Bilder: © Elatec

Sicherheit und Transparenz mit System

Berührungslose Authentifizierungslösung für Reinraumumgebungen

Burhan Gündüz

Eine zuverlässige Zutritts- und Zugriffskontrolle ist in Reinräumen ebenso wie in Laboren essenziell, um Menschen, Maschinen und Daten zu schützen. Nicht zuletzt hilft sie, eine Kontamination der Umgebung zu vermeiden, indem sie Unbefugte am Zutritt hindert. Um die hohen Anforderungen zu erfüllen, die mit einer Reinraumumgebung in Bezug auf Sicherheit und Hygiene einhergehen, eignet sich eine berührungslose Authentifizierungslösung auf Basis von RFID und mobilen Technologien. Fünf Kriterien gilt es bei der Auswahl des richtigen Lesegeräts besonders zu beachten.

Die Arbeit in Reinräumen erfordert von den Mitarbeitern besondere Kenntnisse. Dies gilt im Hinblick auf die strengen Hygienevorschriften wie auch in Bezug auf den Umgang mit kostspieligen und sensiblen Geräten sowie empfindlichen, gegebenenfalls gesundheitsgefährdenden Materialien. Doch nicht nur das: Auch externe Dienstleister wie Reinigungskräfte müssen die hier geltenden Regeln einhalten. Je höher die Schutzstufe oder die Reinraumklasse, desto strenger die Sicherheitsvorgaben. Für Betreiber bedeutet das: Wo die Vorschriften es erfordern, muss gewährleistet sein, dass nur autorisierte und geschulte Personen Zutritt zu den Räumen und Zugang zu Anlagen und Systemen erhalten. Eine weitere zentrale Herausforderung ist die Systemsicherheit: Es gilt Maschinen, Anlagen und Peripheriegeräte ebenso wie sensible und wertvolle Daten wirksam vor unbefugtem Zugriff zu schützen.

Reibungslose und sichere Benutzerauthentifizierung mit RFID und mobilen Technologien

Ein modernes Benutzerauthentifizierungs- und Zugangskontrollsystem auf Basis von RFID, das auch den Einsatz mobiler Berechtigungsausweise erlaubt, ist eine einfache und sichere Lösung, um Personen, Daten und Inventar zu schützen. So lassen sich der Zutritt zu Laboren und Reinräumen sowie der Zugang zu sensiblen Maschinen, Geräten, Vorräten und Substanzen effizient und zuverlässig regeln. Auch Single Sign-on (SSO) für Computersysteme, Netzwerke und Drucker sowie elektronische Unterschriftsauthentifizierung für Manufacturing Execution Systems (MES) oder Labor-Informations-Management-Systeme (LIMS) lassen sich darüber abbilden. Ein weiterer Vorteil: Prozesse können so zuverlässig und mit geringem Aufwand dokumentiert werden, was beispielsweise das Qualitätsmanagement oder die Arbeitszeiterfassung erheblich erleichtert.

Eine ebenso unkomplizierte wie günstige Option zur Implementierung von Benutzerauthentifizierung und Zugangskontrollen ist ein Ausweis, der mit einem RFID-Tag ausgestattet ist – und den die meisten Mitarbeiter bereits in Form einer ID-Karte oder eines Tokens bei sich tragen. Auch der Einsatz von Wearables, bspw. in Form von Armbändern, ist möglich. Wird ein solcher physischer Ausweis an das Lesegerät gehalten, erfolgt der Authentifizierungsprozess automatisch. Die autorisierte Person erhält umgehend Zutritt zu den Laborräumen und kann reibungslos auf alle Computersysteme oder Anlagen zugreifen, für die sie berechtigt ist. Je nach Qualifikation der Mitarbeiter lassen sich die Berechtigungen dabei einfach und individuell anpassen.

Eine weitere Möglichkeit ist der Einsatz von digitalen Berechtigungsnachweisen, sogenannten mobile Credentials. Sie basieren auf den Technologien Near Field Communication (NFC) oder Bluetooth Low Energy (BLE), mit denen ein Großteil aller mobilen Endgeräte wie Smartphones ausgestattet ist. Der internationale Übertragungsstandard NFC erlaubt den kontaktlosen und gesicherten Austausch von Daten auf kurzer Distanz. Die Transaktion wird also abgewickelt, wenn sich das Smartphone in der Nähe eines Multifrequenz-Lesegeräts befindet. Bei der Funktechnik BLE hingegen muss das Handy für den Authentifizierungsprozess nicht mehr zwingend aktiv an das Lesegerät gehalten werden – je nachdem, welche Distanz im System festgelegt ist. Sowohl physische als auch digitale Berechtigungsnachweise erlauben eine komfortable, berührungslose und damit hygienische Authentifizierung.

