Informationssicherheit bei iba-Produkten

Leitfaden

Ausgabe 2.0

Messsysteme für
Industrie und Energie

Herausgeber

iba AG

Königswarterstr. 44

90762 Fürth

Deutschland

Kontakte

Zentrale	+49 911 97282-0
Support	+49 911 97282-14
Technik	+49 911 97282-13
E-Mail	iba@iba-ag.com
Web	www.iba-ag.com

Autor

iba AG

Technischer Support & Informationssicherheit

support@iba-ag.com

Ausgabe	Datum	Autor	Änderungen
2.0	02-2024	mk/rm	Erweiterung ibaManagementStudio; Kapitel Ports neu gegliedert und ergänzt; neue GUIs; Beschreibung Benutzerverwaltung und Zertifikate reduziert

Inhalt

1 Vorwort

Mit der Konvergenz von Information Technology (IT) und Operation Technology (OT) im Zuge von Industrie 4.0 und der zunehmenden Integration von intelligenten Sensoren, die direkt mit einer Cloud kommunizieren, sowie der Anforderung, Messdaten aus der Produktion auch im IT-Netzwerk zu nutzen, entstehen für die Betreiber von OT-Netzwerken neue Risiken.

Viele dieser Risiken sind bereits bekannt aus dem Office-IT-Umfeld und es wird daher versucht, diese mit den gleichen Mitteln zu mindern. Da in OT-Netzwerken jedoch andere Prioritäten vorherrschen, müssen die klassischen Lösungen an das neue Umfeld angepasst oder gar neue Lösungen gefunden werden.

Mit diesem Leitfaden soll es Ihnen erleichtert werden, das iba-System sicher in Ihr Netzwerk zu integrieren, sodass die Sicherheitsanforderungen im IT- und OT-Umfeld bei der Messdatenerfassung, -aufzeichnung und -auswertung erfüllt werden können.

2 Industrial Security

2.1 Unterschiede zwischen Office und Industrial Security

Die klassische Informationssicherheit bezieht sich zu oft nur auf den Office-IT-Bereich. Hier haben Schutzziele wie Vertraulichkeit und Integrität einen sehr hohen Stellenwert. Funktionale Einschränkungen, wie z. B. Netzwerkausfälle, Netzwerkprobleme wie Jitter bzw. Störungen von VoIP-Verbindungen oder allgemeine Fehler bei der Bildübertragung in Videokonferenzen werden dagegen eher toleriert.

Im industriellen Bereich mit Automatisierungssystemen, die mit „Echtzeitprotokollen“ kommunizieren, können Netzwerkausfälle oder die zuvor genannten Jitter schnell zu Fehlfunktionen oder Schäden an den Anlagen führen. Im schlimmsten Fall kommen dadurch Menschen in Gefahr, wenn z. B. Signale nicht rechtzeitig eintreffen. Daher hat in OT-Umgebungen das Schutzziel Verfügbarkeit einen sehr hohen Stellenwert. Neben Verfügbarkeit ist auch die Integrität sehr wichtig. Würden über eine Manipulation die Signale für Soll- und Istwert vertauscht werden, hätte dies genauso fatale Auswirkungen wie ein Ausfall! Um diese Schutzziele zu gewährleisten, darf die Sicherheit der eingesetzten Komponenten sowie deren richtige Konfiguration und der Aufbau der Netzwerke nicht außer Acht gelassen werden.

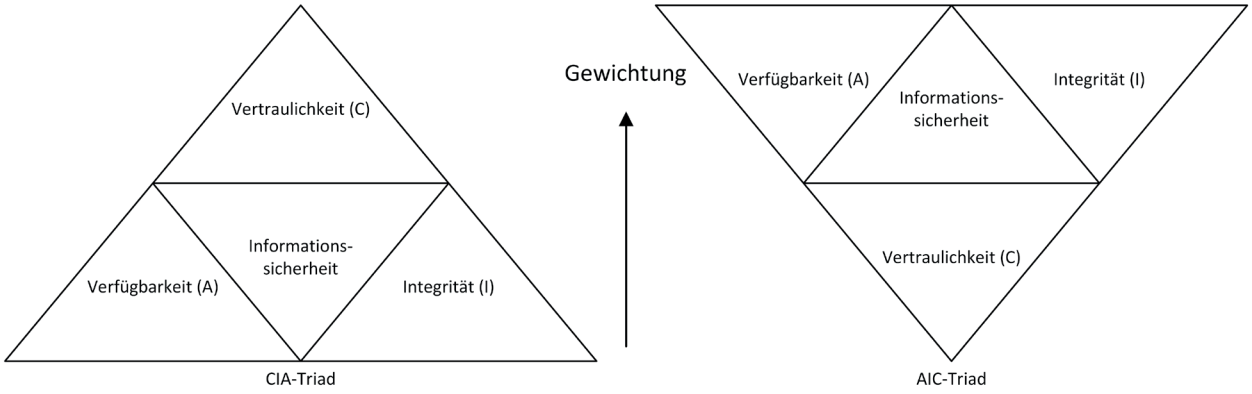


Abb. 1: Vergleich der Prioritäten im IT- (links) und im OT-Bereich (rechts)

Des Weiteren muss beim Einsatz von Antivirus-, Firewall- oder Deep-Packet-Inspection-Lösungen in OT-Netzen darauf geachtet werden, dass Latenzen sowie der Ressourcenverbrauch durch entsprechende Konfiguration den Betrieb der Anlage nicht negativ beeinflussen.

Daher sind die technischen Schutz- und Sicherheitsmaßnahmen aus der klassischen Office-IT nicht direkt 1:1 auf den industriellen Bereich abbildbar.

2.2 Informationssicherheit-Managementsystem (ISMS)

Das Management der Informationssicherheit ist keine einmalige, sondern eine kontinuierliche Aufgabe, die meist in Prozessen abgebildet wird. Diese Prozesse sollen sicherstellen, dass Informationssicherheit über einen Zeitraum ein akzeptables Niveau erreicht oder hält. Die nachstehende Grafik veranschaulicht diese Konzeption und vergleicht diese mit dem Ansatz, wenn Sicherheit nur als Projekt aufgefasst wird.

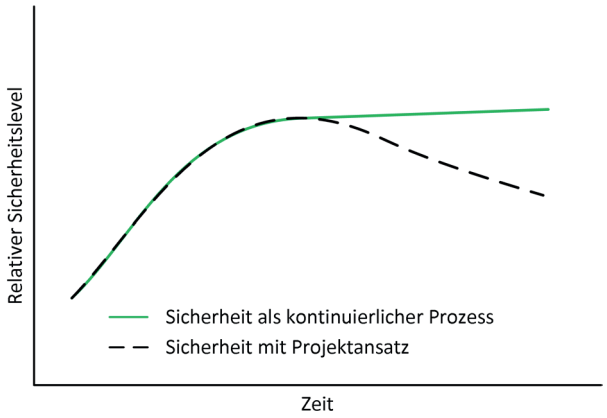


Abb. 2: Sicherheitslevel über die Zeit (Quelle: IEC 62443-1-1)

Die nötigen Prozesse sind in einem ISMS (Informationssicherheitsmanagementsystem) zusammengefasst und können so leichter verwaltet werden.

Im ersten Schritt werden in einer Phase der Bestandsaufnahme im Unternehmen alle Beteiligten Systeme, Prozesse und Mitarbeiter in einer Risikoanalyse identifiziert und nach möglichen Schwachstellen und Auswirkungen beurteilt. Diese Analyse ist die Grundlage für die weiteren Schritte zur Erstellung von technischen und organisatorischen Maßnahmen wie z. B. zu dokumentierende Richtlinien und Einführung von Lösungen zur Minimierung von gefundenen Schwachstellen bzw. Risiken. Im Nachgang werden diese Maßnahmen fortwährend auf deren Wirksamkeit sowie Effizienz überprüft und auch nachgebessert.

Dieser Prozess wiederholt sich zyklisch und verbessert somit das Sicherheitsniveau fortwährend.

Abb. 3: Kontinuierlicher Prozess mit einem ISMS

Schritt	Beschreibung
Risikoanalyse	In diesem Schritt geht es um das Identifizieren und Beurteilen von Risiken in der Anlage. Welche Gefahren und Schwachstellen sind vorhanden? ■ Erfahrungswerte aus der Vergangenheit ■ Umfangreiche und tiefgründige Analyse von Netzwerkzonen, offenen Ports, Systemen und Berechtigungen ■ Engpässe bei Ressourcen (Netzwerk, System) und daraus entstehende DoS-Effekte (Denial of Service) ■ Unzureichend definierte Benutzerrechte oder granulares Berechtigungskonzept ■ Veraltete Software, Ausnutzung von Schwachstellen durch Schadsoftware ■ Nicht ausreichende Firewall-Konfiguration ■ Etc.
Richtlinien, organisatorische Maßnahmen	Für manche Risiken gibt es entweder keine technische Lösung oder diese steht finanziell nicht im Verhältnis zum Risiko. Solche Risiken werden am besten durch Richtlinien und gezielte Schulungen zur Sensibilisierung der Mitarbeiter gemindert. Zu diesen Maßnahmen zählt bspw. auch die Benennung von Verantwortlichen, die bei einem Wiederanlauf der Produktion nach einem Sicherheitsvorfall definierte und erlernte Abläufe zur Analyse und Dokumentation durchlaufen.
Technische Maßnahmen	Hier werden die Risiken mit Hilfe von maßgeschneiderten technischen Lösungen minimiert, die eine Kontrolle der organisatorischen Maßnahmen ermöglichen und dem Unternehmen erlauben, Sicherheitsstandards nach aktuellem Stand der Technik umzusetzen.
Prüfung und Verbesserung	Es sollten unabhängige Prüfungen durchgeführt werden. Am ehesten eignen sich betriebsfremde Sicherheitsexperten, die einen kritischen Blick auf die technische Infrastruktur werfen. Sie können neutral beurteilen, ob die eingesetzten Maßnahmen wirken und Empfehlungen zum Nachbessern geben.

Tab. 1: Schritte zur Sicherstellung der IT-Sicherheit

2.3 Das iba-System im ISMS

Das iba-System muss in das ISMS und den kontinuierlichen Prozess des Anwenders mit einbezogen werden. Es ist die Aufgabe des Anwenders, den sicheren Betrieb und die sichere Integration des iba-Systems bei der Konnektivität zum Prozess, der Datenaufzeichnung, der (automatisierten) Auswertung sowie der Ausgabe von iba-Daten in das übergeordnete System zu gewährleisten.

Wertvolle Hinweise zu einem sicheren Betrieb liefert dieser Leitfaden.

3 Sicherheitsmaßnahmen der iba AG

3.1 Sicherung der Lieferkette

Die iba AG arbeitet mit langjährigen Partnern zusammen, zu denen ein enger Austausch über gesicherte Kanäle besteht. Die Vertragspartner der iba AG unterliegen den Informationssicherheitsvereinbarungen für Lieferanten, die im Rahmen der ISO 27001-Zertifizierung neu gefasst wurden. In diesen Vereinbarungen sind technische und organisatorische Maßnahmen beschrieben, die Informationssicherheit priorisieren, Fehler bei der Produktion auf ein Minimum reduzieren und ein Kompromittieren der Lieferkette erheblich erschweren.

Im Rahmen der AEO-Zertifizierung (Zugelassener Wirtschaftsbeteiligter, englisch „Authorized Economic Operator“) wurden noch weitere Auflagen und Prüfungen für die Mitarbeiter sowie Zutrittssicherung der Standorte und Räumlichkeiten eingeführt, um die Waren vom Auftragseingang bis zu deren Versand zu sichern.

3.2 Produktlebenszyklus

Das Einbringen von Sicherheitsanforderungen kann nicht erst im Nachhinein als sog. „Bolt-On-Lösung“ geschehen. Dies ist auch aus wirtschaftlichen Gründen kein gangbarer Weg. Daher werden die Sicherheitsanforderungen ab der Produktidee in allen Prozessphasen vom Produktlebenszyklus mitberücksichtigt, angepasst und überprüft.

3.3 iba Rechnersysteme

Die Rechnersysteme der iba AG sind mit der aktuellen IoT Enterprise Edition von Microsoft Windows ausgestattet und werden vor der Auslieferung mit den aktuellsten Windows Updates versehen sowie mittels mehrerer Testverfahren geprüft. Diese Tests haben eine Mindestdauer von 24 h und stellen die korrekte Funktion des Rechnersystems sicher.

Auf den Rechnersystemen ist nur die zum Betrieb nötige Software installiert, diese setzt sich aus dem Grundsystem (Windows) und der im Auftrag genannten Software zusammen.

Weitere Software, wie sie teilweise auf kommerziellen PC-Systemen großer Hersteller zu finden ist, wird auf den Rechnersystemen der iba AG nicht installiert, da diese die Performance im industriellen Umfeld negativ beeinflussen kann.

In der Standardkonfiguration sind keine weiteren Sicherungsmaßnahmen getroffen. Das heißt USB-Anschlüsse sowie Wechselmedien sind nicht blockiert.

Das Netzwerk ist nur durch die in Windows integrierte Firewall geschützt. Damit ist zunächst sichergestellt, dass das System in beliebigen Kundennetzwerken sofort ablauffähig ist. Es ist aber in der Regel erforderlich, dass kundenseitig Einstellungen zur Erhöhung der Sicherheit vorgenommen werden müssen.

3.4 iba Hardware

Schon während der Entwicklung wird Wert auf den sicheren Betrieb der Geräte gelegt, so sind z. B. die Updates gegen Manipulation gesichert. Zudem werden neben den sonstigen Prüfungen wie EMV (Elektromagnetische Verträglichkeit) auch Schwachstellentests, sog. "penetration tests" oder kurz "Pentests" durchgeführt, die die Sicherheit der Geräte verbessern. Die Ergebnisse der Pentests fließen direkt zurück in den Entwicklungsprozess und werden bei Neu- und Weiterentwicklungen berücksichtigt.

3.5 iba Software

Ebenso wie bei der Hardware werden auch hier Pentests und Analysen der Angriffsfläche genutzt, um die Software stetig zu verbessern. Wo immer möglich werden Verschlüsselungs- und Signaturalgorithmen verwendet, die dem aktuellen Stand der Technik entsprechen (siehe Abb. 4, Seite 13). Ausnahmen bilden hier ältere Protokolle, die keine Verschlüsselung unterstützen (z. B. SNMP v1, ModBus oder S7-300 Kommunikation).

Alle Installationspakete sind mit einer digitalen Signatur versehen, so dass eine Manipulation des Installationspaketes leicht erkannt werden kann (siehe Abb. 5, Seite 13).

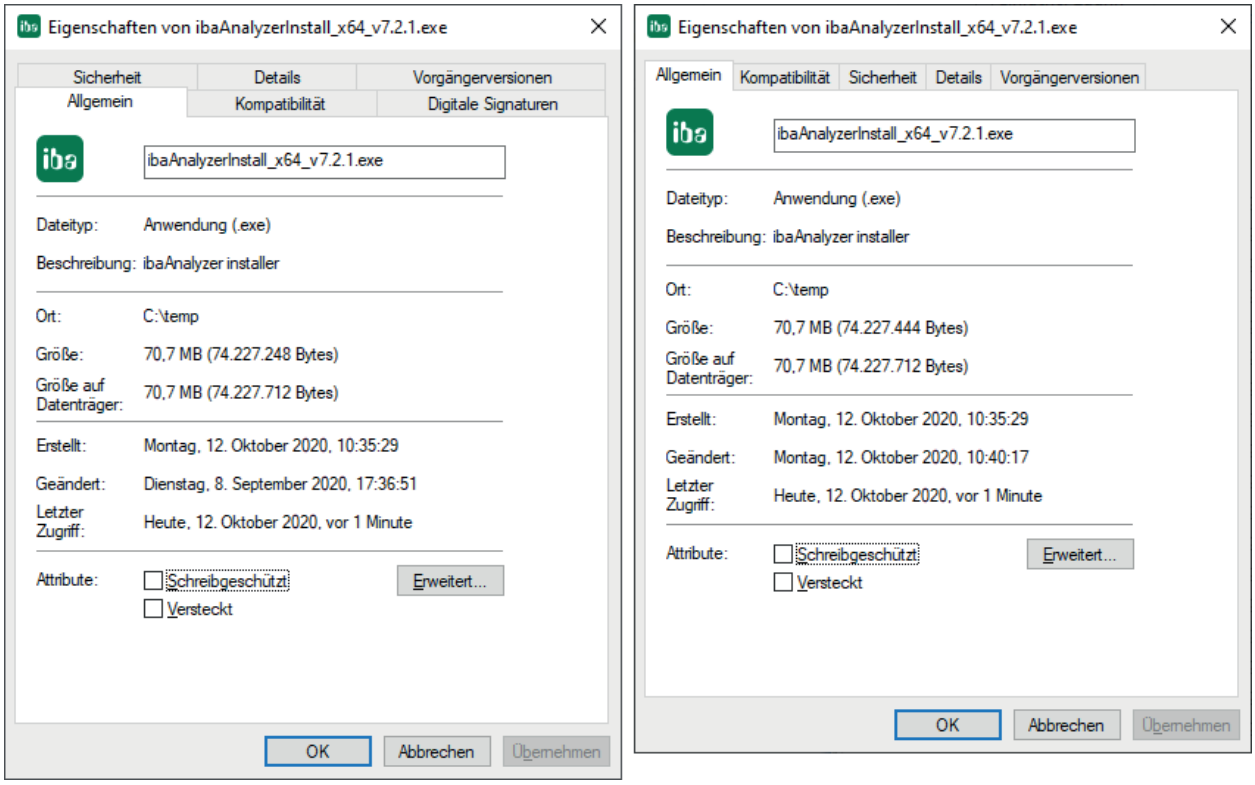


Abb. 4: Eigenschaften des Installationspakets

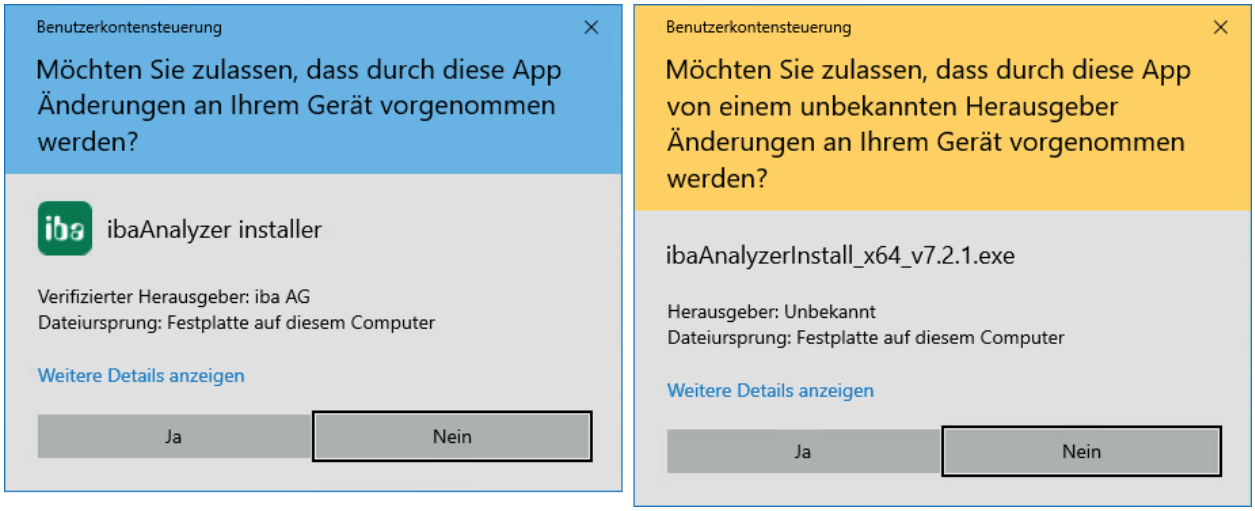


Abb. 5: Original (links) und modifiziertes Paket (rechts)

3.6 Datenformat

3.6.1 iba DAT-File

Mit Einführung von ibaPDA-Version 7 wurde das von iba verwendete Dat-Format für Messdateien grundlegend überarbeitet und bietet neben anderen Neuerungen auch die Möglichkeit einer Verschlüsselung des Inhalts an.

