Zentrum für sichere Informationstechnologie – Austria
Secure Information Technology Center – Austria

A-SIT

Seidlgasse 22 / 9, 1030 Wien
Tel.: (+43 1) 503 19 63–0
Fax: (+43 1) 503 19 63–66

Inffeldgasse 16a, 8010 Graz
Tel.: (+43 316) 873-5514
Fax: (+43 316) 873-5520

http://www.a-sit.at
E-Mail: office@a-sit.at

DVR: 1035461
ZVR: 948166612
UID: ATU60778947

DEVICE ENROLMENT MIT FLEXIBLER AUTHENTIFIZIERUNG

Version 1.0 vom 02.10.2017
Bernd Prünster – bernd.pruenster@a-sit.at

Im Corporate-Bereich sind Managed-Devices bereits etabliert. Kleinunternehmer und Endbenutzer profitieren jedoch wenig von derart komplexen Systemen und Infrastrukturen dieser Größenordnung. Des Weiteren sind Managed-Device-Lösungen meist an externe Infrastrukturen gekoppelt.
Im Rahmen dieses Projekts wurden Konzepte und Prototypen zur flexiblen Authentifizierung von Geräten erarbeitet. Dabei liegt der Fokus auf der erstmaligen Geräteauthentifizierung bzw. dem Enrolmentverfahren sowie einfacher Widerrufbarkeit von Berechtigungen. Die initiale Authentifizierung muss flexibel genug gestaltet sein, um auch die unterschiedlichen Eigenschaften von Endnutzergeräten miteinzubeziehen. Die eigentliche Kommunikation und der Kommunikationsaufbau zwischen Gerät und Dienst greift hingegen auf etablierte Standards wie Transport Layer Security (TLS) zurück. Dadurch wird dieser Aspekt einerseits möglichst unkompliziert und konzeptionell einfach gehalten, andererseits kann nur so größtmögliche Kompatibilität auch zu bestehenden Diensten garantiert werden. Auf Grund der Leistungsfähigkeit aktueller Endgeräte, sowie deren umfangreichen Featuresets und der breiten Unterstützung von Technologien wie TLS ist auch der notwendige Unterbau für eine praktische Umsetzung der erarbeiteten Konzepte vorhanden. Um die tatsächliche Machbarkeit zu veranschaulichen wurde ein Demonstrator entwickelt.

Inhaltsverzeichnis

1. Einleitung

Im Corporate-Bereich sind Managed-Devices bereits etabliert. Kleinunternehmer und Endbenutzer profitieren jedoch wenig von derart komplexen Systemen und Infrastrukturen dieser Größenordnung. Des Weiteren sind Managed-Device-Lösungen meist an externe Infrastrukturen gekoppelt.
Betrachtet man in diesem Zusammenhang aktuelle Nutzergewohnheiten (mehrere unterschiedliche Geräte pro Nutzer, bzw. Nutzerin[1]) sowie ein zunehmend dynamisches Umfeld mit zunehmend mehr mobilen Geräten, ergeben sich Anforderungen, welche über die Möglichkeiten von Managed-Device-Lösungen hinausgehen.
Unabhängig von Sicherheitsprotokollen, Berechtigungen von Angestellten und Nutzungsrichtlinien von Geräten innerhalb einer Organisation muss einerseits eine Zuordnung von Geräten zu deren Nutzern und Nutzerinnen hergestellt werden, andererseits ein initiales Vertrauensverhältnis zu den Geräten selbst hergestellt werden. Üblicherweise wird dies bei stationären Geräten implizit über eine Vorkonfiguration durch Systemadministratoren und/oder eine Domänenverwaltung realisiert, während für Mobilgeräte oftmals Managed-Device-Ansätze verfolgt werden. Um diese Prozesse zu vereinheitlichen und auch traditionelle Endgeräte, wie z.B. Desktopcomputer im Rahmen eines umfassenden Enrolmentverfahrens in (Firmen-)Netzwerke aufnehmen und verwalten zu können, sind abstraktere, flexiblere Konzepte notwendig. Im Wesentlichen geht es dabei um die Frage, wie die Zugehörigkeit eines Geräts zu einem Verbund oder Netzwerk nachgewiesen werden kann. Hierfür gibt es unterschiedliche Mechanismen, angefangen von simpler lokaler Zugehörigkeit (z.B. über ein kabelgebundenes Firmennetzwerk), Krypto-Token, bis hin zu PKI-basierten Methoden.
Im Rahmen dieses Projekts wurde ein Konzept für ein Enrolmentframework erarbeitet, welches sich dieser Frage annimmt. Die daraus hervorgegangene Lösung wurde in Form eines Demonstrators umgesetzt, um auch die Machbarkeit zu belegen. Nachfolgend werden prinzipielle Anforderungen an eine solche Lösung auf Basis der Ziele dieses Projekts erläutert.

