

Anmeldung am Stationsarbeitsplatz: Citrix, Entra ID, Karte und schneller Benutzerwechsel



Wissen

Alle Beiträge der Serie rund um Kliniken, Klinikverbünde und Microsoft 365:

[Microsoft 365 im Krankenhaus](#)

Beratung

Anmeldekonzert für Station und Funktionsbereich, von der PKI bis zur KIS-Sitzung:

[Microsoft-365-Beratung für Krankenhäuser](#)

Schulung

Wissen für IT-Team und Rufbereitschaft, damit die Kartenanmeldung keine Blackbox bleibt:

[Microsoft-365-Schulung für Krankenhäuser](#)

Es ist 6:05 Uhr, Übergabe im Dienstzimmer. Drei Pflegekräfte, ein Stationsrechner, eine Patientenliste, die gleich ausgedruckt werden soll. Die erste meldet sich an, das Profil lädt, das KIS startet, die Gruppenrichtlinien denken nach. Neunzig Sekunden später ist der Bildschirm bereit, und die Kollegin vom Nachtdienst steht mit der Jacke in der Hand daneben. Am Ende der Woche wundert sich die IT-Leitung, warum auf dieser Station seit Jahren alle unter einem Konto namens »Station 3« arbeiten. Die Antwort steht in der Übergabe: Weil es schneller geht.

Die **Anmeldung am Stationsarbeitsplatz** ist eines der unterschätztesten Themen der Krankenhaus-IT. Sie muss schnell sein, weil Pflege und Ärzte keine Zeit für Ladebalken haben. Sie muss sicher sein, weil hinter dem Bildschirm das KIS mit Patientendaten wartet. Und sie muss nachvollziehbar sein, weil im Zweifel jemand wissen will, wer wann welche Akte geöffnet hat. Diese drei Ziele widersprechen sich gern, und jede technische Variante – Citrix oder Remote Desktop mit zentralen Sitzungen, Karten und Badges, Entra ID mit Zertifikatsanmeldung, Windows Hello for Business, schneller Benutzerwechsel – verschiebt das Gewicht zwischen ihnen.

Dieser Beitrag ordnet die Varianten ein, zeigt die Anmeldekette vom Kartenleser bis zur KIS-Sitzung und erklärt, warum am Ende fast immer PKI und Kerberos über Erfolg oder Frust entscheiden. Er gehört zur Serie [Microsoft 365 im Krankenhaus](#). Microsoft 365 ist dabei nicht die Bühne für Patientendaten – die gehören ins KIS und seine Subsysteme –, aber Entra ID ist in

vielen Häusern längst die Identitätsplattform, an der auch die Anmeldung am Stationsrechner hängt.

Fakten: Das Wichtigste in Kürze

- Am Stationsrechner konkurrieren drei Ziele: schnell, sicher, nachvollziehbar. Sammelkonten erfüllen nur das erste und sind trotzdem verbreitet.
- Zentrale Sitzungen über Citrix oder Remote Desktop mit Karte und PIN erlauben, dass die Sitzung der Person folgt statt am Gerät zu kleben. Das ist im Schichtdienst der größte Zeitgewinn.
- Der Citrix Federated Authentication Service stellt nach Herstellerangaben Zertifikate im Namen des Benutzers aus, damit der Sitzungshost eine Smartcard-Anmeldung sieht, auch wenn sich der Mensch vorher an Entra ID angemeldet hat. Damit wird die interne CA zum Bestandteil jeder Anmeldung.
- Windows Hello for Business ist an Person und Gerät gebunden und eignet sich deshalb schlecht für Rechner, an denen sich dreißig Menschen pro Tag abwechseln. FIDO2-Sicherheitsschlüssel funktionieren laut Microsoft nicht in Citrix-, VDI- oder RDP-Sitzungen, außer über WebAuthn-Umleitung.
- Seit dem Windows-Update vom 9. September 2025 akzeptieren Domänencontroller für die Zertifikatsanmeldung nur noch stark zugeordnete Zertifikate. Wer Karten oder FAS einführt, muss das von Anfang an einplanen.

Schnell, sicher, nachvollziehbar: drei Ziele, die sich gern widersprechen

Wer auf Station fragt, was an der Anmeldung stört, hört selten das Wort Sicherheit. Man hört: »Dauert zu lange«, »Ich muss mich dauernd neu anmelden«, »Das Kennwort läuft ständig ab«, »Wenn ich vom Patientenzimmer zurückkomme, ist der Bildschirm gesperrt«. Wer in der Informationssicherheit fragt, hört das Gegenteil: »Warum steht da seit drei Stunden eine offene KIS-Sitzung?«, »Wer war um 14:12 Uhr in dieser Akte?«, »Warum hat das Konto Station 3 Zugriff auf alle Fachabteilungen?«. Beide Seiten haben recht. Die Aufgabe der IT ist, ein Verfahren zu bauen, bei dem beide Seiten ein bisschen weniger recht haben.

Schnell: Sekunden zählen, aber anders als man denkt

Geschwindigkeit hat am Stationsarbeitsplatz zwei Dimensionen. Die erste ist die Zeit bis zum arbeitsfähigen Bildschirm: Windows-Anmeldung, Profil, Gruppenrichtlinien, Start des KIS-Clients, Anmeldung im KIS. Bei einer lokalen Erstanmeldung an einem Rechner, an dem die Person noch nie war, kommen schnell ein bis zwei Minuten zusammen. Die zweite Dimension ist die Häufigkeit. Eine Pflegekraft wechselt in einer Schicht dutzendfach zwischen Patientenzimmer, Dienstzimmer, Medikamentenraum und Visitenwagen. Jede Anmeldung, die zehn Sekunden kostet, summiert sich. Jede Anmeldung, die neunzig Sekunden kostet, führt dazu, dass niemand sich abmeldet.

Der größte Hebel liegt deshalb nicht darin, die Anmeldung um zwei Sekunden schneller zu machen, sondern darin, die Arbeitsumgebung nicht jedes Mal neu aufzubauen. Wenn die Sitzung zentral weiterläuft und nach dem Auflegen der Karte am nächsten Gerät einfach wieder erscheint, ist die zweite Anmeldung in der Schicht eine Sache von Sekunden.

Sicher: Wer vor dem Bildschirm sitzt, ist nicht automatisch der Angemeldete

Sicherheit heißt am Stationsrechner vor allem: Die Person, die gerade Daten sieht und dokumentiert, ist die Person, die angemeldet ist. Das klingt trivial und ist es nicht. Ein Rechner im Dienstzimmer ist für jeden erreichbar, der durch die Tür kommt, einschließlich Besuchern, Patienten und Handwerkern. Eine offene Sitzung ist eine offene Akte. Dazu kommen die klassischen Risiken: Kennwörter auf Zetteln, geteilte Kennwörter, Konten ohne zweiten Faktor, und nicht zuletzt Angriffe auf Anmeldedaten, die über ein kompromittiertes Konto den Weg ins Netz finden. Zwei-Faktor-Anmeldung mit etwas, das man hat (Karte), und etwas, das man weiß (PIN), ist hier deutlich robuster als jedes Kennwort.

