



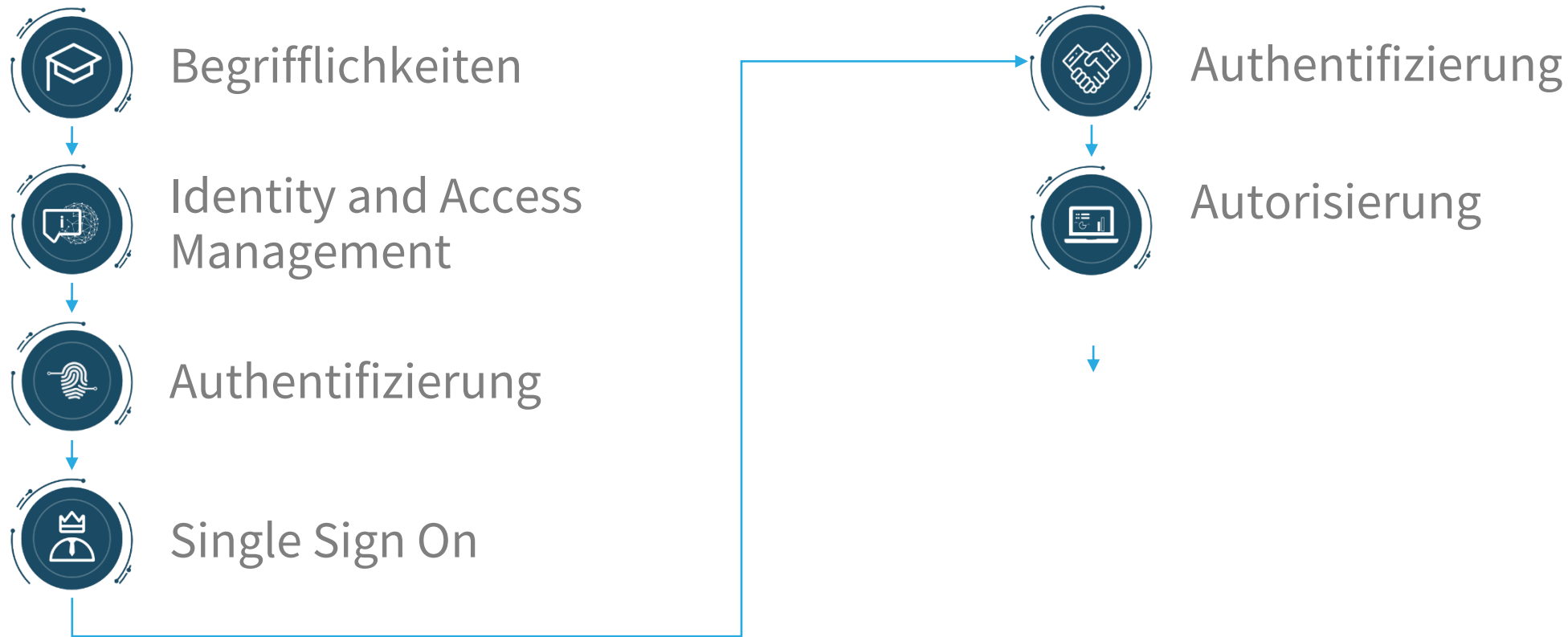
Operation System Security

07 – Authentisierung und Autorisierung



SECURNITE

OSSEC 07 – Authentisierung und Autorisierung





Begrifflichkeiten

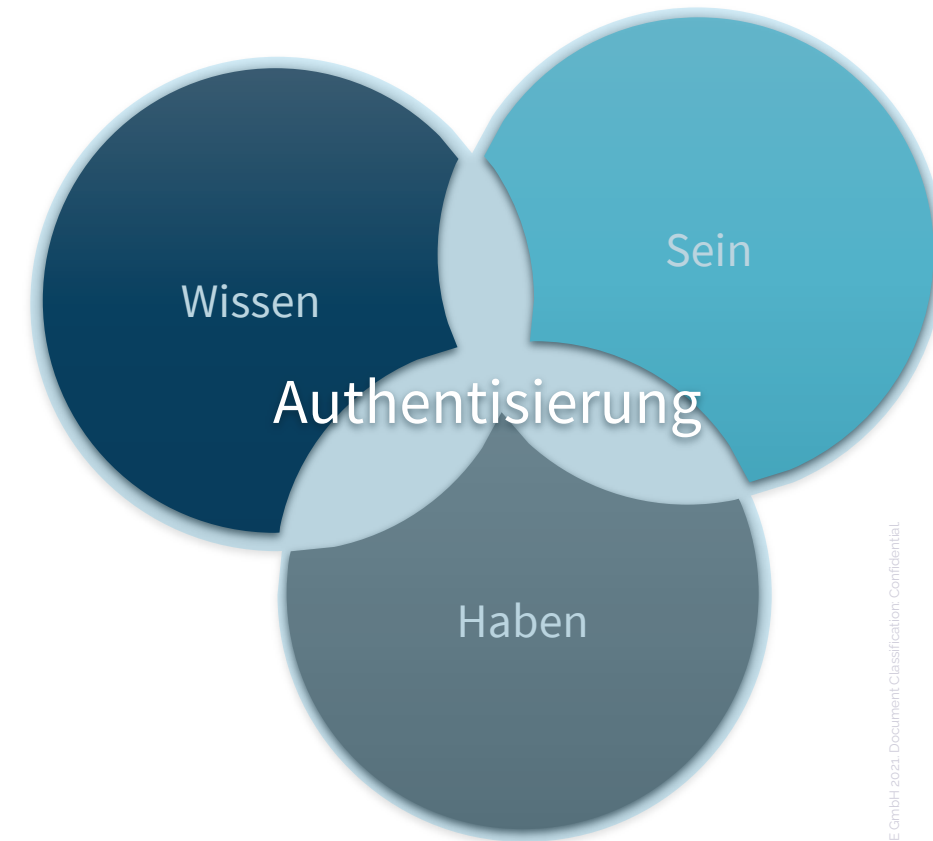
Authentisierung



- **Nachweis** einer Person, dass sie die Person **ist**, die sie **vorgibt** zu **sein**
- Auch anwendbar für Objekte, Tiere, Dienste usw.

Authentisierung

- Erfolgt durch Vorlegen eines **Nachweises**, der die Identität **bestätigen** sollen
 - geheime **Informationen** (z.B. Passwort)
 - **Identifizierungsgegenstand** (z.B. Personalausweis)
 - **Identifizierungsobjekt** (z.B. biometrische Merkmale)
- „**Starker Authentisierung**“ = Kombination mehrerer dieser Verfahren



Authentifizierung



- **Prüfung** (Verifikation) der behaupteten Authentisierung
- Prüfer **überprüft** die Angaben auf **Echtheit**
- Findet **nach** einer Authentisierung statt



Autorisierung



- **Einräumung** von speziellen **Rechten**
- **Prüfung** der Rechte und **Konsequenz**
- Erfolgreiche **Identifikation** heisst **nicht** automatisch **erlaubte Nutzung** oder **Zugriff** auf bereitgestellte Dienste, Leistungen oder Ressourcen

Nachvollziehbarkeit & Claims



Nachvollziehbarkeit

- Definiert das **Mass**, **inwieweit** und **zweifelsfrei** Handlungen von Benutzern oder Systemen **aufgezeichnet** (Logging) werden müssen

Claim

- **Eigenschaft** einer Identität, die **für** den **Zugriff entscheidend** ist (z.B. Alter oder Zugehörigkeit zu einer Berufsgruppe)

Identity Management



- **Umfasst** (nach ISO/IEC JTC 1/SC 27/WG 5 „A framework for IdM“)
 - Die sichere **Verwaltung** von **Identitäten**
 - Den **Identifikationsprozess** einer Einheit (inkl. optionaler Authentisierung)
 - Die **Information**, die mit der Identifikation einer **Einheit** innerhalb eines **Kontexts** verbunden ist
- **Einheit** = alles, was **eindeutig** als solche erkannt werden kann (Person, Tier, Gerät, Objekt, Gruppe, Organisation, etc.)
- **Einheiten** können **mehrere Identitäten** haben, die in verschiedenen **Kontexten** verwendet werden können

Identity Management



- regelt die **Erstellung**, Speicherung, Synchronisation und Löschung von Identitäten
- **organisatorische Anforderungen** sind weit schwieriger zu erfüllen, als die **technischen**
- **Tools** und **Technologien**:
 - LDAP (Speicherung und Zugriff auf Identitäten)
 - Metadirectory (Identitäten in verschiedenen Verzeichnissen synchronisieren und bereitstellen)

Access Management



- Regelt den **Zugriff** eines Subjekts auf ein Objekt
- Beinhaltet **Authentisierung** und **Autorisierung**
- **Zugriff** auf Ressourcen muss **gesteuert** werden
- **Protokolle**
 - Kerberos
 - HTTP Basic Auth
 - SAML



Identity and Access Management

Identity and Access Management



- Fasst **Identity Management** und **Access Management** zusammen
- Wichtiges Instrument, um **Datenzugriff** und **Prozesse** dynamischen Anforderungen effektiv **anzupassen**

Gruppenübung (15 Minuten)



- Sie wollen ein **IAM** in Ihrem **Unternehmen** einführen. Wie machen Sie die Idee Ihrem **Management** schmackhaft?
- Präsentieren Sie Ihre **Ideen** (max. 5 Minuten). Gehen Sie dabei besonders auf die **Treiber** für IAM ein.

Identity and Access Management



Kernprozesse

Steuerung	Governance	Risiko Management	Compliance
Verwaltung	Identitäten	Zugriffsregeln	Logs
	Claims	Credentials	
Runtime	Access Control	Audit Trail	

Identity and Access Management



- **Governance**
 - Definition einer Policy
 - Festlegung von Organisation, Domänen, Akteuren und Prozessen
 - Treffen von Entscheidungen in Bezug auf die Strategie
- **Risikomanagement**
 - Analysieren und Behandeln der Risiken im Zusammenhang mit IAM
- **Compliance**
 - Sicherstellen der Einhaltung der regulatorischen Rahmenbedingungen
 - Prüfen der Einhaltung (Auditing)

Identity and Access Management

- **Verwaltung der Identitäten:** Registrieren, Mutieren, Löschen
- **Verwaltung der Zugriffsregeln:** Zuweisen, Mutieren, Löschen
- **Verwaltung von Claims:** Zuweisen, Mutieren, Löschen
- **Verwaltung von Credentials:** Erstellen, Zuweisen, Revozieren
- **Auswertung der Logs:** Analyse der Logfiles auf Anomalien hin

Identity and Access Management



- **Access Control**
 - **Runtime** Element
 - Verantwortlich für **Authentisierung** und **Autorisierung**
- **Audit Trail**
 - Erstellen einer **Logdatei**, welche die **Nachvollziehbarkeit** aller Handlungen sicherstellt