2. Anforderungen

Unabhängig davon, welche Methoden für Authentifizierung im Rahmen von Device-Enrolment zum Einsatz kommen, ist es aus technischer Sicht vorerst nicht weiter relevant, was es bedeutet, dass ein Gerät Teil eines Verbunds bzw. einer Organisation ist. Folglich lassen sich entsprechende Verfahren auf alle Geräteklassen anwenden, wodurch sich folgende, allgemeine Voraussetzungen für ein flexibles Enrolmentkonzept ableiten lassen:

- Der Nachweis der Zugehörigkeit muss nicht nur unabhängig von der verwendeten Geräteklasse, sondern auch dienst- und applikationsunabhängig möglich sein. Somit kommen für eine einheitliche Lösung nur standardisierte, allgemeine unterstützte Verfahren in Frage.
- Die Überprüfung von Zugehörigkeiten und Berechtigungen soll zum Zeitpunkt der Überprüfung in jedem Fall nicht von einer einzigen zentralen Instanz abhängen, unter anderem um hohe Lasten an einer einzelnen Komponente zu vermeiden.
- Nutzungsverhalten unterschiedlicher Geräteklassen muss formalisierbar und im Rahmen von Zugriffsrechten auch automatisiert überprüfbar sein, wobei für ersteres unerheblich ist, wie dies geschieht, so lange ein maschinenlesbares Format verwendet wird, das eine automatische Überprüfung ermöglicht.
- Die erstmalige Authentifizierung muss möglichst flexibel umsetzbar sein, um auch unterschiedliche Szenarien für den Aufbau eines Vertrauensverhältnisses abzudecken.
- Die erstmalige Authentifizierung muss situationsabhängig und gleichzeitig möglichst komfortabel gestaltbar sein.
- Die Gültigkeitsdauer von Zugriffsberechtigungen, bzw. Zugehörigkeitsnachweisen muss frei definierbar sein. In diesem Zusammenhang sind auch Möglichkeiten vorzusehen, welche (automatisiert, bzw. automatisierbar) unterschiedliche Nutzungsverhalten verschiedener Geräteklassen reflektieren.
- Eine (legitime) Verlängerung von Berechtigungen muss im Regelfall möglichst automatisiert vonstattengehen.

[1] https://www.statista.com/statistics/333861/connected-devices-per-person-in-selected-countries/

- Im Falle einer Kompromittierung muss der Widerruf von Zugehörigkeiten sowohl von Betroffenen, als auch z.B. von Vorgesetzten oder Systemadministratoren schnell und einfach durchführbar sein, um eventuelle negative Auswirkungen minimal zu halten.
- Zugriffsberechtigungen müssen möglichst granular erteilbar, verwaltbar und widerrufbar sein:
    - Zugriffsberechtigungen müssen für unterschiedliche Dienste individuell verwaltbar sein.
    - Die Kompromittierung bzw. missbräuchliche Nutzung von Berechtigungen für einen Dienst darf keine nachteilige Auswirkung auf andere Dienste haben.
    - Die Überprüfung entsprechender Berechtigungen soll nach wie vor direkt vom Dienst selbst durchführbar sein, ohne dass hierfür zusätzliche, externe Abhängigkeiten entstehen („Offline-Überprüfung“). Folglich müssen auch hierfür standardisierter Verfahren eingesetzt werden, welche umfassend unterstützt werden.

Besonders kritisch ist im Allgemeinen die erstmalige Authentifizierung, da hierdurch erst ein Vertrauensverhältnis zum jeweiligen Gerät hergestellt wird. Dieser Aspekt, im Speziellen unterschiedliche Authentifizierungsfaktoren und –arten werden im folgenden Abschnitt näher erläutert.

3. Authentifizierung

Der Bedarf nach Authentifizierung ergibt sich im Wesentlichen durch die Notwendigkeit, sicher zu stellen, dass ein Kommunikationskanal tatsächlich zwischen den gewünschten Parteien aufgebaut wird und Informationen nur an die Instanzen übermittelt werden, für die sie bestimmt sind. Diverse wohldefinierte, standardisierte kryptografische Verfahren und Protokolle können hierfür herangezogen werden. Zuvor muss jedoch erst eine Bindung zwischen einer Instanz und beispielsweise dem dieser Instanz eindeutig zuordenbarem kryptografischen Material hergestellt werden. Hierfür können die im nachfolgenden Abschnitt diskutierten Authentifizierungsfaktoren verwendet werden.

3.1. Authentifizierungsfaktoren

Üblicherweise werden die unterschiedlichen Faktoren, an Hand derer Authentifizierung vollzogen werden kann – die Basis, auf der eine Authentifizierung stattfindet – in folgende Klassen unterteilt [1]:

- *Knowledge Factor (Wissensfaktor)*: Etwas, das eine Person weiß, wie z.B. ein Passwort oder eine PIN – im Allgemeinen irgendeine Form von geheimem Wissen.
- *Possession Factor (Besitzfaktor* oder *Habenfaktor)*: Etwas, das man besitzt, wie z.B. kryptografische Token, Smartcards, aber auch mechanische Schlüssel.
- *Inherence Factor (Sein-Faktor)*: Unter diesen Begriff fallen biometrische Faktoren, welche wiederum wie folgt unterteilt werden:
    - *Dynamische Biometrie*: Etwas, das man tut, wie z.B. das Schriftbild von Handschriften oder Stimmmuster.
    - *Statische Biometrie*: Etwas, das man ist. Hierbei handelt es sich um Merkmale wie z.B. Fingerabdrücke, Netzhautcharakteristika oder die biometrischen Eigenschaften des Gesichts.