Nachvollziehbar: Wer war es?

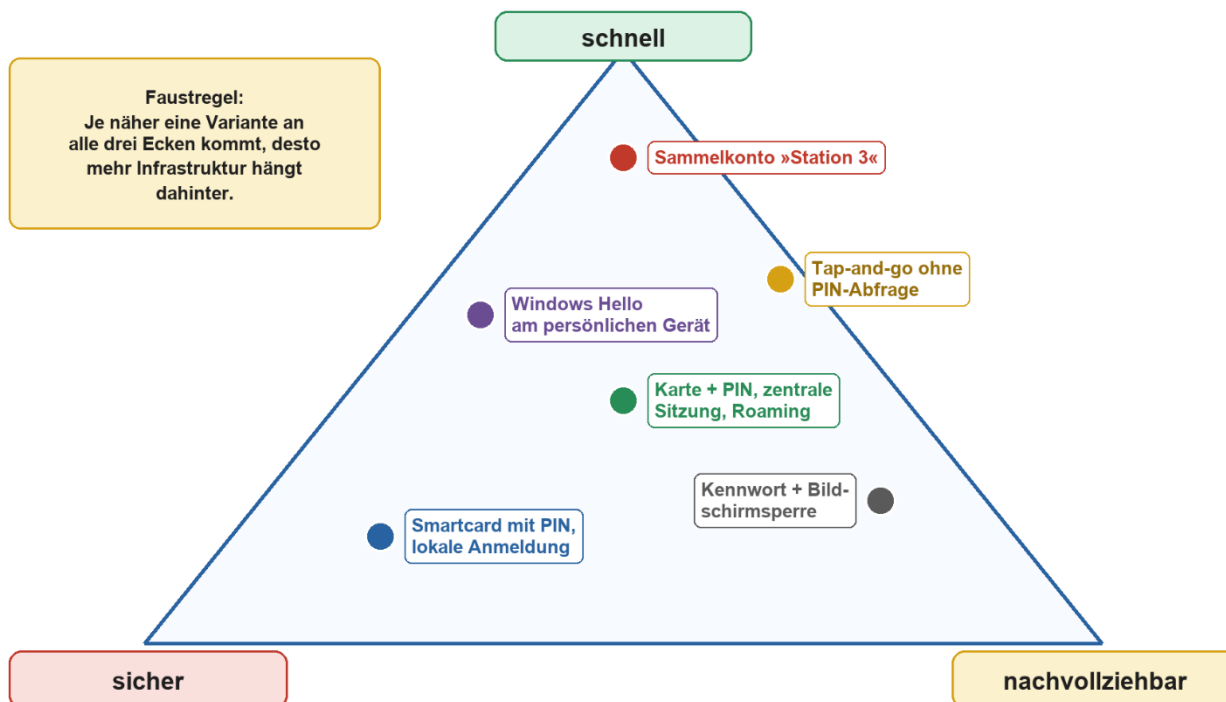
Das KIS protokolliert Zugriffe auf Patientendaten, das verlangen Datenschutz und Berufsrecht. Diese Protokolle sind aber nur so gut wie die Anmeldung, auf der sie beruhen. Meldet sich im KIS die Person persönlich an, während Windows unter einem Sammelkonto läuft, ist das KIS nachvollziehbar und der Rest nicht: Dateiablage, Drucker, Browser, Microsoft 365. Wird auch das KIS über ein gemeinsames Konto geöffnet, gibt es gar keine Nachvollziehbarkeit mehr, nur noch die Information, dass irgendjemand von Station 3 es war. Für die Aufklärung eines Vorfalls, für Auskunftersuchen und für die Forensik nach einem Sicherheitsvorfall ist das wertlos.

Warnung: Das Sammelkonto ist kein Kompromiss, sondern ein Befund

Gemeinsam genutzte Konten wie »Station 3« oder »Pflege-OP« entstehen fast immer aus gutem Willen: Die Anmeldung war zu langsam, also hat jemand eine Abkürzung gebaut. Sie werden dann weitergegeben, nie geändert, stehen auf dem Monitorrand und haben über die Jahre mehr Rechte gesammelt als jedes persönliche Konto. Im Audit, bei der Prüfung nach § 391 SGB V oder im Ernstfall nach einem Angriff fällt das Konto auf, und dann ist die Frage nicht mehr, ob es weg muss, sondern wie schnell.

Das Gegenmittel ist nicht das Verbot, sondern eine persönliche Anmeldung, die schneller ist als das Sammelkonto. Erst dann verschwindet es von selbst.

Das Zieldreieck am Stationsrechner und wo die Varianten landen



Das Zieldreieck: Sammelkonten liegen ganz oben bei »schnell«, die lokale Smartcard-Anmeldung nahe »sicher«. Karte mit PIN und zentraler Sitzung kommt der Mitte am nächsten – und bringt die meiste Infrastruktur mit.

Die Varianten: von der Kennwortanmeldung bis zur Sitzungsübernahme

In deutschen Krankenhäusern begegnen einem im Wesentlichen sechs Bausteine, die sich kombinieren lassen. Kaum ein Haus nutzt nur einen davon; typisch ist eine Mischung aus Thin Clients mit zentralen Sitzungen auf Station, klassischen Arbeitsplatzrechnern in der Verwaltung und Sonderlösungen in Funktionsbereichen wie OP, Intensivstation, Labor oder Radiologie.

Lokale Anmeldung mit Kennwort und Bildschirmsperre

Der Ausgangspunkt fast aller Häuser: Jeder Mensch hat ein Konto im Active Directory, meldet sich am Fat Client mit Benutzername und Kennwort an, das KIS startet lokal oder als veröffentlichte Anwendung. Das funktioniert, ist einfach zu betreiben und hängt an wenig Infrastruktur. Am Stationsrechner ist es aber die langsamste und unbeliebteste Variante: Jeder Wechsel bedeutet Abmelden, Anmelden, Profil laden, KIS starten. Die Folge sind offene Sitzungen, Sammelkonten oder beides. Für Verwaltungsarbeitsplätze mit einer Person pro Gerät ist diese Variante dagegen oft völlig ausreichend, idealerweise ergänzt um Windows Hello for Business.

Zentrale Sitzungen mit Citrix oder Remote Desktop

Bei Citrix Virtual Apps and Desktops oder den Remote Desktop Services von Microsoft läuft die Arbeitsumgebung nicht am Stationsrechner, sondern auf einem Sitzungshost im Rechenzentrum. Am Arbeitsplatz steht ein Thin Client oder ein schlanker Windows-Rechner, der nur das Bild anzeigt. Der entscheidende Vorteil für die Station: Die Sitzung ist vom Gerät entkoppelt. Wer sich am Dienstzimmer-PC trennt und am Visitenwagen wieder anmeldet, findet dort dieselbe Sitzung mit demselben geöffneten KIS-Fenster vor. Citrix nennt das Sitzungs-Roaming, bei Remote Desktop übernimmt der Verbindungsbroker die Wiederverbindung mit der getrennten Sitzung.