Erfordert das Arbeitsumfeld außerdem eine starke Zwei-Faktor-Authentifizierung, kann RFID in Verbindung mit Passwortsystemen verwendet werden. Auch eine Kombination mit biometrischen Systemen ist möglich. Ein Beispiel sind Wearables, die mit der digitalen Identität eines Mitarbeiter verknüpft sind. Mit dem Arbeitsbeginn wird das Band angelegt, im Zuge dessen der Mitarbeiter einmalig den Finger auf einen Fingerabdruckscanner legt und das Band so aktiviert. Im weiteren Verlauf des Tages wird das Band einfach an ein Lesegerät gehalten, das mit NFC oder Bluetooth arbeitet. So kann schnell und kontaktlos eine Authentifizierung ausgeführt werden.

Fünf Kriterien für die Wahl des richtigen Lesers

Herzstück moderner Zutritts- und Zugangskontrollsysteme sind universelle Lesegeräte. Besonders für den Gebrauch in Reinräumen und Laboren müssen spezielle Anforderungen erfüllt werden – nicht zuletzt, um sicherzustellen, dass gesetzliche Standards eingehalten werden. Daher sind bei der Auswahl des richtigen Systems besonders folgende fünf Aspekte zu beachten:

Sicherheit von Daten, Systemen und Personen: Beim Zutritt zu Räumlichkeiten sowie dem Zugang zu Computernetzwerken und Softwaresystemen erfordern Labor- und Reinraumumgebungen ein hohes Maß an Sicherheit. Das bedeutet, dass die verwendeten Lesegeräte sowohl gegen physische Manipulationen als auch gegen Hackerangriffe resistent sein müssen. Leser, die in Hochsicherheitslabors oder Produktionsumgebungen eingesetzt werden, sollten daher eine fortschrittliche Verschlüsselungstechnologie unterstützen. Verschlüsselte RFID- oder BLE-/NFC-Signale sind schwerer abzufangen oder zu fälschen. Für zusätzliche Sicherheit sorgen Lesegeräte, die mit biometrischen Verfahren (z.B. Wrist-Band) für eine Zwei-Faktor-Authentifizierung kompatibel sind.

Nicht zuletzt gilt es, die Mitarbeiter durch eine Zutrittskontrolle zu schützen. Denn viele Materialien, mit denen in Reinräumen und Laboren gearbeitet wird, können bei unsachgemäßer Nutzung eine erhebliche Gesundheitsgefahr darstellen.

So funktionieren RFID, BLE UND NFC

RFID-Karten haben einen eingebetteten Chip (oder Tag), der aus zwei Hauptkomponenten besteht: **einer integrierten Einheit,** die Informationen speichern und verarbeiten kann und **einer Antenne** zum Senden oder Empfangen eines Signals.

- Auf jeder RFID-Karte ist ein eindeutiger Datensatz – beispielsweise eine Nummer – gespeichert, der zur Identifizierung der Karte und damit auch der Person dient, die sie bei sich trägt. Befindet sich eine Karte mit einem eingebetteten RFID-Tag in der Nähe eines RFID-Lesegeräts, sendet der Reader ein Funksignal aus, um diesen Datensatz abzufragen. Das Signal aktiviert den Tag, der diese Energie dann nutzt, um dem Leser seine eindeutige ID mitzuteilen.
- Sowohl NFC als auch BLE sind Technologien für den kontaktlosen Datenaustausch. Ihr Hauptunterschied zu RFID besteht darin, dass die Informationsträger (z. B. Smartphones) aktive Funksender sind und eine Stromquelle benötigen.
- NFC basiert auf hochfrequenter RFID-Technologie (13,56 MHz) und ermöglicht einen kontaktlosen Datenaustausch in der Nahfeldkommunikation (<10 cm).
- BLE ist eine Kurzstrecken-Funktechnologie für Entfernungen bis zu zehn Metern im Frequenzbereich von 2,4 GHz.
- Werden Smartphones für die Benutzerauthentifizierung und Zugangskontrolle verwendet, fungieren sie als Kartenemulatoren und senden eine eindeutige Benutzer-ID an das Lesegerät.