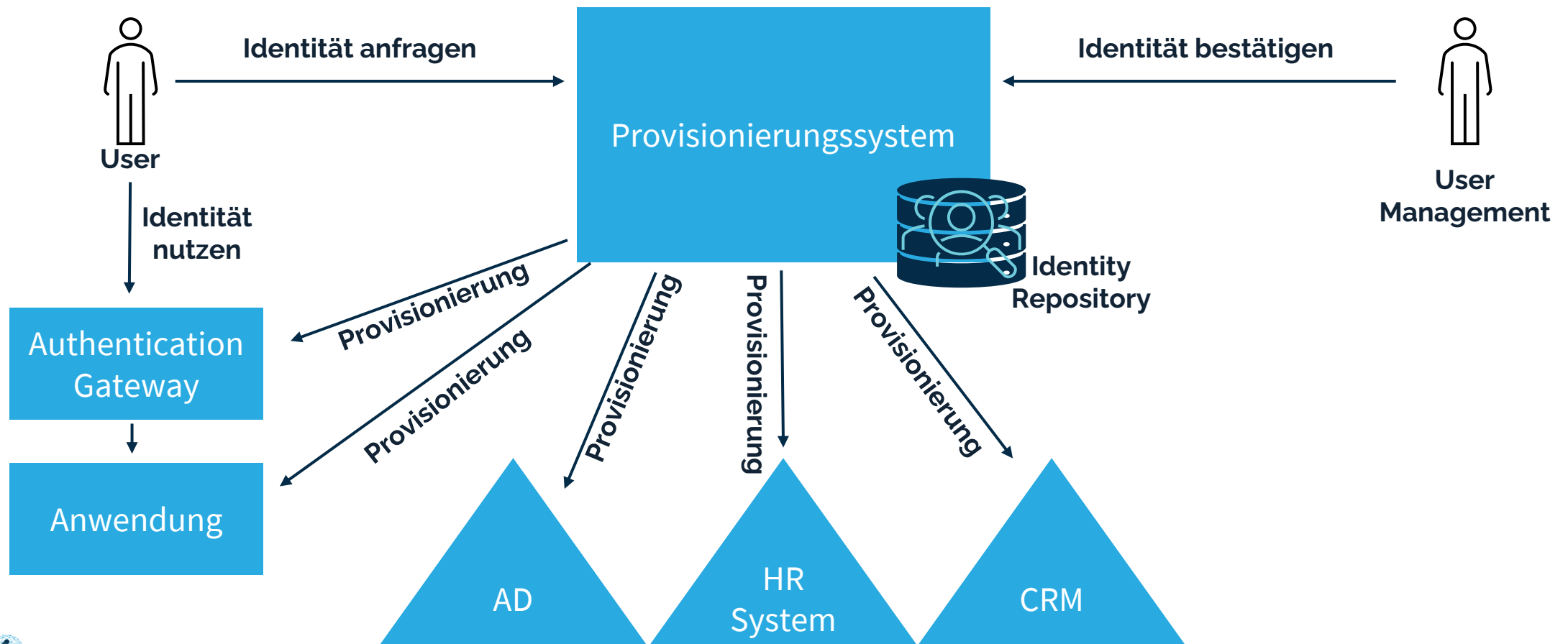
Verwaltung von Identitäten



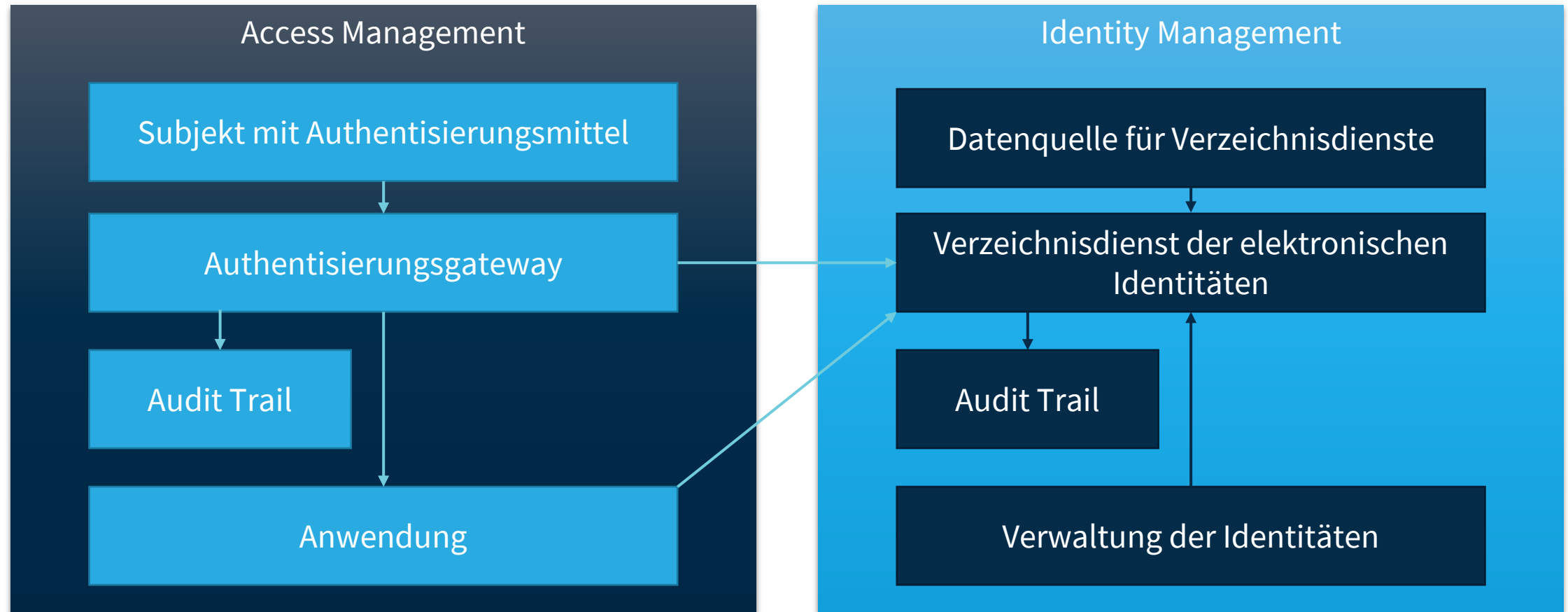
- Primär ein Problem der **richtigen Prozesse** (und deren **Einhaltung**) und weniger eine technische Herausforderung
- Zu klärende **Punkte**:
 - **Erteilen** von Zugriffsrechten („wer - wem - welche“)
 - Umgang mit „**Externen**“ (Beratern, Lieferanten, Kunden, ...)
 - Umgang mit **Personalwechsel** (Versetzung, Pensionierung, Kündigung (geordnet oder im Streit), ...)
 - **Abgabe** von „Schlüsseln“ aller Art (auch elektronischen!)
 - **Sperren** von Konten, Entziehen von Rechten, ...
 - **Vergessene** Zugangscodes (Passwörter, Smartcards, etc.)

Verwaltung von Identitäten

Provisionierung



IAM-Komponenten



IAM-Komponenten



- **Datenquellen:** enthalten Daten zu Identitäten, z.B. ein Verzeichnis mit Telefonnummern oder Benutzernamen
- **Verzeichnisdienst** mit digitalen Identitäten
 - enthält die digitalen Identitäten
 - beantwortet Anfragen nach Identitäten und Attributen
- **Verwaltungsinterface** zur Pflege der Identitäten
- **Audit Trail:** Aufzeichnung sämtlicher Aktionen im Zusammenhang mit digitalen Identitäten

IAM-Komponenten



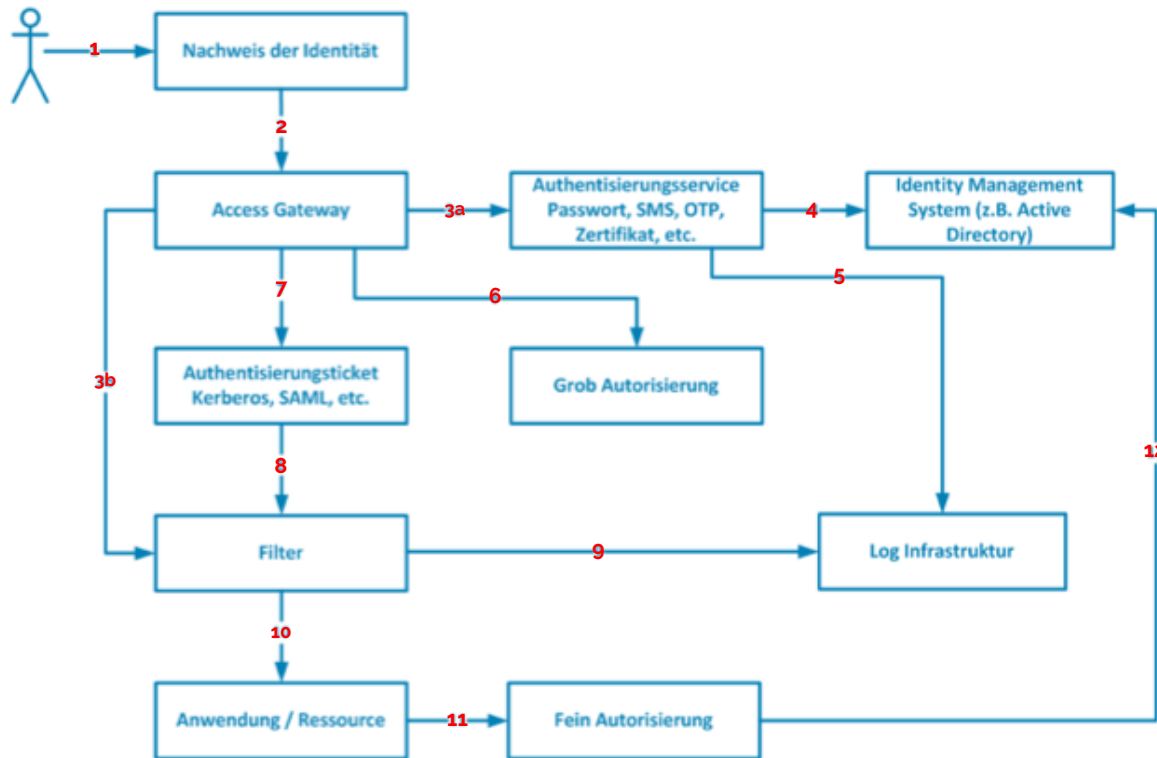
- **Subjekt**, das sich mit einem Authentisierungsmittel authentisiert (z.B. eine Person, die sich mit Passwort ausweist)
- **Authentisierungsgateway**
 - nimmt die Authentisierung entgegen
 - prüft, ob diese korrekt ist
 - stellt ein Authentisierungsticket (z.B. Kerberos) bereit
 - übergibt dieses der angefragten Applikation
- **Anwendung** gewährt **Zugang** auf der Basis dieses Tickets

IAM-Komponenten

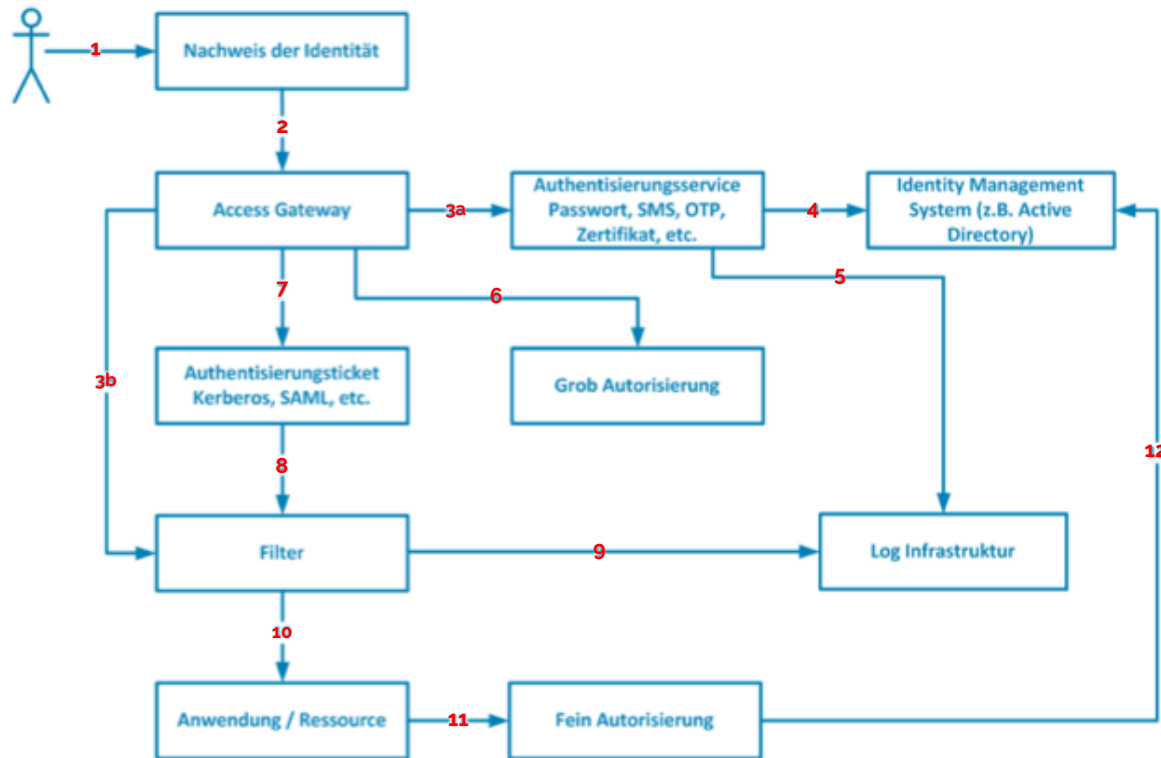


- Alle Aktionen werden **aufgezeichnet** (Audit Trail)
- Teilweise ist die Aufgabe der Prüfung an einen **zusätzlichen Server** delegiert
 - AAA-Server / Triple-A Server (Authentisierung, Autorisierung und Accounting)
 - kann verschiedene **Authentisierungsmittel** prüfen
 - Kann **Autorisierung** und **Abrechnung** machen