Damit diese Übernahme schnell geht, muss die Anmeldung am Endgerät selbst schnell sein. Hier kommen Karten ins Spiel: Karte auflegen, PIN eingeben, Sitzung erscheint. Karte abziehen oder

Leerlaufzeit überschritten, Sitzung wird getrennt, aber nicht beendet. Viele Häuser setzen dafür zusätzliche Single-Sign-on-Lösungen von Drittanbietern ein, die den Kartenleser an die Sitzungsverwaltung koppeln und auch Anwendungen jenseits von Windows mit Anmeldedaten versorgen. Die Herstellerlandschaft ist überschaubar; welche Lösung passt, hängt stark von KIS, Thin-Client-Plattform und Kartensystem ab.

Citrix Federated Authentication Service und Entra ID

Interessant wird es, wenn die erste Anmeldung nicht mehr mit einem Kennwort am Active Directory passiert, sondern über Entra ID – etwa weil Citrix Workspace aus der Cloud genutzt wird, weil bedingter Zugriff und Mehrstufen-Authentifizierung zentral in Entra ID gesteuert werden sollen oder weil der Zugang von außen über dieselbe Identität laufen soll. Dann hat die Citrix-Infrastruktur ein Problem: Der Mensch hat sich bei Entra ID angemeldet, etwa über SAML, aber der Sitzungshost ist ein Windows-Server in der Domäne und braucht eine Anmeldung, die Active Directory akzeptiert. Ein Kennwort, das man durchreichen könnte, gibt es nicht.

Diese Lücke schließt der Citrix Federated Authentication Service (FAS). Nach der Herstellerdokumentation läuft das so: StoreFront oder Workspace authentifiziert den Benutzer mit einem der unterstützten Verfahren und wendet sich beim Start einer Sitzung an den FAS. Der FAS stellt ein Ticket für genau diese Sitzung aus und beantragt bei der ausstellenden Microsoft-CA ein Zertifikat der Smartcard-Klasse im Namen des Benutzers. Der VDA auf dem Sitzungshost löst das Ticket beim FAS ein, das Zertifikat wird der Sitzung als virtuelle Smartcard zugeordnet, und der Domänencontroller sieht eine gewöhnliche Smartcard-Anmeldung. Der private Schlüssel verlässt den FAS dabei nicht; Signatur- und Entschlüsselungsvorgänge in der Sitzung werden an den FAS weitergereicht. Für den Schutz der Schlüssel nennt Citrix TPM oder Hardware-Sicherheitsmodul.

Die Konsequenz ist bemerkenswert: Der FAS darf im Namen jedes Benutzers, für den er berechtigt ist, ein Anmeldezertifikat beantragen. Citrix selbst bezeichnet ihn als privilegierte Komponente. Wer den FAS-Server übernimmt, kann sich als jeder dieser Benutzer anmelden. Er gehört deshalb in dieselbe Schutzstufe wie Domänencontroller und CA, und die Registrierungsagent-Berechtigung, mit der er Zertifikate für andere beantragt, muss auf die Benutzergruppen beschränkt werden, die sie wirklich brauchen – Administratoren gehören nicht dazu.

Wichtig: Architektur gegen die aktuelle Dokumentation prüfen

Citrix entwickelt Workspace, StoreFront, FAS und die Cloud-Dienste laufend weiter, Microsoft ebenso Entra ID und die Zertifikatsanmeldung. Die Beschreibung oben gibt den Stand der Herstellerdokumentation zum Zeitpunkt dieses Beitrags wieder. Bevor Sie planen, prüfen Sie Komponenten, unterstützte Identitätsanbieter, Versionen und Schlüsselschutz gegen die aktuelle Citrix-Dokumentation und gegen learn.microsoft.com – und lassen Sie sich vom Hersteller Ihres KIS bestätigen, dass dessen Single Sign-on in diesem Aufbau funktioniert.

Karten und Badges: Smartcard ist nicht gleich Ausweis

Fast jedes Krankenhaus hat bereits einen Mitarbeiterausweis mit Chip – für Zutritt, Zeiterfassung, Kantine, Parkhaus. Die naheliegende Idee lautet: Den nehmen wir auch für die Anmeldung. Das ist oft eine gute Idee, aber es lohnt der genaue Blick, was der Chip kann.

- **Kontaktlose Ausweise, bei denen nur die Kartenummer gelesen wird:** Der Leser liest eine Seriennummer und meldet sie an die Single-Sign-on-Lösung, die daraus den Benutzer ableitet. Das ist schnell und bequem, aber die Kartenummer ist kein Geheimnis. Je nach Kartentechnik lässt sie sich mit wenig Aufwand auslesen oder nachbilden. Ohne PIN oder zweiten Faktor ist das eine Identifikation, keine Authentifizierung.

- **Karten mit kryptografischem Chip und Zertifikat:** Auf dem Chip liegt ein Schlüsselpaar, das Zertifikat stammt aus der internen PKI, die PIN schützt den Schlüssel. Die Anmeldung läuft per Kerberos-PKINIT direkt am Domänencontroller. Das ist eine echte Zwei-Faktor-Anmeldung, braucht aber Kartenverwaltung, Zertifikatsausgabe und Sperrprozesse.
- **Mischformen:** Kontaktlose Erkennung für die schnelle Sitzungsübernahme innerhalb einer Schicht, PIN oder vollständige Anmeldung beim ersten Mal und nach einer definierten Zeit. Das ist in der Praxis oft der vernünftigste Kompromiss – vorausgesetzt, die Regeln sind dokumentiert und mit Informationssicherheit und Interessenvertretung abgestimmt.

Die Telematikinfrastruktur mit elektronischem Heilberufsausweis und Institutionskarte ist eine eigene Welt und kein Ersatz für die Anmeldung am Stationsrechner. Wer beides auf einer Karte vereinen möchte, landet schnell bei Fragen, die Kartenhersteller, gematik-Vorgaben und die interne PKI gemeinsam beantworten müssen. Die Abgrenzung beschreibt den Beitrag [PKI im Krankenhaus: Zertifikate für Geräte, WLAN, Anmeldung und Klinikanwendungen](#).

Windows Hello for Business: stark am persönlichen Gerät

Windows Hello for Business ersetzt das Kennwort durch einen Schlüssel, der im TPM des Geräts liegt und mit PIN, Gesichtserkennung oder Fingerabdruck freigegeben wird. Für Verwaltung, Chefarztsekretariat, Controlling oder die Notebooks der Oberärzte ist das hervorragend: schnell, phishing-resistent, ohne Karte. Am Stationsrechner hat es einen strukturellen Haken. Der Schlüssel ist an die Kombination aus Person und Gerät gebunden. Jede Person muss sich an jedem Gerät einmal registrieren, bevor sie Hello dort nutzen kann. Bei dreißig Pflegekräften, Ärzten, Therapeuten und Springern, die sich über den Tag an einer Handvoll Stationsrechner abwechseln, wird daraus ein Registrierungs-marathon, der genau das Gegenteil von schnell ist.