Hier kommen verschiedene Algorithmen zum Einsatz, die die Daten vor Manipulation bzw. unautorisiertem Zugriff schützen. Nachfolgend eine Liste der verwendeten Algorithmen:

- SHA512
- Ed25519
- XChaCha20
- Poly1305
- BTEA
- ARGON2ID13

Hinweis

Wenn Sie die Passwortfunktion nutzen, um Ihre aufgezeichneten Daten zu schützen, verwahren Sie das genutzte Passwort an einem sicheren Ort. Geht dieses Passwort verloren, sind die aufgezeichneten Daten nicht mehr zugänglich. Auch iba kann in diesem Fall keine Hilfestellung leisten. Empfehlung ist hierbei die Nutzung eines Passwort-Managers.

4 Empfehlungen für Anwender

Nach Auslieferung der Produkte hat die iba AG keine Kontrolle über die Sicherheitsmechanismen in Ihrem Unternehmen. Trotzdem gibt es einige von iba empfohlene Maßnahmen zur Verbesserung der Informationssicherheit, die Sie als Anwender berücksichtigen können und sollten.

4.1 Standardpasswörter und Benutzermanagement

Standardpasswörter
Ändern Sie nach dem Erhalt eines unserer PC- bzw. DAQ-Systeme die Zugangsdaten der voreingestellten Benutzer. Damit wird potentiellen Angreifern der Zugang zum System erschwert.

Benutzerverwaltung
Nutzen Sie die von den Anwendungen bereitgestellte Benutzerverwaltung, um den Zugriff auf bestimmte Personen-/gruppen einzuschränken. Prüfen Sie die Berechtigungen der Benutzer bei Änderung von Abteilungszugehörigkeiten oder falls Zugangsrechte nicht mehr benötigt werden.

4.2 Malwareschutz

Die iba AG empfiehlt generell die Nutzung von Malwareschutz-Lösungen, um das iba-Rechnersystem und dessen Betriebssystem vor Befall mit bekannten Schadprogrammen zu schützen. Halten Sie die eingesetzte Lösung durch regelmäßige Updates auf dem neusten Stand.

Die von iba geprüfte Lösung stammt aus dem Enterprise-Bereich von Trend Micro und ist für die Verwendung mit iba-Produkten freigegeben.

4.3 Firewall

iba PC- sowie DAQ-Systeme werden nur mit der in Windows integrierten Firewall ausgeliefert. Wenn Sie eine zusätzliche Lösung einsetzen, müssen die von den Anwendungen verwendeten Ports evtl. freigeschaltet werden.

Eine Liste der verwendeten Ports finden Sie hier: ↗ *Ports*, Seite 53.

4.4 Updates

iba PCs sowie DAQ-Systeme haben bei der Auslieferung die aktuellen Windows-Updates installiert. Um die entsprechenden Systeme weiterhin sicher zu betreiben, müssen Sie zyklisch aktuelle Windows-Updates installieren. Ohne diese Updates häufen sich Schwachstellen an den Systemen.

Seit der Einführung von Windows 10 können hierzu kumulative Updatepakete aus dem Microsoft Update Catalog [1)] bezogen werden. Vereinzelt muss vor der Installation eines Updatepakets ein Service Stack Update (kurz SSU) installiert werden. Ob dies für ein Updatepaket notwendig ist, geht aus dem Knowledgebase-Artikel zum kumulativen Updatepaket hervor.

1) https://www.catalog.update.microsoft.com/

4.5 Kommunikation über öffentliche Netze

Wenn iba-Systeme (Soft- oder Hardware) über öffentliche Netze miteinander kommunizieren, ist es unerlässlich, dass die Verbindung durch zusätzliche Maßnahmen geschützt wird. Meist werden Firewalls mit VPN Verbindungen zur durchgängigen verschlüsselten Kommunikation eingesetzt. Die eingesetzten Systeme sollten sich nicht direkt unverschlüsselt und ohne VPN-Verbindung zu anderen Systemen verbinden.

Die Verbindung zwischen Standorten oder auch Verbindungen von Office- zu Industrie-Netzen sollte weiterhin mittels einer Firewall oder VPN-Verbindung abgesichert sein, um ein Mitlesen bzw. die Manipulation des Datenverkehrs zu erschweren oder zu verhindern. Bei der Konfiguration der VPN-Verbindung muss darauf geachtet werden, dass nur sichere Algorithmen zum Einsatz kommen und die Authentifizierung sicher gestaltet wird.

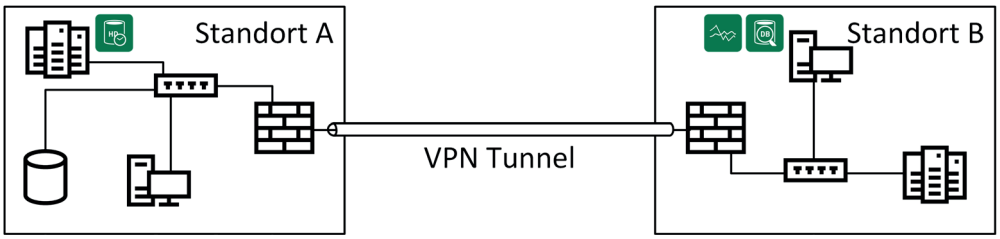


Abb. 6: ibaPDA und ibaAnalyzer greifen von Standort B auf Standort A zu

4.6 Backup

Je nach Ausstattung ist der iba-Rechner mit einem RAID ausgeführt. Dies bietet ein Mindestmaß an Datensicherheit ist aber **kein** Ersatz für ein Backup, das z. B. vor Ransomware oder dem Ausfall von Hardware-Komponenten schützt.

Für die Festlegung der richtigen Backup-Strategie sind folgende Fragen zu klären:

- Wie lange müssen die Daten aufbewahrt werden?
- Welche Daten müssen gesichert werden?
- Wann ist der beste Zeitpunkt für eine Sicherung?
  - täglich
  - zum Schichtwechsel
  - während der Instandhaltungsmaßnahmen
- Sicherung über ein Netzwerk:
  - Bandbreite des Netzwerks?
  - Was wird durch einen Backup-Job evtl. beeinflusst?
- Wie schnell können die Daten im Notfall (Recovery Time Objective, RTO) wiederhergestellt werden?
- Muss die 3-2-1 Backup-Regel angewandt werden?

3-2-1 Backup-Regel

3 Die Daten liegen in 3-facher Ausführung vor; z. B. 1x als Live-System und 2x als Backup mit weit zurückgehenden Restorepoints

2 Backups auf zwei unterschiedlichen Technologien; z. B. Backup-to-Disk, Backup-to-Tape u.a.

1 Ein Backup immer außer Haus bzw. an einem anderen Standort., wegen der Verfügbarkeit der Daten im Katastrophenfall

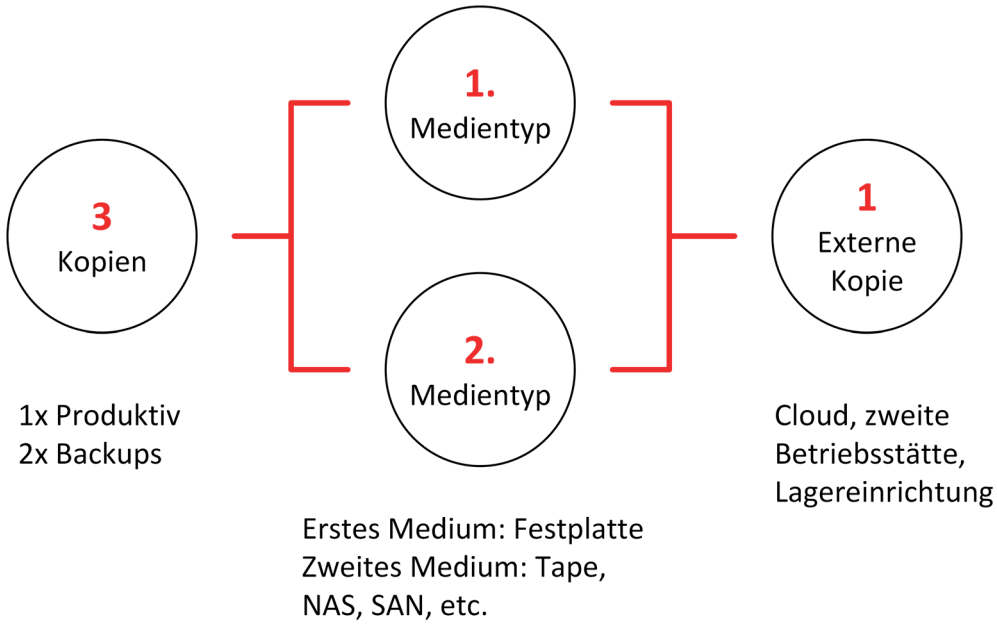


Abb. 7: Backup-Prinzip nach der 3-2-1-Regel

5 Hinweise zum sicheren Betrieb von iba-Software

In diesem Kapitel werden die folgenden Themen behandelt

- Dienstkonten (5.1, Seite 18)
- Benutzerverwaltung (5.2, Seite 41)
- Zertifikate (5.3, Seite 42)
- Ports (Firewall) (5.4, Seite 53)

Anhand der folgenden Tabelle können Sie erkennen, welche Unterkapitel für Ihre eingesetzte Software zutreffen.

	Dienstkonten	Benutzerverwaltung	Zertifikate	Ports (Firewall)
ibaPDA	-	•	•	•
ibaAnalyzer	-	-	-	•
ibaDatCoordinator	•	•	-	•
ibaHD-Server	-	•	•	•
ibaCapture	•	•	-	•
ibaDaVIS	•	•	•	•
ibaManagementStudio	•	•	•	•
ibaCMC	-	•	-	•

Tab. 2: iba-Softwareprodukte und anwendbare Sicherheitsmaßnahmen

- nicht anwendbar, • anwendbar

5.1 Dienstkonten

In einer Standard-Installation werden die Windows-Dienste der Anwendungen, wie beispielsweise ibaDatCoordinator, unter dem lokalen Systemkonto (LOCAL SYSTEM ACCOUNT) installiert.

Sobald der Rechner in einer Domäne betrieben wird, haben Sie die Möglichkeit ein verwaltetes Dienstkonto einzurichten. Dies macht aus Sicht der Informationssicherheit wesentlich mehr Sinn, da mit dem initial installierten Benutzerkonto in der Regel umfangreiche Berechtigungen für den betreffenden Rechner verknüpft sind. Insbesondere in zentral verwalteten IT-Landschaften wird daher von Administratoren und Security-Verantwortlichen verlangt, dass die Dienste unter speziellen Benutzerkonten laufen, denen exakt die Rechte zugestanden werden, die sie zur Erfüllung ihrer Aufgaben und Dienste benötigen.

Für einen sicheren Betrieb empfehlen wir daher die entsprechenden Dienste jeweils mit einem verwalteten Dienstkonto (Group Managed Service Account) in der Domäne zu betreiben. Nachfolgend wird am Beispiel die Konfiguration von iba-Softwarepaketen in der Domäne EXCORP der Example Corporation beschrieben.

Die Informationen für die Konfiguration anderer iba-Softwarepakete kann ebenfalls dem Anhang des Benutzerhandbuchs der jeweiligen Software entnommen werden.

Fiktive Domäne "EXCORP"

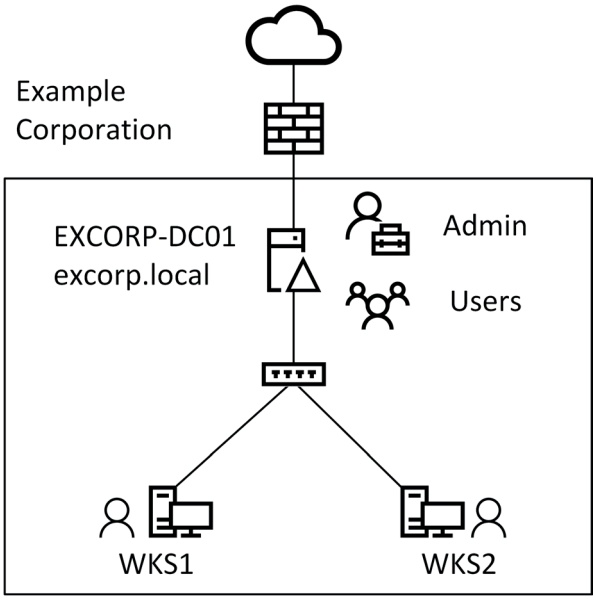


Abb. 8: Überblick - Domäne EXCORP

In der Domäne EXCORP befinden sich folgende Objekte.

- Domänen-Controller (Kurz: DC): EXCORP-DC01
- Domänen-Administrator: Administrator (Kurz: Admin)
- Computer: WKS1, WKS2
- Benutzer: John, Jane

5.1.1 Verwaltetes Dienstkonto erstellen

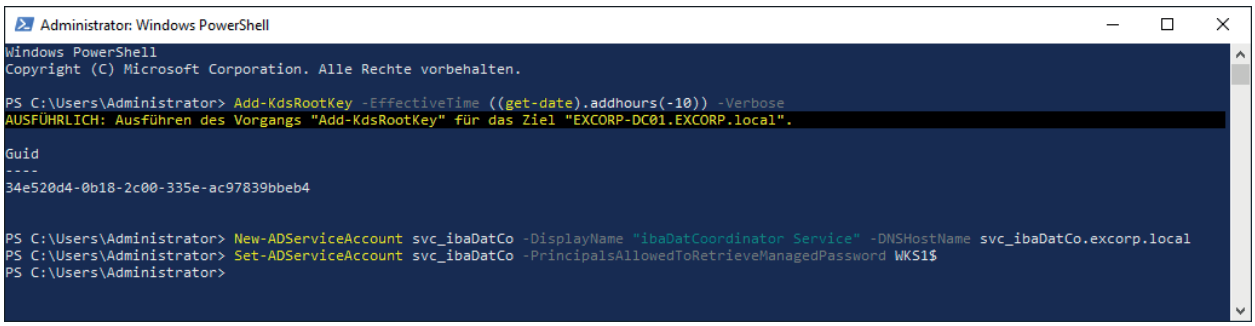
Auf dem DC (Domänen-Controller) muss zunächst das neue Dienstkonto erstellt werden. Dazu wird eine PowerShell-Konsole mit Administratorenrechten benötigt, in der folgendes ausgeführt wird.

```
Add-KdsRootKey -EffectiveTime ((get-date).addhours(-10)) -Verbose
```

```
New-ADServiceAccount svc_iba -DisplayName "iba Software Service" -DNSHostName svc_iba.excorp.local
```

```
Set-ADServiceAccount svc_iba -PrincipalsAllowedToRetrieveManagedPassword WKS1$
```

Beispiel *ibaDatCoordinator*-Konto:



Damit kann das neue Dienstkonto auf dem Computer WKS1 verwendet werden. Soll es darüber hinaus noch auf dem Computer WKS2 verwendet werden, muss der letzte Befehl wiederholt werden mit `WKS2$` anstatt `WKS1$`.

Kommando	Beschreibung
`Add-KdsRootKey`	Erstellt einen neuen Root-Key für den Microsoft Group Key Distribution Service (KdsSvc) und setzt das Datum ab dem dieser Schlüssel gültig ist auf das aktuelle Datum minus 10 Stunden.
`New-ADServiceAccount`	Erstellt ein neues verwaltetes Dienstkonto im Active Directory mit Namen „svc_iba“, setzt den Anzeigenamen auf einen verständlichen Wert und setzt den DNS-Eintrag für das Dienstkonto auf <dienstname>.<domain-name>.local
`Set-ADServiceAccount`	Fügt das System mit dem Namen „WKS1$“ zu den Mitgliedern des Dienstkontos „svc_iba“ hinzu und erlaubt somit die Nutzung des Kontos auf dem System.

Damit Berechtigungen granularer vergeben werden können, empfiehlt es sich für die Softwareprodukte jeweils eigene Dienstkonten zu erstellen.

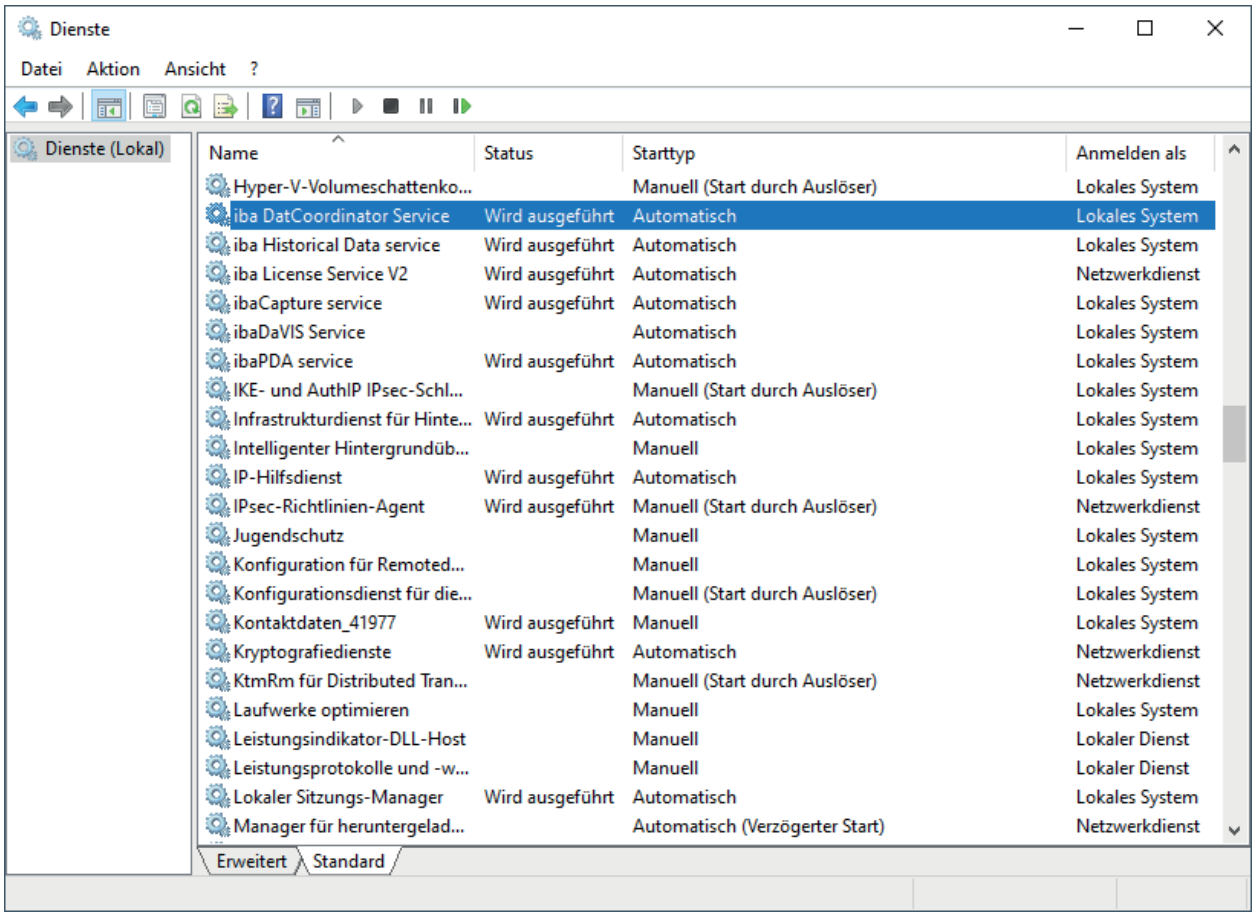
Beispiele für ibaDatCoordinator und ibaCapture:

- ibaDatCoordinator: svc_ibaDatCo
- ibaCapture: svc_ibaCapture

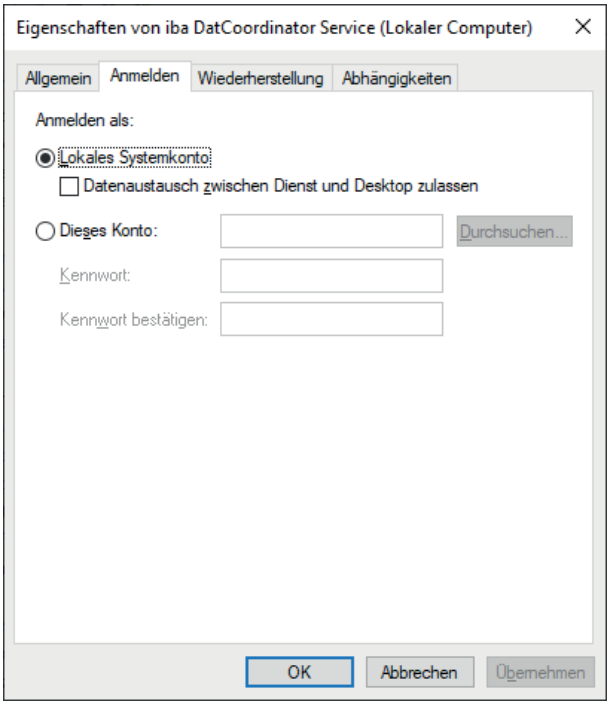
5.1.1.1 Verwaltetes Dienstkonto verwenden