Ablauf eines Zugriffs



Ablauf eines Zugriffs

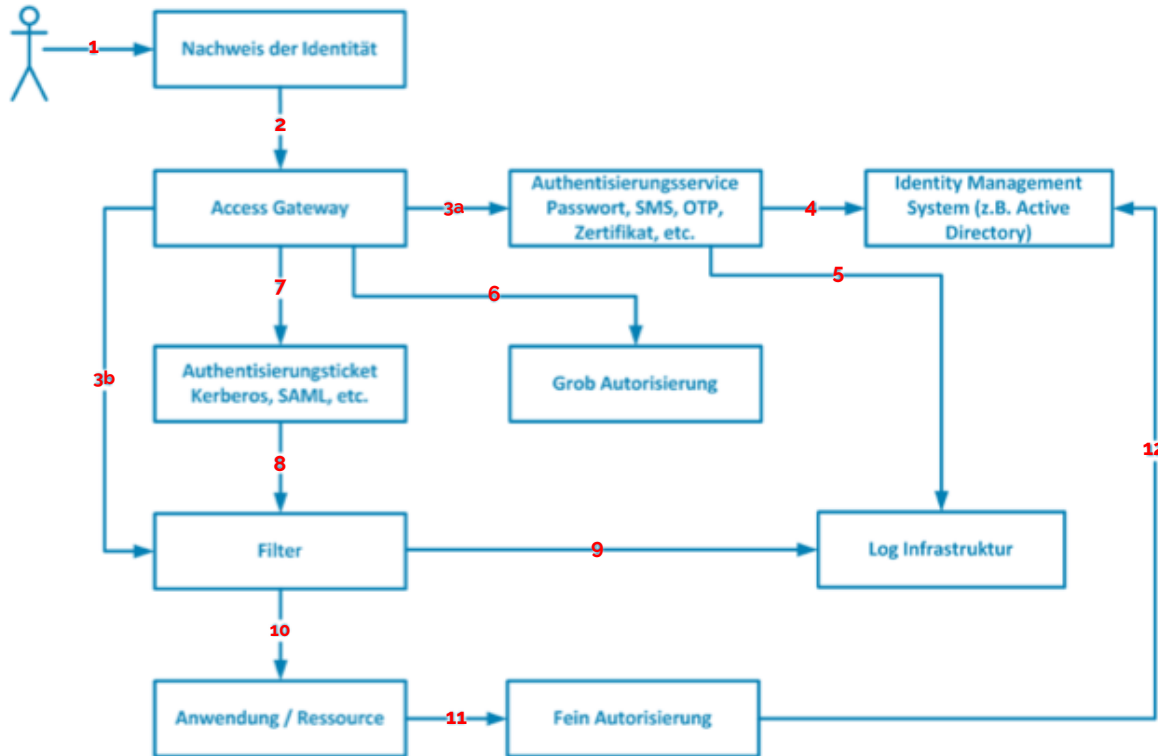


3. b. bei einem **anonymen** Zugriff wird 4-8 übersprungen

4. Der **Authentisierungsdienst** macht eine Abfrage zur **Identität** beim **Identity Management System**

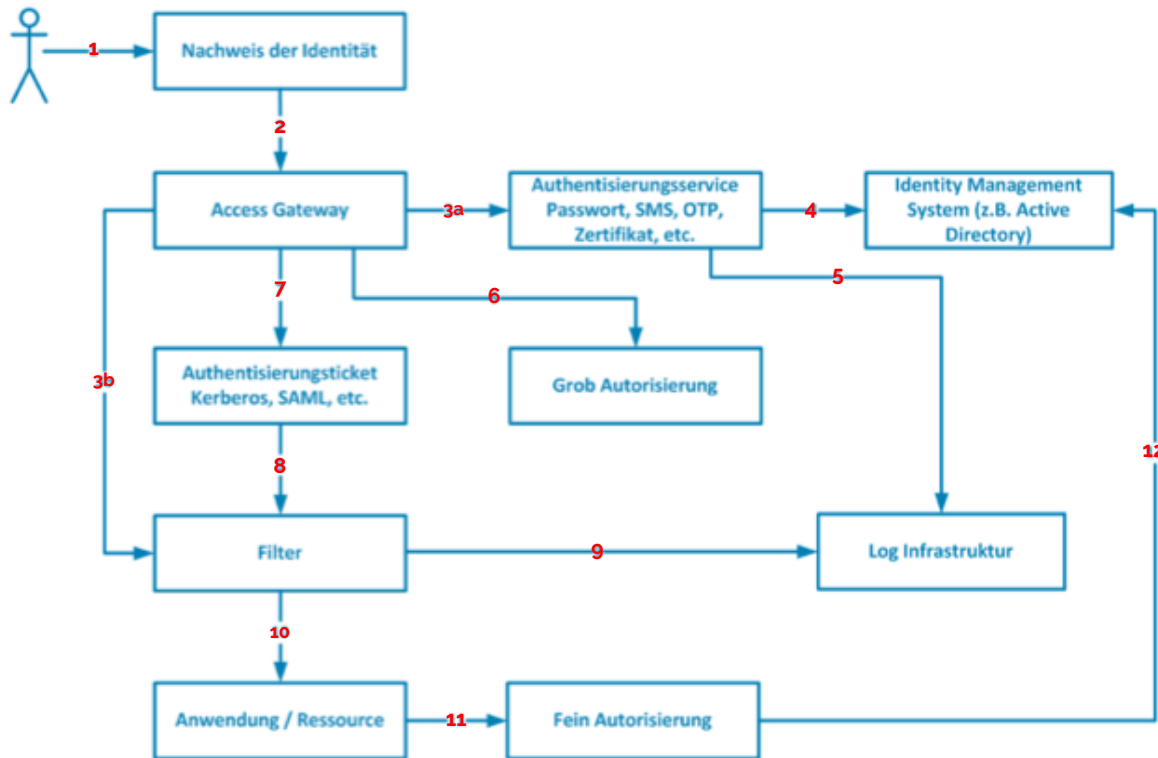
5. **Alle Aktionen** werden **zentral geloggt** (von **allen** beteiligten Systemen)

Ablauf eines Zugriffs



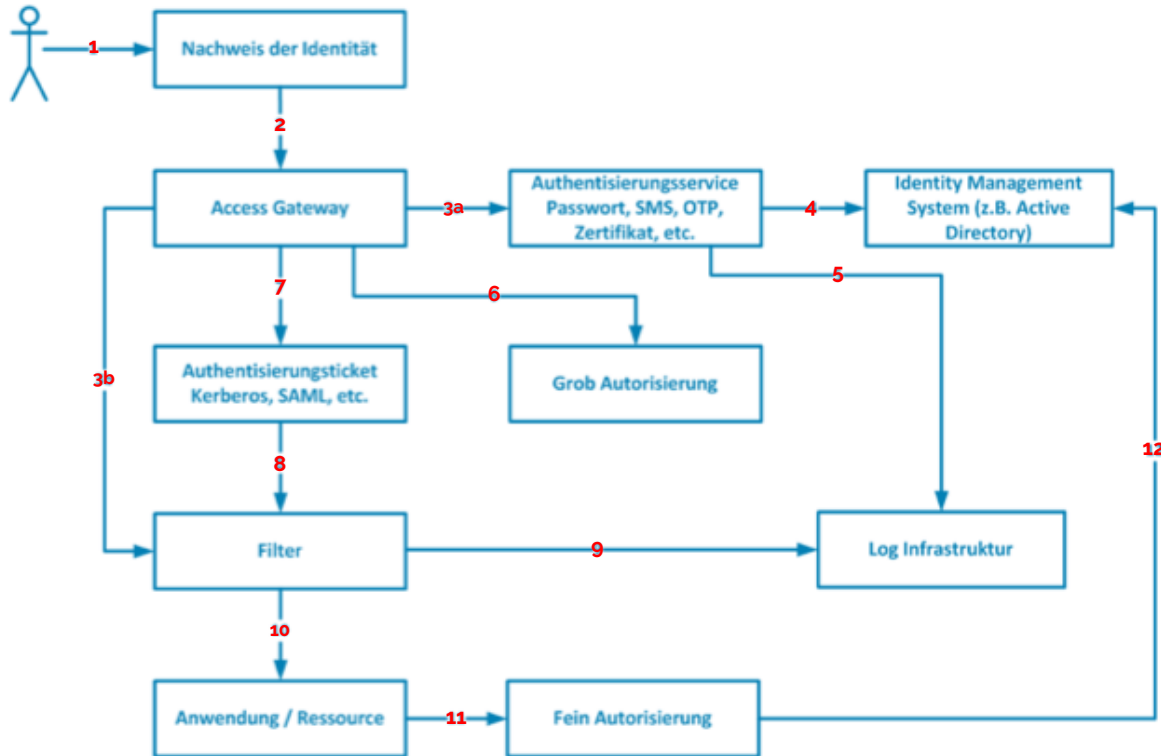
6. Nun erfolgt eine **Grob-Autorisierung**, d.h. hat dieser Benutzer (resp. seine Rolle) **Zugriff** auf eine **bestimmte Anwendung** oder **Ressource**?
7. Falls alle **Prüfungen erfolgreich** waren, erhält der Benutzer sein **Ticket** (häufig Kerberos oder SAML). Mit dem Ticket kann er sich bei der **Ressource** als **authentisiert** ausweisen.

Ablauf eines Zugriffs



8. Nun erfolgt der Zugriff auf den **Filter-Dienst**. **Anonyme** und **authentisierte** Zugriffe **vereinigen** sich wieder
9. Für die **Angriffserkennung** und für die **Fehlersuche** ist es von grosser Wichtigkeit, die Filteraktionen zu **loggen**
10. Nun erfolgt der **Zugriff** auf die **Ressource / Anwendung**

Ablauf eines Zugriffs



11. Die **Anwendung** führt eine **Feinautorisierung** durch

12. Dazu kontaktiert sie wiederum das **Identity Management System**

IAM-Konzepte



- **Isolierte Benutzer** und **Berechtigungsnachweise** pro Anwendung: Identitäten werden direkt in der Anwendung gespeichert verwaltet
- **Zentralisierte** Benutzerverwaltung
 - Single SignOn (**SSO**) Identitätsdomäne (z.B. Kerberos, .NetPassport)
 - **Meta-Verzeichnisse** (Synchronisation von Identitäten über verschiedene Domänen)
 - Gemeinsame Benutzeridentität/Zertifikat für alle Services (**PKI**)



- **Ziele:**
 - Eine Organisation kann die **Identitäten** von Personen **von anderen Organisationen akzeptieren** und diesen **vertrauen**
 - **Verwaltung** von Identitäten **vereinfachen**
 - Dem Benutzer ermöglichen, **mit einer Identität** auf **Ressourcen** in **anderen Bereichen** zugreifen zu können
- Ermöglicht **organisationsübergreifende Prozesse** und **Informationsflüsse**
- Geht weiter als zentralisierte Identitätsverwaltung (z.B. Active Directory), da **Sicherheitsgrenzen überschritten** werden

IAM-Konzepte



- Föderales Model mit **einer** virtuellen **Identitätsdomäne**
 - **Trennung** des **Identity Service Provider** vom **IT-Service Provider** (z.B. SAML, Liberty Alliance, Shibboleth)
- **Benutzerzentrierte** Modelle
 - z.B. OpenID, CardSpace, Passwort Stores (virtuelles SSO)
 - Verwendung eines **Personal Authentication Device** (HW oder SW)

Federation Beispiel



Bei ILIAS anmelden über SWITCHaai

SWITCHaai Login

Um sich über SWITCHaai anzumelden, klicken Sie bitte auf den Anmelde-Button und Sie auf der folgenden Seite Ihre Organisation aus.
Bei Fragen dazu, wenden Sie sich bitte an die HSLU Hotline.