Für zentrale Sitzungen gilt eine weitere Einschränkung: Um sich mit Windows Hello for Business in einer Remote-Desktop-Sitzung anzumelden, muss laut Microsoft ein zusätzliches Zertifikat in den Hello-Container ausgerollt werden; Microsoft empfiehlt als Alternative Remote Credential Guard. Wer Hello am Thin Client erwartet, sollte die Kette also genau planen.

FIDO2-Sicherheitsschlüssel und Zertifikatsanmeldung an Entra ID

FIDO2-Sicherheitsschlüssel sind das, was viele sich unter einer modernen Karte vorstellen: ein Token mit NFC oder USB, der nicht an ein Gerät gebunden ist und sich an jedem freigegebenen Windows-Rechner nutzen lässt. Für gemeinsam genutzte Geräte ist das attraktiv. Microsoft unterstützt die Windows-Anmeldung mit FIDO2-Schlüsseln an Geräten, die mit Entra ID verbunden oder hybrid verbunden sind, nicht aber an rein lokal domänengebundenen Geräten. Und – das ist für Kliniken mit Citrix entscheidend – Szenarien wie RDP, VDI und Citrix, in denen der Schlüssel anders als über WebAuthn-Umleitung genutzt wird, nennt Microsoft ausdrücklich als nicht unterstützt. Die Einzelheiten stehen in der [Anleitung von Microsoft zur Windows-Anmeldung mit FIDO2-Sicherheitsschlüsseln](#).

Eine weitere Option ist die zertifikatsbasierte Authentifizierung von Entra ID: Benutzer melden sich mit dem Zertifikat ihrer Smartcard direkt bei Entra ID an, auch bei der Windows-Anmeldung an Geräten, die mit Entra ID oder hybrid verbunden sind, und erhalten danach ein Primäres Aktualisierungstoken. Bei hybrid verbundenen Geräten muss nach Microsoft-Dokumentation zuerst die Anmeldung am lokalen Active Directory gelingen. Für Häuser, die ohnehin eine Karten-PKI betreiben, kann das ein Baustein sein, um dieselbe Karte auch für Microsoft 365 im Browser zu nutzen.

Schneller Benutzerwechsel am lokalen Rechner

Windows kennt seit Langem den schnellen Benutzerwechsel: Mehrere Personen sind gleichzeitig am selben Rechner angemeldet, jede in ihrer eigenen Sitzung, und man wechselt, ohne sich

abzumelden. Am Stationsrechner klingt das verlockend und ist in der Praxis selten eine gute Idee. Jede Sitzung belegt Arbeitsspeicher, jede startet ihren eigenen KIS-Client, und manche KIS-Clients oder Gerätetreiber vertragen mehrere parallele Instanzen schlecht. Nach drei Schichten hängen zwölf Sitzungen am Rechner, von denen niemand mehr weiß, wem sie gehören. Für gemeinsam genutzte lokale Windows-Geräte gibt es zusätzlich den Modus für freigegebene PCs und Richtlinien für eine schnellere Erstanmeldung von Entra-Konten (etwa EnableFastFirstSignIn); deren aktuellen Funktionsumfang und Status sollten Sie vor einer Planung auf learn.microsoft.com prüfen. Wie gemeinsam genutzte Geräte auf Station insgesamt organisiert werden können, beschreibt der Beitrag [Frontline in der Pflege: Gemeinsam genutzte Geräte, Schichtwechsel und Stationsrechner](#).

Die Varianten im Vergleich

Variante	Geschwindigkeit	Sicherheit	Abhängigkeiten	Nachvollziehbarkeit
Sammelkonto	sehr hoch	sehr niedrig	kaum	keine
Kennwort lokal	niedrig, jeder Wechsel kostet Profil- und KIS-Start	mittel, ohne zweiten Faktor schwach	AD, Netz	gut, solange niemand Sitzungen offen lässt
Citrix oder RDS mit Kennwort	mittel, Sitzung bleibt erhalten	mittel	AD, Sitzungshosts, Broker oder StoreFront	gut
Citrix oder RDS mit Karte und PIN	hoch, Sitzungsübernahme in Sekunden	hoch, zwei Faktoren	PKI, Sperrlisten, KDC-Zertifikate, Kartenverwaltung, ggf. SSO-Lösung	sehr gut
Citrix mit Entra ID und FAS	hoch nach Erstanmeldung	hoch, wenn FAS und CA wie Tier 0 geschützt sind	Entra ID, Internet, FAS, ADACS, Sperrlisten, Kerberos	sehr gut, über Entra- und AD-Protokolle
Kontaktloser Ausweis ohne PIN	sehr hoch	niedrig bis mittel, Kartenummer ist kein Geheimnis	SSO-Lösung, Kartensystem	mittel, Karte kann weitergegeben werden
Windows Hello for Business	hoch am persönlichen Gerät, niedrig an Geräten mit vielen Nutzern	hoch	TPM, Entra ID oder Kerberos-Vertrauensmodell, ggf. PKI	sehr gut
FIDO2-Sicherheitsschlüssel	hoch an lokalen Geräten	hoch, phishing-resistent	Entra-verbundene oder hybride Geräte; nicht in Citrix-, VDI- oder RDP-Sitzungen ohne WebAuthn-Umleitung	sehr gut
Schneller Benutzerwechsel lokal	mittel, hoher Ressourcenverbrauch	mittel	leistungsfähige Hardware, KIS-Client mehrfach lauffähig	gut

Schichtwechsel am Stationsrechner: Sitzung folgt der Person, nicht dem Gerät



Schichtwechsel mit zentralen Sitzungen: Die Sitzung folgt der Karte von Gerät zu Gerät. Wer die Karte vergisst, wird nach der Leerlaufzeit getrennt, aber nicht abgemeldet.