Um das neue Dienstkonto zu konfigurieren, müssen folgende Schritte durchgeführt werden:

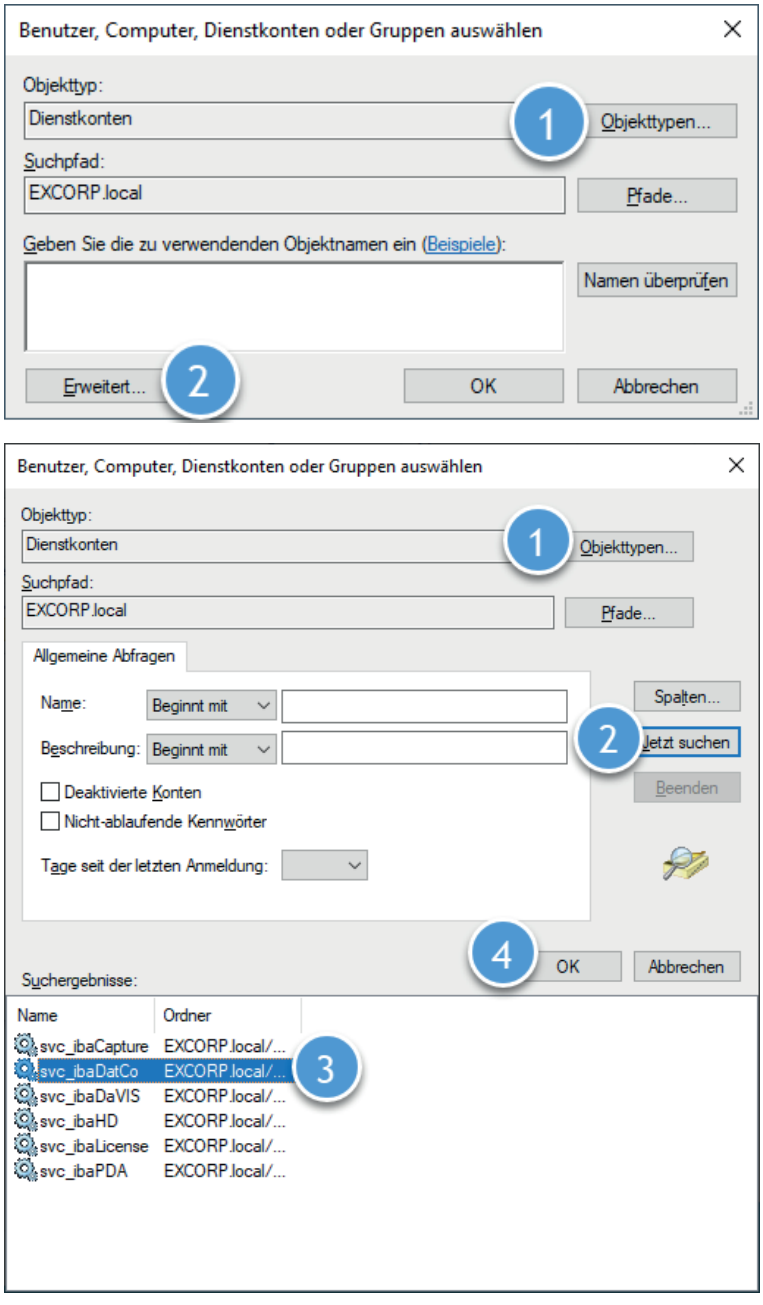
1. Melden Sie sich auf dem System WKS1 mit einem Administratorzugang an.
2. Öffnen Sie die Computerverwaltung und selektieren Sie den Punkt *Dienste* in der Baumansicht.

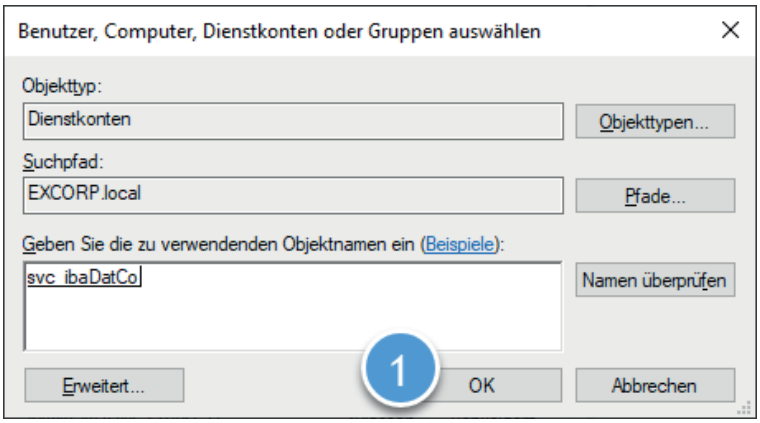


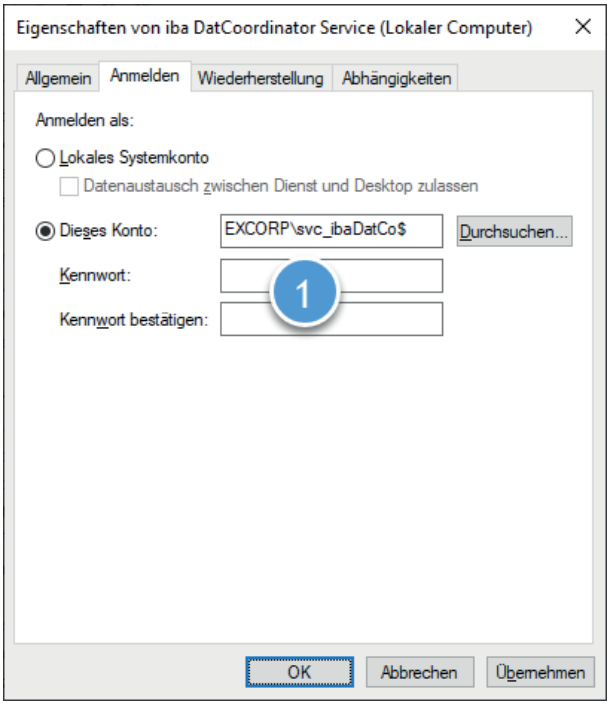
3. Stoppen Sie den entsprechenden Dienst, hier als Beispiel „iba DatCoordinator Service“.
4. Öffnen Sie die Eigenschaften des Dienstes und selektieren Sie die Lasche *Anmelden*.



5. Wählen Sie den Punkt *Dieses Konto*.
6. Tragen Sie das Dienstkonto in das Feld *Benutzername* in der Form „<Domain-Name>\<Account-Name>$“ hier „EXCORP\svc_ibaDatCo$“ ein.
   Alternativ können Sie auch mit Hilfe von <Durchsuchen> das entsprechende Konto auswählen.
   In den folgenden Abbildungen kennzeichnen die Ziffern die Reihenfolge und Stellen der Betätigungen bzw. Eingaben.







7. Verlassen und bestätigen Sie die Dialoge mit <OK>.
8. Starten Sie den Dienst.

Für eine ordnungsgemäße Funktion des geänderten Dienstes kann es erforderlich sein, dass auf dem System WKS1 noch weitere Berechtigungen gesetzt werden müssen.

Die benötigten Berechtigungen können in der aktuellen Form aus dem Handbuch der jeweiligen Software entnommen werden.

5.1.1.2 Zurücksetzen des Kontos

1. Öffnen Sie eine Kommandozeile mit Administratorrechten.
2. Führen Sie folgenden Befehl aus:

```
sc config "ibaDatCoordinatorService" obj= "LocalSystem" password= ""
```

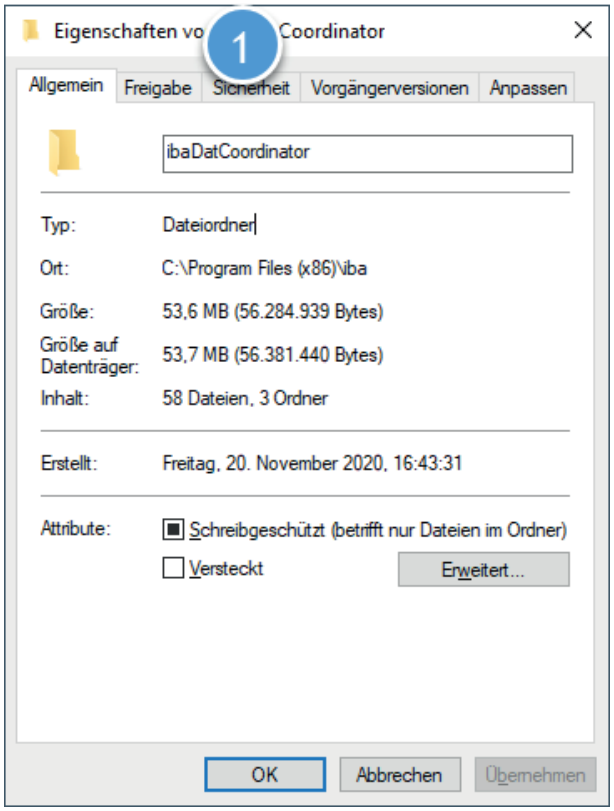
Den Dienstnamen können Sie den Eigenschaften des Dienstes entnehmen.

5.1.2 Setzen von Verzeichnisberechtigungen

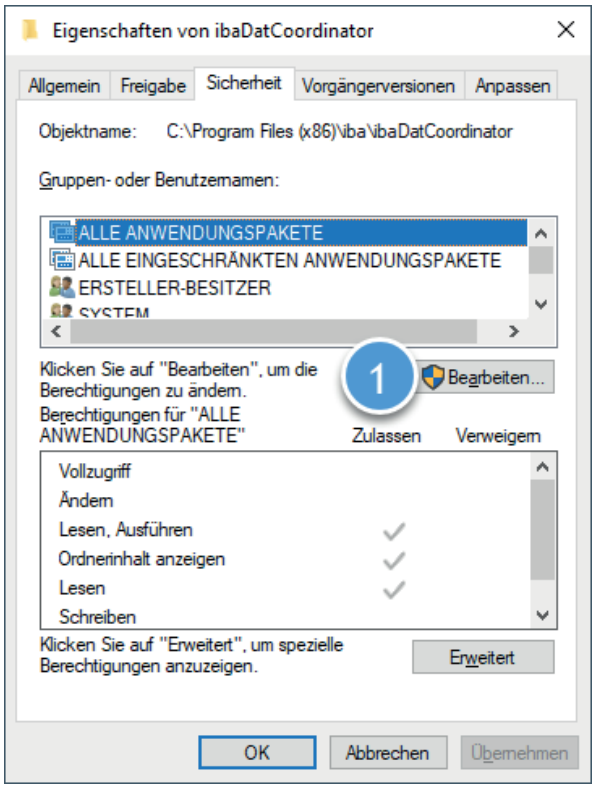
Da durch das Verwenden von Dienstkonten die Berechtigungen eingeschränkt werden, fehlen der Anwendung die Rechte, um Änderungen an bestimmten Dateien bzw. Verzeichnissen vorzunehmen. In diesem Abschnitt wird am Beispiel von *ibaDatCoordinator* gezeigt, wie Berechtigungen für Verzeichnisse gesetzt werden, damit die Anwendung beispielsweise Konfigurations- und Logdateien anlegen kann.

Für die hier beschriebenen Schritte wird vorausgesetzt, dass man auf dem System WKS1 mit einem Administratorzugang angemeldet ist und zuvor ein verwaltetes Dienstkonto erstellt wurde.

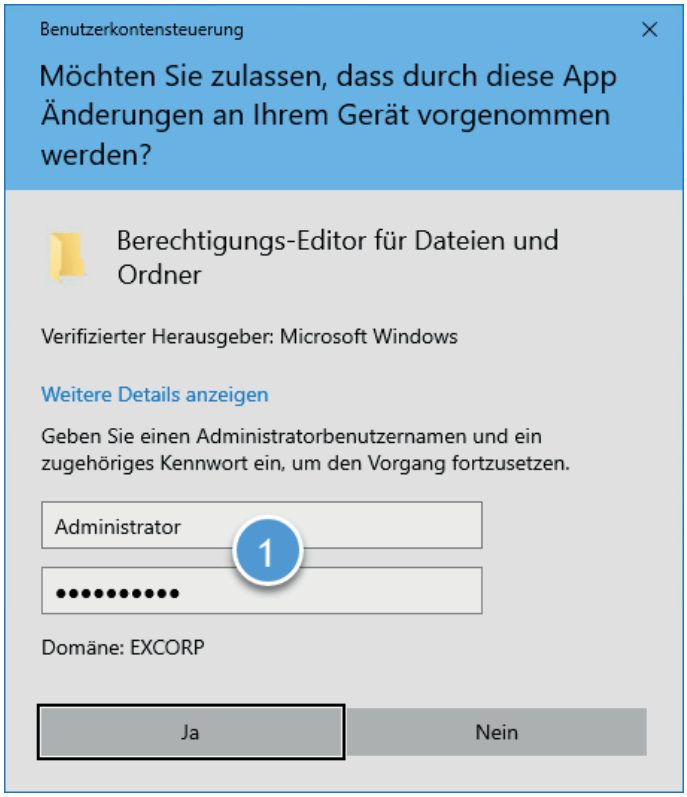
1. Öffnen Sie den Windows Explorer und navigieren Sie zu dem folgenden Pfad: "C:\Program Files (x86)\iba"
2. Öffnen Sie die Eigenschaften des Ordners *ibaDatCoordinator* mithilfe des Kontextmenüs im Explorer und selektieren Sie die Lasche *Sicherheit* (1).



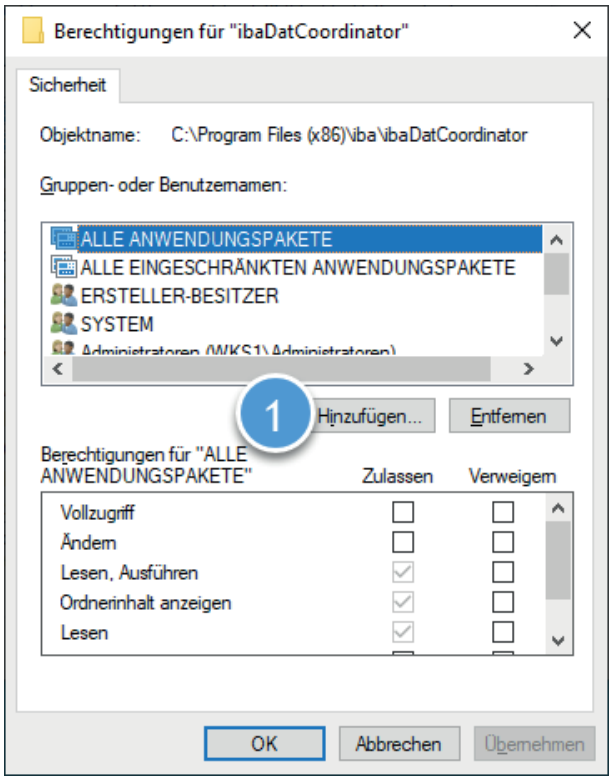
3. Klicken Sie auf <Bearbeiten> (1), um die Gruppen- und Benutzerberechtigungen zu ändern oder neue hinzuzufügen.



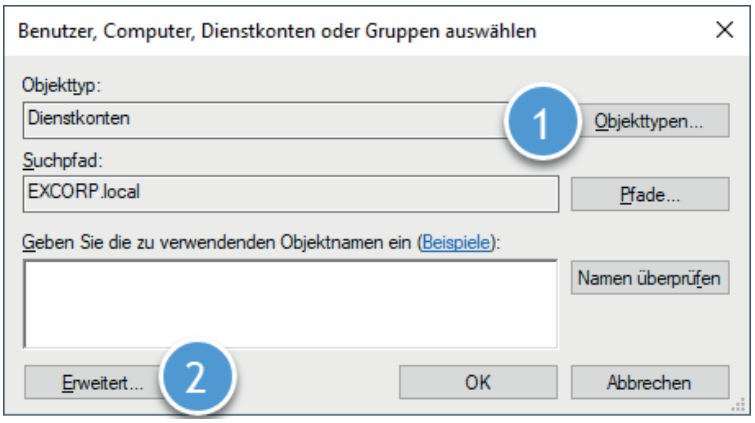
4. Als normaler Benutzer müssen Sie noch eine Autorisierung (1) durchführen, um die Einstellungen bearbeiten zu können.



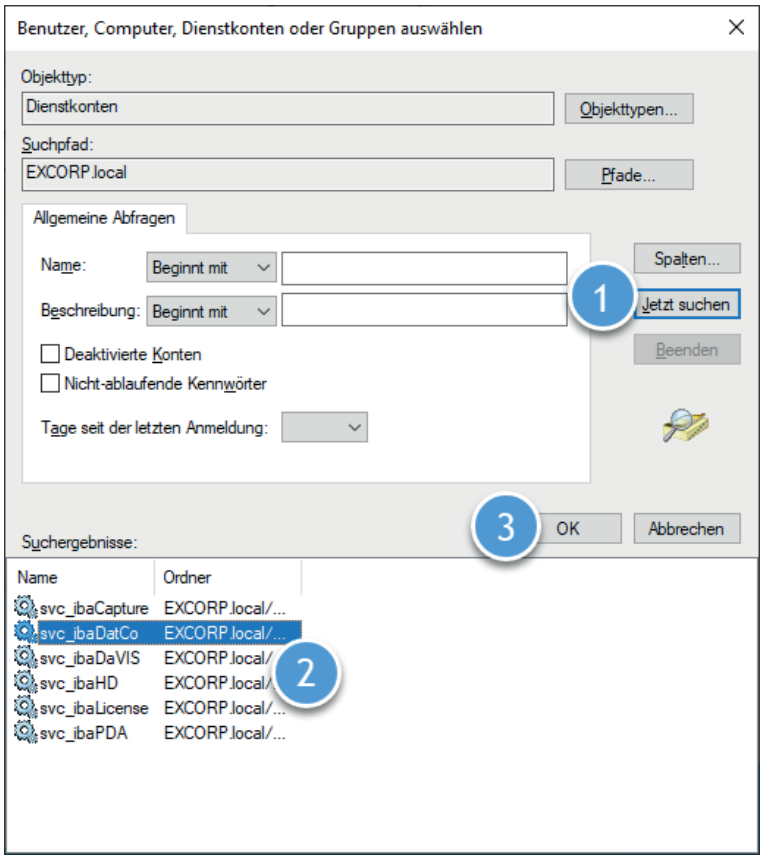
5. Nach erfolgreicher Autorisierung können Sie mit <Hinzufügen...> (1) das neue Dienstkonto als Benutzer hinzufügen.



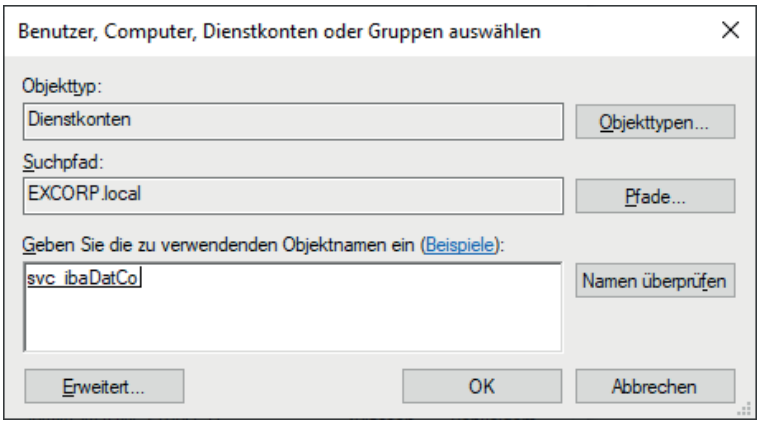
6. Ändern Sie zunächst die Auswahl bei den Objekttypen (1), sodass nur noch "Dienstkonten" ausgewählt ist. Klicken Sie auf <Erweitert> (2), um die erweiterte Dialogfunktion zu öffnen.