Wissens- und Besitzfaktoren ermöglichen Authentifizierungsmethoden, welche nicht an persönliche Informationen gebunden sind – die Abfrage eines Passworts erfordert keine Verarbeitung von personenbezogener Daten. Dies hat unter anderem Vorteile bezüglich Datenschutz und Privatsphäre und ermöglicht anonyme bzw. pseudonyme Authentifizierung, da z.B. Zugehörigkeit zu einer Gruppe oder Nutzungsberechtigungen überprüft werden können, ohne dass es eine technische Notwendigkeit gibt, festzustellen, um wen (oder welches Gerät) es sich konkret handelt. Des Weiteren ist der Verzicht auf personenbezogene Daten eine Grundvoraussetzung, um auch Geräte in Situationen authentifizieren zu können, in denen es irrelevant ist, wer ein Gerät nutzt, oder in Szenarien, wenn Dienste z.B. nur von Managed Devices aus genutzt werden dürfen – oder eben für die kontinuierliche Authentifizierung im Rahmen von Device-Enrolment. Trotzdem können

biometrische Faktoren jedoch insofern für die erstmalige Authentifizierung im Rahmen von Geräte-Enrolment eingesetzt werden, als dass ein Administrator sich beispielsweise über biometrische Faktoren authentifiziert, um ein neues Gerät zu registrieren. Für kontinuierliche Geräteauthentifizierung nach dem initialem Enrolmentvorgang, muss jedoch auf Wissens-, bzw. Besitzfaktoren zurückgegriffen werden, wenn dies ohne Nutzerinteraktion stattfinden soll.
Werden mehrere Authentifikationsfaktoren im Rahmen eines Authentifikationsprozesses kombiniert, spricht man von *Mehrfaktorauthentifikation* (*Multi-Factor Authentication*, MFA). Im folgenden Abschnitt werden unterschiedliche Authentifikationsmethoden und deren Nutzung der unterschiedlichen Authentifikationsfaktoren diskutiert.

3.2. Authentifizierungsmethoden

Wie bereits erwähnt, sind im Zusammenhang mit Device Enrolment Authentifizierungsmethoden auf Basis von Wissens- und Besitzfaktoren von besonderer Relevanz. Im Rahmen dieses Abschnitts werden zuerst Methoden basierend auf einem Authentifizierungsfaktor, gefolgt von Mehrfaktorauthentifizierung, diskutiert.

3.2.1. Passwortbasierte Authentifizierungsmethoden

Die wohl bekannteste wissensfaktorbasierte Methode ist passwortbasierte Authentifizierung, bei der Benutzer bzw. Benutzerinnen ein (geheim zu haltendes) Passwort bzw. eine PIN eingeben müssen. Allerdings muss auch hier weiter zwischen zwei Arten von passwortbasierten Methoden unterschieden werden [2]:

- Methoden basierend auf wiederverwendbaren (Langzeit-)Passwörtern
- Methoden basierend auf Einwegpasswörtern oder Token

Besonders die Sicherheit von Langzeitpasswörtern ist jedoch auf Grund menschlicher Faktoren in Frage zu stellen: Passwörter werden (wider besseren Wissens) aufgeschrieben und ein und dasselbe Passwort wird oftmals für verschiedene Dienste wiederverwendet. Außerdem neigen Nutzerinnern und Nutzer dazu, leicht zu merkende und damit leichter zu erratende Passwörter zu wählen, wenn ihnen die Möglichkeit der freien Passwortwahl eingeräumt wird [2]. Ohne den Einsatz entsprechender technischer Gegenmaßnahmen, oder bei unsachgemäßer (z.B. unverschlüsselter) Speicherung von Passwörtern, können diese einfach errechnet, bzw. erraten oder gestohlen werden.
Einwegpasswörter bieten demgegenüber einige Vorteile. Wenn beispielsweise für jeden (Authentifikations-)Vorgang ein neues Passwort verwendet werden muss, ist ein erbeutetes, oder erratenes bereits verwendetes Passwort wertlos, da dieses nicht mehr eingesetzt werden kann. Sollten passwortbasierte Verfahren zum Aufbau verschlüsselter Kommunikationskanäle zum Einsatz kommen, kann mit Einwegpasswörtern *Forward Secrecy* erreicht werden: Wird ein Passwort erbeutet, kann damit nachträglich lediglich der Informationsfluss entschlüsselt werden, der mit diesem Passwort verschlüsselt wurde, nicht aber vergangene, oder zukünftige.
Im Allgemeinen kann im Rahmen von *Challenge-Response* Authentifikationsmethoden mittels Einwegpasswörtern sichergestellt werden, dass es sich tatsächlich um eine Neuauthentifizierung handelt, und nicht um eine *Replay-Attacke* d.h. dass von einem Angreifer aufgezeichnete vergangene Authentifikationsinformationen wiederverwendet werden.
Für Benutzerauthentifizierung kommen Einwegtoken üblicherweise im Rahmen von Merhfaktorauthentifikation in Kombination mit einem Besitzfaktor zum Einsatz. Ein Beispiel hierfür ist die österreichische Handy-Signatur, auf deren Prinzipien in Abschnitt 3.2.3 zum Thema Mehrfaktorauthentifizierung näher eingegangen wird. Eine weitverbreitete Authentifizierungsmethode welche auf Besitzfaktoren aufbaut, ist die im folgenden Abschnitt diskutierte zertifikatbasierte Authentifizierung.