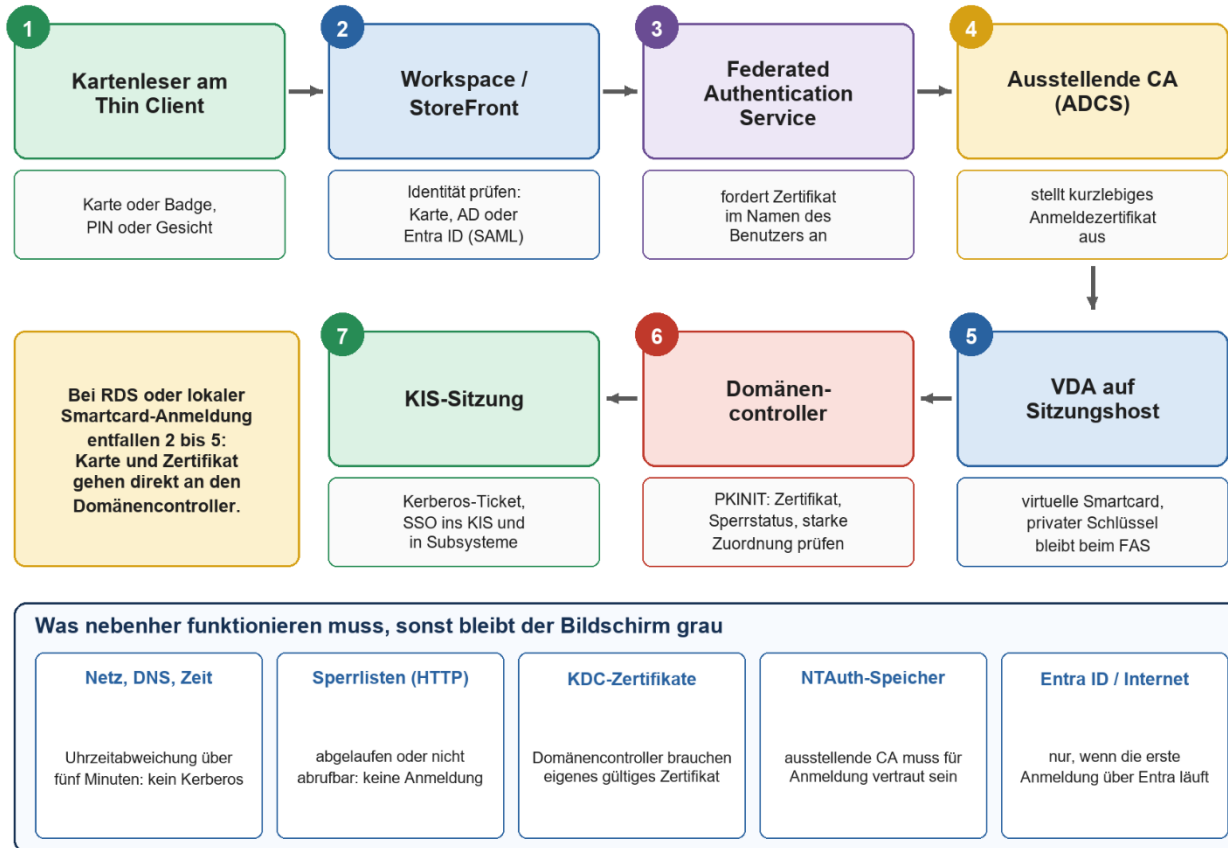
Tip: Leerlaufzeiten mit der Station festlegen, nicht für sie

Die Zeit bis zur Bildschirmsperre ist eine der umstrittensten Einstellungen im Haus. Zu kurz, und die Sperre schlägt mitten in der Dokumentation zu; zu lang, und die Sitzung steht offen im Flur. Legen Sie die Werte je Bereich fest – Dienstzimmer, Flur, Intensivstation, Ambulanz –, begründen Sie sie in einer Verfahrensanweisung und prüfen Sie sie nach einigen Wochen mit der Pflegedirektion. Mit Kartenanmeldung darf die Sperre kürzer sein, weil das Entsperren nur Sekunden dauert.

Die Anmeldekette: Warum am Ende PKI und Kerberos entscheiden

Egal ob Smartcard, Citrix FAS oder Windows Hello mit Zertifikat: Sobald eine Anmeldung per Zertifikat am Active Directory stattfindet, landet sie beim Domänencontroller, und der stellt eine Reihe von Fragen, bevor er ein Kerberos-Ticket herausgibt. Wer diese Fragen kennt, versteht, warum die Kartenanmeldung am Montagmorgen funktioniert und am Dienstagmorgen nicht.

Die Anmeldekette vom Kartenleser bis zur KIS-Sitzung (Beispiel Citrix mit FAS)



Die Anmeldekette am Beispiel Citrix mit FAS: vom Kartenleser über StoreFront, FAS und CA zum Sitzungshost, zum Domänencontroller und in die KIS-Sitzung. Bei RDS oder lokaler Smartcard-Anmeldung ist die Kette kürzer, die Abhängigkeiten im unteren Kasten bleiben.

Was der Domänencontroller bei der Zertifikatsanmeldung prüft

- **Vertraut die Gesamtstruktur der ausstellenden CA?** Die CA muss im NTAuth-Speicher des Active Directory eingetragen sein. Eine CA, die dort nicht steht, kann Zertifikate ausstellen, so viel sie will – für die Anmeldung sind sie wertlos.
- **Ist das Zertifikat gültig und nicht gesperrt?** Der Domänencontroller prüft die Sperrliste. Ist sie abgelaufen oder nicht abrufbar, scheitert die Anmeldung. Das ist die häufigste Ursache für »Die Karte geht plötzlich nicht mehr«.
- **Lässt sich das Zertifikat eindeutig einem Konto zuordnen?** Seit dem Update vom 11. Februar 2025 erzwingen Domänencontroller standardmäßig eine starke Zuordnung, etwa über die SID-Erweiterung im Zertifikat. Mit dem Update vom 9. September 2025 ist der Rückweg in den Kompatibilitätsmodus entfallen. Eine Microsoft-Unternehmens-CA trägt die SID-Erweiterung bei online ausgestellten Zertifikaten selbst ein; Citrix verweist für FAS genau darauf. Wer eine Fremd-CA nutzt oder Karten mit Zertifikaten aus Offline-Vorlagen bestückt, muss das ausdrücklich prüfen.
- **Hat der Domänencontroller selbst ein passendes Zertifikat?** Für PKINIT braucht der Domänencontroller ein KDC-Zertifikat, dem der Client vertraut. Läuft es ab, scheitern Zertifikatsanmeldungen an genau diesem Domänencontroller – mit etwas Pech nur an einem von mehreren, was die Fehlersuche zu einem Glücksspiel macht.
- **Stimmt die Uhrzeit?** Kerberos toleriert in der Standardeinstellung eine Zeitabweichung von fünf Minuten. Ein Thin Client mit falscher Uhr oder ein Sitzungshost mit hängendem Zeitdienst ist ein überraschend häufiger Grund für Anmeldefehler.

Was eine CA im Krankenhaus sonst noch trägt, wie man ihre Vorlagen härtet und warum die Sperrliste der Offline-Root einen festen Kalendertermin braucht, beschreiben der Beitrag [PKI im Krankenhaus: Zertifikate für Geräte, WLAN, Anmeldung und Klinikanwendungen](#) und der [Kompetenzbereich PKI mit ADCS](#).

Warnung: Die Sperrliste läuft nicht zu Bürozeiten ab

Eine abgelaufene Sperrliste der ausstellenden CA oder ein ausgefallener Webserver, auf dem sie liegt, legt die gesamte Kartenanmeldung lahm – auf allen Stationen gleichzeitig, typischerweise nachts oder am Wochenende. Überwachen Sie die Gültigkeit aller Sperrlisten und die Erreichbarkeit aller Verteilpunkte aktiv, hinterlegen Sie einen Alarm für die Rufbereitschaft und beschreiben Sie das Vorgehen in der Notfallanweisung.