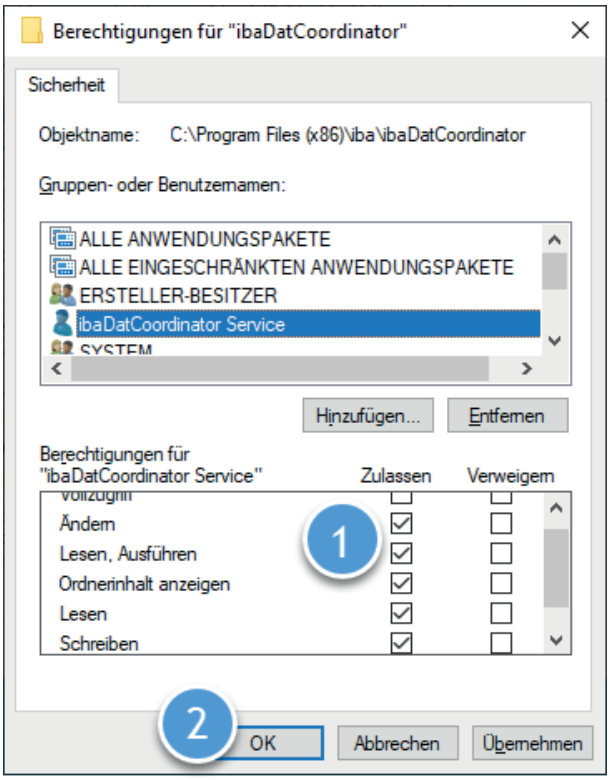
7. Klicken Sie auf <Jetzt suchen> (1) und es werden alle vorhandenen Dienstkonten in der Domäne aufgelistet. Anschließend kann das entsprechende Konto aus der Liste ausgewählt (2) und der Dialog mit einem Klick auf <OK> (3) verlassen werden.



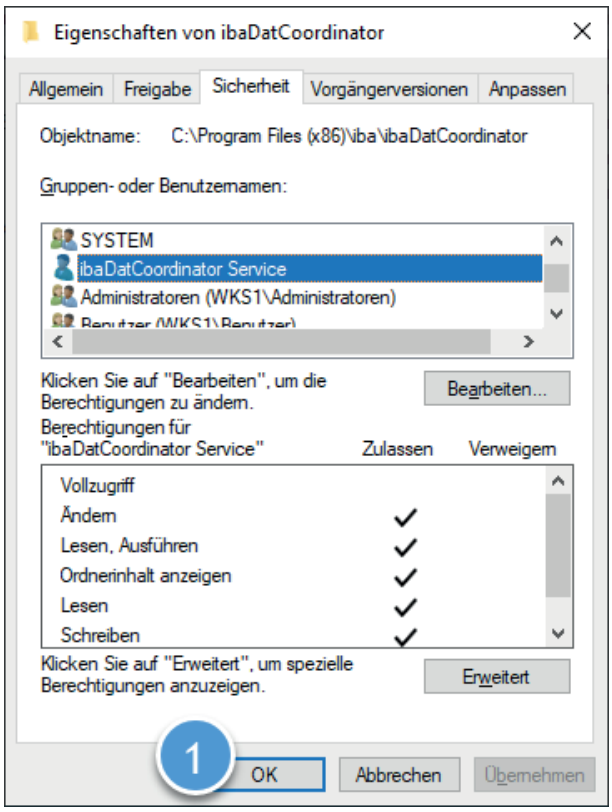
8. Bestätigen Sie den folgenden Dialog mit <OK>, damit das Dienstkonto hinzugefügt wird.



9. Räumen Sie nun dem neuen Benutzer die folgenden Berechtigungen ein(1):
   - Ändern
   - Lesen, Ausführen
   - Ordnerinhalt anzeigen
   - Lesen
   - Schreiben



10. Verlassen Sie den Dialog mit <OK> (2).
11. Um die Konfiguration abzuschließen und die Eigenschaften zu speichern, verlassen Sie auch den nächsten Dialog mit <OK> (1).



5.1.3 Konfiguration - ibaCapture

Zum Erstellen eines verwalteten Dienstkontos gehen Sie nach den Schritten in Kapitel 5.1.1 vor und vergeben einen eindeutigen Namen sowie einen verständlichen Anzeigenamen für das neue Konto.

Nach dem erfolgreichen Erstellen des Kontos gehen Sie nach den Schritten in Kapitel 5.1.1.1 vor, um das neue Konto beim "ibaCapture Service" zu verwenden.

5.1.3.1 Verzeichnisberechtigungen

Damit *ibaCapture* Logs schreiben sowie die Konfiguration speichern kann, benötigt das neue Dienstkonto die Berechtigungen

- Ändern
- Lesen, Ausführen
- Ordnerinhalt anzeigen
- Lesen
- Schreiben

für die Verzeichnisse

- „C:\ProgramData\iba\ibaCapture\Server\log\“
- „C:\ProgramData\iba\ibaCapture\Server\Backup\“
- „C:\ProgramData\iba\ibaCapture\Server\MEMDIAG“
- „C:\ProgramData\iba\ibaCapture\Server\“
- „C:\ProgramData\iba\ibaCapture\Server\currentconfig.xml“

Wie Verzeichnisberechtigungen gesetzt werden, können Sie dem Abschnitt ↗ *Setzen von Verzeichnisberechtigungen*, Seite 24 entnehmen.

5.1.3.2 SNMP-Server

Da die SNMP Komponente in mehreren iba-Produkten zum Einsatz kommt, finden Sie deren Konfiguration im Kapitel ↗ *SNMP-Server-Komponente*, Seite 37.

5.1.4 Konfiguration - ibaDatCoordinator

Um den *ibaDatCoordinator* Dienst mit einem verwalteten Dienstkonto zu betreiben, folgen Sie den Schritten unter Punkt 5.1.1.1 und 5.1.2. In diesen beiden Abschnitten wird die Konfiguration am Beispiel von *ibaDatCoordinator* erklärt.

5.1.4.1 Verzeichnisberechtigungen

Damit *ibaDatCoordinator* die Konfiguration zwischenspeichern kann, muss die Anwendung in das Installationsverzeichnis schreiben können. Dazu benötigt das neue Dienstkonto die folgenden Berechtigungen für das Verzeichnis „C:\ProgramData\iba\ibaDatCoordinator“:

- Ändern
- Lesen, Ausführen
- Ordnerinhalt anzeigen
- Lesen
- Schreiben

Wie Verzeichnisberechtigungen gesetzt werden, können Sie dem Abschnitt ↗ *Setzen von Verzeichnisberechtigungen*, Seite 24 entnehmen.

5.1.4.2 DCOM-Berechtigungen

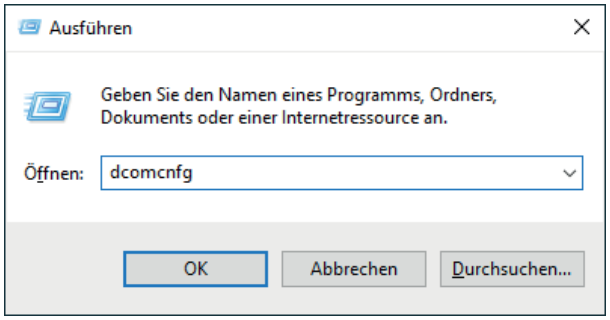
Sobald *ibaDatCoordinator* mit einem Dienstkonto betrieben wird, fehlt diesem Konto die Berechtigung zum Starten der Anwendung *ibaAnalyzer*.

Dies zeigt sich als folgendes Fehlerbild im Protokoll von *ibaDatCoordinator*:

```
Failed to create an instance of ibaAnalyzer: Retrieving the COM class factory for
component with CLSID {C4B00861-0324-11D3-A677-000000000000} failed due to the fol-
lowing error: 80070005 Access is denied. (Exception from HRESULT: 0x80070005 (E_
ACCESSDENIED)).
```

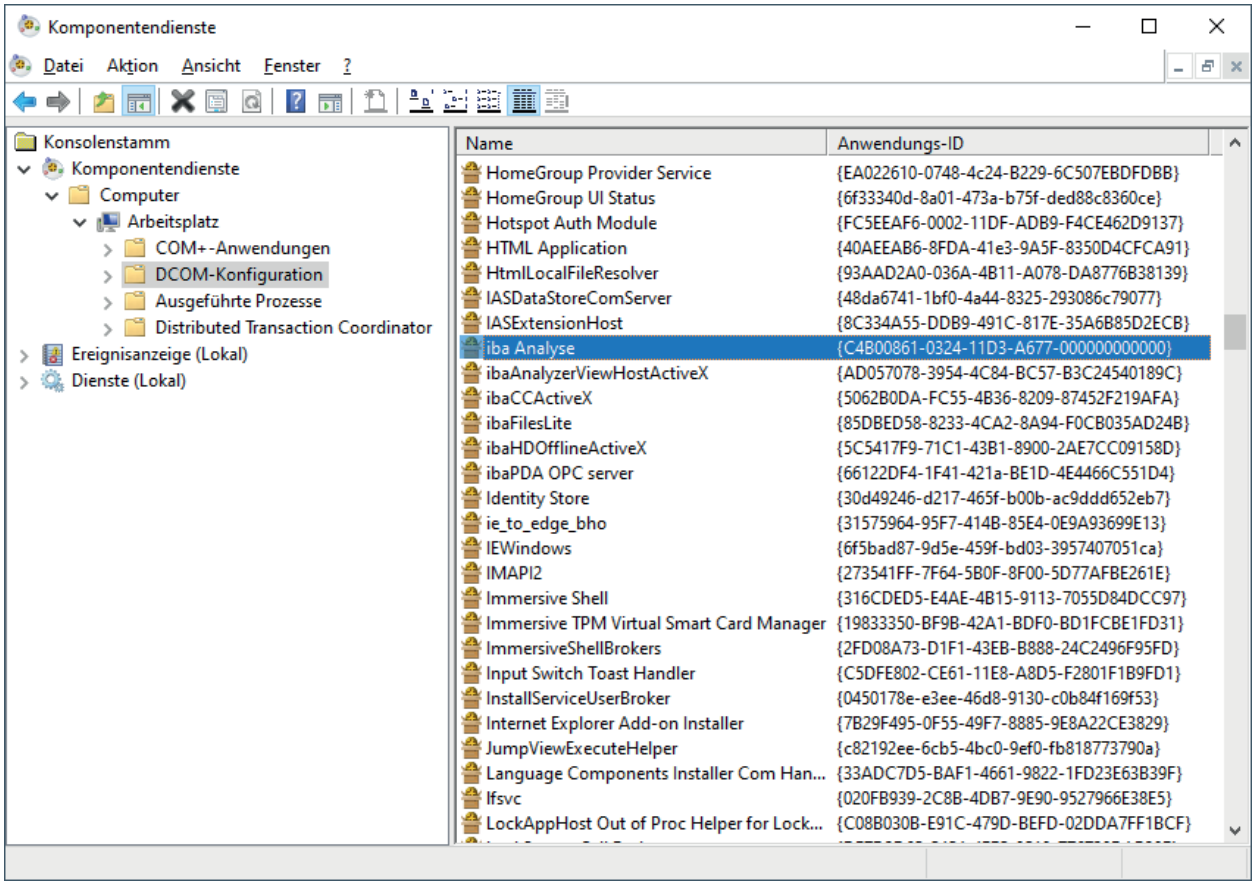
Um dieses Fehlerbild zu beseitigen, muss dem Dienstkonto erlaubt werden, *ibaAnalyzer* mittels der COM-Komponente zu starten. Hierzu müssen verschiedene Berechtigungen in der DCOM-Konfiguration vorgenommen werden. Gehen Sie dazu wie folgt vor:

1. Öffnen Sie die Komponentendienste mittels <Windows>+<R>, Eingabe von "dcomcnfg" und Selektion des Punktes DCOM-Konfiguration in der Baumansicht.

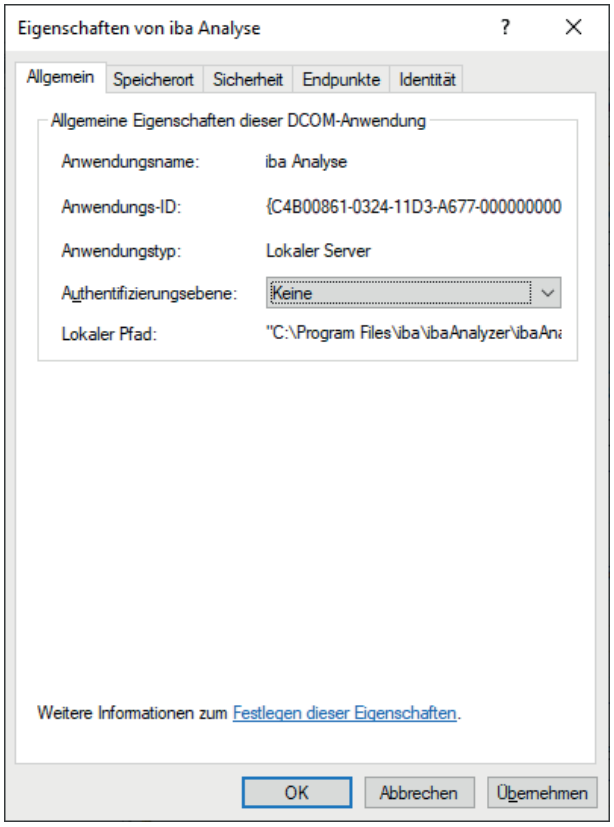


2. Als normaler Benutzer müssen Sie noch eine Autorisierung durchführen, um die Einstellungen ändern zu können.

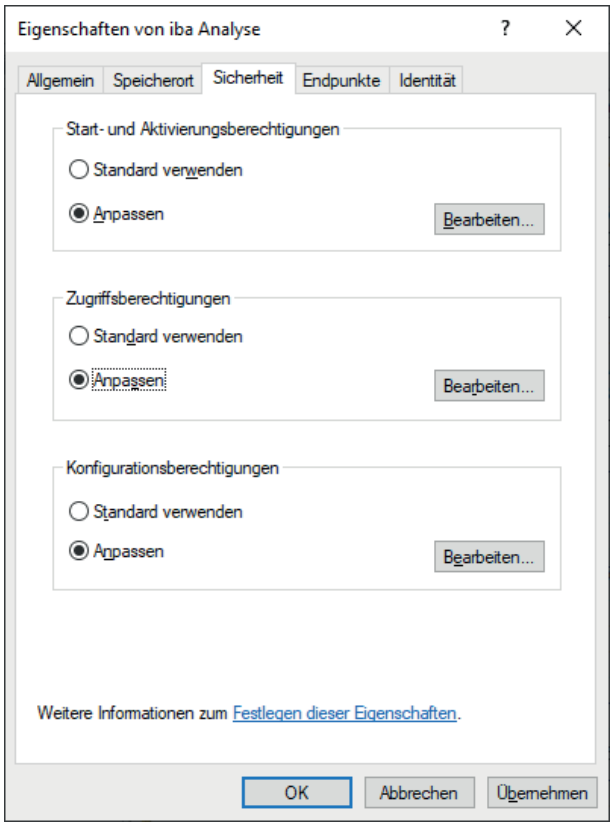
3. Schalten Sie um auf die Detailansicht.
4. Wählen Sie das Element "iba Analyse" aus und gleichen Sie die Anwendungs-ID mit der CL-SID aus der Fehlermeldung ab.



5. Öffnen Sie die Eigenschaften der Komponente.
6. Setzen Sie in der Lasche *Allgemein* die *Authentifizierungsebene* von "Standard" auf "Keine".

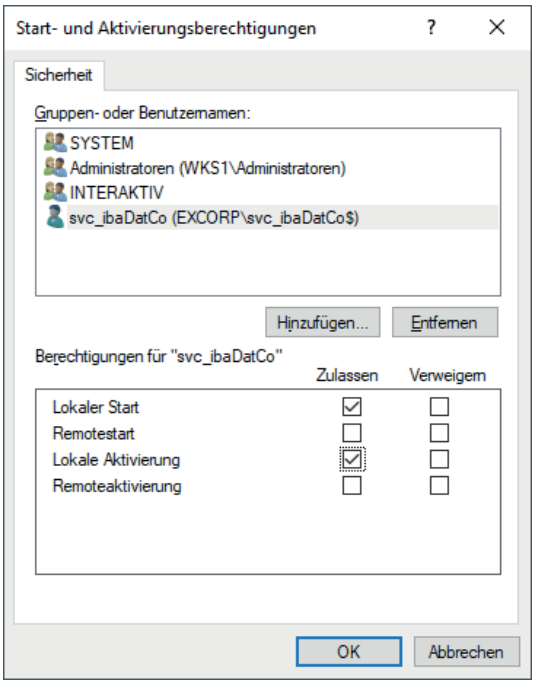


7. Wechseln Sie zur Lasche *Sicherheit*.
8. Wählen Sie bei *Start- und Aktivierungsberechtigungen* und bei *Zugriffsberechtigungen* jeweils den Punkt "Anpassen" aus.



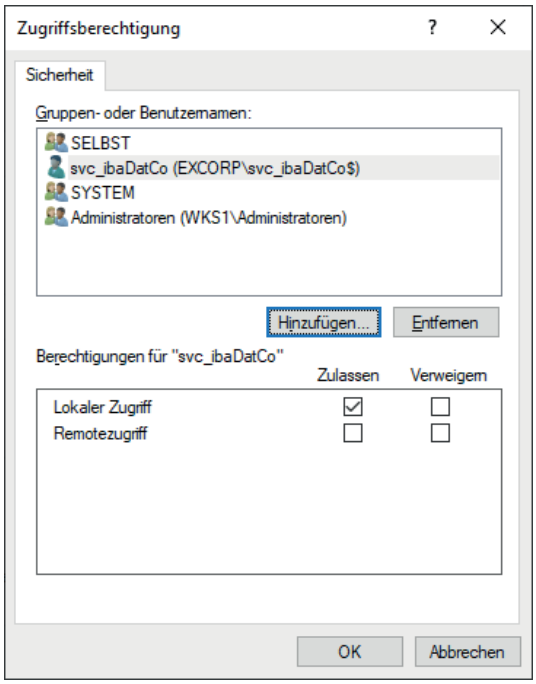
9. Fügen Sie den beiden Berechtigungsarten jeweils über <Bearbeiten...> das neue Dienstkonto hinzu und räumen Sie dem die folgenden Berechtigungen ein:

   - Start- und Aktivierungsberechtigungen
     - Lokaler Start
     - Lokale Aktivierung



   - Zugriffsberechtigungen

- Lokaler Zugriff



5.1.4.3 SNMP-Server

Da die SNMP Komponente in mehreren iba-Produkten zum Einsatz kommt, finden Sie deren Konfiguration im Kapitel ↗ *SNMP-Server-Komponente*, Seite 37.

5.1.5 Konfiguration - ibaDaVIS

5.1.5.1 Dienstkonfiguration

Gehen Sie für den Dienst „ibaDaVIS Service“ anhand der beispielhaften Konfiguration im Abschnitt ↗ *Verwaltetes Dienstkonto verwenden*, Seite 20 vor und verwenden das entsprechende Dienstkonto für den Dienst.

5.1.5.2 Verzeichnisberechtigungen

Damit *ibaDaVIS* die Konfiguration speichern sowie Logs anlegen kann, benötigt das Dienstkonto die folgenden Rechte für das Verzeichnis „C:\ProgramData\iba\ibaDaVIS“.

- Ändern
- Lesen, Ausführen
- Ordnerinhalt anzeigen
- Lesen
- Schreiben

Wie Verzeichnisberechtigungen gesetzt werden, können Sie dem Abschnitt ↗ *Setzen von Verzeichnisberechtigungen*, Seite 24 entnehmen.

5.1.5.3 Öffentlich zugänglich

Wenn *ibaDaVIS* über ein öffentliches Netz erreichbar sein soll, so muss das System mindestens mit einer Firewall geschützt werden. Als weitere Schicht empfiehlt sich der Einsatz eines Reverse Proxys, sodass keine direkte Kommunikation zwischen den Clients und *ibaDaVIS* erfolgt. In der Firewall muss der entsprechende Port für das Webinterface (siehe ↗ *ibaDaVIS*, Seite 61) von *ibaDaVIS* freigeschaltet werden. Durch die Kanalisierung des Datenverkehrs über den Reverse Proxy können auch noch weitere Schutzmaßnahmen ergriffen werden. Dies können Virenscanner oder auch Paketfilter sein. Wenn der Reverse Proxy ebenfalls zur Verschlüsselung des Datenverkehrs mittels SSL-Zertifikat eingesetzt wird, entlastet dies den *ibaDaVIS* Webserver.

