

Einsatzgebiete

- KRITIS Anlagen (Kritische Infrastrukturen nach BSI IT-Sicherheitsgesetz)
- Industrie-Anlagen mit hoher Produktions-Verfügbarkeit
- gleichzeitiger Einsatz von Produktionsleitsystemen mit unterschiedlichen Herstellern
- Produktionsanlagen an unterschiedlichen dezentralen Standorten
- viele Benutzer / User / Arbeitsplätze
- mehrere Benutzergruppen, die unterschiedliche Berechtigungen erhalten

Folgende Leitsysteme werden unterstützt

- Siemens : PCS7, WinCC
- Wonderware : InTouch, Terminal Services, Industrial Application Server (IAS)
- General Electric : Proficy iFIX, FIX32, Proficy iBatch
- Microsoft : Windows 7 oder höher, Windows Server (Versionen auf Anfrage)
- weitere Systeme in Vorbereitung (z.B.: CopaData Zenon, Emerson DeltaV, ...)

ID Systeme

- RFID Kartenlesegeräte mit RFID Karten
- NFC Hardware mit Security Key
- weitere Systeme in Vorbereitung (z.B.: Fingerprint, Werkausweise, ...)

Interesse ? ... dann sprechen Sie uns an !

Tel: **+49(0) 421 792 88 - 0** oder E-Mail an: **info2016@segno.de**

oder RÜCKFAX an **+49(0) 421 792 88 - 22**

Firma: _____

Ansprechpartner: _____

Telefon: _____

Email: _____



Zwei-Faktor Authentifizierung für PLS Leitsysteme mit zentralem Benutzer- und Passwortmanagement SEGNO Login Management System

Anforderung → sicherer Betrieb von Produktionsanlagen

In Produktionsanlagen werden einzelne oder mehrere, teilweise auch unterschiedliche Bedien- und Beobachtungssysteme für die Produktionstechnik betrieben. Um den sicheren Betrieb einer Produktion gewährleisten zu können, ist es zwingend erforderlich, den Zugang zu diesen Systemen dahingehend abzusichern, dass nur ein hierfür vorgesehener Personenkreis Zugang zu den Systemen bekommt. Außerdem muss nachvollziehbar dokumentiert werden, von welchem Benutzer ein System zu welchem Zeitpunkt bedient wurde.

Stand der Technik - Absicherung von Leitsystem-Zugängen

- Verwendung „sicherer Passwörter“ mit entsprechender Länge, großen und kleinen Buchstaben, Sonderzeichen usw.
- Änderung der Passwörter in regelmäßigen Abständen
- Nutzung einer Zwei-Faktor-Authentifizierung mit „Wissen“ und „Besitz“ (PIN und Karte)

Die Realität sieht anders aus!

IT Sicherheit in Produktionsanlagen - heute

- viele Systeme werden ohne Benutzerverwaltung betrieben
- die Benutzerverwaltung ist nur mit einem Benutzer und einem Passwort angelegt
- es werden keine oder nur einfache Passwörter verwendet
- Passwörter werden selten oder nie geändert
- der zuerst angemeldete Benutzer bleibt über Wochen, Monate oder gar Jahre angemeldet, alle weiteren Benutzer haben jederzeit Zugang zum System
- Eingriffe von Systemadministratoren auf Betriebssystemebene werden nicht registriert