Hygiene: Da in einer Reinraumumgebung jeder überflüssige Berührungspunkt vermieden werden sollte, ist eine kontaktlose Authentifizierungslösung die richtige Wahl. Damit entfällt die Eingabe von Passwörtern oder Codes auf gemeinsam genutzten Pinpads bei der Zutritts- und Zugangskontrolle. Die besonderen Hygienestandards in Reinraumumgebungen machen jedoch weitere Überlegungen bei der Wahl des richtigen Lesegeräts notwendig. So erlauben die besonderen Anforderungen von GMP (Good Manufacturing Practice)-Umgebungen die Verwendung herkömmlicher Reader zumeist nicht. Geräte, die in einfache Kunststoffgehäuse eingebaut sind, können nicht regelmäßig mit Desinfektionsmitteln oder starken Reinigungsmitteln behandelt werden, da die Gehäuse bei der Verwendung aggressiver Substanzen und häufigen Reinigungszyklen schnell Schaden nehmen. Gerade in Reinräumen kann das sogar zu einer Beeinträchtigung der Arbeitsergebnisse führen, denn ein angegriffenes Gehäuse birgt die Gefahr, dass freigesetzte Partikel die Umgebung kontaminieren. Es empfiehlt sich daher der Einsatz von Lesegeräten, die in ein Gehäuse aus Edelstahl und Glas integriert sind, also Materialien, die üblicherweise für GMP-Anwendungen verwendet werden. Sie halten den strengen Reinigungs- und Hygieneanforderungen stand. Die Gehäuse sollten ohne Ecken, Kanten oder offene Anschlüsse konzipiert sein und der Schutzklasse IP65 (Schutz gegen Niederdruck-Strahlwasser aus allen Richtungen sowie gegen Kondens- und Spritzwasser) entsprechen.

Flexibilität: Weltweit sind Dutzende verschiedene RFID-Kartentechnologien im Einsatz, die jeweils über eigene Datenformate, Kommunikationsfrequenzen und Sicherheitsfunktionen verfügen. Die Karten können grob in Hochfrequenz- (HF) und Niederfrequenzkarten (LF) unterteilt werden, je nachdem, welchen Frequenzbereich sie für die Kommunikation nutzen. Innerhalb dieser Kategorien haben die Karten der verschiedenen Hersteller jedoch ihre eigenen, einzigartigen Formate. Besonders Unternehmen mit mehreren Standorten oder bereits vorhandenen Benutzerauthentifizierungs- und Zugangskontrollsystemen sollten auf universelle Lesegeräte setzen, die für den weltweiten Einsatz zertifiziert sind und eine Vielzahl an Technologien unterstützen. Multifrequenz-Lesegeräte erlauben es, alle aktuell und in Zukunft im Unternehmen eingesetzten Transpondertechnologien zu verarbeiten und sind darüber hinaus auch für die Smartphone-Authentifizierung mit BLE- oder NFC-Technologie geeignet. Sie bieten Unternehmen so eine All-in-One-Lösung, die die Komplexität reduziert und dabei hilft, Zeit und Kosten zu sparen. Eine gute Wahl sind beispielsweise Reader-Modelle des Lösungsanbieters Elatec, die bis zu 60 gängige Transpondertechnologien verarbeiten können.

Zukunftssicherheit: Änderungen an Betriebssystemen, der Einsatz neuer Transpondertechnologien oder aufkommende Sicherheitsbedrohungen können es erforderlich machen, Lesegeräte zu aktualisieren oder neu zu konfigurieren. Es empfiehlt sich daher Lesegeräte zu implementieren, die über eine offene Programmierschnittstelle verfügen. Damit sind die Geräte bei sich ändernden Anforderungen maximal anpassungsfähig und zukunftssicher, denn es lassen sich jederzeit Updates und Upgrades durchführen. Wichtig dabei: Diese sollten sich via Fernwartung vornehmen lassen. So kann vermieden werden, dass Techniker jedes einzelne Gerät aufwendig ausbauen, anpassen und wieder einbauen müssen. Das spart nicht nur Zeit und Kosten, sondern hat auch den Vorteil, dass der Reinraum nicht unnötig von Dienstleistern betreten werden muss. Außerdem sollten Lesegeräte so programmierbar sein, dass sie spezifische Funktionen für anspruchsvolle PC-Anmeldesoftware ermöglichen und mobile Zugangskontrolltechnologien unterstützen. So erfüllen die Lesegeräte die Bedürfnisse von Reinraum-Betreibern und -Nutzern über einen langen Zeitraum.

Ergonomie: Nicht zuletzt sollte die ergonomische Eignung der Lesegeräte in einer derart stark reglementierten Branche, in der sich Mitarbeiter mehrfach täglich authentifizieren müssen, nicht außer Acht gelassen werden. Eine ergonomisch passende Lösung für den entsprechenden Arbeitsplatz sollte grundsätzlich gewährleistet sein. Empfehlenswert ist daher die Wahl eines Lesers, der im Idealfall in verschiedenen Ausführungen erhältlich ist und so ein breites Spektrum an räumlichen und ergonomischen Anforderungen abdeckt.

KONTAKT

Burhan Gündüz
Global VP Secure Printing
ELATEC GmbH, Puchheim
Tel.: +49 89 552 9961 - 0
info-rfid@elatec.com
www.elatec.com