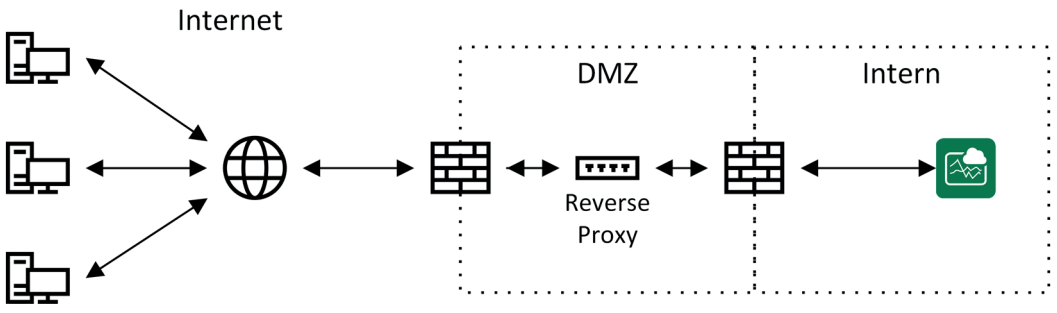


Abb. 9: Betrieb mit Firewall und Reverse Proxy

5.1.6 Konfiguration - ibaManagementStudio

Zum Erstellen eines verwalteten Dienstkontos folgen Sie den Schritten unter ↗ *Verwaltetes Dienstkonto erstellen*, Seite 19 und vergeben einen eindeutigen Namen sowie einen verständlichen Anzeigenamen für das neue Konto.

Nach dem erfolgreichen Erstellen des Kontos folgen Sie den Schritten unter ↗ *Verwaltetes Dienstkonto verwenden*, Seite 20, um das neue Konto beim Agenten bzw. Server zu verwenden.

Komponente	Anzeigename
Agent	ibaManagementStudio Agent service
Server	ibaManagementStudio service

5.1.6.1 Verzeichnisberechtigungen

Damit der entsprechende Dienst die Konfiguration zwischenspeichern kann, muss die Anwendung in bestimmte Verzeichnisse schreiben können. Dazu benötigt das neue Dienstkonto die folgenden Berechtigungen für das Verzeichnis „C:\ProgramData\iba\ibaManagementStudio\“ und dessen Unterordner:

- Ändern
- Lesen, Ausführen
- Ordnerinhalt anzeigen
- Lesen
- Schreiben

Wie Verzeichnisberechtigungen gesetzt werden, können Sie dem Abschnitt ↗ *Setzen von Verzeichnisberechtigungen*, Seite 24 entnehmen.

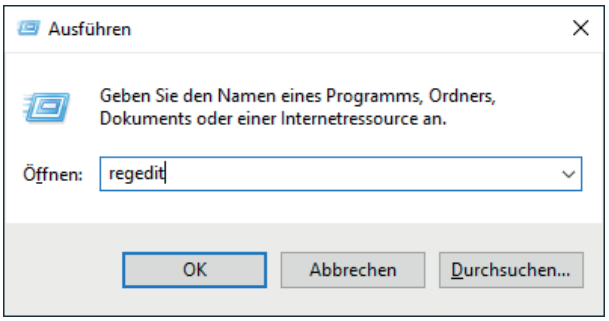
5.1.7 SNMP-Server-Komponente

Damit der SNMP-Server funktioniert, benötigt dieser Lese-/Schreib-Zugriff auf bestimmte Pfade in der Registry:

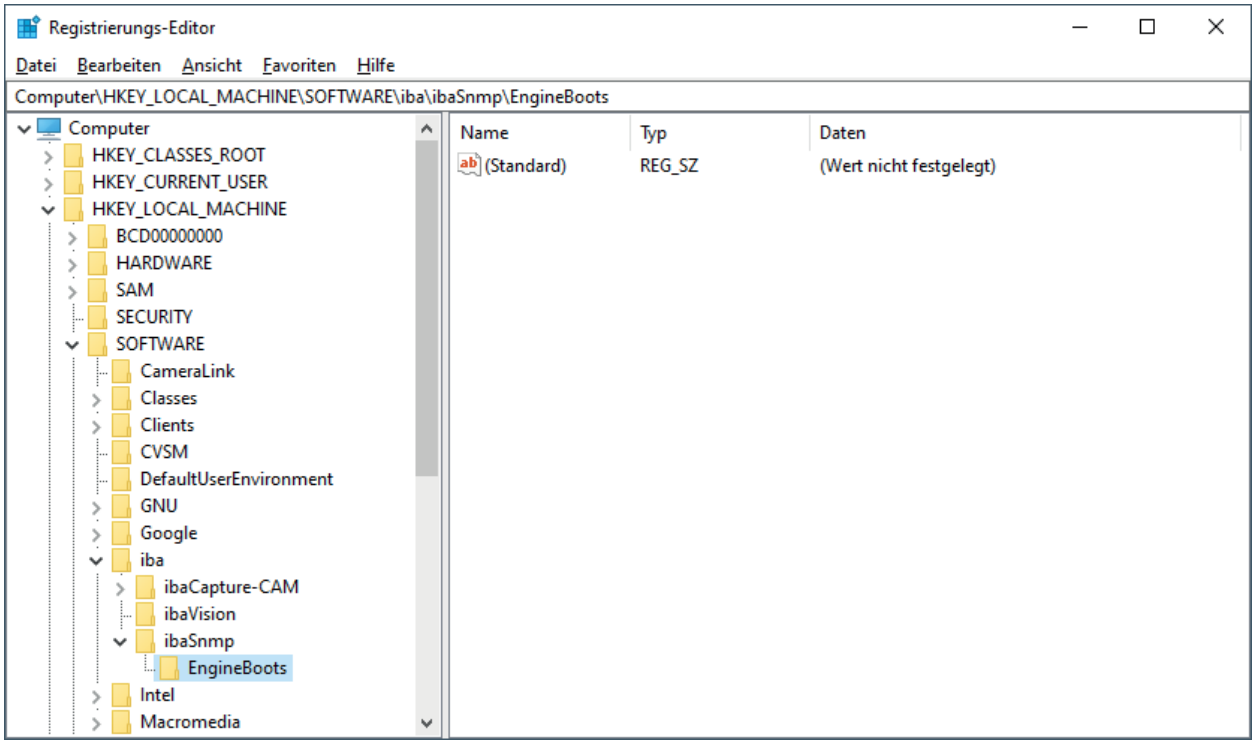
```
HKEY_LOCAL_MACHINE\SOFTWARE\iba\ibaSnmp\EngineBoots\
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\iba\ibaSnmp\EngineBoots\
```

Gehen Sie wie folgt vor.

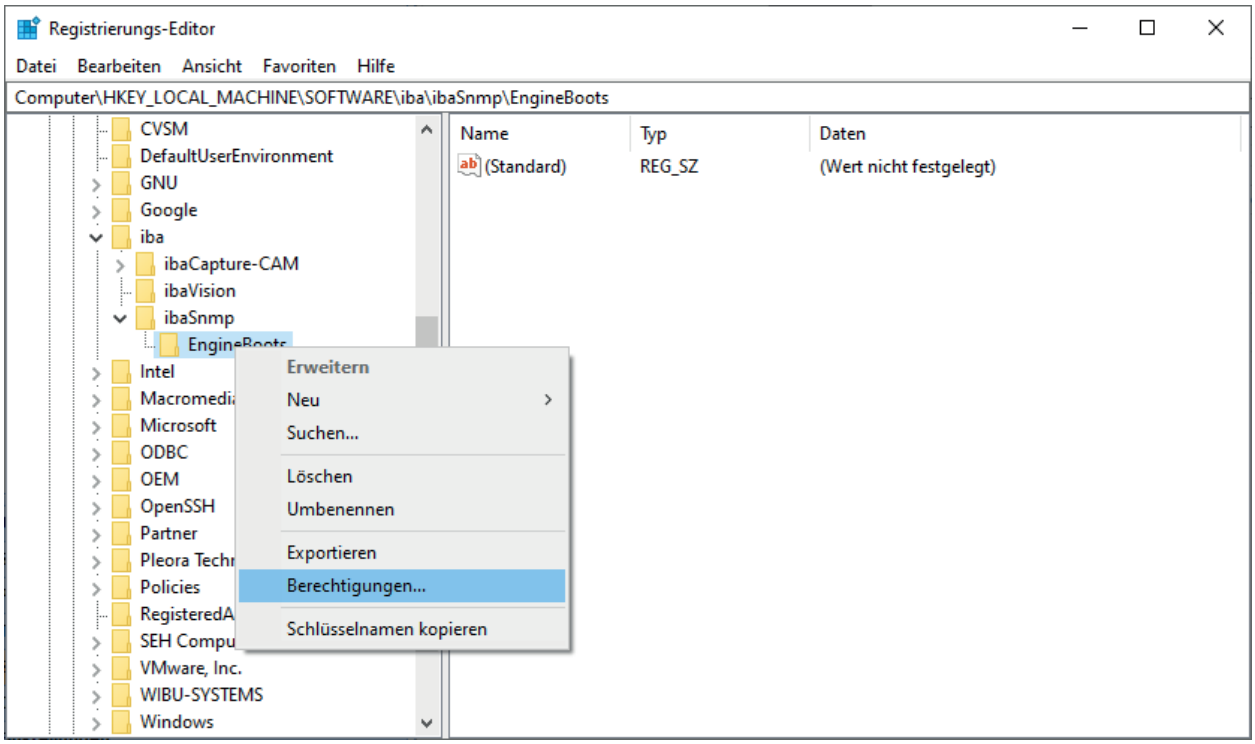
1. Öffnen Sie den Registrierungseditor mit <Windows>+<R> und Eingabe von "regedit".



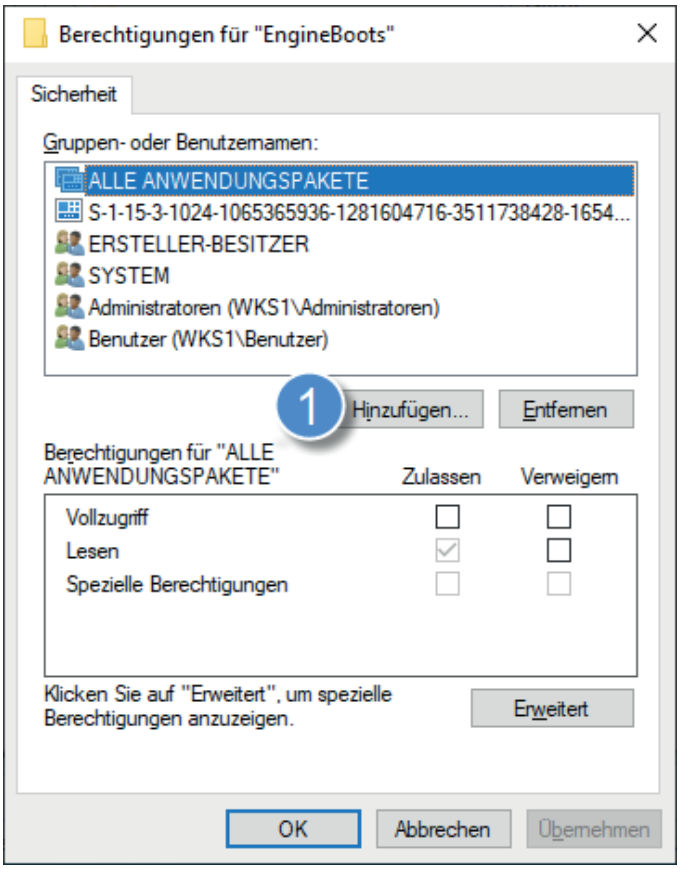
2. Navigieren Sie zum ersten der oben genannten Pfade bzw. Schlüssel.
   Sollte dieser nicht existieren, dann erstellen Sie ihn.



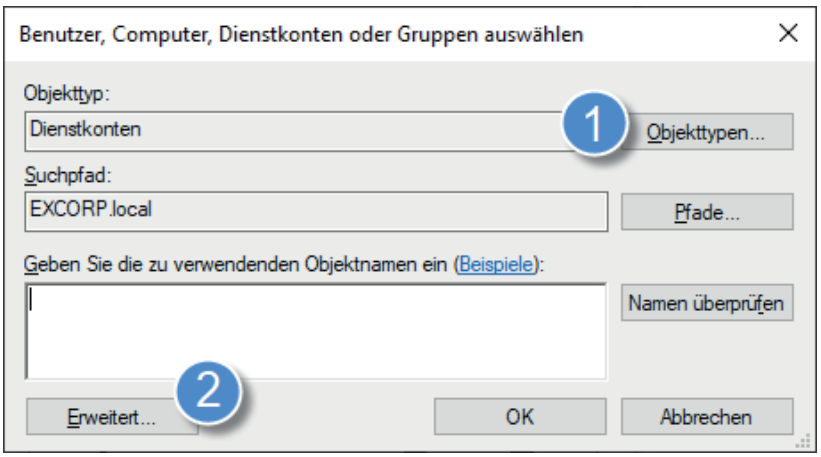
3. Öffnen Sie den Punkt *Berechtigungen…* im Kontextmenü des Schlüssels *EngineBoots*



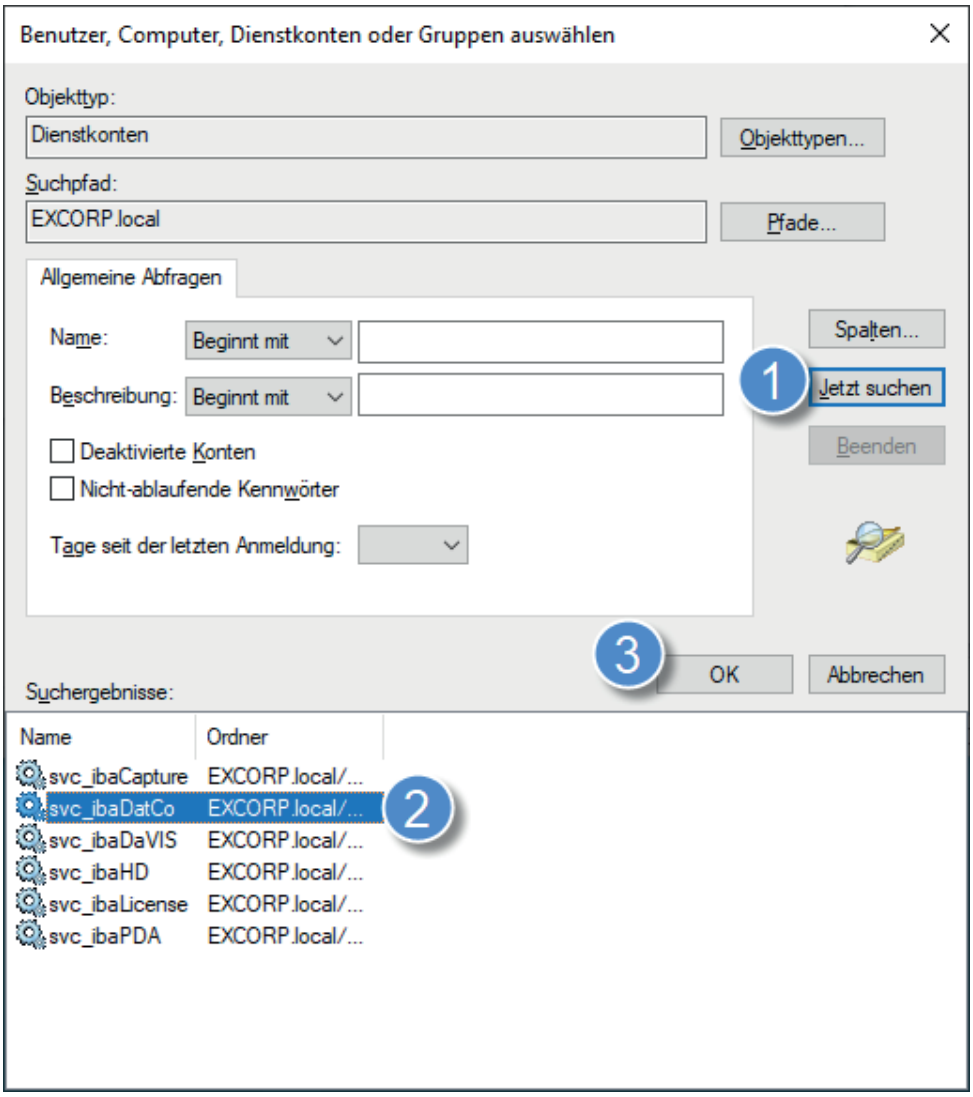
4. Klicken Sie im Dialog "Berechtigungen" auf <Hinzufügen>, um das neue Dienstkonto hinzuzufügen.



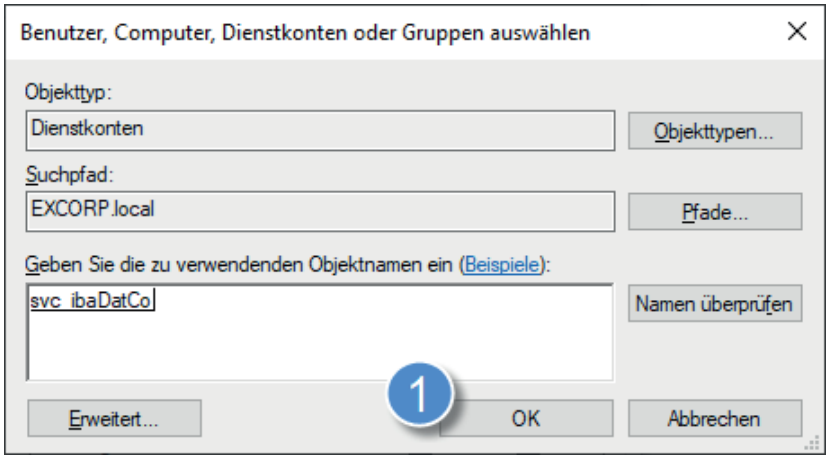
5. Wählen Sie anschließend mit <Objekttypen...> "Dienstkonten" aus und klicken Sie anschließend auf <Erweitert...>.



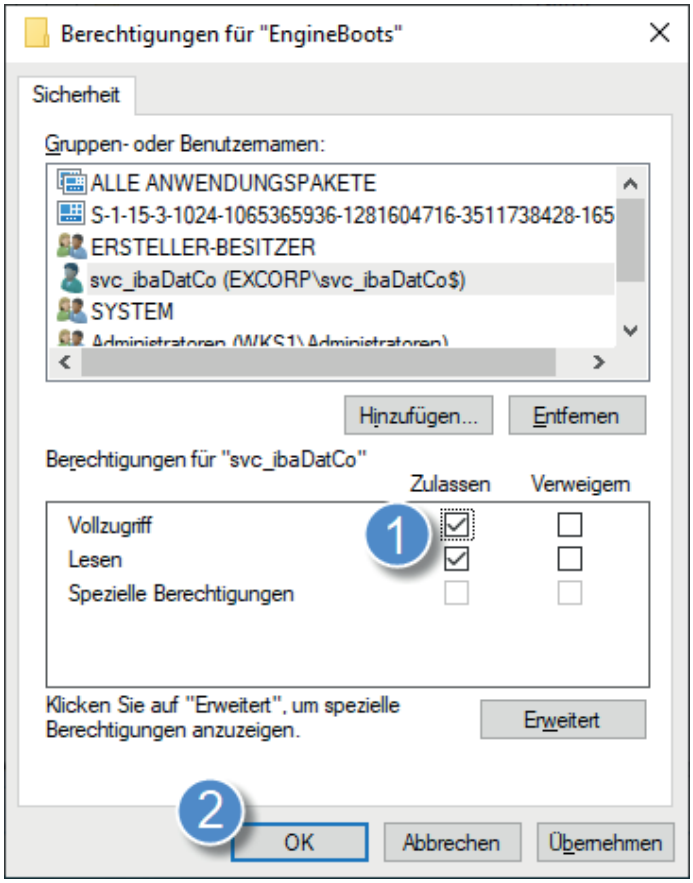
6. Klicken Sie auf <Jetzt suchen>, wählen Sie anschließend das gewünschte Dienstkonto aus den Suchergebnissen aus und verlassen Sie den Dialog mit <OK>.