SEGNO Login Management System

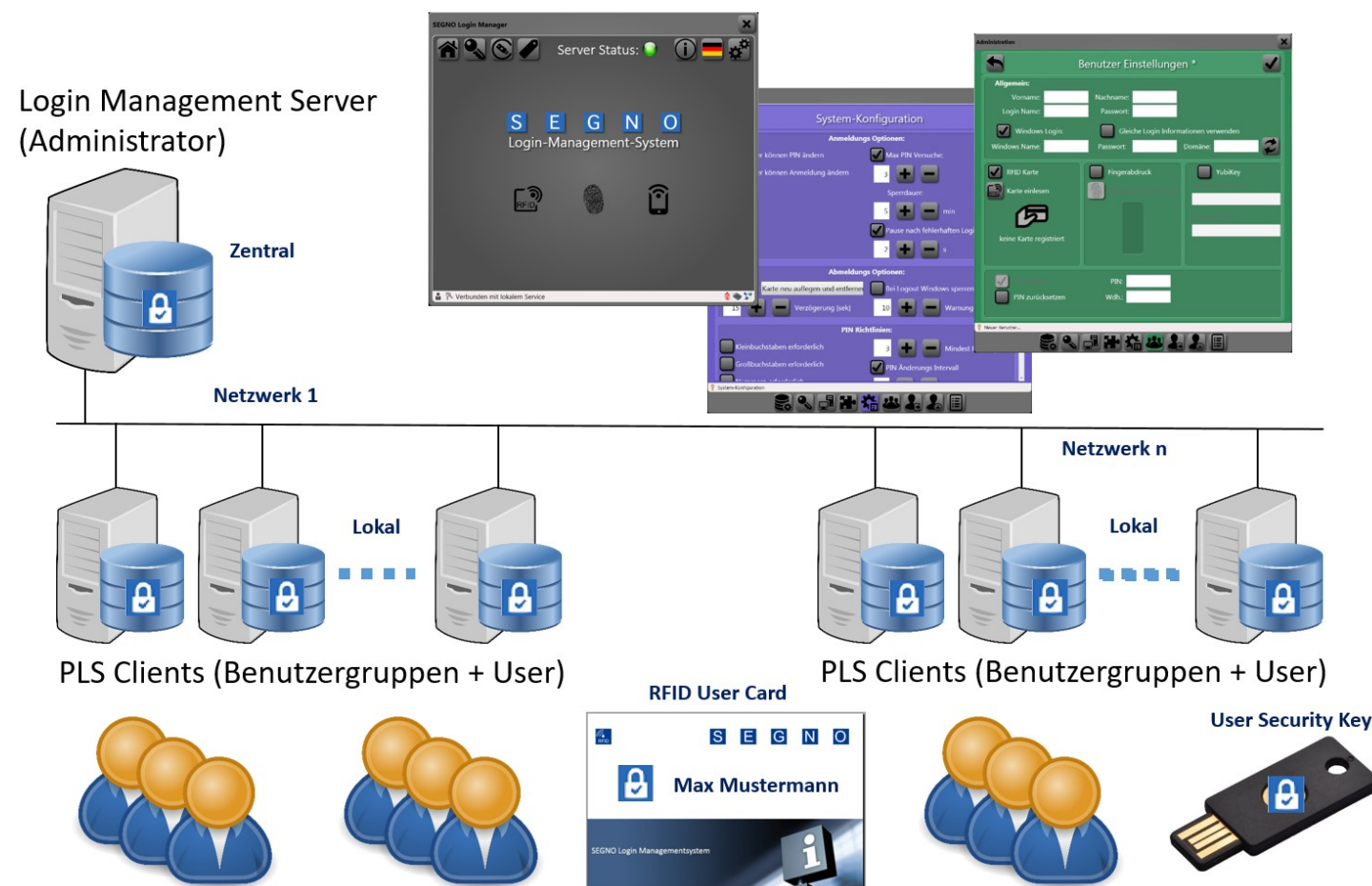


Abbildung: Prinzipieller Einsatz SEGNO Login Management System

Die Lösung – IT Sicherheit einfach gemacht

Betreiber von Produktionsanlagen sollten ein **zentrales Standardsystem** für eine **Zwei-Faktor-Authentifizierung** für Betriebs- und Prozessleitsysteme mit Wissen und Besitz einführen. Für genau diese Aufgabenstellung ist das **SEGNO Login Management System** entwickelt worden. Auf einfacher Weise wird ein sicheres und schnelles Login Management für Ihre Systeme aufgebaut.

Das **SEGNO Login Management System** basiert auf die vom **BSI** empfohlene Zwei-Faktor-Authentifizierung. Bei diesem Login-Managementsystem benötigt der Benutzer lediglich eine **PIN (Wissen)** und eine **Identkarte**, Chip, NFC Token o. ä. (**Besitz**). Bei der Anmeldung prüft das SEGNO Login Management System die Zugangsberechtigung. Wird die Berechtigung von der zentralen Managementkonsole bestätigt, wird das „echte“, n-Stellige Passwort an das Leitsystem übergeben. Die Kommunikation zwischen Client und zentraler Managementkonsole ist zur **Erhöhung der Sicherheit** verschlüsselt.

Heute: Stand der Technik!

Ihre Vorteile

- ✓ **Zwei-Faktor-Authentifizierung** für PLS verschiedener Hersteller
- ✓ Einfache Handhabbarkeit durch **kurze PIN** anstelle eines langen und komplexen Passwortes
- ✓ **Sichere Verschlüsselung** aller Datenbankeinträge nach aktuellen Standards
- ✓ Hoher Systemschutz durch Verwendung **gehärteter Passwörter**
- ✓ **Zentrale Passwortgenerierung**
- ✓ Zentrale Administration der Benutzer- und Zugangsdaten
- ✓ Zentrale benutzerbezogene Rechteverwaltung
- ✓ Zentrale Datenbank für alle System- / Benutzer- und Zugangsdaten
- ✓ Zwei-Faktor-Authentifizierung an Windows-Workstation und Windows-Server-Systemen
- **Nutzung herkömmlicher Kartenlesegeräte, RFID-Lesegeräte etc.**
- **Verwendung vorhandener Karten, RFID-Chips, wie z.B. Mitarbeiterausweise**
- ✓ **Sicherheit** durch Automatische Replikation der zentralen Datenbank
- ✓ Flexible Anpassung auf kundenspezifische Zugangsrichtlinien
- ✓ **Logging-Funktionen** für alle Aktivitäten in Zusammenhang mit der Authentifizierung