3.2.2. Zertifikatsbasierte Authentifizierung

Zertifikatsbasierte Authentifizierung kann wie folgt charakterisiert werden: Eine vertrauenswürdige Zertifizierungsstelle stellt digitale Zertifikate aus, welche mittels asymmetrischer kryptografischer Verfahren von der Zertifizierungsstelle digital signiert werden.
Zertifikate beinhalten unter anderem Informationen über die Identität, auf die sie ausgestellt wurden, Daten der ausstellenden Instanz, eine Gültigkeitsdauer, den öffentlichen Teil eines *Public/Private Key Pair*, sowie Informationen wofür dieser Schlüssel eingesetzt werden darf. Durch den Besitz des zugehörigen privaten Schlüssels (bzw. dem Erstellen einer digitalen Signatur mit diesem Schlüssel) kann der entsprechende Identitätsnachweis erbracht werden. Eine essentielle Eigenschaft von digitalen Zertifikaten ist, dass sie alle Informationen enthalten, welche für deren Überprüfung notwendig sind. Eine Echtheitsprüfung erfolgt über die Verifikation der von der Zertifizierungsstelle erstellen Signatur. Hierfür ist – außer für Widerrufsinformationen, die in diesem Dokument später diskutiert werden – keine Kontaktaufnahme zu Dritten notwendig („Offline-Verifikation“). Voraussetzung dafür ist jedoch, dass die ausstellende Instanz als vertrauenswürdig anerkannt wird. Sieht man von technischen Fragen wie Sicherheit der verwendeten kryptografischen Verfahren und Kompatibilität ab, ergeben sich im Zusammenhang mit zertifikatsbasierten Authentifizierungsverfahren hauptsächlich Fragen bezüglich der Verwaltung von Zertifikaten:

- Wie lange sollen Zertifikate gültig sein?
- Wofür sollen sie berechtigen?
- Welche Instanz wird als vertrauenswürdig angesehen?
- Welche initialen Authentifizierungsmethoden kommen zum Einsatz, um Zertifikate auszustellen?

Umfassende technische Umsetzung von zertifikatsbasierter Authentifizierung ist gegeben und kann vollautomatisiert und ohne Benutzereingaben vonstattengehen. Daher ist dieses Verfahren auch für kontinuierliche (Neu-)Authentifizierung im Zusammenhang mit Device Enrolment geeignet. Der technische Aufbau von Zertifikaten selbst, sowie der Rolle von Zertifizierungsstellen und Echtheitsprüfungen sind im Rahmen des Standards *X.509* als *Public Key Infrastructures* standardisiert [3].
Nachdem zuvor erwähnte Verwaltungsfragen üblicherweise nicht Endbenutzern überlassen werden, sondern Fachpersonal wie Systemadministratorinnen und Systemadministratoren, bestehen in der Praxis keine der durch menschliches Fehlverhalten verursachten Probleme passwortbasierter Authentifizierung.

3.2.3. Mehrfaktorauthentifizierung

Kommt eine Kombination aus mehreren Authentifikationsfaktoren im Rahmen einer Authentifizierungsmethode zu Einsatz, wird dies als *Mehrfaktorauthentifizierung*, bzw. *Multifaktorauthentifizierung* (MFA) oder *mehrstufige Authentifizierung* bezeichnet. Die im E-Government-Bereich eingesetzten eID- bzw. Handy-Signatur-basierten Challenge-Response-Verfahren sind Beispiele dafür: Die Authentifizierung mittels Handy-Signatur erfordert abgesehen vom Wissensfaktor Signaturpasswort auch den Besitzfaktor SIM-Karte, die zum Empfang eines für jeden Authentifizierungsvorgang neu generierten Einweg-Token benötig wird, welcher im Rahmen eines Authentifizierungsvorgangs nach Eingabe von Mobiltelefonnummer und Signaturpasswort ebenfalls eingegeben werden muss [4].
Die hohe Sicherheitsmarge derartiger Verfahren ergibt sich unter anderem durch den Einsatz voneinander unabhängiger Kommunikationskanäle (im Rahmen der Handy-Signatur sind dies eine Internetverbindung und das Mobilfunknetz). Wird hingegen ein einziges Endgerät für die Verarbeitung aller Authentifikationsfaktoren herangezogen, ergäbe sich dieses Endgerät ein einziger Angriffspunkt, was sich Sicherheitsniveau der Methode schwächen kann.

Im Folgenden werden auf Basis der in Abschnitt 2 definierten Anforderungen und hier diskutierten Authentifizierungsmethoden und -faktoren die Eigenschaften eines Enrolment-Konzepts auf Basis flexibler Authentifizierungsverfahren abgeleitet.