7. Verlassen Sie den Dialog mit <OK>.



8. Gewähren Sie dem hinzugefügten Konto im Feld *Berechtigungen* "Vollzugriff" und schließen Sie den Dialog mit <OK>.



9. Wiederholen Sie die Schritte 2 bis 8 für den zweiten Schlüssel.

5.2 Benutzerverwaltung

Die iba-Softwareprodukte bieten in der Regel eine Benutzerverwaltung, die für die Verwaltung lokaler Benutzer und deren Berechtigungen in dem betreffenden Programm genutzt werden kann. In den meisten Fällen werden auch Domänenbenutzter per Active Directory unterstützt (siehe Tabelle). Damit werden nicht nur lokale Benutzer der Programme akzeptiert sondern auch Domänenbenutzer oder -gruppen, die von der IT-Administration definiert wurden.

Software	Lokaler Benutzer	Domänenbenutzer
ibaPDA	•	•
ibaHD-Server	•	•
ibaCapture	•	•
ibaDaVIS	•	•
ibaManagementStudio	•	•
ibaDatCoordinator	-	-
ibaLogic	•	-
ibaAnalyzer	-	-
ibaCMC	•	-

Grundsätzlich betreffen die in der Benutzerverwaltung verwalteten Rechte ausschließlich Funktionen der jeweiligen Software. Berechtigungseinschränkungen dienen dazu, missbräuchliche oder versehentliche Fehlbedienungen der jeweiligen Software zu vermeiden. Sie haben aber wenig Relevanz bzgl. IT-Sicherheit.

Andere Dokumentation

Eine ausführliche Beschreibung der Benutzerverwaltung finden Sie jeweils im Handbuch zum Softwareprodukt.

5.3 Zertifikate

Zur Absicherung des Datenaustauschs zu anderen Systemen oder Applikationen und zur Authentifizierung der Kommunikationspartner werden zum Teil Zertifikate verwendet.

Dazu gehören:

- ibaPDA OPC UA-Server
- ibaPDA MQTT (Interface und Datenaufzeichnung)
- ibaHD-Server mit ibaDaVIS via ibaHD-API
- ibaHD-Server OPC UA-Server
- ibaDaVIS mit ibaHD-Server via ibaHD-API
- ibaDaVIS mit Web-Client
- ibaDatCoordinator OPC UA-Server

5.3.1 Funktionsweise

Wenn auch unbewusst, werden Zertifikate täglich verwendet. Beispielsweise beim Besuch einer Webseite, z. B. https://www.iba-ag.com, wird die Verbindung mit Hilfe von Zertifikaten abgesichert.

Zertifikate selbst beinhalten verschiedene Informationen über den Inhaber (z. B. Firma, Name, E-Mail-Adresse usw.) sowie zwei weitere Teile, einen privaten Schlüssel, der geheimgehalten wird, und einen öffentlichen Schlüssel, den jeder kennen darf.

Damit man bei der Vertrauensfrage von Zertifikaten nicht mit dem "Henne-Ei-Problem" konfrontiert wird, haben externe Zertifizierungsstellen die Eigenschaft, dass Ihnen blind vertraut wird. Um die Funktion des "Blind-Trust" sicherzustellen, sind die Zertifikate der externen Zertifizierungsstellen im Betriebssystem und im Webbrowser integriert.

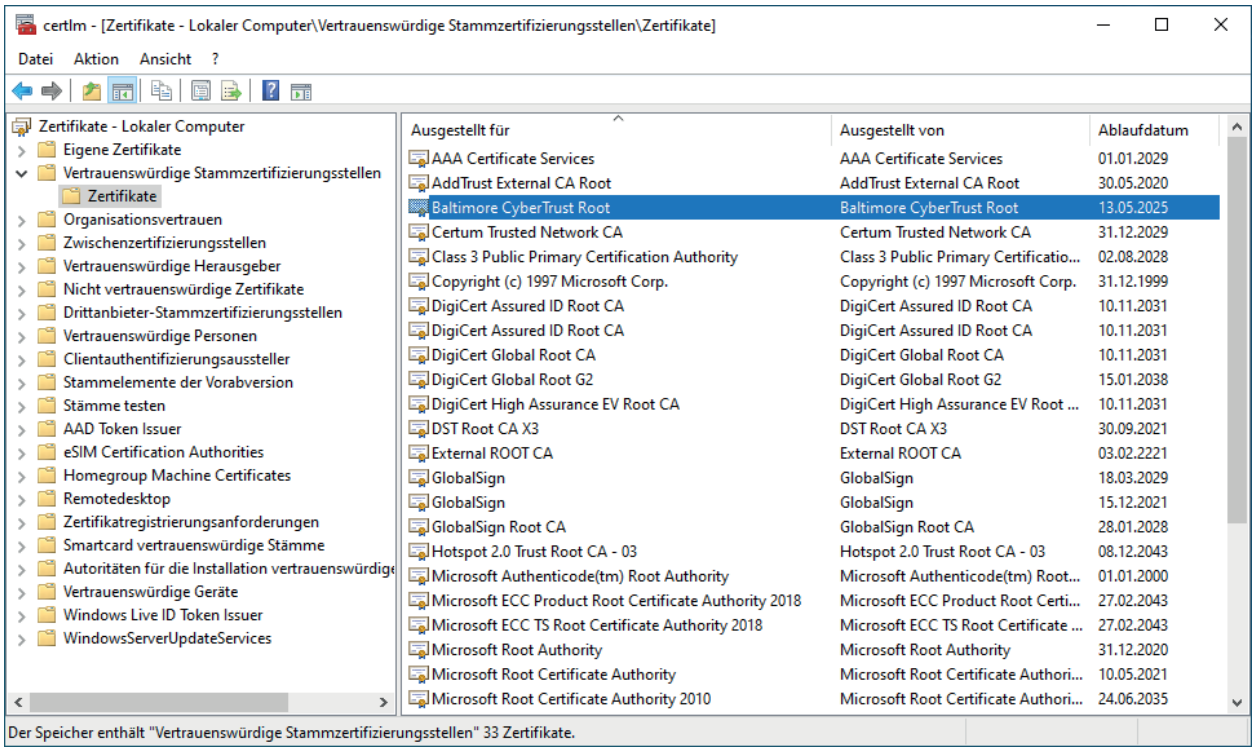


Abb. 10: Windows Zertifikatsspeicher

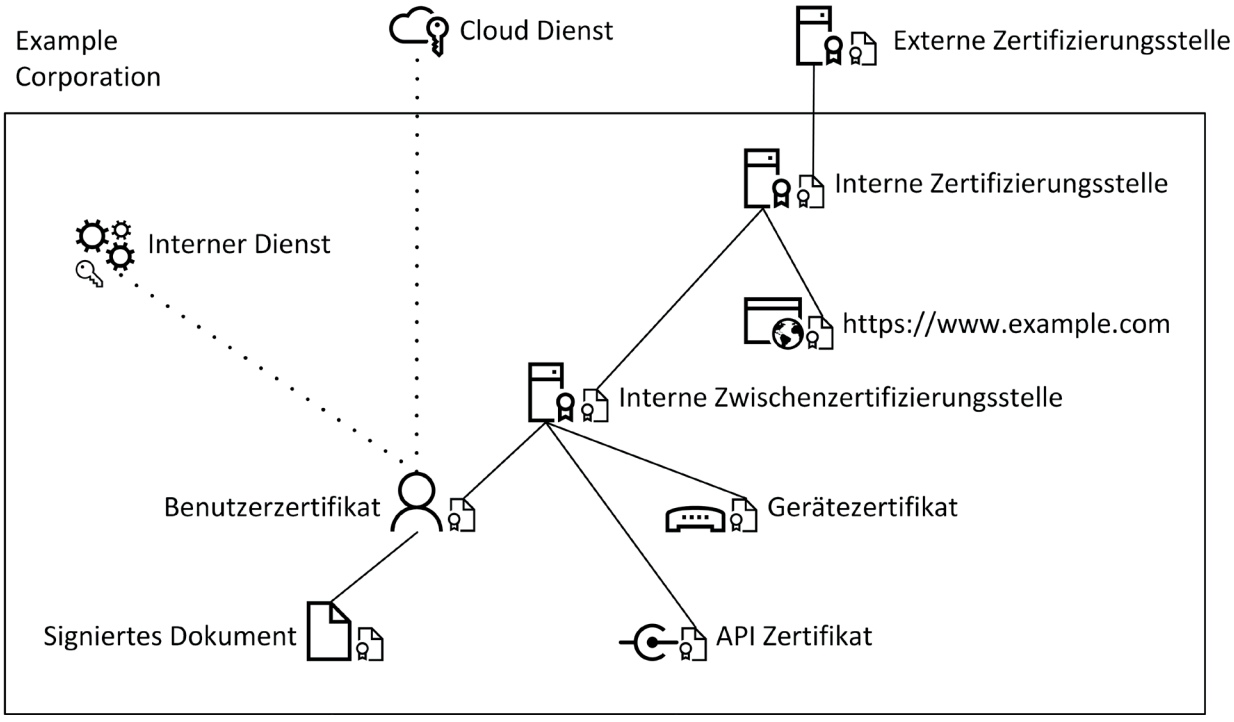


Abb. 11: Beispielarchitektur der Domäne Excorp mit Zertifizierungsstellen

Beispielablauf für die interne Zertifizierungsstelle

1		Interne Zertifizierungsstelle
2		Erstellt einen privaten Schlüssel während der ersten Einrichtung
3		Erstellt eine Zertifikatsanfrage (CSR) und sendet diese zur externen Stelle
4		Externe Zertifizierungsstelle
5		Signiert die Anfrage (CSR) und stellt das Zertifikat (CRT) aus
6		Signiertes Zertifikat (CRT) wird bei der internen Stelle hinterlegt
7		Interne Zertifizierungsstelle mit validem Zertifikat

Tab. 3: Ablauf - Ausstellung eines Zertifikats

Bei der ersten Einrichtung hat die interne Zertifizierungsstelle kein oder nur ein selbstsigniertes Zertifikat. Damit andere der Stelle vertrauen, stellt sie zunächst eine Zertifikatsanfrage aus. Diese wird dann bei der externen Zertifizierungsstelle geprüft und signiert. Als Resultat erhält man das Zertifikat für die interne Stelle, das durch die externe Stelle signiert wurde. Dadurch ergibt sich ein Zertifizierungspfad von der externen zur internen Stelle. Da der externen Stelle blind vertraut wird und diese die interne Stelle signiert hat, wird auch dieser Stelle vertraut. Wenn die interne Stelle wiederum ein Zertifikat ausstellt, z. B. für eine Webseite der Organisation, wird diesem Zertifikat ebenfalls aufgrund des Zertifizierungspfads vertraut.

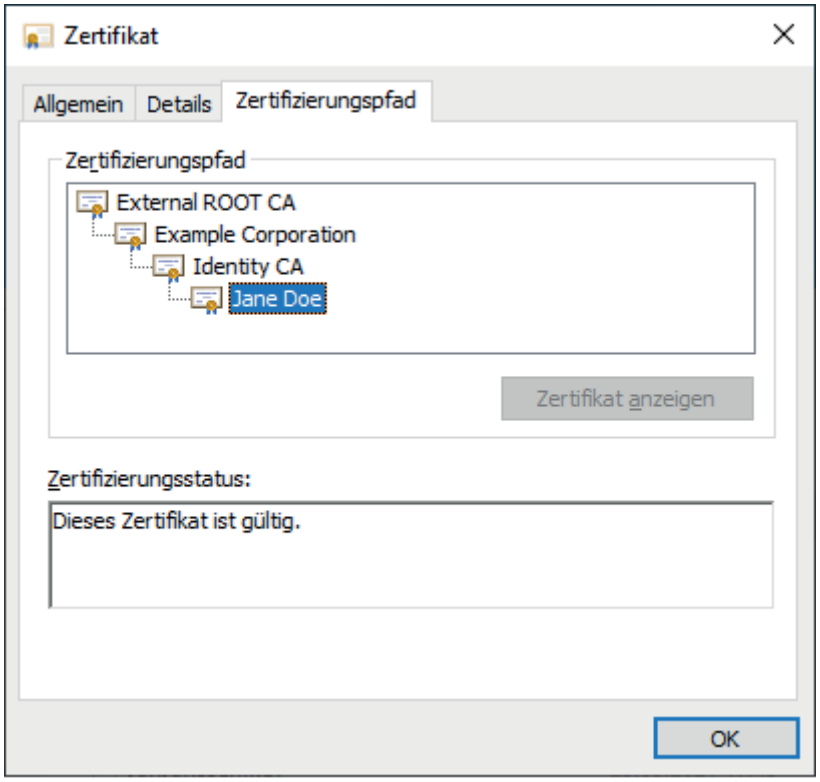


Abb. 12: Zertifizierungspfad

Wie zu sehen ist, wird dem Zertifikat für Jane Doe aufgrund des durchgängigen Zertifizierungspfades vertraut, da die Zwischenzertifizierungsstelle (Identity CA) durch die interne Zertifizierungsstelle signiert wurde.

Inhalt eines CSR (dekodiert)

```
Certificate Request:
    Data:
        Version: 1 (0x0)
        Subject: C = US, ST = Georgia, L = Alpharetta,
                 O = Example Corporation, CN = Jane Doe
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:af:71:5e:f6:08:f2:3c:67:ee:ba:cb:b7:03:c2:
                    ...
                Exponent: 65537 (0x10001)
        Attributes:
            a0:00
    Signature Algorithm: sha256WithRSAEncryption
         1b:22:14:81:55:38:2a:7e:4c:f6:82:84:72:35:e3:23:d6:25:
         ...
```

Neben dem Öffentlichen Schlüssel (Public Key) befinden sich im CSR noch die Informationen über den Antragssteller.

- Country (C): Ländercode
- State (ST): Bundesland/Bundesstaat
- Locality (L): Stadt
- Organization (O): Firma
- Common Name (CN): Name des Antragsstellers oder FQDN

Optional:

- Organizational Unit (OU): Abteilungsname innerhalb der Firma
- emailAddress: Kontaktadresse

Inhalt eines signierten Zertifikats (dekodiert):