Bei ILIAS anmelden

Benutzername *

Passwort *

* Erforderliche Angabe

- Verwendet **Shibboleth** als Basis für Identity Federation, resp. für SSO
- **AAI** = Authentication and Authorization Infrastructure

Shibboleth

- frei verfügbar
- unter **Apache** Lizenz

Federation Beispiel



Bei ILIAS anmelden über SWITCHaai

SWITCHaai Login


Um sich über SWITCHaai anzumelden, klicken Sie bitte auf den Anmelde-Button und Sie auf der folgenden Seite Ihre Organisation aus.
Bei Fragen dazu, wenden Sie sich bitte an die HSLU Hotline.

Bei ILIAS anmelden

Benutzername *

Passwort *

* Erforderliche Angabe

 **SECURNITE**

Shibboleth

- basiert auf **SAML** (Security Assertion Markup Language)
- **Ziele:**
 - **SSO** (Single Sign on)
 - Bereitstellen und Aufbereiten von Informationen aus Identity Management Systemen **für Dritte**
 - **Verteilte Zugriffe**
 - **Lokale & zentrale Identity Provider**

Federation Beispiel



Bei ILIAS anmelden über SWITCHaai

SWITCHaai Login


Um sich über SWITCHaai anzumelden, klicken Sie bitte auf den Anmelde-Button und Sie auf der folgenden Seite Ihre Organisation aus.
Bei Fragen dazu, wenden Sie sich bitte an die HSLU Hotline.

Bei ILIAS anmelden

Benutzername *

Passwort *

* Erforderliche Angabe

 **SECURNITE**

Shibboleth

- **Hauptkomponenten**
 - **Identity Provider:** von der Organisation bereitgestellt, deren Benutzer Zugriff auf einen eingeschränkten Dienst möchten
 - **Service Provider:** Dienst, auf den Benutzer zugreifen möchten (beim Anbieter des Dienstes)
 - **Lokalisierungsdienst:** Zeigt an, woher ein Benutzer kommt

Federation Beispiel



Bei ILIAS anmelden über SWITCHaai

SWITCHaai Login


Um sich über SWITCHaai anzumelden, klicken Sie bitte auf den Anmelde-Button und Sie auf der folgenden Seite Ihre Organisation aus.
Bei Fragen dazu, wenden Sie sich bitte an die HSLU Hotline.

Bei ILIAS anmelden

Benutzername *

Passwort *

* Erforderliche Angabe

 **SECURNITE**

Shibboleth

- **Sicherheit**
 - Transportweg wird durch **SSL** geschützt
 - Authentisierung der Systeme auf Basis von **Zertifikaten** (nur Zertifikate aus Liste anerkannter CAs)
 - Assertions werden mit **SAML** realisiert
 - Jede Organisation, die bei Switch AAI mitmacht, unterstellt sich gewissen **organisatorischen Bedingungen**

Federation



- **CardSpace**
 - Von Microsoft entwickelt
 - Ziel: Widerstandsfähigkeit gegen Angriffe
 - Baut auf Webservices Protocol Stack auf (WS-*)
- **OpenID**
 - Von vielen grossen Anbietern wie Yahoo oder Google verwendet
 - Basiert auf offenem Standard
 - Verzichtet auf eine zentrale Verwaltung der Identitäten
- **Liberty Alliance / Kantara**
 - SAML und WS-Trust als Basis



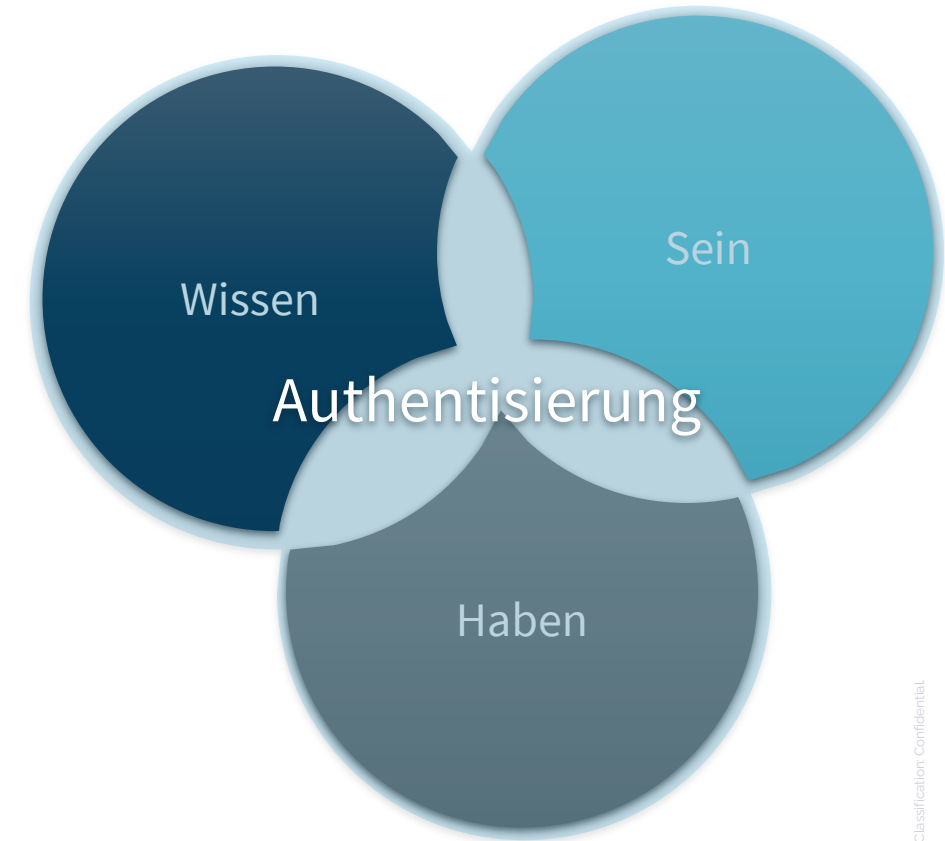
Authentisierung

Wiederholung: Authentisierung

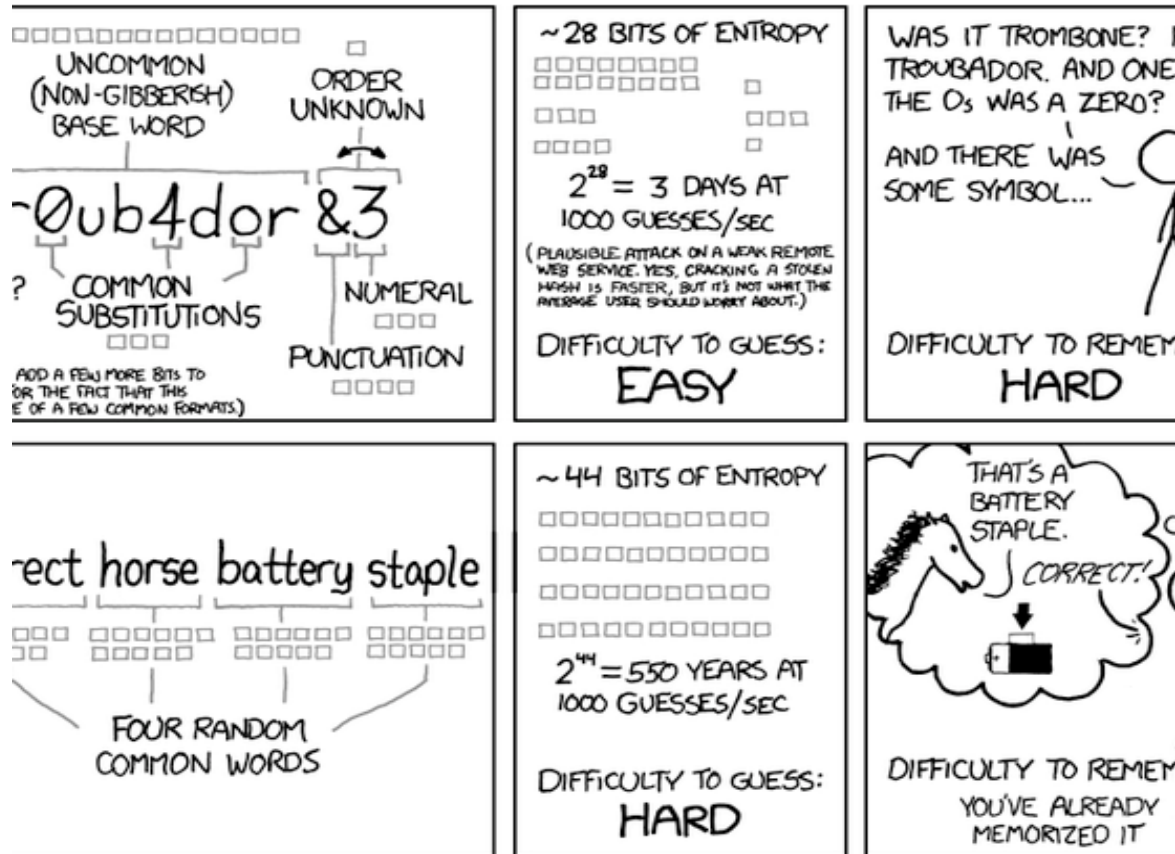
- **Nachweis** einer Person, dass sie die Person **ist**, die sie **vorgibt** zu **sein**
- Auch anwendbar für Objekte, Tiere, Dienste usw.
- **Zwei** Schritte nötig:
 - **Identifizierung**, Erkennung ohne Vorwissen
 - **Überprüfung** (Verifikation) der Identität

Wiederholung: Authentisierung

- Erfolgt durch Vorlegen eines **Nachweises**, der die Identität **bestätigen** sollen
 - geheime **Informationen** (z.B. Passwort)
 - **Identifizierungsgegenstand** (z.B. Personalausweis)
 - **Identifizierungsobjekt** (z.B. biometrische Merkmale)
- „**Starker Authentisierung**“ = Kombination mehrerer dieser Verfahren



Authentisierung



THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

TO BEHEWBER? BUT EASY FOR COMPUTERS TO GUESS?
EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS
TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

- Weit verbreitet, sehr häufiges **Angriffsziel**
- **Angriffsarten**
 - Direktes In-Erfahrung-Bringen
 - Selektives Durchprobieren
 - Systematisches Durchprobieren („brute-force-Attack“)

Exkurs: Passwort Cracking



Entropie

- Stärke eines Passwords wird in “Entropie Bits” angegeben
- Passwort mit **42 Entropie Bits** hat die Stärke eines Passwords mit 42 vollständig **zufallsgenerierten** Bits
- Passwort mit **42 Entropie Bits** benötigt **2^{42} Versuche**, um alle Möglichkeiten in einem Brute Force Angriff auszuschöpfen

Exkurs: Passwort Cracking



Entropie

- Berechnung der Entropie eines zufallsgenerierten Passworts mit **Länge L** aus der Anzahl der **Symbole N**
- N^L mögliche Passwörter

$$\text{Entropie } H = \log_2(N) L$$

Exkurs: Passwort Cracking



Entropie

- **Beispiel:** Alphanumerisches Characterset, Case Insesitive (**N = 36**)
 - Entropie = 5,170 Bits / pro Symbol
 - Für ein 42 Entropie Bit starkes Passwort werden 9 Symbole, also eine Passwort Länge von 9 benötigen ($42 / 5,17 = 8,1$)
- $2^{42} = 4'398'046'511'104$ Passwörter
- Kommerzielle PCs schaffen mit GPU 2'800'000 Passwörter pro Sekunde → 18 Tage nötig, um alle Möglichkeiten durchzuprobieren

Authentisierung



- **Probleme:**
 - Es werden eine Vielzahl von Passwörtern benötigt → SSO
 - „Gute“ Passwörter sind schwer zu merken
- **Massnahmen zur Angriffsabwehr:**
 - **Lange** Passwörter, Grosse **Zeichensätze**
 - **Sperren** von Zugängen nach wenigen erfolglosen Versuchen
 - **Logging** der Versuche zur Angriffserkennung
 - **Ausbildung** der Benutzer
 - **Richtlinien** erlassen und durchsetzen (Passwort Policy)
 - **Technische Massnahmen** (Länge, Gültigkeitsdauer, ...)