4. Möglichkeiten für Device-Enrolment mit flexibler Authentifizierung

Aus den diskutierten Anforderungen wie Interoperabilität und Kompatibilität ergibt sich die Notwendigkeit, auf standardisierte Verfahren zurückzugreifen, welche auch umfassend unterstützt werden. Folglich scheiden Neuentwicklungen, was die Überprüfung von Zugehörigkeit, bzw. Methoden für die kontinuierliche Authentifizierung anschließend an den initialen Enrolmentvorgang angeht, aus. Da insbesondere Geräte authentifiziert werden müssen, kann auch nicht auf Methoden basierend auf Wissensfaktoren oder Biometrie zurückgegriffen werden.
Diese Einschränkungen gelten jedoch nicht für den erstmaligen Authentifizierungsvorgang. Größtmögliche Flexibilität kann hier auch durch den Einsatz von neuartigen Verfahren erreicht werden, da keine Notwendigkeit für Kompatibilität besteht. Allerdings bieten sich X.509-Zertifikate für alle weiteren Authentifizierungsvorgänge an.
Ein Vorteil einer zertifikatsbasierten PKI-Methode z.B. im Gegensatz zu Challenge-Response-Verfahren ist, dass diese kein Zutun vom Gerätebenutzer, bzw. der Gerätenutzerin erfordern. Ein einmal als vertrauenswürdig anerkanntes Gerät kann sich folglich immer wieder vollautomatisiert authentifizieren. Im Gegensatz zu Authentifizierungsprotokollen wie z.B. *Kerberos* ermöglichen PKI-Ansätze Offline-Verifikation. Besonders in (auch betriebsintern) heterogenen Umgebungen, in denen eine Vielzahl unterschiedlicher Dienste genutzt wird ist dies ein Vorteil, da der vorübergehende Ausfall einzelner Komponenten keine Auswirkung auf Authentifizierungsprozesse hat. Hier ist es auch z.B. durch den Einsatz von jeweils einem Zertifikat pro Dienst möglich, im Rahmen des Enrolments für kritischere Dienste, stärkere Authentifizierungsverfahren und kürzere Gültigkeitsdauern vorzuschreiben. Durch den Einsatz separater Zertifikate zur Authentifizierung gegenüber unterschiedlichen Diensten wirkt sich die Kompromittierung einzelner Zertifikate auch nicht auf andere Dienste aus. Des Weiteren können über so genannte *Extensions* Berechtigungen, bzw. Authentifizierungsanforderungen für die Erneuerung von Zertifikaten direkt in Zertifikate selbst kodiert werden.
Theoretisch könnte vorausgesetzt werden, dass ein Zertifikat, welches zum Nutzen eines bestimmten Dienstes berechtigt, auch eine entsprechende Extension aufweist. Praktisch setzt eine automatisierte Überprüfung derartig kodierter Berechtigungen jedoch eine Unterstützung vom betroffenen Service voraus. Daher erscheint eine Durchsetzung von Berechtigungen auf diese Weise zumindest für bestehende Dienste nicht realistisch. Tatsächlich lassen sich solche auf mehreren Ebenen feingranulare Zugriffberechtigungen jedoch ebenfalls über dedizierte Zertifikatsketten pro Dienst umsetzen.
Mit *Transport Layer Security* (TLS) [5] sind alle technischen Voraussetzungen für die Realisierung derartiger Enrolmentverfahren mit zertifikatsbasierten Authentifizierungsmechanismen gegeben. Beispiele hierfür sind das *Simple Certificate Enrolment Protocol* (SCEP) [6], *Certificate Management over CMS* (CMC) [7], und das *Internet X.509 Public Key Infrastructure Certificate Management Protocol* (CMP) . Die grundlegenden Konzepte von Protokollen wie SCEP sind jedoch unabhängig vom Protokoll für Enrolmentprozesse und kontinuierliche Authentifizierung einsetzbar.
Auch wenn die SCEP-Spezifikation kontinuierlich aktualisiert wird und breite Unterstützung seitens der Industrie erfährt [6], basiert diese teilweise auf statischen Annahmen und Vorschriften bezüglich einzusetzender Technologien und Abhängigkeiten zum *Domain Name System* (DNS), was in dynamischen Umgebungen zu Problemen führen kann. Aus diesem Grund wurden im Rahmen dieses Projekts einige wesentliche Konzepte von SCEP für die Umsetzung eines Enrolment-Frameworks mit flexibler Authentifizierung herangezogen, generell jedoch auf Protokollkonformität verzichtet. Gleichzeitig wurde auf Flexibilität im Bereich kryptografischer Primitive verzichtet. Stattdessen werden lediglich aktuelle Algorithmen und Schlüssellängen unterstützt. Da das hier konzipierte Enrolment-Framework jedoch nur für Ausstellung und Widerrufung von Zertifikaten eingesetzt wird, muss auf Kompatibilität zu jenen Diensten (wie z.B. VPN, Netzwerkdateisysteme, …) geachtet werden, welche die tatsächlichen Zertifikatsprüfungen durchführen. Dies ergibt sich direkt aus angestrebten universellen Einsetzbarkeit und dem Fokus auf Flexibilität.
Als Basis für die Auswahl an unterstützen kryptografischen Methoden wurden die 2016 veröffentlichten Sicherheitsempfehlungen für Behörden [8] herangezogen, welche einen Algorithmenkatalog definieren, bestehend aus Cipher-Suites, die einerseits ausreichende Sicherheitsniveaus bieten, gleichzeitig aber auch hohen Kompatibilitäts- und Interoperabilitätsansprüchen genügen.