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            7d:fd:25:09:b6:5b:57:63:0f:21:0d:e6:14:79:93:47:4c:0f:da:ee
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN = Identity CA, ST = Bavaria, C = DE,
                emailAddress = it@excorp.local, O = Identity CA,
                OU = IT-Department, L = Fuerth
        Validity
            Not Before: Mar 23 16:49:31 2021 GMT
            Not After : Mar 23 16:49:31 2023 GMT
        Subject: C = US, ST = Georgia, L = Alpharetta,
                 O = Example Corporation, CN = Jane Doe
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:af:71:5e:f6:08:f2:3c:67:ee:ba:cb:b7:03:c2:
                    ...
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Authority Key Identifier:
                keyid:1D:D2:37:DD:9B:CF:DE:DC:14:71:87:D0:C9:4B:5D:3C:B7:C0:B4:D5
            X509v3 Key Usage:
                Digital Signature, Non Repudiation, Key Encipherment,
                Data Encipherment
    Signature Algorithm: sha256WithRSAEncryption
         7d:ab:3b:b0:24:e6:3b:09:69:27:ad:9f:fa:1e:0a:fb:84:4d:
         ...
```

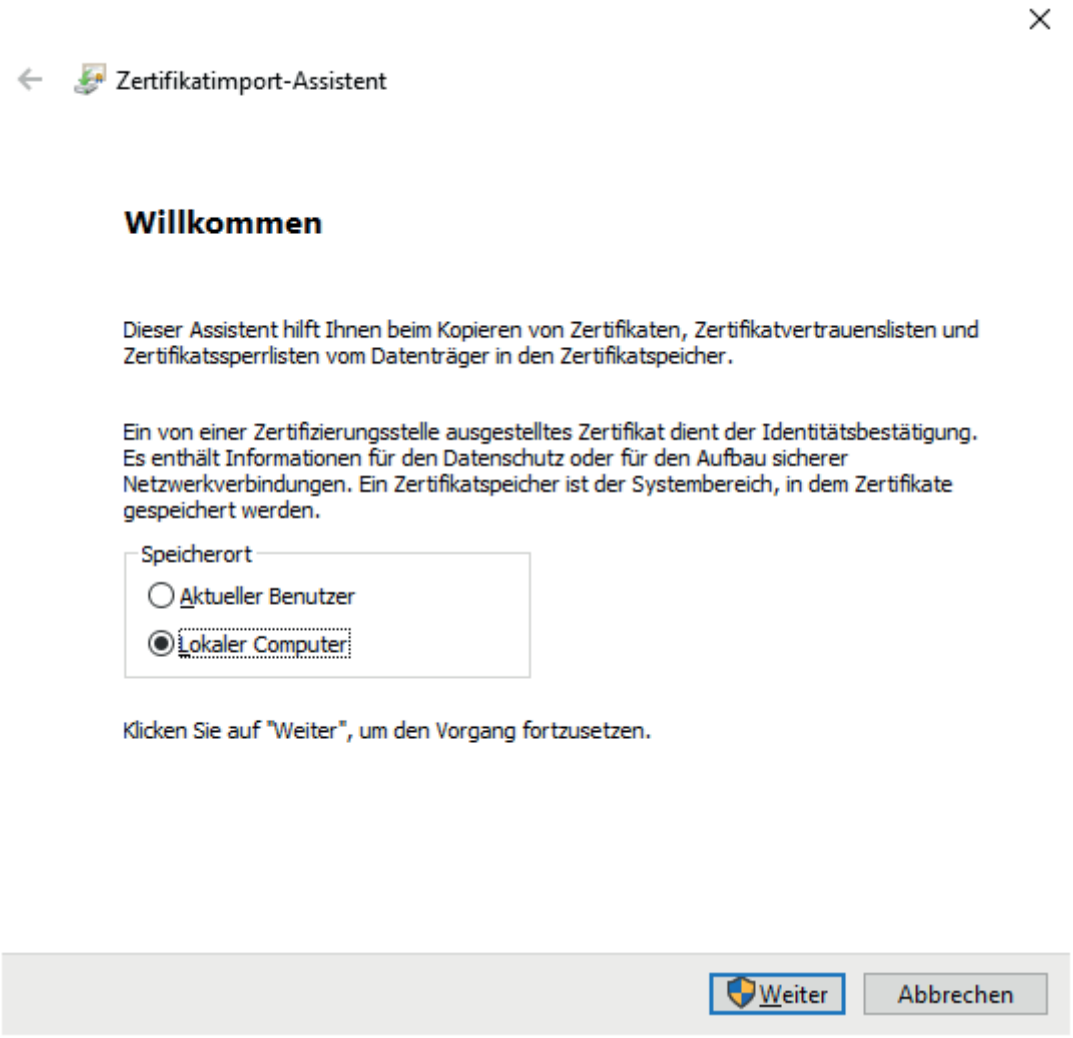
Nach dem Signieren der Zertifikatsanfrage enthält das Zertifikat dann ebenfalls Informationen über die Zertifizierungsstelle sowie Gültigkeit und erlaubte Verwendungszwecke (X509v3 Key Usage) des Zertifikats.

Um sich mit dem Zertifikat z. B. bei internen oder externen (Cloud) Diensten zu authentifizieren, muss nur der Öffentliche Schlüssel (Public Key) bei dem entsprechenden Dienst hinterlegt werden. Danach kann sich der Benutzer oder das Gerät ohne Passwort beim Dienst anmelden.

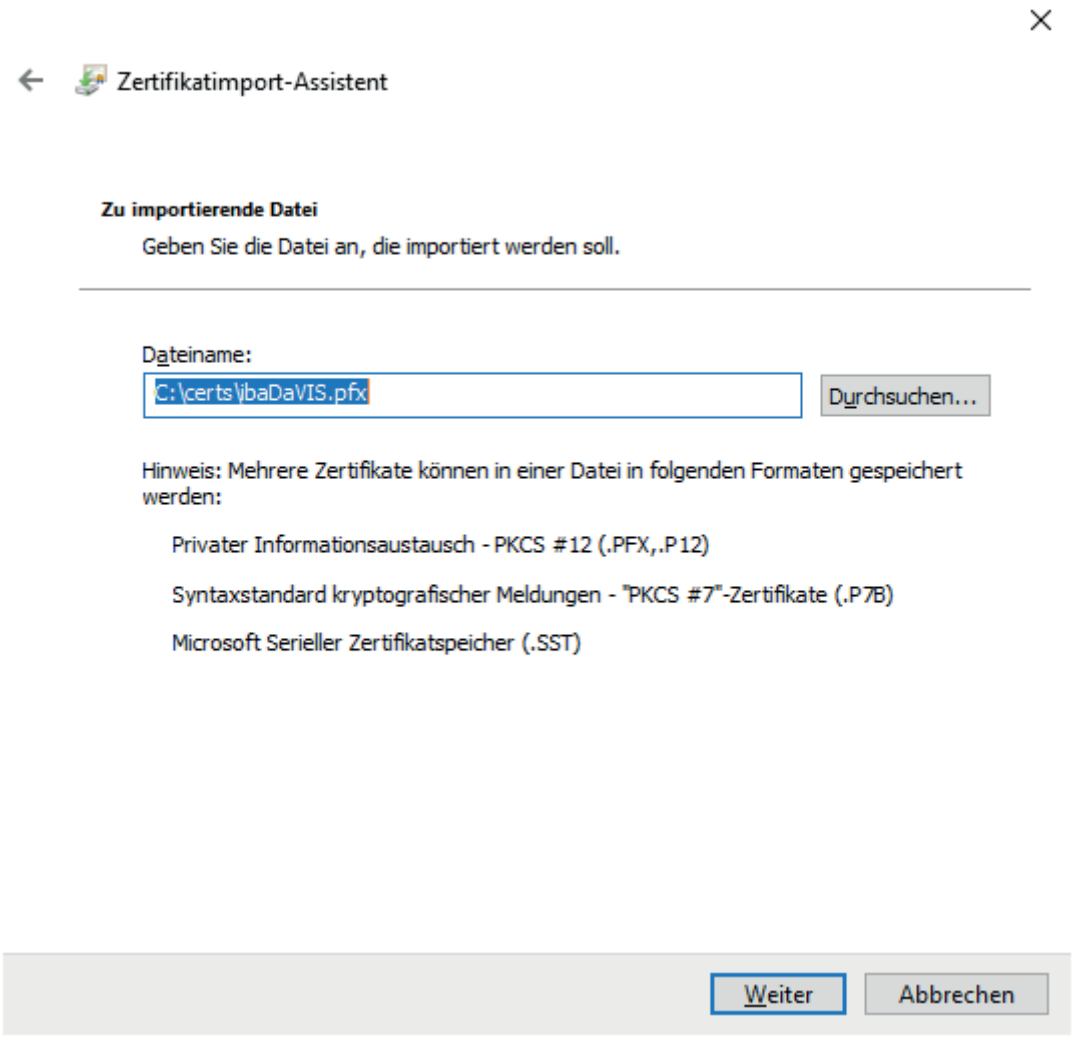
5.3.2 Installation eines Zertifikats im Zertifikatspeicher

Die Installation eines Zertifikats mit privatem Schlüssel kann auf mehrere Arten durchgeführt werden. In diesem Abschnitt wird gezeigt, wie eine PFX-Datei mittels des Zertifikatimport-Assistenten installiert wird.

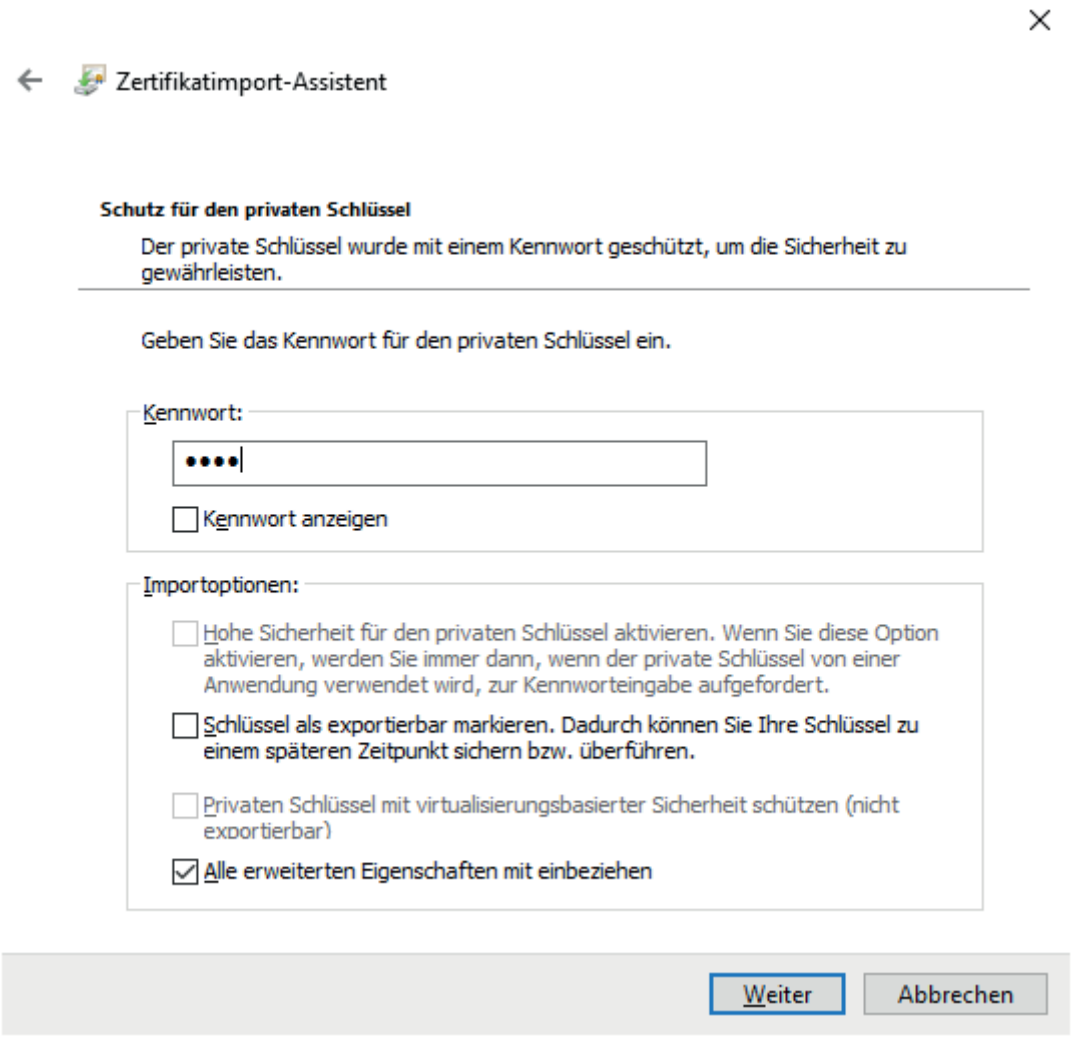
1. Machen Sie einen Doppelklick auf die PFX-Datei. Es öffnet sich der Assistent.



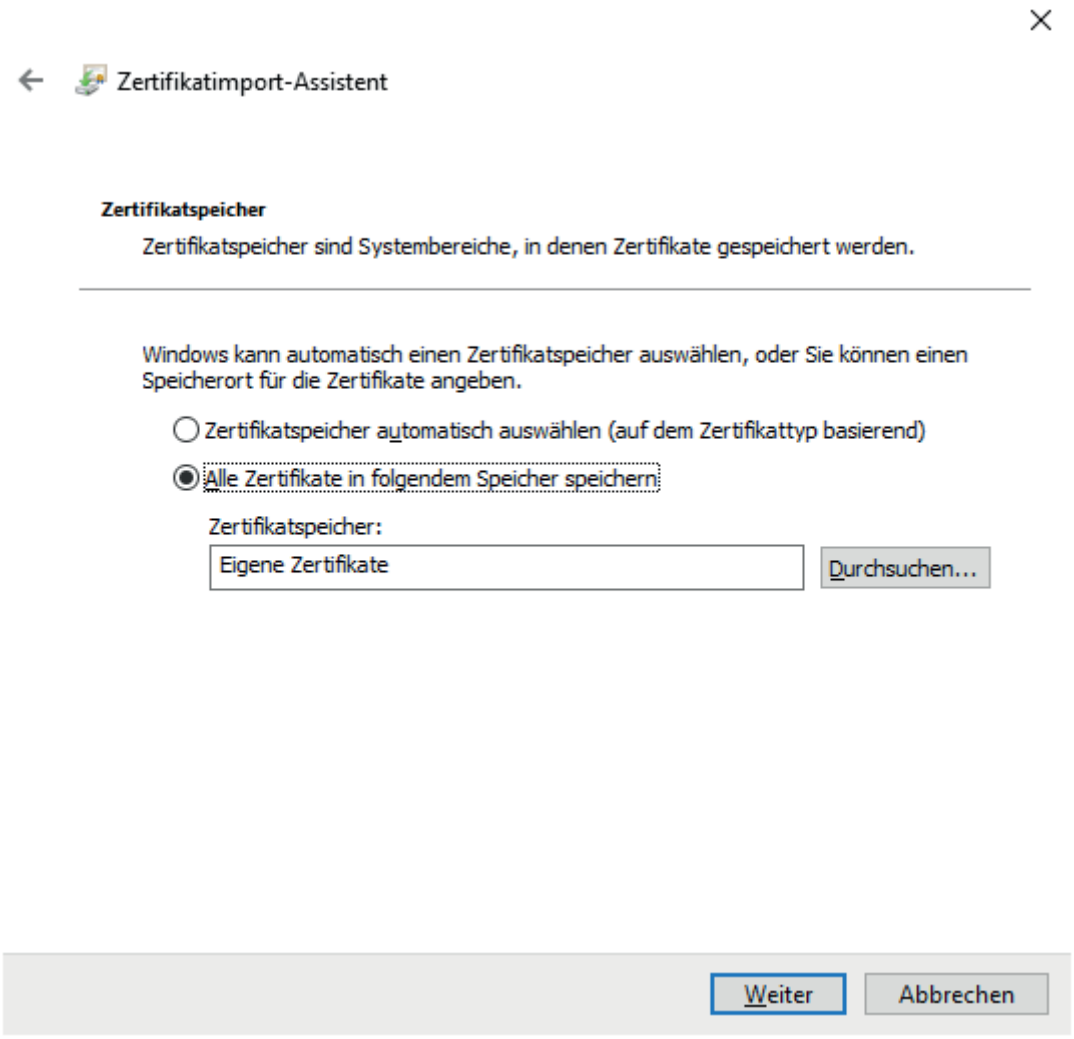
2. Wählen Sie "Lokaler Computer", klicken Sie auf <Weiter>.



3. Prüfen Sie, ob Pfad und Dateiname korrekt sind. Falls nicht, können Sie mit <Durchsuchen...> zur korrekten Datei navigieren. Klicken Sie auf <Weiter>.



4. Geben Sie das Kennwort der PFX-Datei ein und klicken Sie auf <Weiter>.



5. Wählen Sie die zweite Option *Alle Zertifikate in folgendem Speicher sichern* und wählen Sie dann mithilfe von <Durchsuchen> den Zertifikatspeicher "Eigene Zertifikate" aus.
6. Klicken Sie auf <Weiter> und überprüfen Sie die Einstellungen. Anschließend mit <Fertigstellen> den Import abschließen.

5.3.3 Zertifikate bei iba Softwareprodukten

Einige iba Softwareprodukte nutzen Zertifikate zur Absicherung der Kommunikation.

Sie greifen dazu in der Regel auf einen zentralen Zertifikatspeicher zu, in dem alle Zertifikate erfasst und verwaltet werden. Bei Bedarf können Zertifikate neu erzeugt werden.

Softwareprodukt	Für Kommunikation mit ...	Typ/Algorithmus	Sicherheitsrichtlinien
ibaPDA	MQTT-Broker	X.509/SHA-256 X.509/SHA-384 X.509/SHA-512	
	OPC UA-Clients		**OPC UA-Server:** Basic 128RSA15 (veraltet) Basic 256 (veraltet) Basic256Sha256 Aes128-Sha256-RsaOaep Aes256-Sha256-RsaPss
ibaDatCoordinator	OPC UA-Clients		
ibaHD-Server	OPC UA-Clients		
	ibaDaVIS via ibaHD-API		
ibaDaVIS	ibaHD-Server via ibaHD-API		
	Web-Clients Oberfläche	SSL	

Andere Dokumentation

Eine ausführliche Beschreibung der Nutzung von Zertifikaten finden Sie jeweils im Handbuch zum Softwareprodukt.

5.3.4 Speichern und Schützen von Zertifikaten

Die Zertifikate werden in der Datei `settings.xml` gespeichert, die im Ordner `c:\ProgramData\iba\Name der Applikation\Certificates` liegt. Diese Datei wird automatisch verschlüsselt.

Für die Verwendung von Zertifikaten mit privatem Schlüssel gibt es eine Reihe von Maßnahmen, um Ihre Identität oder die Identität Ihrer Organisation zu schützen. Konkret sind dies Maßnahmen, um den einfachen Export und die Weiterverwendung in Windows oder anderen Applikationen zu erschweren.

- Zertifikate werden stets in verschlüsselter Form gespeichert.
- Für Zertifikate mit privatem Schlüssel ist die Eingabe eines Kennworts erforderlich,...
  - wenn ein neues Zertifikat erzeugt wird
  - wenn ein Zertifikat mit privatem Schlüssel exportiert wird
  - wenn ein Zertifikat mit privatem Schlüssel importiert wird
- Zertifikate mit privatem Schlüssel können nur exportiert werden, wenn es für den Schlüssel auch ein Kennwort gibt. Gibt es kein Kennwort oder ist das Kennwort unbekannt, kann das Zertifikat nicht mehr exportiert werden. Bewahren Sie daher die Kennwörter an einem sicheren Ort auf.
- Das Kennwort eines privaten Schlüssels kann nicht geändert werden.
- Für die Nutzung eines Zertifikats ist keine Kennworteingabe erforderlich. Die Datei `settings.xml` kann von einer Installation zu einer anderen kopiert werden, um die Zertifikate dorthin zu übertragen. Auch dafür ist keine Kennworteingabe nötig.

Falls der private Schlüssel in die falschen Hände gerät, sind viele Formen des Missbrauchs denkbar. Daher achten Sie auf die sichere Verwahrung der Kennwörter.

5.4 Ports

Damit iba-Software richtig funktioniert, müssen gewisse Ports in der Firewall der Systeme freigeschaltet werden, auf denen der Dienst (Server) läuft. Die Ports in den folgenden Abschnitten sind dabei unterteilt in Ports, die ein Dienst von sich aus immer öffnet und Ports, die nur bei Bedarf verwendet werden. Des Weiteren handelt es sich bei den Angaben um Standardports, die zum Teil geändert werden können ("modifizierbar").

5.4.1 ibaPDA Service

Ports, die ibaPDA-Server (Dienst) öffnet

Schnittstelle	Port-Bereich		Protokoll	Multicast-Adressen	Bemerkung
ibaPDA Client*	9170	9170	TCP		Modifizierbar
ibaPDA Discovery	12800	12800	UDP	IPv4: 226.254.92.220	Fest

Tab. 4: Ports, die ibaPDA öffnet

Ports, die ibaPDA-Server (Dienst) nach Bedarf nutzt
Die verwendeten Ports sind abhängig von der Lizenz des Produkts. Ist eine Schnittstelle nicht lizenziert, so wird der entsprechende Port auch nicht verwendet.

Schnittstelle	Port-Bereich		Protokoll	Multicast-Adressen	Bemerkung
AB-Xplorer (1761-NET-ENI)	44818	44818	TCP		
AB-Xplorer (Direct)	2222	2222	TCP/ UDP		
AN-X-DCSNet	47920	47920	UDP		
B&R Xplorer (PLC Connection)	11159	11159	TCP		
B&R Xplorer (PVI Manager)	20000	20000	TCP		
Codesys V2	1200	1200	TCP		
Codesys V3	11740	11740	TCP		
Codesys V3 Scan	1742	1742	UDP		
CP1616 (PROFINET)	34962	34964	TCP/ UDP		
DTBox Request UDP	10000	10399	UDP		
E-Mail SMTP	25	25	TCP		
E-Mail SMTP with STARTTLS	587	587	TCP		
Ethernet Global Data (EGD)	18246	18246	UDP		

Schnittstelle	Port-Bereich		Proto-koll	Multicast-Adressen	Bemerkung
EtherNet/IP	44818	44818	TCP/ UDP		
Flex Device configura-tion	62101	62101	TCP		
Flex Device discovery	62010	62010	UDP		
Flex UDP Communicati-on Port	62012	62012	UDP		
ibaPQU-S Computed Values	62303	62303	UDP		
Generic TCP	5010	5017	TCP		
Generic UDP	5010	5017	UDP		
HiPAC request	2000	2000	TCP		
HiPAC request (disco-very)	26008	26008	UDP		
HPCi Request	13245	13245	UDP		
ibaNet-E	7072	7072	TCP/ UDP		
ibaNet-E (NBNS)	137	137	UDP		
ibaCapture	9121	9121	TCP/ UDP		
ibaCapture-HMI	9172	9172	TCP		
ibaLogic TCP	40002	40002	TCP		
ibaPDA Multistation	9175	9175	TCP		
ibaPDA Multistation Multicast	9176	9176	UDP	IPv4: 226.227.228.100 (default)	
ibaPDA SNMP	1611	1611	UDP		
IEC 61850 Client	102	102	TCP		
IEC 61850 Server	102	102	TCP		
Kafka	9092	9092	TCP		
Kafka (Azure EventHub)	9093	9093	TCP		
AMQP & Kafka (Azure EventHub)	5671	5672	TCP		
LANDSCAN	1050	1050	TCP		
LMI-Gocator	3220	3220	UDP		
Logix-Xplorer (Direct)	44818	44818	TCP		
MELSEC-Xplorer	4888	4888	TCP/ UDP		
Micro-Epsilon	8000	8000	UDP		
Micro-Epsilon	61000	61000	UDP		

Schnittstelle	Port-Bereich		Proto-koll	Multicast-Adressen	Bemerkung
Micro-Epsilon for Dis-covery	3956	3956	UDP		
MindSphere	443	443	TCP		
MMC Request	6115	6115	TCP		
Modbus TCP Client	502	502	TCP		
Modbus TCP Server	502	502	TCP		
OPC DA	135	135	TCP		
OPC DA	137	137	UDP		
OPC DA	138	138	UDP		
OPC DA	139	139	TCP		
OPC DA	445	445	TCP		
OPC UA Client	4840	4840	TCP		
OPC UA Server	48080	48080	TCP		
PTPv2 (ptp-event)	319	319	UDP	IPv4: [IANA] 224.0.1.129 - 224.0.1.132 IPv6 [1)]: [IANA] FF02::6B FF0x::181 FF0x::182 FF0x::183 FF0x::184	
PTPv2 (ptp-general)	320	320	UDP	IPv4: [IANA] 224.0.1.129 - 224.0.1.132 IPv6 [1)]: [IANA] FF02::6B FF0x::181 FF0x::182 FF0x::183 FF0x::184	
Raytek MPx linescanner	2727	2727	TCP		
S7 TCP/UDP	4170	4170	TCP/ UDP		
S7-Xplorer	102	102	TCP		
S7-Xplorer Proxy	9190	9190	TCP		
SAP Hana	39013	39013	TCP		
Sigmatek-Xplorer	1954	1954	TCP		
SIMOTION-Xplorer	102	102	TCP		
SINAMICS-Xplorer	102	102	TCP		
Sisteam TCP	8738	8738	TCP		

Schnittstelle	Port-Bereich		Proto-koll	Multicast-Adressen	Bemerkung
TCP Generic (Output)	5010	5010	TCP		
TCP/IP Text	1500	1500	TCP		
TDC TCP/UDP	4171	4171	TCP/ UDP		
TwinCAT ADS	48898	48898	TCP		
TwinCAT-PLC Broadcast Search	48899	48899	UDP		
TwinCAT-Xplorer	48898	48898	TCP		
VIP TCP/UDP	5001	5001	TCP/ UDP		
Watchdog	40001	40001	TCP/ UDP		
X-Pact Request	17477	17477	UDP		

Tab. 5: Ports, die ibaPDA Service für die verschiedenen Schnittstellen benutzt

[1)] Diese fest zugewiesenen Multicast-Adressen sind über alle Bereiche gültig. Dies wird durch ein "x" im Bereichsfeld der Adresse angezeigt, das einen beliebigen gültigen Bereichswert bedeutet.

5.4.2 ibaPDA Client

Ports, die ibaPDA-Client nutzt

Schnittstelle	Port-Bereich		Proto-koll	Multicast-Adressen	Bemerkung
ibaPDA Discovery	12900	12910	UDP	IPv4: 226.254.92.220	
ibaPDA Service	9170	9170	TCP		
ibaQPanel (Webbrow-ser)	80	80	TCP		
ibaQPanel (Webbrow-ser)	443	443	TCP		

Tab. 6: Ports, die ibaPDA Client bei Verbindung zu den verschiedenen Servern nutzt

5.4.3 ibaPDA-S7-Xplorer Proxy

Ports, die ibaPDA-S7-Xplorer Proxy nutzt

Schnittstelle	Port-Bereich		Proto-koll	Multicast-Adressen	Bemerkung
ibaPDA Service	9190	9190	TCP		

Tab. 7: Ports, die ibaPDA-S7-Xplorer Proxy nutzt

5.4.4 ibaPDA Server Status

Ports, die ibaPDA-Server-Status nutzt

Schnittstelle	Port-Bereich		Proto-koll	Multicast-Adressen	Bemerkung
ibaPDA Service	9190	9190	TCP		

Tab. 8: Ports, die ibaPDA-Server-Status nutzt

5.4.5 ibaHD-Server Service

Ports, die ibaHD-Server (Dienst) öffnet

Schnittstelle	Port-Bereich		Proto-koll	Multicast-Adressen	Bemerkung
ibaHD-Server	9180	9180	TCP		
ibaHD-Server Discovery	12880	12880	UDP	IPv4: 226.254.92.221	
SNMP	1614	1614	UDP		
ibaHD-API	9003	9003	TCP		

Tab. 9: Ports, die der ibaHD-Server-Dienst öffnet

5.4.6 ibaHD-Server Client

Ports, die ibaHD-Server-Client nutzt

Schnittstelle	Port-Bereich		Proto-koll	Multicast-Adressen	Bemerkung
ibaHD-Server	9180	9180	TCP		

Tab. 10: Ports, die ibaHD-Server-Client nutzt

5.4.7 ibaHD-Server Status

Ports, die ibaHD-Server-Status nutzt

Schnittstelle	Port-Bereich		Proto-koll	Multicast-Adressen	Bemerkung
ibaHD-Server	9180	9180	TCP		

Tab. 11: Ports, die ibaHD-Server-Status nutzt

5.4.8 ibaCapture Service

Ports, die ibaCapture-Server (Dienst) öffnet

Schnittstelle	Port-Bereich		Proto-koll	Multicast-Adressen	Bemerkung
ibaCapture Discovery	2378	2378	UDP	IPv4: 238.23.7.78	Fest
ibaCapture WCF ser-vices	14809	14809	TCP		Fest
ibaPDA communication	9120	9120	TCP		Modifizierbar
ibaPDA communication debugging	6000	6000	TCP		Modifizier-bar; optional
PTPv2 (ptp-event)	319	319	UDP	IPv4: [IANA] 224.0.1.129 - 224.0.1.132 IPv6 [1)]: [IANA] FF02::6B FF0x::181 FF0x::182 FF0x::183 FF0x::184	Fest; optional
PTPv2 (ptp-general)	320	320	UDP	IPv4: [IANA] 224.0.1.129 - 224.0.1.132 IPv6 [1)]: [IANA] FF02::6B FF0x::181 FF0x::182 FF0x::183 FF0x::184	Fest; optional
