neuen SiPass Version erstellen.

15. Die zuvor kopierten SQLARC Files wieder in den Standard-Ordner kopieren.
    Wenn der Config-Client gestartet wird, werden die alten SQLARC Files in das neue SQLite Format migriert.



Empfolen wird mit den letzten 3 Tagen der SQLARC Files zu starten.
Nachdem bekannt ist wie viel Zeit für 3 Tage benötigt wird, können nun die anderen SQLARC-Files, je nach verfügbarer Zeit, migriert werden.
Jedesmal wenn der Config Client gestartet wird, schaut dieser nach SQLARC Files un bietet dann die Migration an.
Die Reports funktionieren erst nach Migration in das neue SQLite format.

16. Nun ist die Kommunikation zu den ACC's wieder herzustellen, ACC-Port zurückstellen.
    Alle Geräte mit der passenden Firmware laden. (Erklärt in der SiPass HW-Installation)
    Die passende Firmware ist auf der original SiPass DVD.

Achtung Info zu Backup / Restore:
Ab 2.80 wird nicht mehr die Optionen "System Settings" and "Local Settings" verwendet.
Drucker und Erfassungsleser müssen manuell wieder eingetragen werden.

16. SiPass integrated Web Client

Der SiPass Web-Server ist Bestandteil der SiPass Installation.
Es ist ab SiPass 2.90 möglich SiPass ohne die Web-Server Funktion zu installieren.
Eine Nachinstallation des SiPass Web-Servers „Website“ ist jederzeit möglich.

Der Web-Client bietet folgende Optionen:

- ✓ Cardholders
- ✓ Visitor (licensed option)
- ✓ Access Levels
- ✓ Access Group
- ✓ Alarms
- ✓ Venues and Bookings
- ✓ Manual Override
- ✓ Activity feed (Ab 2.95 nicht mehr vorhanden)
- ✓ Area Monitoring (Ab 2.95 nicht mehr vorhanden)

Karten-Designe und -Ausdruck muss pro Web-Client lizenziert und installiert werden.

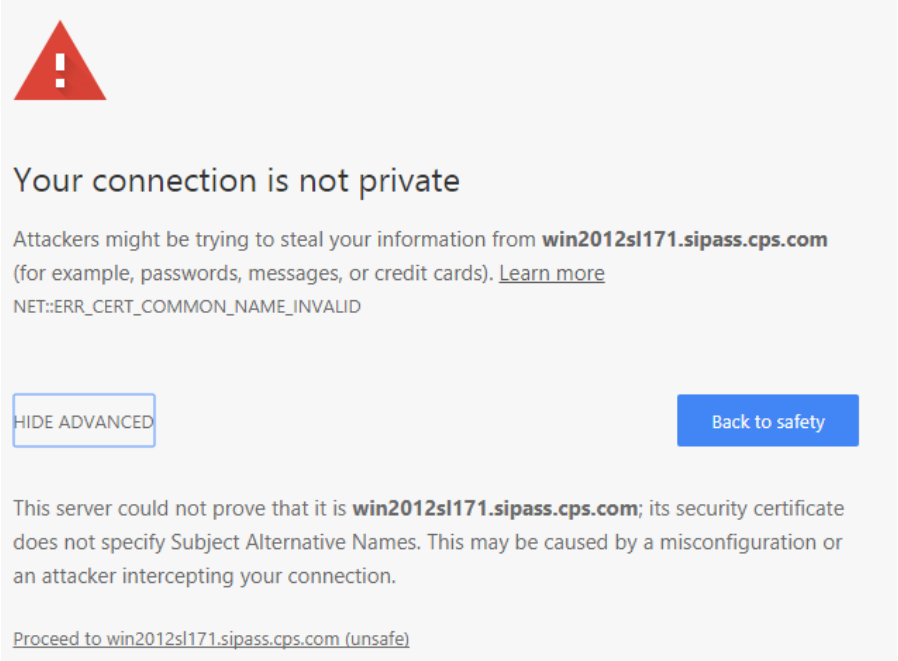
Web-Client Login Seite:

Login mit vorhandenem SiPass Benutzer: Name und Passwort, Sprache wählen.

Web Browser am Beispiel Chrome:

- Chrome starten
- Web Client Adresse aufrufen: https://PC-Name :5443/sipass

(Beim ersten Mal muss evtl. eine Ausnahme hinzugefügt werden:
Erweitert wählen und auf *Proceed to PC-Name* klicken, Ausnahme bestätigen)



Web Browser am Beispiel Firefox:

- Firefox starten
- Folgende Seite aufrufen: https://PC-Name :8743/API/Product
- Ausnahme hinzufügen
- Es erscheint dieses Fenster:

Dieser Schritt ist nur beim ersten Mal notwendig.

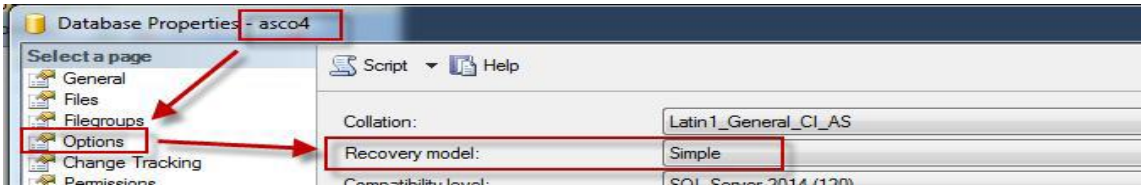
- Web Client Seite aufrufen: https://PC-Name :5443/sipass
- Web Client Login erscheint mit Bild und Popup Menü zur Sprachauswahl

17. Empfohlene SQL Datenbank Einstellungen

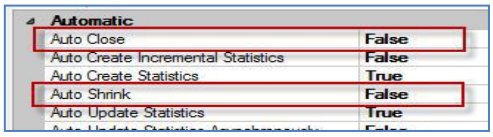
Um die nachfolgenden Einstellungen vorzunehmen, muss das SQL Management Studio manuell installiert werden. SiPass Setup installiert dieses Tool nicht, es muss manuell installieren. Es ist im DVD Image unter folgendem Pfad zu finden: *SQL Server Express\SQL Server Management Studio v18.5.1*.

Bitte führen Sie nachfolgende Schritte nur aus, wenn Sie bereits mit dem SQL Management Studio vertraut sind!

1. Standardmäßig ist der Recovery Modus auf **FULL** eingestellt. Es wird die Einstellung **SIMPLE** empfohlen.

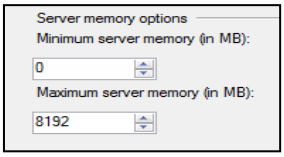


2. **Auto Close** und **Auto Shrink** müssen auf **False** gesetzt werden.



3. Setzen Sie den **Autogrowth** Wert auf 100 MB für **asco4** und **asco4_log**.

4. Setzen Sie die maximale Größe für die asco4_log Datei auf 500 MB.



5. Weisen Sie 50% des installierten Arbeitsspeichers SQL zu (SQL Server Einstellungen). 8192 MB sind 50% von 16 GB Arbeitsspeicher.

6. Es sollte kein SQL Backup für die asco4 DB eingerichtet werden. Die Wiederherstellung eines SiPass Systems ist nur mit dem SiPass eigenem Backup möglich. SQL Backups werden nur in seltenen Fällen zur Fehleranalyse durch die Entwickler verwendet.