4.1. Bereitstellung von Widerrufsinformationen

Nachdem Informationen über den Widerruf von Zertifikaten genau wie Zertifikate selbst von vertrauenswürdigen Instanzen signiert werden müssen, um einer Echtheitsprüfung standzuhalten, ergibt sich die Frage nach der Verteilung dieser Informationen. Zu diesem Zweck wurden *Certificate Revocation Lists* (CRLs) [3] standardisiert. Dabei handelt es sich um ein Containerformat, welches eine digital signierte Liste von revozierten Zertifikaten enthält. Der Ort, von dem diese Liste abgerufen werden kann (welcher als *CRL Distribution Point* bezeichnet wird), wird im Zuge der Zertifikatsausstellung in Zertifikate kodiert. Die Gültigkeitsdauer dieser Listen kann vom Ersteller frei gewählt werden. Im Rahmen der Zertifikatsprüfung kann der Widerrufsstatus des zu prüfenden Zertifikats durch den Abruf einer aktuellen CRL überprüft werden. Durch die Notwendigkeit, einen CRL Distribution Point im Zuge der Zertifikatsverifikation zu kontaktieren, ist jedoch keine Offline-Verifikation mehr möglich. Über längere Gültigkeitsdauern kann diese Abhängigkeit zu Lasten der Aktualität von Widerrufsinformationen jedoch zumindest reduziert werden.
Ein weiteres Konzept, Widerrufsinformationen bereitzustellen, wurde mit dem *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol* (OCSP) [9] standardisiert: Anstatt vollständige Listen über den Widerrufsstatus aller von einer Zertifizierungsstelle ausgestellten Zertifikate abzurufen, kann eine Anfrage zu einem konkreten Zertifikat an so genannte *OCSP Responder* gesendet werden. Folglich können auch mittels OCSP keine Offline-Verifikationen durchgeführt werden. Dieses Problem wurde schließlich mit der *Certificate Status Request*-Erweiterung [10] (besser bekannt als *OCSP Stapling*) gelöst. Im Wesentlichen wird dabei im Rahmen zertifikatsbasierter Authentifizierung zusätzlich zum Zertifikat eine zuvor von einem OCSP Responder abgerufene Statusinformation übertragen. Folglich kann eine vollständige Zertifikatsprüfung inklusive Widerrufsinformationen allein auf Basis der von der zu authentifizierenden Partei zur Verfügung gestellten Informationen stattfinden. Mangels breiter Unterstützung ist jedoch ein universeller Einsatz dieses Verfahrens nicht möglich. Da ein flexibel einsetzbares Enrolment-Framework jedoch größtmögliche Kompatibilität bieten muss, ist OCSP Stapling aktuell kein gangbarer Weg, um Widerrufsinformationen bereitzustellen. Hierfür sind CRLs und OCSP eher geeignet. Das Problem mangelnder Offline-Verifikationsmöglichkeit kann jedoch zumindest innerhalb von Netzwerken, welche von einer einzigen Instanz verwaltet werden, umgangen werden: Werden dedizierte Zertifikatsketten für jeden Dienst verwendet, kann neben jedem Dienst (am selben Server) ein für diesen Dienst zuständiger OCSP Responder, bzw. ein CRL Distribution Point betrieben werden.
Nachfolgend werden nicht-technische Aspekte diskutiert, welche für die Konzipierung eines Enrolmentverfahrens basierend auf flexibler Authentifizierung bedacht werden müssen

4.2. Nicht-technische Aspekte

Im Gegensatz zu bestehenden Device-Enrolment-Lösungen im Enterprise-Bereich, welche vergleichsweise rigide Abläufe für die Authentifizierung vorschreiben, ist das hier vorgestellte Konzept auf größtmögliche Flexibilität ausgelegt. Allerdings ist auf Grund aktueller Nutzungsgewohnheiten (mehrere unterschiedliche Geräte pro Benutzer) ein gewisses Mindestmaß und Flexibilität ohnehin erforderlich, um auf das auch im Corporate-Bereich mittlerweile übliche heterogene Geräteumfeld reagieren zu können. Wird ein Gerät beispielsweise vom Administrator für Angestellte vorkonfiguriert, sind keine besonderen Authentifizierungsmaßnahmen notwendig, da es sich hierbei um ein implizit vertrauenswürdiges Gerät handelt. Dieser Vorgang ist jedoch ebenfalls mittels zertifikatsbasierten Methoden formalisierbar, wodurch sich die Zugehörigkeit eines Geräts in weiterer Folge automatisiert überprüfen lässt.
Zugriff auf firmeninterne Services und Dienste wie z.B.: E-Mail werden typischerweise über eine passwortbasierte Authentifizierung oder auch nur eine Identifikation über Benutzernamen realisiert. Oftmals kommt auch eine Kombination unterschiedlicher Verfahren zum Einsatz, sodass beispielsweise Zugriffe auf Netzwerkdateisysteme über Zugehörigkeiten zu Windows-Domänen realisiert werden, VPN-Zugänge hingegen über X.509-Zertifikate.
Tatsächlich werden X.509-PKI-Methoden jedoch bereits seit längerem umfassend unterstützt. Folglich ist es nach erfolgreicher initialer Authentifizierung durchaus realistisch, Angestellten von unterschiedliche Geräteklassen aus über zertifikatsbasierte Authentifizierungsmechanismen Zugriff auf betriebsinterne Dienste zu erlauben.