Kerberos bis ins KIS

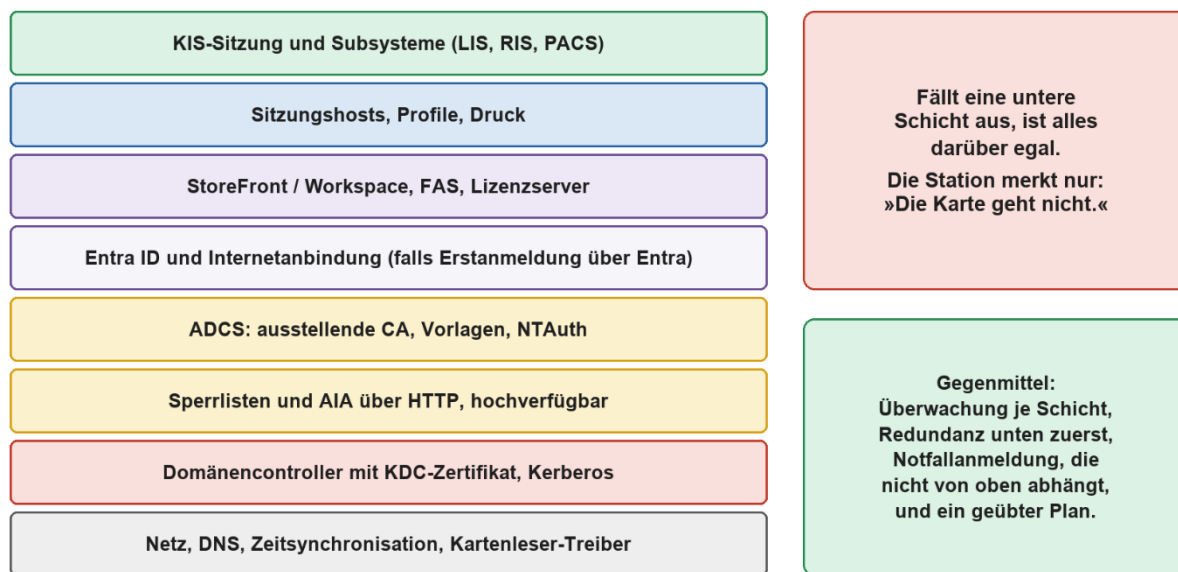
Ist die Windows-Anmeldung gelungen, hat die Sitzung ein Kerberos-Ticket. Ob die Person danach im KIS noch einmal Benutzername und Kennwort eingeben muss, hängt vom KIS ab. Viele Systeme unterstützen eine integrierte Windows-Anmeldung, bei der das KIS die Windows-Identität übernimmt. Technisch läuft das idealerweise über Kerberos, in gewachsenen Umgebungen allzu oft noch über NTLM. Spätestens beim Abschalten von NTLM zeigt sich, welche Subsysteme, Kommunikationsserver und Medizintechnik-Oberflächen noch auf das alte Verfahren angewiesen sind. Der Beitrag [NTLM abschalten im Krankenhaus: Medizingeräte, Altanwendungen und Kerberos](#) beschreibt, wie man das herausfindet, ohne den Stationsbetrieb zu gefährden; die Grundlagen zu Tickets, Dienstprinzipalnamen und Delegation finden Sie im [Kompetenzbereich Kerberos](#).

Im Klinikverbund kommt eine weitere Ebene hinzu: Arbeiten Pflegekräfte oder Ärzte standortübergreifend, liegen Benutzerkonto und KIS-Server womöglich in unterschiedlichen Domänen, verbunden über Vertrauensstellungen. Kerberos über Vertrauensstellungen funktioniert, setzt aber saubere DNS-Auflösung, korrekte Dienstprinzipalnamen und passende Vertrauenseinstellungen voraus. Wie man solche Strukturen aufräumt, zeigt der Beitrag [Active Directory im Klinikverbund: Vertrauensstellungen, Altdomänen und der Weg zur Konsolidierung](#).

Entra ID als erste Station der Kette

Läuft die erste Anmeldung über Entra ID, gewinnen Sie zentrale Steuerung: bedingter Zugriff je nach Gerät, Standort und Risiko, einheitliche Mehrstufen-Authentifizierung, eine Identität für Citrix, Microsoft 365 und andere Cloud-Anwendungen. Sie verlieren dafür Unabhängigkeit. Ist die Internetanbindung gestört oder Entra ID nicht erreichbar, kann sich niemand neu anmelden, auch wenn das KIS im eigenen Rechenzentrum tadellos läuft. Für die Station ist das kein theoretisches Risiko. Planen Sie deshalb einen Notfallweg, der ohne Cloud auskommt – etwa die direkte Kartenanmeldung am lokalen StoreFront oder Sitzungshost –, und testen Sie ihn regelmäßig. Wie Sie Konten, Rollen und bedingten Zugriff in Entra ID sauber aufsetzen, beschreibt der [Kompetenzbereich Microsoft Entra ID](#).

Der Abhängigkeitsturm: was alles stehen muss, damit die Karte funktioniert



Der Abhängigkeitsturm: Jede Schicht muss stehen, damit oben die KIS-Sitzung erscheint. Ausfälle unten zeigen sich auf Station immer als »Die Karte geht nicht«.

Tipp: Notfallanmeldung, die nicht von der Kette abhängt

Legen Sie fest, wie sich die Station anmeldet, wenn Karte, CA, FAS oder Entra ID ausfallen: persönliche Konten mit Kennwort und zweitem Faktor als Rückfallebene, versiegelte Notfallzugänge für definierte Bereiche mit nachträglicher Prüfung, Papierprozesse für den Fall, dass gar nichts geht. Beschreiben Sie das in einer Verfahrensweisung, die im QM-Handbuch gelenkt wird und auch offline vorliegt, und üben Sie es mindestens einmal im Jahr mit Rufbereitschaft und Station.

Organisation, Mitbestimmung und Nachweise

Die Technik ist die halbe Miete. Die andere Hälfte entscheidet sich in Prozessen, die mit IT nur am Rande zu tun haben: Wer gibt Karten aus? Was passiert, wenn eine Karte verloren geht? Wer darf Protokolle der Anmeldung auswerten? Und wie beweist das Haus im Audit, dass das alles geregelt ist?