Authentisierung

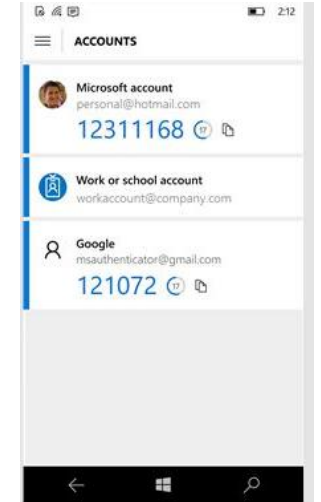
- Enthalten **X.509 Zertifikate** von PKIs
- Verwendung z.B. bei **Full Disc Encryption (FDE)** (vgl. OSSEC 04)
- Durch **Kombination** des Besitzes eines **Zertifikats** auf einer Smart Cards und einer **PIN** für das Entsperren des Schlüssels auf der Smart Cards gilt dies als sehr **sicheres Authentisierungsmittel**
- **Beispiel SuisselD:** für Signatur und zur Authentisierung
 - In **Kartenform** oder **Kryptostick** mit USB-Anschluss
 - Schlüsseloperationen werden immer auf der Karte ausgeführt



Authentisierung

- Verschiedene **Ausprägungen**

- Zeitgesteuert
- Ereignisgesteuert
- Challenge-Response Verfahren



- **Ablauf:**

- Client & Server machen **unabhängig** voneinander eine **Berechnung**
- Benutzer **überträgt Resultat** des Clients zum Server
- **Server überprüft** Gleichheit des Resultats gleich und gewährt Zugriff

- **Beispiele:** RSA SecureID, Tan Liste auf Papier, Microsoft Authenticator App

Authentisierung



- Basieren auf **Merkmalen** einer Person, welche **einmalig** sind
- **Beispiele:**
 - Retina, Iris
 - Fingerabdruck
 - Stimme
- **Datenbank** mit biometrischen Merkmalen unterliegt **allerhöchsten Schutzanforderungen**

Authentisierung

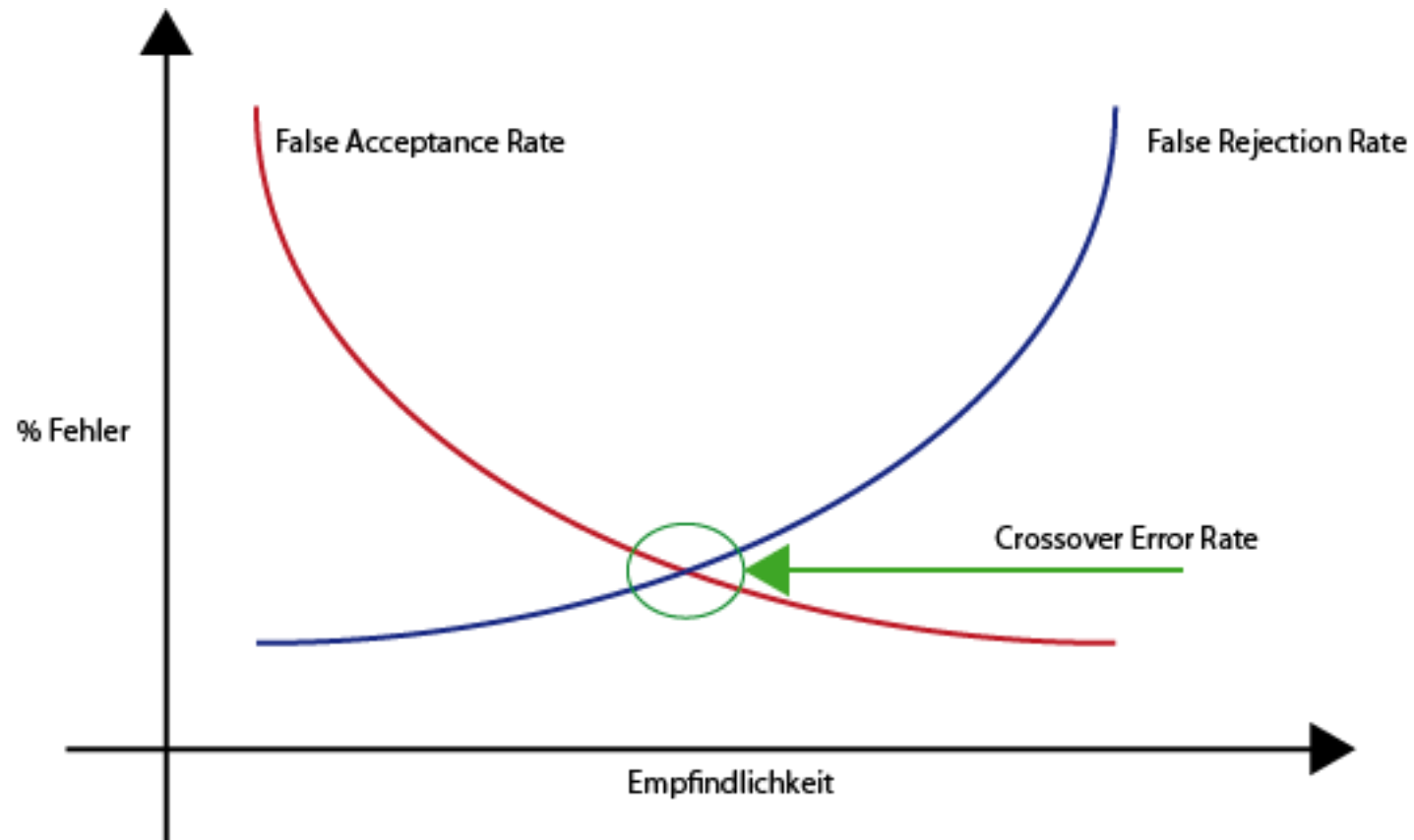


- Qualitätsmessung mit **Cross Over Error Rate**
 - definiert Schnittpunkt der False Acceptance und False Rejection Rate Kurven
 - **False Acceptance** = unberechtigte Person wurde zugelassen
 - **False Rejection** = berechtigte Person wurde abgewiesen
- Je höher **Empfindlichkeit** des Sensors
 - Desto **sicherer** wird das System
 - Desto **häufiger** werden berechtigte Personen **abgewiesen**

Authentisierung



Biometrische Zutrittskontrollen





Single Sign On

Single Sign On



- Ermöglicht es einem Benutzer, sich nur **ein** einziges **Mal authentisieren** zu müssen und danach **Zugriff** auf alle Ressourcen zu erhalten, für die er die entsprechenden **Rechte** besitzt
- **Technologien:**
 - **Kerberos** (im Unternehmensumfeld)
 - **SAML** (Security Assertion Markup Language) für Webanwendungen
 - Einsatz von **Zertifikaten** einer PKI, wenn alle Anwendungen die Authentisierung via Zertifikat unterstützen

Gruppenübung (15 Minuten)



- Die **Kerberos-Authentifizierung** ist gegenwärtig die Standard-Authentifizierungstechnologie unter **Windows** und auch für Apple OS, FreeBSD, UNIX und **Linux** gibt es **Implementierungen**
- Recherchieren Sie
 - Welche **Hauptelemente** bei dem Verfahren zum Einsatz kommen
 - Die Funktionsweise der **Angriffe**, durch die Kerberos bedroht ist
 - **Gruppe 1:** Pass-the-Ticket
 - **Gruppe 2:** Golden Ticket
 - **Gruppe 3:** DCShadow Angriff
 - Welche **Massnahmen** ein Administrator treffen kann

Single Sign On



- Markup Sprache zur Übertragung von **Sicherheitsinformationen** auf Basis von **XML**
- **Transportprotokoll:** HTTPs
- **Hauptbestandteile**
 - **Assertions:**
 - Informationen zur Authentifizierung und zur Autorisierung
 - Unterscheidung nach Authentication Assertion und Attribute Assertions (zur Autorisierung)

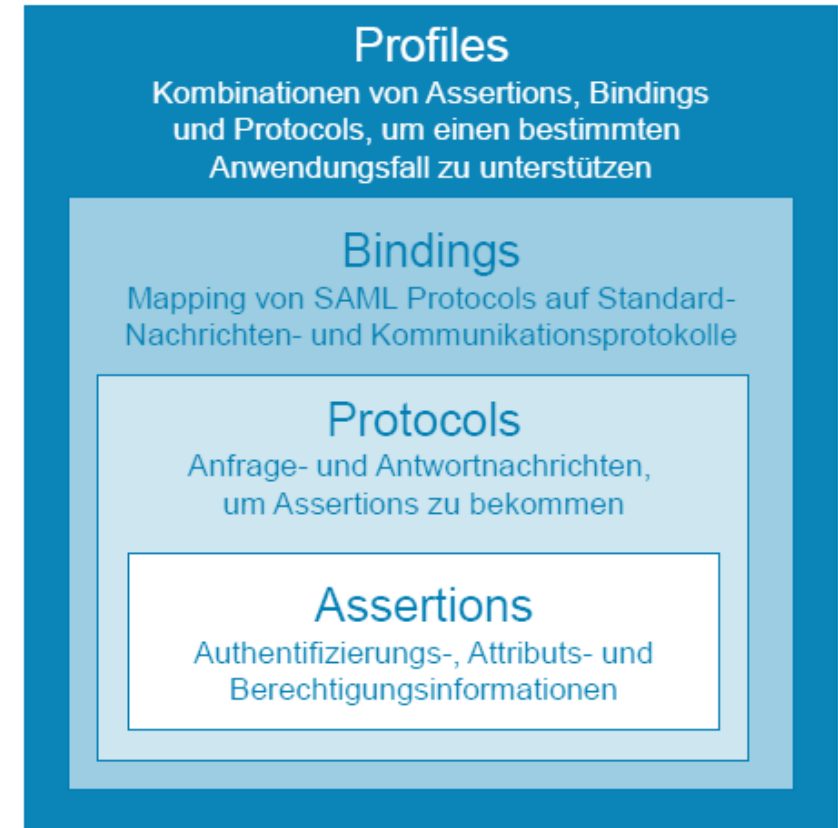
Single Sign On



SAML

- **Hauptbestandteile**

- **Protocol:** Definition, wie SAML Assertions angefordert und übermittelt werden
- **Bindings:** Definiert Einbindung von SAML Assertions in Protokolle und Frameworks
- **Profile:** Genaue Zusammenstellung von Assertion, Protocol und Binding, für bestimmten Use Case



Single Sign On



PKI

- Benutzer weist sich mit **Smart Card** aus, resp. dem darauf gespeicherten X.509 **Zertifikat**
- Benutzer **entsperrt** Smart Card durch Eingabe eines **PINs**
- Benutzer kann sich an allen Anwendungen **anmelden**, die der **PKI vertrauen** und die für **Zertifikatsbasierte Authentisierung** eingerichtet sind
- Es werden **keine Autorisierungsinformationen** übermittelt
- Problem der **Rechtevergabe** muss gesondert gelöst werden

Single Sign On



- **Diebstahl:** Hat ein Angreifer eine Identität gestohlen, hat er sofort Zugriff auf alle Systeme dieses Benutzers
- **Verfügbarkeit:** steht das SSO nicht zur Verfügung, kann niemand auf Ressourcen zugreifen
- Sehr **attraktives Ziel** für jeden Angreifer
- Sicherheit des SSO Systems muss sich nach dem **höchsten Schutzbedarf aller** daran angeschlossenen **Anwendungen** richten