Allerdings müssen in diesem Zusammenhang, je nach Geräteklasse und -nutzung, klare Regeln definiert werden, angefangen bei der erstmaligen Authentifizierung eines Geräts, bzw. dessen Enrolment. So ergibt es beispielsweise wenig Sinn, dass ein Administrator oder eine Administratorin im Rahmen der Vorkonfiguration eines Geräts einen mehrstufigen Authentifizierungsprozess durchlaufen muss, um dieses Gerät zu authentifizieren. In solchen Fällen reicht es aus, das durch den Konfigurationsprozess implizit vertrauenswürdige Gerät auch explizit im Firmennetzwerk als solches zu registrieren.
Im Rahmen von Bring-your-own-Device-Lösungen (BYOD-Lösungen) sind hingegen üblicherweise striktere Sicherheitsmaßnahmen zu setzen, um ein Vertrauensverhältnis zu einem Gerät zu etablieren. Hierbei kann für mehrstufige Authentifizierungsverfahren auf die Eigenschaften aktueller Endgeräte, wie z.B. Kamera, Bluetooth, … zurückgegriffen werden, um diesen Prozess trotzdem möglichst komfortabel zu gestalten. Gleichzeitig kann durch die von modernen Mobilbetriebssystemen umgesetzten Sandboxing-Mechanismen von vornherein ein verhältnismäßig hoher Grad an Datensicherheit umgesetzt werden, da von außen kein direkter Zugriff auf Daten einer Applikation möglich ist. Im Gegensatz zu stationären Geräten sind hier Geräteverlust und Gerätediebstahl im Rahmen einer Risikoabschätzung zu bedenken.
Nachfolgend werden die im Rahmen dieses Projekts entwickelte Proof-of-Concept Implementierung und deren Einsatzmöglichkeiten diskutiert.

5. Demonstrator

Auf Basis der eingangs abgeleiteten Anforderungen und unter Berücksichtigung der technischen Möglichkeiten für eine Umsetzung, wurde die nachfolgend beschriebene Architektur konzipiert.

5.1. Architektur

Der im Rahmen dieses Projekts entwickelte Demonstrator eines Enrolmentframeworks basiert auf folgenden Komponenten:

- Eine einfach zu konfigurierende Zertifizierungsstelle, welche nach erfolgtem Enrolment Zertifikate ausstellen, verlängern und im Bedarfsfall widerrufen kann.
- Ein Authentifizierungsframework, welches Schnittstellen für die Implementierung von Authentifizierungsmethoden für den initialen Enrolmentvorgang zur Verfügung stellt, bestehend aus folgenden Untermodulen:
    - Authentifizierungskanäle auf Seiten der Zertifizierungsstelle, welche beliebige Authentifizierungsmethoden umsetzen können.
    - Plattformunabhängige Clients, welche die von Authentifizierungskanälen geforderten Verfahren durchführen
- CRL Distribution Points

Die Integration in bestehende Dienste ist durch das Verteilen von Zertifikaten möglich. Dabei kann auch für die zu nutzenden Dienste selbst ein Enrolment durchgeführt werden, um auch deren Zertifikate von der zentralen Zertifizierungsstelle verwalten zu lassen. Somit lässt sich eine gänzlich einheitliche Verwaltung von Zugriffsberechtigungen und Vertrauensverhältnissen sowohl client- als auch serverseitig umsetzen. Dies ist insbesondere für das Bereitstellen von Widerrufsinformationen ein kritischer Aspekt, da nicht nur Services über kompromittierte Geräte Bescheid wissen müssen, sondern auch umgekehrt. Daher wurde das Verlängern und Widerrufen von Berechtigungen bzw. Zugehörigkeiten ebenfalls zertifikatsbasiert umgesetzt. Spezielle Authentifizierungskanäle, welche selbst zertifikatsbasierte Authentifizierung verlangen, werden wie folgt umgesetzt:
Zertifikate für bestimmte Berechtigungen, bzw. Zertifikate entsprechend bestimmten Zugehörigkeiten können erneuert, bzw. widerrufen werden, indem eine zertifikatsbasierte Authentifizierung über einen dafür vorgesehenen Authentifizierungskanal stattfindet.
In beiden Fällen wird somit wird kein Wissensfaktor benötigt, dessen Verwaltung potentiell problematisch ist.

Die Integration der vorgestellten Lösung in beliebige Dienste findet über die Verteilung der entsprechenden Zertifikate statt. Dabei werden für jeden Dienst dedizierte Zertifikatsketten verwendet.
Widerrufsinformationen werden über CRLs zur Verfügung gestellt, welche von der Zertifizierungsstelle in regelmäßigen Abständen an CRL Distribution Points verteilt werden. Diese werden im Idealfall am selben Ort wie die betreffenden Dienste betrieben, um weiterhin Offline-Verifikationen zu ermöglichen. Um Denial-of-Service-Angriffen vorzubeugen, ist für das Verteilen von Widerrufsinformationen ebenfalls eine zertifikatsbasierte Authentifizierung notwendig. Ohne diese Vorsichtsmaßnahme wäre es Unbefugten beispielsweise möglich, bestehende CRLs durch leere Dateien zu überschreiben. Dabei handelt es sich konzeptionell lediglich um einen Webservice, welcher TLS-basierte Client-Authentifizierung voraussetzt um eine Datei hochzuladen, und diese anschließend ohne Authentifizierung bereitstellt. Daher wurde diese Komponente nicht als Teil des nachfolgend beschriebenen Demonstrators umgesetzt.