Kartenausgabe, Kartenverlust und die Leute ohne Karte

Eine Kartenanmeldung ist nur so gut wie der Prozess, der die Karte zur richtigen Person bringt. Klären Sie, wer die Identität beim Ausgeben prüft, wie Zertifikate auf die Karte kommen, wie schnell eine verlorene Karte gesperrt wird und wie eine Ersatzkarte ausgegeben wird – auch am Wochenende, denn die Pflegekraft ohne Karte steht am Samstag um 6 Uhr vor dem Rechner. Denken Sie an die Menschen, die nicht in den Standardprozess passen: Leasingkräfte und Zeitarbeit, Honorarärzte, Medizinstudenten im Praktischen Jahr, Auszubildende, Mitarbeiterinnen und Mitarbeiter externer Dienstleister. Für sie braucht es befristete Karten oder befristete Ersatzverfahren, nicht ein Sammelkonto »Aushilfe«.

Protokolle und Mitbestimmung

Jede Kartenanmeldung erzeugt Protokolle: Wer hat sich wann an welchem Gerät angemeldet, wann wurde die Sitzung getrennt, wann übernommen? Diese Daten sind für Sicherheit und Forensik wertvoll, und sie eignen sich gleichzeitig dazu, Verhalten und Leistung von Menschen zu überwachen. Damit sind sie ein Fall für die Interessenvertretung, und zwar bevor die Technik eingeführt wird.

Wichtig: Hinweis: Mitbestimmung je nach Trägerschaft – keine Rechtsberatung

In privaten und freigemeinnützigen Häusern mit Betriebsrat greift das Mitbestimmungsrecht bei technischen Einrichtungen, die zur Überwachung von Verhalten oder Leistung geeignet sind, nach § 87 Absatz 1 Nummer 6 Betriebsverfassungsgesetz. In öffentlichen und kommunalen Häusern gilt das Personalvertretungsrecht des jeweiligen Bundeslandes oder des Bundes, das sich in Zuständigkeiten und Verfahren unterscheidet. Kirchliche Häuser haben ihre eigenen Regelungen für die Mitarbeitervertretung. Klären Sie mit Ihrer Rechtsabteilung oder externer Rechtsberatung, welche Regelung für Ihr Haus gilt, und vereinbaren Sie Zweck, Auswertungsrechte und Löschfristen der Anmeldeprotokolle schriftlich.

Wie das je nach Trägerschaft aussieht und welche Punkte in eine Dienst- oder Betriebsvereinbarung gehören, beschreibt der Beitrag [Betriebsrat, Personalrat oder MAV: Mitbestimmung bei Microsoft 365 je nach Trägerschaft](#).

Informationssicherheit und Nachweise

§ 391 SGB V verpflichtet Krankenhäuser, nach dem Stand der Technik angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität und Vertraulichkeit ihrer informationstechnischen Systeme zu treffen, soweit diese für die Funktionsfähigkeit des Hauses und den Schutz der Patienteninformationen maßgeblich sind. Für Betreiber kritischer Anlagen gelten stattdessen die Pflichten des BSI-Gesetzes. Der branchenspezifische Sicherheitsstandard »Medizinische Versorgung« der Deutschen Krankenhausgesellschaft liegt in Version 1.3.1 vor. Wie diese Pflichten zusammenspielen und was sie für Microsoft 365 bedeuten, steht im Beitrag [NIS2, § 391 SGB V und B3S: Was die Sicherheitspflichten für Microsoft 365 bedeuten](#).

Für die Anmeldung am Stationsarbeitsplatz heißt das konkret: Auditoren wollen sehen, dass Konten personalisiert sind, dass Sammelkonten begründet, begrenzt und dokumentiert sind, dass starke Authentifizierung eingesetzt wird, wo es angemessen ist, und dass die zugrunde liegende Infrastruktur – CA, FAS, Domänencontroller – entsprechend geschützt und überwacht wird. Ein Anmeldekonzert als gelenktes Dokument im QM-Handbuch mit Verweis auf die Verfahrensanweisungen für Kartenausgabe, Kartenverlust, Leerlaufzeiten und Notfallanmeldung beantwortet die meisten dieser Fragen, bevor sie gestellt werden.

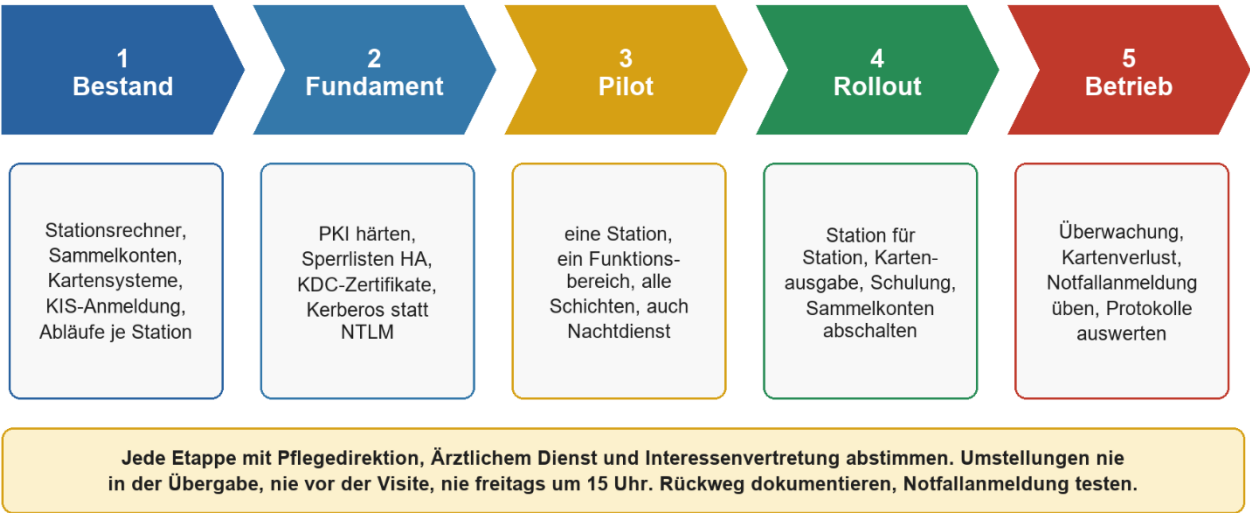
Aus der Praxis: Erfahrung aus einem Klinikverbund

In der langjährigen Begleitung eines Krankenhausverbunds mit mehreren Standorten standen genau die Themen im Mittelpunkt, an denen jede Kartenanmeldung hängt: Vertrauensstellungen zwischen Domänen, die schrittweise Abschaltung von NTLM zugunsten von Kerberos sowie Aufbau und Härtung der PKI. Die wichtigste Lehre daraus: Die Anmeldung am Stationsrechner wird nicht am Kartenleser stabil, sondern in den Schichten darunter. Wer Kerberos, Sperrlisten und Zertifikatsvorlagen im Griff hat, kann sich bei der Wahl der Anmeldevariante nach den Bedürfnissen der Station richten statt nach den Launen der

Infrastruktur.

Fahrplan: vom Sammelkonto zur persönlichen Anmeldung

Vom Sammelkonto zur persönlichen Kartenanmeldung in fünf Etappen



Fünf Etappen von der Bestandsaufnahme bis zum Betrieb. Die Reihenfolge ist wichtiger als das Tempo: erst das Fundament, dann der Pilot, dann die Fläche.