SNMP	1616	1616	UDP		Modifizier-bar; optional
RTSP Server	8554	8554	TCP		Modifizier-bar; optional
Camera replay stream port	24950	24950	TCP		Modifizier-bar; je Kame-ra
Camera live stream port	25950	25950	TCP		Modifizier-bar; je Kame-ra; optional

Tab. 12: Ports, die der ibaCapture Dienst öffnet

[1)] Diese fest zugewiesenen Multicast-Adressen sind über alle Bereiche gültig. Dies wird durch ein "x" im Bereichsfeld der Adresse angezeigt, das einen beliebigen gültigen Bereichswert bedeutet.

Hinweis: Standardmäßig verwenden Kamera-Livestreams dynamische Ports. Feste Livestream-Ports erlauben Ihnen die Einrichtung von Firewall-Regeln.

Außerdem werden für Verbindungen zum Zugriff auf Kameras weitere Ports verwendet, die hier aber nicht dokumentiert sind.

5.4.9 ibaCapture GigE Vision Encoder

Ports, die ibaCapture GigE Vision Encoder öffnet

Schnittstelle	Port-Bereich		Protokoll	Multicast-Adressen	Bemerkung
ibaCapture GigE Vision Encoder WCF services	9868	9868	TCP		Modifizierbar; nur localhost
ibaCapture GigE Vision Encoder WCF services	14810	14810	TCP		Fest; nur localhost

Tab. 13: Ports, die ibaCapture GigE Vision Encoder öffnet

5.4.10 ibaCapture-ScreenCam

Ports, die ibaCapture-ScreenCam öffnet

Schnittstelle	Port-Bereich		Protokoll	Multicast-Adressen	Bemerkung
ibaCapture-ScreenCam discovery	7072	7072	UDP	IPv4: 226.254.92.221	Fest
ibaCapture-ScreenCam WCF services	9191	9191	TCP		Modifizierbar
ibaCapture-ScreenCam camera instance	9700	9700	TCP		Modifizierbar je Instanz
ibaPDA communication	9892	9892	TCP		Modifizierbar

Tab. 14: Ports, die ibaCapture-ScreenCam öffnet

5.4.11 ibaVision

Ports, die ibaVision öffnet

Schnittstelle	Port-Bereich		Proto-koll	Multicast-Adressen	Bemerkung
ibaVision discovery	3702	3702	UDP	IPv4: 239.255.255.250	Fest
ibaVision WCF services	7110	7110	TCP		Modifizier-bar;
Video output module	7110	7110	TCP		Modifizier-bar; je Modul
ibaPDA input module	7111	7111	TCP		Modifizier-bar: je Modul
ibaPDA output module	7111	7111	TCP		Modifizier-bar: je Modul

Tab. 15: Ports, die ibaVision öffnet

Hinweis: Die Default-Portnummer ist stets die gleiche, aber ibaVision weist bei der Konfiguration unterschiedliche Portnummern zu.

5.4.12 ibaDatCoordinator

Ports, die ibaDatCoordinator öffnet

Schnittstelle	Port-Bereich		Proto-koll	Multicast-Adressen	Bemerkung
ibaDatCoordinator	8800	8800	TCP		
ibaDatCoordinator service discovery	12861	12861	UDP	IPv4: 226.254.92.220	

Tab. 16: Ports, die ibaDatCoordinator öffnet

Ports, die ibaDatCoordinator nutzt

Schnittstelle	Port-Bereich		Proto-koll	Multicast-Adressen	Bemerkung
ibaHD-Server	9180	9180	TCP		
SNMP	1612	1612	UDP		
TCP/IP Watchdog	40002	40002	TCP		
OPC UA Server	48081	48081	TCP		

Tab. 17: Ports, die ibaDatCoordinator nutzt

5.4.13 ibaLicenseService-V2

Ports, die ibaLicenseService-V2 öffnet

Schnittstelle	Port-Bereich		Proto-koll	Multicast-Adressen	Bemerkung
Configuration PortBe	8766	8766	TCP		
Data	9033	9033	TCP		
Transport port for Sup-port file	8767	8767	TCP		

Tab. 18: Ports, die ibaLicenseService-V2 öffnet

5.4.14 ibaAnalyzer

Ports, die ibaAnalyzer nutzt

Schnittstelle	Port-Bereich		Proto-koll	Multicast-Adressen	Bemerkung
ibaHD-Server	9180	9180	TCP		
Microsoft SQL-Sever	1433	1433	TCP		
Oracle	1521	1521	TCP		
MySql/MariaDB	3306	3306	TCP		
PostgreSQL	5432	5432	TCP		
IBM DB2	50000	50000	TCP		

Tab. 19: Ports, die ibaAnalyzer nutzt

5.4.15 ibaDaVIS

Ports, die ibaDaVIS nutzt

Interface	Port range		Protocol	Multicast addresses	Bemerkung
Microsoft SQL-Sever	1433	1433	TCP		
MySQL/MariaDB	3306	3306	TCP		
Oracle	1521	1521	TCP		
PostgreSQL	5432	5432	TCP		
Webinterface HTTP	80	80	TCP		
Webinterface HTTPS	443	443	TCP		
ibaHD-API	9003	9003	TCP		

Tab. 20: Ports, die ibaDaVIS nutzt

5.4.16 ibaManagementStudio

Server

Schnittstelle	Port-Bereich		Proto-koll	Multicast-Adressen	Bemerkung
Web interface	10522	10522	TCP		Modifizierbar
Agents (WAN Mode)	10519	10519	TCP		Modifizierbar

Tab. 21: Ports, die ibaManagementStudio Server öffnet

Agent

Schnittstelle	Port-Bereich		Proto-koll	Multicast-Adressen	Bemerkung
Software interaction	10521	10521	TCP		Modifizierbar
Agent discovery	10517	10517	UDP	IPv4: 238.23.7.100	Fest
Agent (LAN Mode)	10518	10518	TCP		Modifizierbar
Agent (WAN Mode)	10519	10519	TCP		Modifizierbar

Tab. 22: Ports, die ibaManagementStudio Agent öffnet

5.4.17 ibaCMC

Schnittstelle	Port-Bereich		Proto-koll	Multicast-Adressen	Bemerkung
MQTT Broker	1883 8883	1883 8883	TCP		Modifizierbar (TLS)
FTP Server (FTPS)	41521	41521	FTP		Modifizierbar
Traces	41514	41514	UDP		Modifizierbar
Webinterface	80	80	TCP		Modifizierbar
Webinterface	443	443	TCP		Modifizierbar

Tab. 23: Ports, die ibaCMC öffnet

Konfiguration und Anpassung der Ports über `appsettings.json`.

5.4.18 ibaLogic Server

Ports, die ibaLogic Server öffnet

Schnittstelle	Port-Bereich		Proto-koll	Multicast-Adressen	Bemerkung
ibaLogic Server	6510	6510	TCP		
ILUS Update	22012	22012	TCP		
Microsoft SQL-Server	1433	1433	TCP		
OPC Control Service Communication	22050	22052	UDP		
OPC UA Endpoint	21060	21061	TCP		
PMAC Communication	21000	21002	TCP		
PMAC Communication	21004	21005	TCP		
PMAC Control Service Communication	22046	22049	UDP		
PMAC Network Disco-very	22044	22045	UDP		

Tab. 24: Ports, die ibaLogic Server öffnet

5.4.19 ibaLogic Client

Ports, die ibaLogic Client nutzt

Schnittstelle	Port-Bereich		Proto-koll	Multicast-Adressen	Bemerkung
ibaLogic PDA Express Communication	21003	21003	TCP		
ibaLogic Server Com-munication	6510	6510	TCP		

Tab. 25: Ports, die ibaLogic Client nutzt

5.4.20 ibaLogic PMAC

Ports, die ibaLogic PMAC nutzt

Schnittstelle	Port-Bereich		Proto-koll	Multicast-Adressen	Bemerkung
ibaLogic OPC Server Communication	21004	21005	TCP		
ibaLogic PDA Express Communication	21003	21003	TCP		

Schnittstelle	Port-Bereich		Proto-koll	Multicast-Adressen	Bemerkung
ibaLogic Server Com-munication	21000	21002	TCP		
PMAC Network Disco-very	22044	22044	UDP		
PMAC Port in ibaLogic V4	23042	23042	?		
Timing-Diagnostics Tool	22013	22013	TCP		

Tab. 26: Ports, die ibaLogic PMAC nutzt

5.4.21 ibaLogic OPC Server

Ports, die ibaLogic OPC-Server nutzt

Schnittstelle	Port-Bereich		Proto-koll	Multicast-Adressen	Bemerkung
OPC UA Endpoint	21060	21061	TCP		
PMAC Communication	21004	21005	TCP		

Tab. 27: Ports, die der ibaLogic OPC Server nutzt

5.4.22 Fremdsoftware

WIBU CodeMeter Runtime

Die Software CodeMeter Runtime ist eine Fremdsoftware, die dazu verwendet wird, iba-Softwareprodukte zu lizenzieren. Daher wird sie überall dort installiert, wo iba-Software über das WIBU-System lizenziert wird.

Ports, die CodeMeter Runtime nutzt

Schnittstelle	Port-Bereich		Proto-koll	Multicast-Adressen	Bemerkung
Standard CodeMeter Kommunikation	22350	22350	TCP		modifizierbar
HTTP (WebAdmin)	22352	22352	TCP		modifizierbar
HTTPS (WebAdmin)	22353	22353	TCP		modifizierbar

Tab. 28: Ports, die WIBU CodeMeter Runtime nutzt

Hinweis

Für weitere Informationen bzgl. Ports und Zugriffsberechtigungen wenden Sie sich bitte direkt an die WIBU-SYSTEMS AG (http://www.wibu.com).

6 Hinweise zum sicheren Betrieb von iba-Hardware

Alle iba-Geräte, die mittels Lichtwellenleiter angeschlossen und mit dem 32Mbit Flex-Protokoll betrieben werden, müssen mit den nachstehenden Ports über den ibaFOB-D Netzwerkadapter kommunizieren können:

Interface	Port Range		Protocol	Multicast addresses
Geräteindentifikation	62000	62000	TCP	
Flex Device configuration	62101	62101	TCP	
Flex Device discovery	62010	62010	UDP	

Tab. 29: Ports, die von ibaFOB-D-Netzwerkadapter verwendet werden

Einige Geräte verfügen darüber hinaus noch über eine Netzwerkschnittstelle, für die weitere Ports in lokalen Netzen an der Firewall freigeschaltet werden müssen, um den korrekten Betrieb sicherzustellen.

6.1 ibaClock

Interface	Port Range		Protocol	Multicast addresses
Daytime	13	13	TCP/UDP	
Time	37	37	TCP/UDP	
Webinterface	80	80	TCP	
NTP	123	123	TCP/UDP	IPv4: [IANA] 224.0.1.1 IPv6 [1]: [IANA] FF0x::101
PTP	319	320	TCP/UDP	IPv4: [IANA] 224.0.1.129 - 224.0.1.132 IPv6 [1]: [IANA] FF02::6B FF0x::181 FF0x::182 FF0x::183 FF0x::184
Flex UDP Communication Port	62012	62012	UDP	

Tab. 30: Ports, die von ibaClock verwendet werden

[1] Diese fest zugewiesenen Multicast-Adressen sind über alle Bereiche gültig. Dies wird durch ein "x" im Bereichsfeld der Adresse angezeigt, das einen beliebigen gültigen Bereichswert bedeutet.

6.2 ibaBM-DP

Interface	Port Range		Protocol	Multicast addresses
Simulationsmodus/Diagnose	999	999	TCP	
Webinterface	80	80	TCP	

Tab. 31: Ports, die von ibaBM-DP verwendet werden

6.3 ibaW-750

Interface	Port Range		Protocol	Multicast addresses
Konfiguration / Discovery	7072	7072	TCP/UDP	
ACQ/PLC	7082	7082	UDP	
NBNS (Name Resolution Service)	137	137	UDP	

Tab. 32: Ports, die von ibaW-750 verwendet werden

6.4 ibaPADU-S-IT, ibaCMU-S, ibaPQU-S

6.4.1 ibaPADU-S-IT

Interface	Port Range		Protocol	Multicast addresses
FTP	21	21	TCP	
Telnet	23	23	TCP	
Webinterface	80	80	TCP	

Tab. 33: Ports, die von ibaPADU-S-IT verwendet werden

6.4.2 ibaCMU-S

Interface	Port Range		Protocol	Multicast addresses
FTP	21	21	TCP	
Telnet	23	23	TCP	
Webinterface	80	80	TCP	

Tab. 34: Ports, die von ibaCMU-S verwendet werden

6.4.3 ibaPQU-S

Interface	Port Range		Protocol	Multicast addresses
Berechnete Werte	62303	62303	UDP	

Tab. 35: Ports, die von ibaPQU-S verwendet werden

6.5 ibaPADU-C

Interface	Port Range		Protocol	Multicast addresses
NTP	123	123	TCP/UDP	IPv4: [IANA] 224.0.1.1 IPv6 [1)]: [IANA] FF0x::101
FTP	21	21	TCP	
DHCP	67	68	UDP	

Tab. 36: Ports, die von ibaPADU-C verwendet werden

[1)] Diese fest zugewiesenen Multicast-Adressen sind über alle Bereiche gültig. Dies wird durch ein "x" im Bereichsfeld der Adresse angezeigt, das einen beliebigen gültigen Bereichswert bedeutet.

6.6 iba-PC, ibaDAQ-Familie und ibaM-DAQ

Bei der Absicherung von iba-Rechnern (ibaRackline, ibaDeskline) sowie ibaDAQ- und ibaM-DAQ-Geräten sind die Anforderungen und technischen Lösungen in Ihrer Umgebung als Maßstab heranzuziehen.

Als Mindestmaß muss sichergestellt sein, dass Ihr System mit einem effizienten Schutz vor Schadsoftware und notwendigen Updates zum Schutz von bekannten Schwachstellen versorgt wird.

Ein abruptes Ausschalten von Windows-Systemen kann eine Beschädigung des Dateisystems nach sich ziehen. Daher wird empfohlen, die Systeme über eine USV (unterbrechungsfreie Stromversorgung) abzusichern. Dadurch kann sichergestellt werden, dass Ihr System vor kurzzeitigen Spannungsschwankungen geschützt ist, und bei längerem Versorgungsspannungsausfall richtig herunterfahren wird.

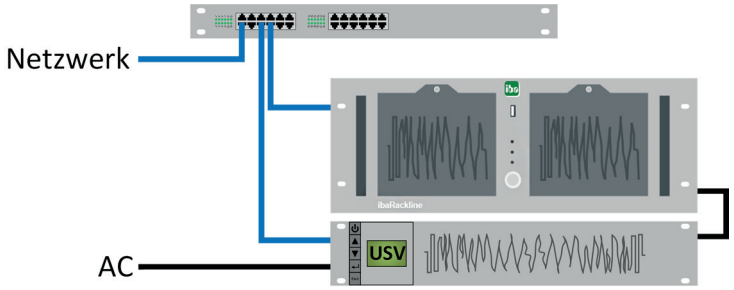


Abb. 13: Beispiel für ibaRackline mit USV

Der ibaRackline-Rechner wird mithilfe einer Zusatzsoftware des USV-Herstellers per Netzwerk heruntergefahren.

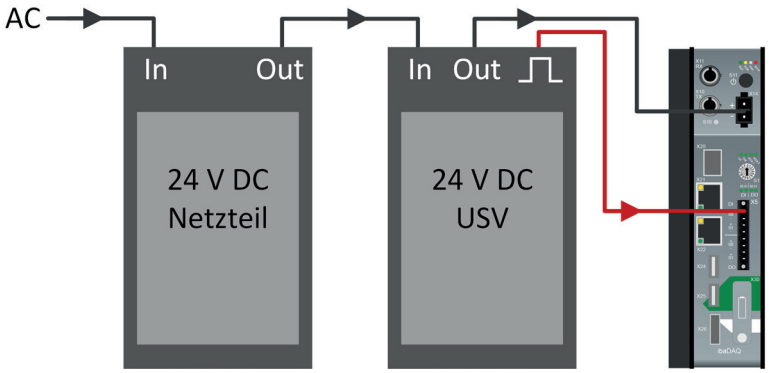


Abb. 14: Beispiel für ibaDAQ mit USV

In dem Beispiel gibt die 24 V DC-USV ein Digitalsignal aus, das von dem ibaDAQ-Gerät ausgewertet und für das geordnete Herunterfahren genutzt wird.

7 Support und Kontakt

Support

Tel.: +49 911 97282-14

E-Mail: support@iba-ag.com

Hinweis

Wenn Sie Support benötigen, dann geben Sie bitte bei Softwareprodukten die Nummer des Lizenzcontainers an. Bei Hardwareprodukten halten Sie bitte ggf. die Seriennummer des Geräts bereit.

Kontakt

Hausanschrift

iba AG
Königswarterstraße 44
90762 Fürth
Deutschland

Tel.: +49 911 97282-0

E-Mail: iba@iba-ag.com

Postanschrift

iba AG
Postfach 1828
90708 Fürth

Warenanlieferung, Retouren

iba AG
Gebhardtstraße 10
90762 Fürth

Regional und weltweit

Weitere Kontaktadressen unserer regionalen Niederlassungen oder Vertretungen finden Sie auf unserer Webseite:

www.iba-ag.com