5.2. Umsetzung

Um auch praktisch eine hohe Kompatibilität zu bestehenden Installationen zu gewährleisten, wurde der im Rahmen dieses Projekts entwickelte Demonstrator plattformunabhängig umgesetzt. Zu Demonstrationszwecken wurden die folgenden Authentifizierungskanäle inklusive zugehöriger Clients umgesetzt:

- *Lokal*: Hierbei handelt es sich um einen Kanal, welcher ausschließlich lokal eingehende Verbindungen akzeptiert. Eine Authentifizierung im eigentlichen Sinn wird nicht durchgeführt. Durch die Einschränkung auf lokale Verbindungen eignet sich dieser Kanal beispielsweise für das erstmalige Ausstellen von Zertifikaten im Rahmen der Vorkonfiguration von Geräten durch den Systemadministrator oder die Systemadministratorin, da davon auszugehen ist, dass Mitarbeiterinnen und Mitarbeiter keinen direkten Zugriff auf die Zertifizierungsstelle haben.
- *TLS:* Der TLS-Kanal setzt ein gültiges Zertifikat voraus und ist für Zertifikatserneuerung nach erfolgtem Enrolment sowie Zertifikatswiderruf gedacht.
- *QR*: Hierbei handelt es sich um eine ortsgebundene Challenge-Response-basierte Authentifizierungsmethode. Im Rahmen der Authentifizierung wird ein zufälliger 64-bit Token mit 60 Sekunden Gültigkeit generiert, welcher als QR-Code angezeigt wird. Der Wert dieses Token ist über dieselbe Verbindung, über die der Authentifizierungsprozess gestartet wurde, zu übermitteln.
  Gegenüber dem lokalen Kanal entfällt das Kopieren ausgestellter Zertifikate z.B. im Rahmen einer Vorkonfiguration eines Geräts. Das Abtippen des Tokens entfällt außerdem, wenn das zu authentifizierende Gerät über eine Kamera verfügt.
- *QR+TLS:* Hierbei handelt es sich um einen Kanal, welcher ein QR-Code-basiertes Challenge-Response-Verfahren umsetzt. Gedacht ist diese Authentifizierungsmethode für die Zertifikatserneuerung. Es handelt sich hierbei um eine mehrstufige Authentifizierung:
  - Es wird ein bestehendes, gültiges Zertifikat benötigt.
  - Der Wert eines zufälligen 64-bit Token mit 60 Sekunden Gültigkeit (welcher in Form eines QR-Codes angezeigt wird), muss ebenfalls übermittelt werden.

  Als möglicher Anwendungsfall hierfür sind Terminals denkbar, welche den Token (als QR-Code) im Rahmen eines Authentifizierungsvorgangs anzeigen. Damit lassen sich komfortable Möglichkeiten einer ortsgebundenen Zertifikatserneuerung für Smartphones realisieren.

Parameter wie z.B. Gültigkeitsdauer von Zertifikaten sind konfigurierbar. Detaillierte Informationen zur Nutzung des Demonstrators sind Teil der bereitgestellten Distribution[2]. Durch die Bereitstellung des Quellcodes und auf Grund der modularen Architektur des Demonstrators kann dieser um beliebige Kanäle und Authentifizierungsmechanismen, wie z.B. Handy-Signatur, erweitert werden. Es besteht auch die Möglichkeit, Kanäle zu integrieren, welche es Administratorinnen und Administratoren erlauben, Berechtigungen anderer Personen oder fremder Geräte zu widerrufen.

[2] http://demo.a-sit.at/wp-content/uploads/2017/10/authdemo.zip

Des Weiteren besteht die Möglichkeit, den zur Verfügung gestellten Demonstrator derart zu erweitern, dass beliebige zusätzliche Informationen in Zertifikate kodiert wird, welche beispielsweise für die Umsetzung feingranularer Zugriffsrechte im Rahmen neu entwickelter Services herangezogen werden können. Da dies jedoch im Speziellen aus Kompatibilitätsgründen für bestehende Dienste nicht relevant ist, wurde auf eine Umsetzung im Rahmen dieses Projekts verzichtet.

Referenzen

[1] W. Stallings, Cryptography and Network Security: Principles and Practice, Upper Saddle River, NJ, USA: Pearson, 2013.

[2] J. M. Kizza, „Authentication," in *Guide to Computer Network Security*, London, GB, Springer, 2015, pp. 205-223.

[3] R. Housley, W. Ford, W. Polk und D. Solo, „Internet X.509 Public Key Infrastructure Certificate and CRL Profile," Internet Engineering Task Force (IETF), RFC 2459, 1991.

[4] C. Orthacker, M. Centner und C. Kittl, „Qualified Mobile Server Signature," in *Security and Privacy – Silver Linings in the Cloud*, Berlin, Deutschland, Springer, 2010, pp. 103-111.

[5] T. Dierks und E. Rescorla, „The Transport Layer Security (TLS) Protocol Version 1.2," Internet Engineering Task Force (IETF), RFC 5246, 2008.

[6] P. Gutmann, „Simple Certificate Enrolment Protocol," Internet Engineering Task Force (IETF), 2017.

[7] J. Schaad und M. Myers, „Certificate Management over CMS (CMC)," Internet Engineering Task Force (IETF), RFC 5272, 2008.

[8] T. Zefferer, J. Feichtner und B. Prünster, „Sicherheitsempfehlungen für Behörden -- Teil 2: SSL/TLS," A-SIT, 2016.

[9] S. Santesson, M. Myers, R. Ankney, A. Malpani, S. Galperin und C. Adams, „X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP," Internet Engineering Task Force (IETF), RFC 6960, 2013.

[10] D. E. 3rd, „Transport Layer Security (TLS) Extensions: Extension Definitions," Internet Engineering Task Force (IETF), RFC 6066, 2011.

[11] M. Autor, „Mustertitel," p. 12, 2017.

[12] C. Adams, S. Farrell, T. Kause und T. Mononen, „Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)," Internet Engineering Task Force (IETF), RFC 4210, 2005.