Rolle	Aufgabe bei der Anmeldung am Stationsarbeitsplatz
Geschäftsführung	Auftrag, Budget für Karten, Leser, Redundanz und SSO-Lösung, Entscheidung über das Ende der Sammelkonten
IT-Leitung und IT-Administration	Konzept, PKI und Kerberos als Fundament, Citrix oder RDS, FAS, Überwachung, Notfallanmeldung
Pflegedirektion und Ärztlicher Direktor	Anforderungen aus dem Stationsalltag, Leerlaufzeiten, Pilotstationen, Akzeptanz
Informationssicherheitsbeauftragter	Risikobewertung, Einordnung in B3S bzw. BSIG-Pflichten, Schutzstufe von CA und FAS
Datenschutzbeauftragter	Zweck und Löschfristen der Anmeldeprotokolle, Rechtsgrundlagen, Auftragsverarbeitung bei Cloud-Diensten
Qualitätsmanagementbeauftragter	Anmeldekonzert und Verfahrensanweisungen als gelenkte Dokumente im QM-Handbuch
Medizintechnik	Geräte und Arbeitsplätze mit eigener Anmeldung, Abstimmung mit Herstellern
Betriebsrat, Personalrat oder MAV	Mitbestimmung bei Kartenanmeldung und Protokollauswertung

Wenn Sie ein Anmeldekonzert für Station und Funktionsbereiche nicht allein aufstellen wollen, unterstützt die [Microsoft-365-Beratung für Krankenhäuser](#) von der Bestandsaufnahme über PKI

und Kerberos bis zum Pilotbetrieb. Damit Rufbereitschaft und IT-Team die Kette auch nachts verstehen, gibt es die [Microsoft-365-Schulung für Krankenhäuser](#).

Häufige Fragen zur Anmeldung am Stationsarbeitsplatz

Können wir Sammelkonten auf Station ganz abschaffen?

In aller Regel ja, aber nur, wenn die persönliche Anmeldung mindestens so schnell ist wie das Sammelkonto. Mit zentralen Sitzungen, Karte und PIN ist das erreichbar. Wo ein gemeinsames Konto aus fachlichen Gründen bleiben muss – etwa für eine reine Anzeige ohne Patientenbezug –, sollte es begründet, auf das Nötigste beschränkt und dokumentiert sein.

Brauchen wir für die Kartenanmeldung zwingend eine eigene PKI?

Für eine echte Smartcard-Anmeldung am Active Directory und für Citrix FAS ja: Die Zertifikate müssen von einer CA stammen, der die Gesamtstruktur für die Anmeldung vertraut. Reine Ausweislösungen, die nur die Kartennummer lesen, kommen ohne PKI aus, bieten dafür aber deutlich weniger Sicherheit.

Funktioniert Windows Hello for Business auf Stationsrechnern?

Technisch ja, praktisch selten gut. Hello ist an Person und Gerät gebunden, jede Person muss sich an jedem Gerät registrieren. An Rechnern mit vielen wechselnden Nutzern ist das unpraktisch. Seine Stärken spielt Hello an persönlichen Geräten in Verwaltung und ärztlichen Leitungspositionen aus.

Können wir FIDO2-Schlüssel in Citrix nutzen?

Für die Anmeldung am lokalen, mit Entra ID verbundenen Windows-Gerät ja. Innerhalb von Citrix-, VDI- oder RDP-Sitzungen nennt Microsoft FIDO2-Schlüssel als nicht unterstützt, sofern sie nicht über WebAuthn-Umleitung genutzt werden. Prüfen Sie den aktuellen Stand bei Microsoft und Citrix, bevor Sie planen.

Was passiert, wenn Entra ID nicht erreichbar ist?

Läuft die Erstanmeldung über Entra ID, kann sich niemand neu anmelden, solange die Verbindung fehlt. Bestehende Sitzungen laufen in der Regel weiter. Deshalb brauchen Sie einen dokumentierten und geübten Notfallweg, der ohne Cloud auskommt.

Warum geht die Karte plötzlich nicht mehr, obwohl niemand etwas geändert hat?

Weil sich etwas von selbst geändert hat: eine abgelaufene Sperrliste, ein abgelaufenes KDC-Zertifikat, ein abgelaufenes Kartenzertifikat, eine falsche Uhrzeit oder ein Windows-Update, das die Zuordnungsregeln verschärft hat. Eine Überwachung dieser Punkte erspart der Rufbereitschaft viele Nachtstunden.

Dürfen wir die Anmeldeprotokolle zur Arbeitszeitkontrolle nutzen?

Das ist eine rechtliche und mitbestimmungspflichtige Frage, die Sie mit Datenschutzbeauftragtem, Interessenvertretung und gegebenenfalls Rechtsberatung klären müssen. Bewährt hat sich, Zweck und Auswertungsrechte von vornherein eng auf Sicherheit und Aufklärung von Vorfällen zu begrenzen und das schriftlich zu vereinbaren.

Fazit: Die schnellste Anmeldung ist die, die man nicht wiederholen muss

Am Stationsarbeitsplatz gewinnt nicht die Variante mit den meisten Sicherheitsmerkmalen und nicht die mit den wenigsten Klicks, sondern die, bei der die persönliche Anmeldung schneller ist

als jede Abkürzung. In den meisten Krankenhäusern läuft das auf zentrale Sitzungen mit Citrix oder Remote Desktop hinaus, auf Karte und PIN, auf eine Sitzung, die der Person von Gerät zu Gerät folgt, und – wo Entra ID die Identität führt – auf den Federated Authentication Service als Brücke ins Active Directory. Windows Hello for Business und FIDO2-Schlüssel haben ihren Platz an persönlichen und lokalen Geräten, nicht zwingend am Thin Client im Flur.

Das Fundament ist immer dasselbe: eine gehärtete PKI mit überwachten Sperrlisten, Domänencontroller mit gültigen Zertifikaten, Kerberos statt NTLM bis ins KIS und eine Notfallanmeldung, die nicht von derselben Kette abhängt. Wer das baut, mit Station, Informationssicherheit und Interessenvertretung abstimmt und im QM-Handbuch dokumentiert, kann das Konto »Station 3« irgendwann in Rente schicken. Es hat lange genug Dienst geschoben.

Weiter im Thema

- › [PKI im Krankenhaus: Zertifikate für Geräte, WLAN, Anmeldung und Klinikanwendungen](#)
- › [NTLM abschalten im Krankenhaus: Medizingeräte, Altanwendungen und Kerberos](#)
- › [Kompetenzbereich Kerberos](#)
- › [Kompetenzbereich Microsoft Entra ID](#)
- › [Frontline in der Pflege: Gemeinsam genutzte Geräte, Schichtwechsel und Stationsrechner](#)
- › [Active Directory im Klinikverbund: Vertrauensstellungen, Altdomänen und der Weg zur Konsolidierung](#)