Authentifizierung

Authentifizierung



Windows Server

- Betriebssystem empfängt **Anmeldeinformationen** vom Dienst oder Benutzer
- Betriebssystem sichert diese Informationen für die zukünftige Präsentation des **authentifizierenden Ziels**
- **Domäne:** hier ist das authentifizierende Ziel der Domänen Controller
- Windows-Anmelde Informationen werden überprüft
 - anhand der **SAM-Datenbank** (Security Accounts Manager) auf lokalem Computer
 - mit Active Directory in einer Domäne über **Winlogon-Dienst**

Authentifizierung



Windows Server

- **Anmeldeinformationen**
 - werden über **Benutzereingaben** auf der Anmelde-Benutzeroberfläche oder
 - **Programmgesteuert** über eine API erfasst
- Lokale **Sicherheitsinformationen** werden in der **Registry** unter HKEY_LOCAL_MACHINE \Security gespeichert
 - **Richtlinien** Einstellungen
 - Standard **Sicherheitswerte**
 - **Kontoinformation** (z.B. zwischengespeicherte Anmeldeinformationen)
 - Kopie der **SAM-Datenbank** (schreibgeschützt)

Authentifizierung

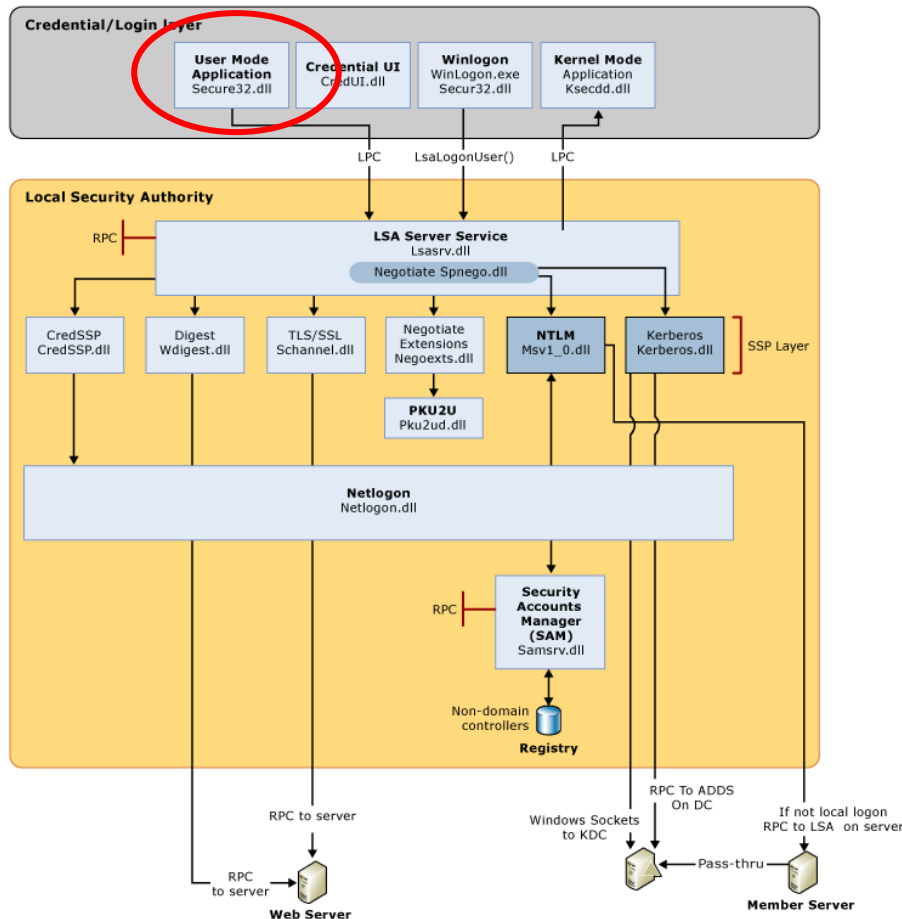


Windows Server

Secur32.dll

Anbieter für mehrfache **Authentifizierung**

Bildet die **Grundlage** für den Authentifizierungsprozess

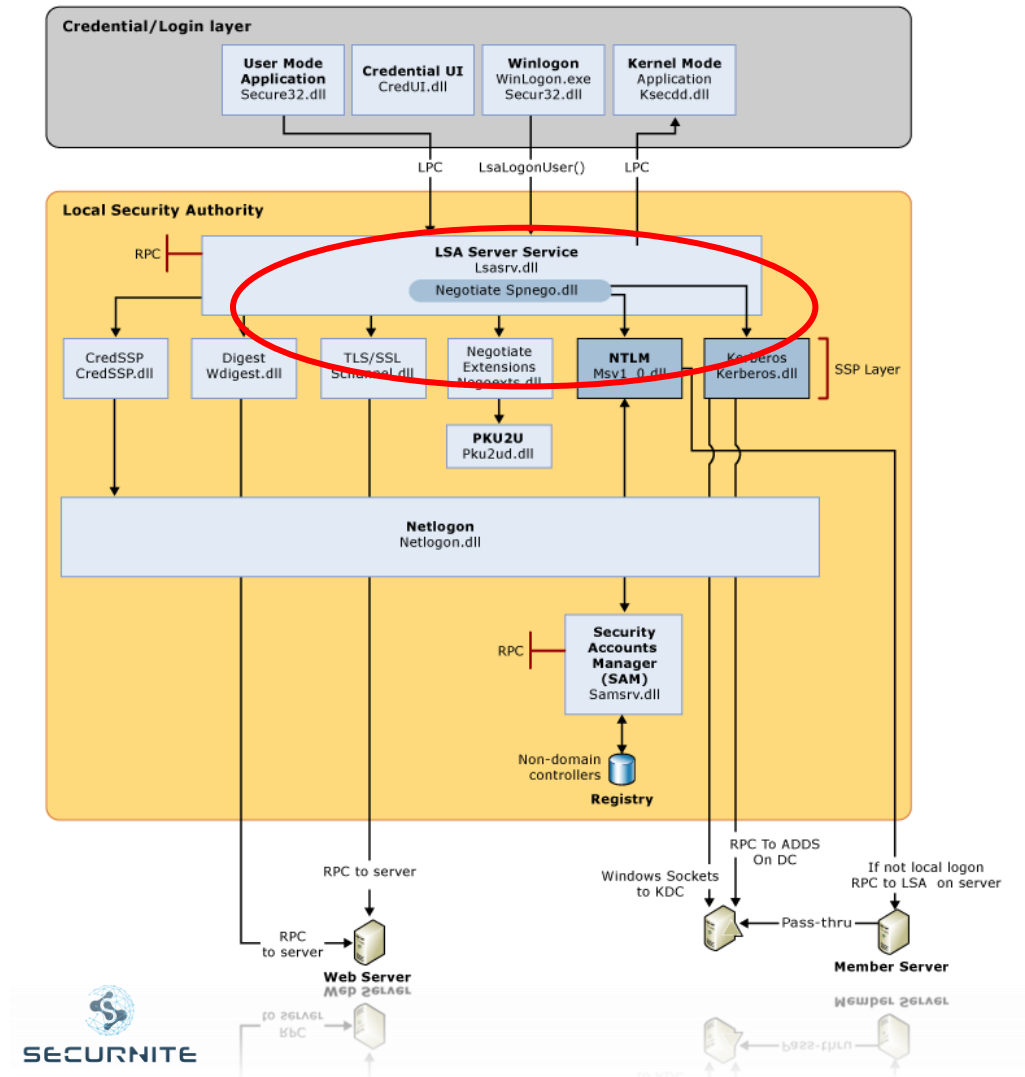


Authentifizierung

Windows Server

Lsarsrv.dll

- Local Security Authority (**LSA**) Service
- **Erzwingt** Sicherheitsrichtlinien
- Fungiert als **Sicherheitspaket-Manager** für die LSA
- LSA enthält Funktion "aushandeln,, → wählt **NTLM-** oder **Kerberos-Protokoll**



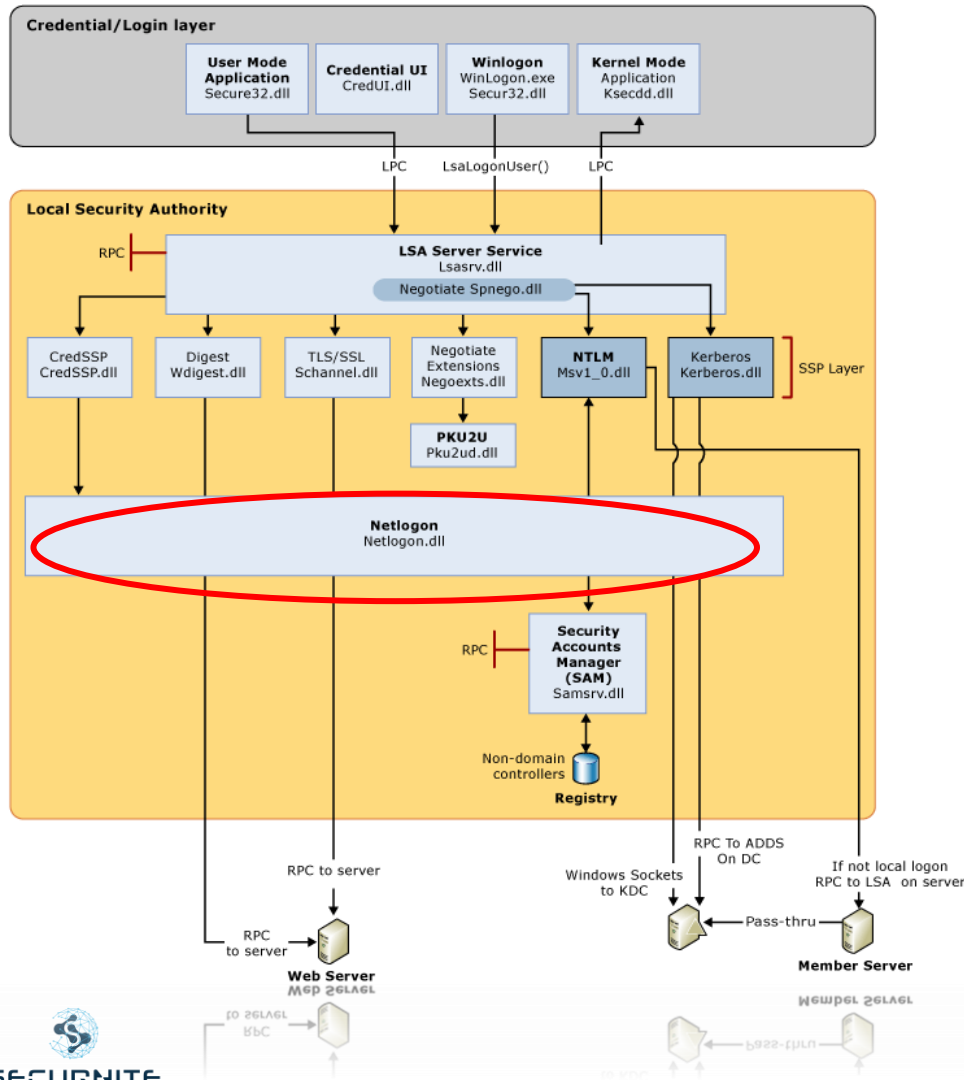
Authentifizierung



Windows Server

Netlogon.dll

- **Funktionen:**
 - Verwaltet **sicheren Kanal** mit Domänen Controller
 - Übergibt **Anmeldeinformationen** über sicheren Kanal an den Domänen Controller
 - Gibt die Domänen **Sicherheits-IDs** (SIDs) und **Benutzerrechte** für den Benutzer zurück

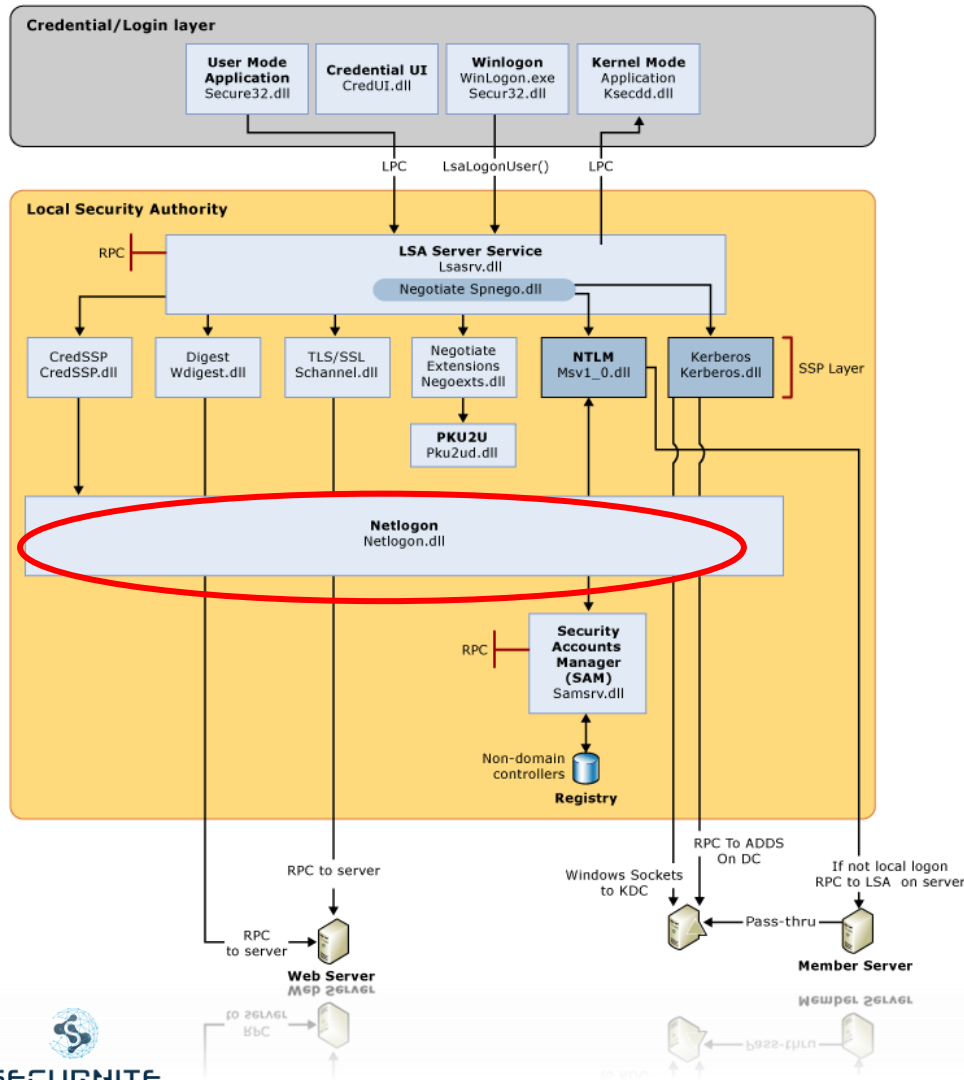


Authentifizierung

Windows Server

Netlogon.dll

- **Funktionen:**
 - Veröffentlicht **Dienst Ressourcen Einträge** im DNS
 - Verwendet DNS, um Namen in die **IP-Adressen** von DCs **aufzulösen**
 - Implementiert Replikations-Protokoll mit **RPCs** zum **Synchronisieren** von primären Domänen Controllern (PDCs) und Sicherungs-Domänen Controllern (BDCs)

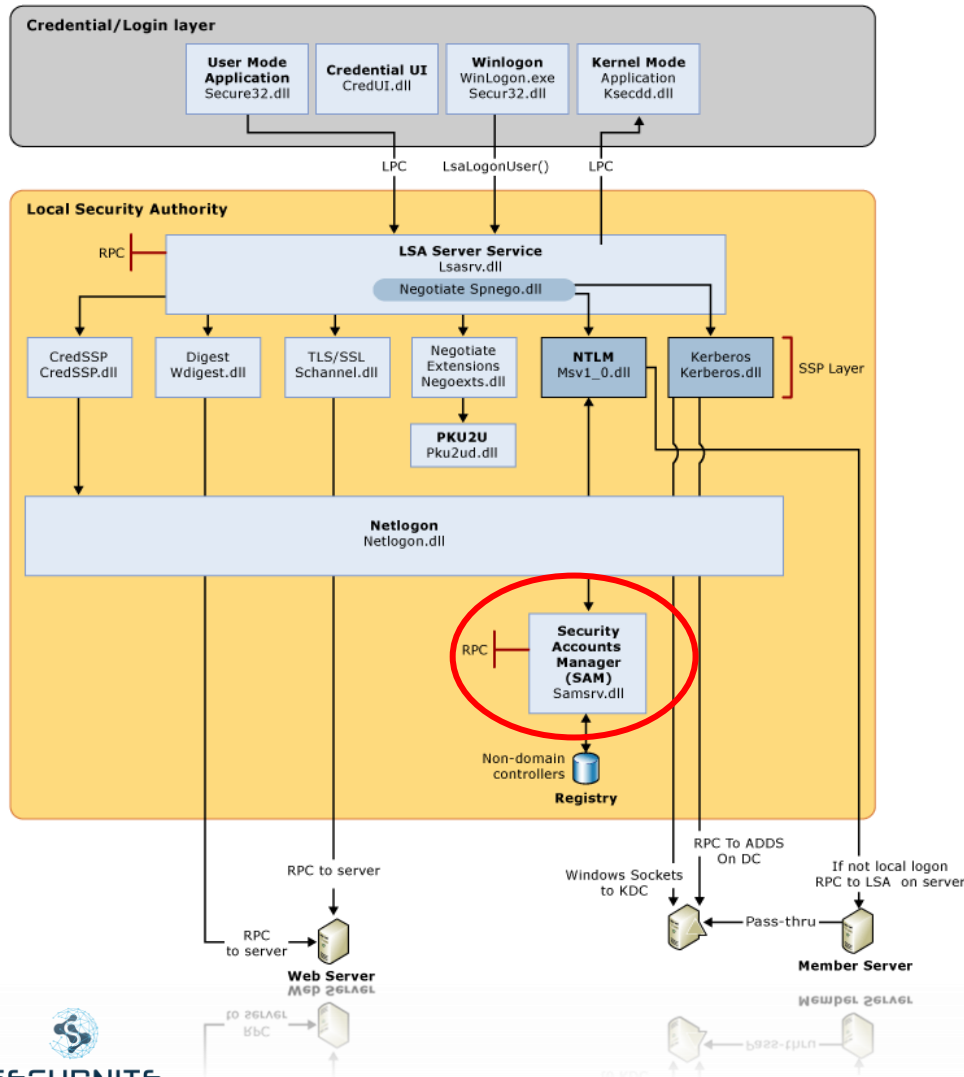


Authentifizierung

Windows Server

Samsrv.dll

- Security Accounts Manager (SAM)
- Speichert lokale **Sicherheitskonten**
- **Erzwingt** lokal gespeicherte **Richtlinien**
- Unterstützt **APIs**

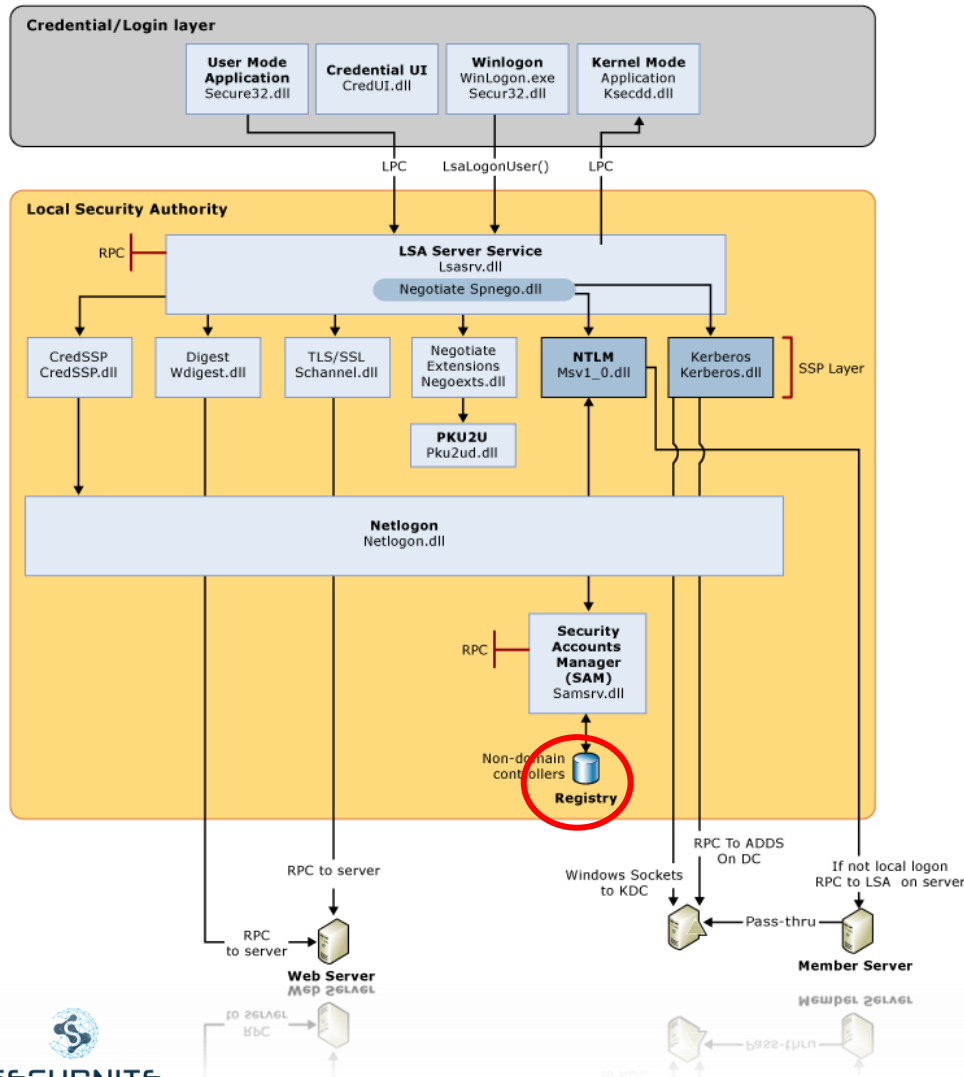


Authentifizierung

Windows Server

Registry

- Enthält
 - Kopie der **SAM-Datenbank**
 - Einstellungen für lokale **Sicherheitsrichtlinien**
 - Standard **Sicherheitswerte** und **Kontoinformationen**, die nur für das System zugänglich sind

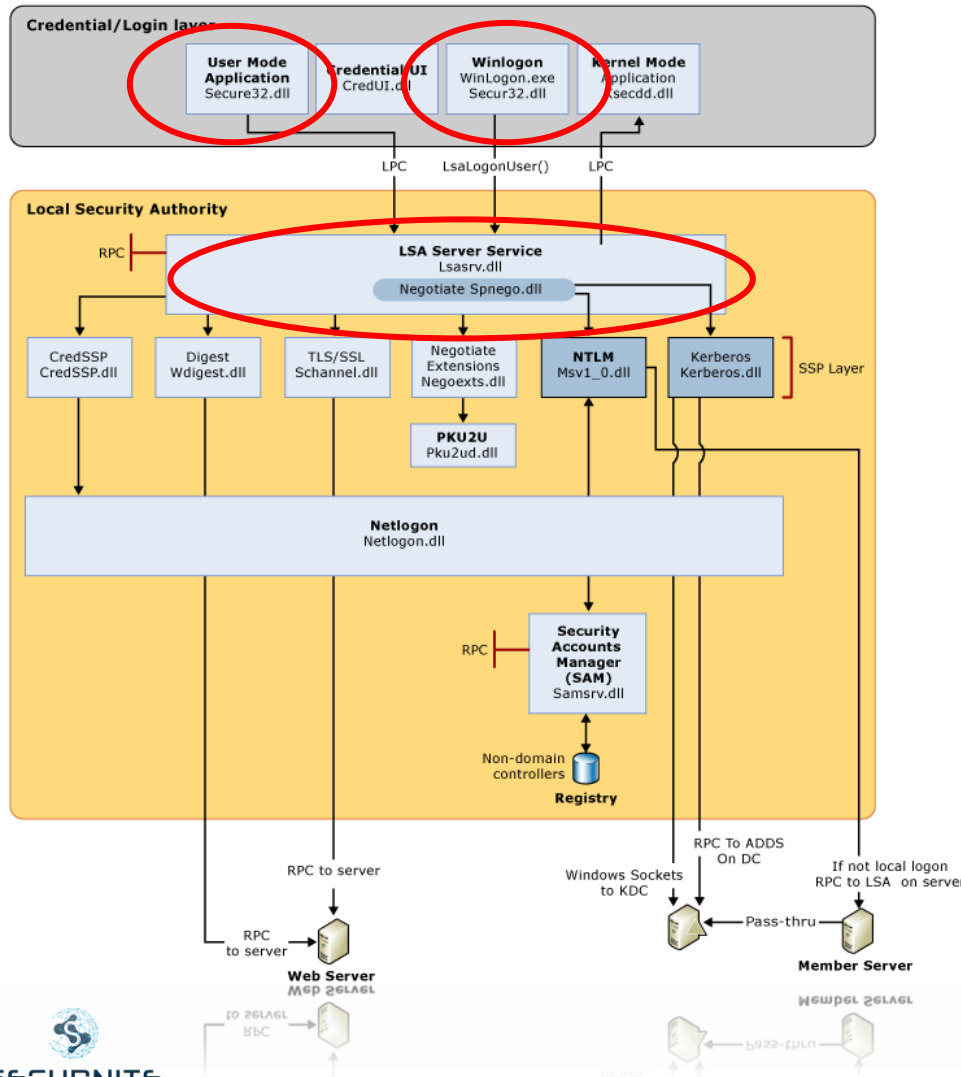


Authentifizierung

Windows Server

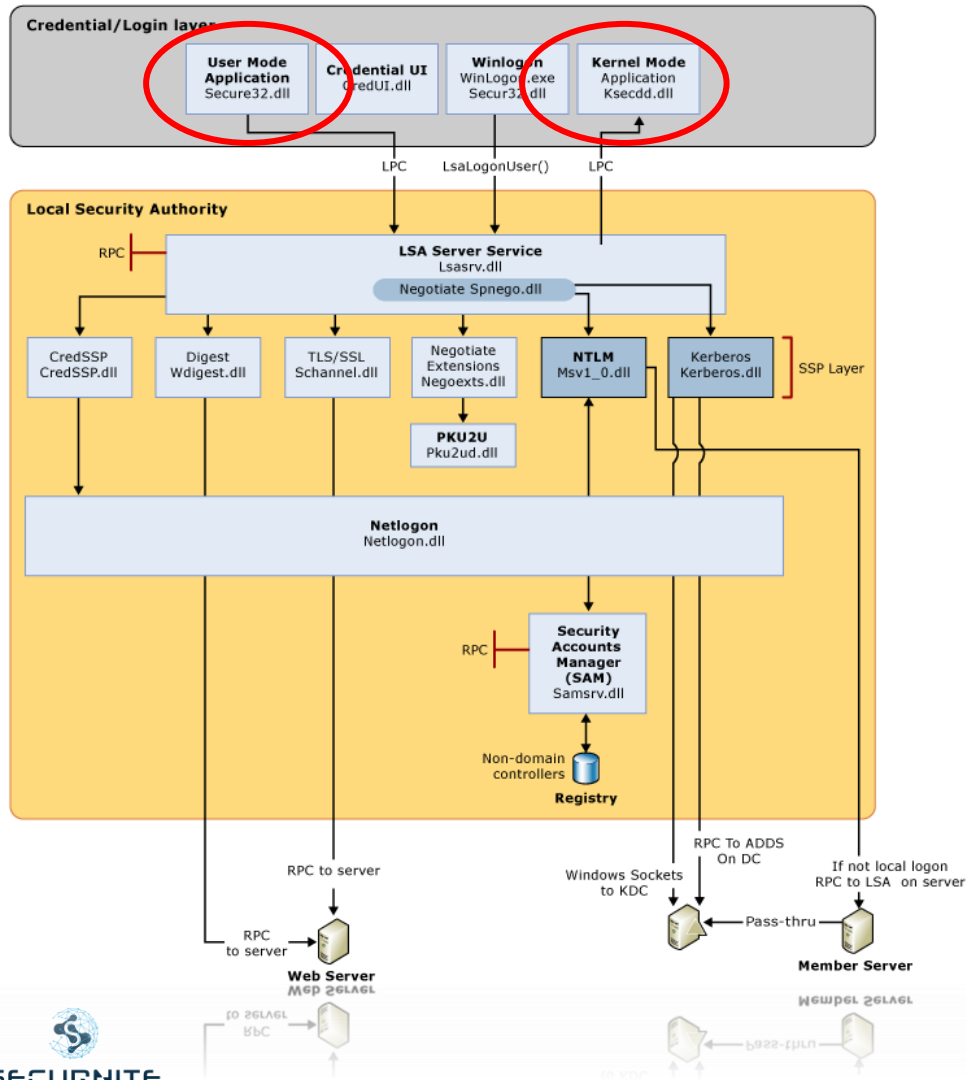
Anmelden des Benutzers

- **Winlogon.exe** ist für Verwaltung sicherer **Benutzerinteraktionen** zuständig
- Initiiert Anmeldevorgang indem gesammelte Anmeldeinformationen über **Secur32.dll** an die Local Security Authority (**LSA**) übergeben werden



Authentifizierung

Windows Server

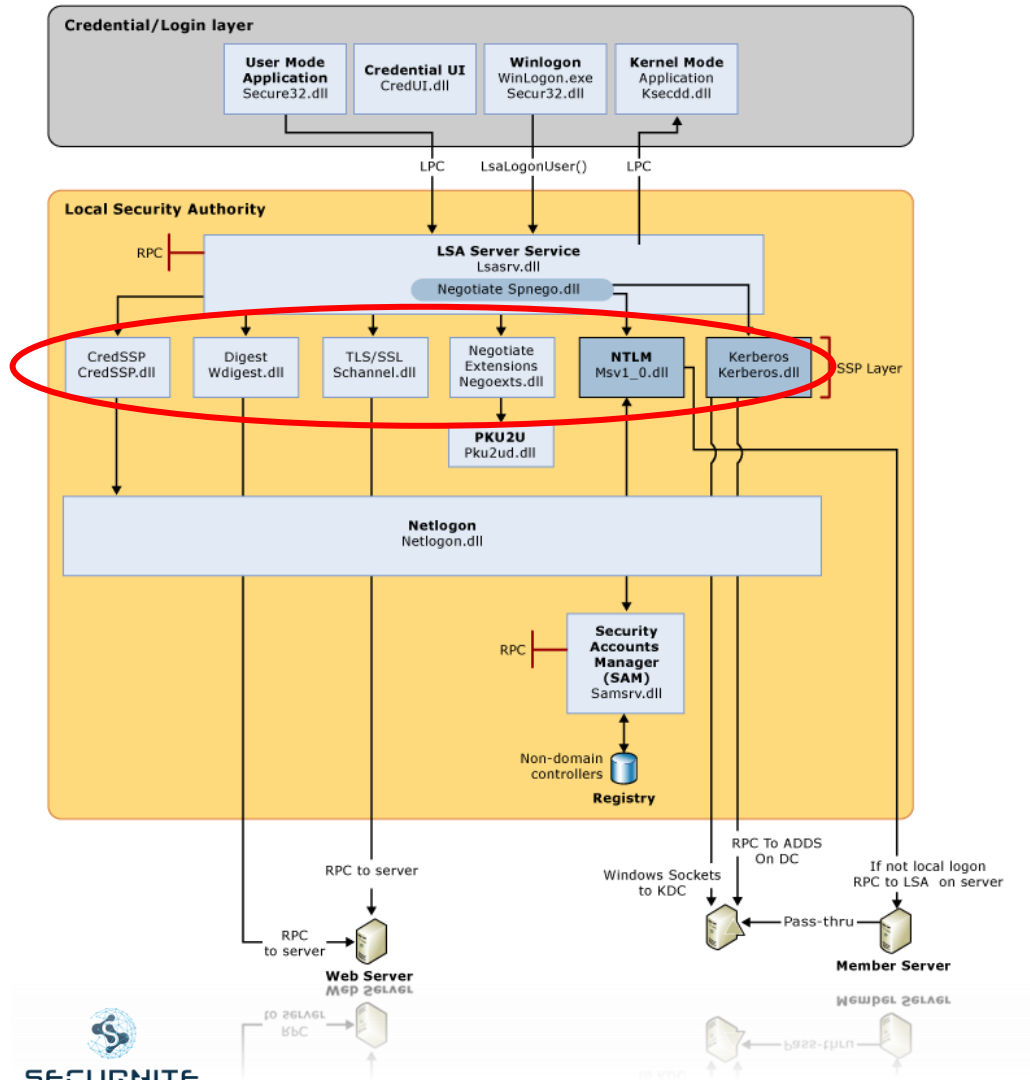


Anwendungsanmeldung

- Erfordert keine interaktive Anmeldung
- Die meisten vom Benutzer initiierten Prozesse werden mithilfe von **Secur32.dll** im **Benutzermodus** ausgeführt
- Prozesse, die beim Start initiiert werden, werden mithilfe von **Ksecdd.sys** im **Kernelmodus** ausgeführt

Authentifizierung

Windows Server



Anbieter für Sicherheitsunterstützung

- Security Support Provider (**SSP**) Layer
- Anbieter, die **Authentifizierungsprotokolle** aufrufen können
- **Standardsatz** ändert sich mit jeder **Windows Version**
- Es können **benutzerdefinierte Anbieter** geschrieben werden



Autorisierung

Discretionary Access Control

- **Benutzerbestimmbare** Zugriffskontrolle
- **Eigentümer** (owner) eines Objektes ist für dessen Schutz **verantwortlich**
- **Rechte** werden für **einzelne Objekte vergeben** bzw. **zurückgenommen**
- **Rechte** können **weitergegeben** werden
- **Keine** Festlegung von **systemweiten Eigenschaften**

Discretionary Access Control



- Modellierung **inkonsistenter Rechte möglich** (z.B. Ausführungsrecht erteilt, Leserecht entzogen)
- Realisierung durch
 - **Passworte**
 - **Access Control List (ACL)**: allgemeine Zuordnung von Benutzern, Zugriffsrechte und Systemressourcen

Mandatory Access Control



- **Systembestimmte** (regelbasierte) Zugriffskontrolle
- Systembestimmte **Rechte** können durch benutzerbestimmte **weiter eingeschränkt** werden (aber **nicht aufgehoben**)
- **Rechte** können **nicht weitergegeben** werden
- Realisierung durch
 - **Dienste des Betriebssystems**
 - **Betriebssystemerweiterungen**, spezielle Versionen (z.B. trusted solaris, SMACK, SELinux, Pitbull LX, GRSecurity Patch)

Role Based Access Control



- Jeder Benutzer wird einer „**Rolle**“ (oder Gruppe) zugeordnet, z.B Administrator, Gast, Backupadmin, FIBUMitarbeiter
- Rolle
 - eine od. mehrere **Profile**
 - Zusammenstellung von **speziellen Rechten** auf Objekte
- **Vorteile:**
 - Ermöglicht klare **Trennung** von Aufgabenbereichen
 - erleichtert **Need-to-know Prinzip**
 - Erleichtert das **Monitoring** sowie generell die **Verwaltung**

4 Augen Prinzip



- Systemkritische Operationen müssen durch **zwei Rollen/Benutzer** ausgeführt werden
- Mögliche **Umsetzung**:
 - **Gleichzeitiges Logon**: Beide Benutzer loggen sich gleichzeitig ein, erst dann kann ein bestimmter Befehl ausgeführt werden
 - **Workflow**: Benutzer1 aktiviert Befehl, der von Benutzer2 zu einem späteren Zeitpunkt ausgeführt werden kann
 - **Organisatorisch**: Beide Benutzer „kontrollieren“ sich physisch gegenseitig bei der Arbeit