„Die SKB und ihre Partner

in der Wirtschaft“

– Führungsunterstützung –

Funktionale IT-Sicherheitsarchitektur
für Einsätze der Bundeswehr

FITSA

1 INHALTSVERZEICHNIS

1 Inhaltsverzeichnis 2

2 Ziel des Dokumentes 3

3 Einleitung 4

4 Aufbau der funktionalen Sicherheitsarchitektur 5

4.1 Rahmenparameter 5

4.2 Zielbild 9

5 Einzelbausteine der Architektur 12

5.1 Endgeräteprofile 12

5.2 Anforderungen an die Datenübertragung 13

5.3 Registratur 15

5.4 Identity & Access Management 18

5.5 Cryptoservice 22

5.6 Labelling 25

5.7 Intrusion Detection System 28

5.8 Service Management 30

5.9 SystemZugang 31

5.10 Architekturübergänge 34

5.11 Anforderung an IT-Services 37

6 Ausblick 39

2 ZIEL DES DOKUMENTES

Das Dokument beschreibt die funktionalen Bausteine einer durchgängigen IT-Sicherheitsarchitektur für Missionsnetzwerke (Mission Networks) aus operativer Sicht. Die Gesamtarchitektur wurde auf Basis der Prämisse „Wir kommunizieren so miteinander, dass unsere Daten operativ nutzbar sind und dennoch deren bestmöglicher Schutz gewährleistet wird“ erstellt und bildet einen sinnvollen Kompromiss zwischen technischem Schutz und operativer Nutzbarkeit.

Ausgangspunkt der Überlegungen ist der Schutzbedarf von Missionsdaten innerhalb einer Sicherheitsdomäne „Mission Secret“. Das Dokument geht davon aus, dass der Schutzbedarf innerhalb einer solchen Sicherheitsdomäne auf der Basis einer risikobasierten Betrachtung beschrieben werden kann. Derart lassen sich auf bestimmte operationelle Umgebungen zugeschnittene Gefährdungsprofile ableiten/ erstellen. Damit kann ein Weg beschritten werden, der den notwendigen Grundschutz für ein operationelles Umfeld profilbasiert beschreibt und von den deutlich strikteren, auf der gültigen Geheimschutzordnung basierenden Verfahren abstrahiert sowie die Effizienz der IT-Sicherheitsmaßnahmen durch Ausrichtung am tatsächlichen Bedarf signifikant erhöht.

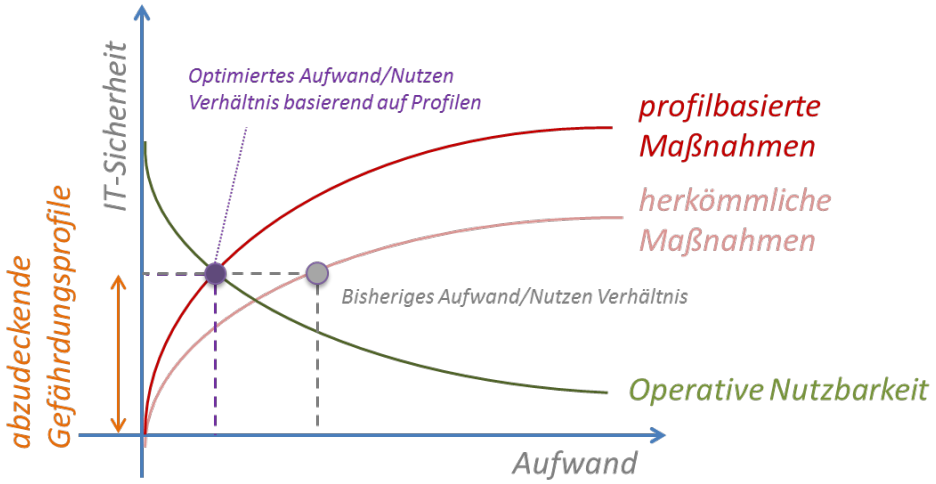

Abbildung 1: Profilbasierte, am operativen Bedarf ausgerichtete IT-Sicherheitsarchitektur

Gezielte Maßnahmen zur Risikominimierung, gepaart mit einer vergleichsweise geringen Gültigkeitsdauer der Informationen in Einsatzumgebungen, erlauben aus operationeller Sicht eine gesamtheitliche, am tatsächlichen Risiko ausgerichtete Sicherheitsvorsorge innerhalb eines Missionsnetzwerkes.

Die weitgehende Verlagerung der Informationsverarbeitung in stationäre und verlegefähige Rechenzentren und die geringe Informationsdichte auf autark arbeitenden, mobilen Endgeräten stellen zusätzliche Faktoren dar, die eine von herkömmlichen Verfahren abweichende Absicherung der Informationen ermöglichen und durch die neue Architektur aufgegriffen werden können.

Das vorliegende Dokument stellt einen Forderungskatalog auf, der als „Schablone“ für zukünftige Einsätze herangezogen und innerhalb des IT-Systems Bundeswehr (IT-SysBw) sowohl für die Basis Inland als auch für Einsatzgebiete einheitlich umgesetzt werden kann. Dem Gedanken einer effizienten Servicebereitstellung folgend, integriert die Sicherheitsarchitektur nationale und multinationale Sicherheitsdomänen mit gleichem oder geringerem Schutzbedarf und deckt damit einen Großteil des in den Einsätzen geforderten Informationsbedarfs ab. Gleichzeitig bietet die Sicherheitsarchitektur die Möglichkeit, Einsatz und „Friedensbetrieb“ unter einem einheitlichen Ansatz zusammen zu führen und beispielsweise auch Attraktivitätsmaßnahmen im „Friedensbetrieb“ (z.B. Telearbeit) in einer ausreichend abgesicherten Umgebung vereinfacht umzusetzen.

3 EINLEITUNG

Multinationale Einsätze sind geprägt von besonderen Herausforderungen im Bereich der Interoperabilität, des kooperativen Zusammenwirkens unterschiedlicher Gruppen von Akteuren, der Datenaustauschkonzepte und der damit verbundenen Sicherheitspolitik.

National unterschiedliche Implementierungen von IT-Sicherheitsanforderungen innerhalb der verwendeten IT-Ausstattungen lassen sich in der Regel nicht für multinationale Einsätze interoperabel verwenden. Eine jeweils national spezifische Umsetzung von Anforderungen an verschiedene Sicherheitsdomänen würde zu einer drastischen Reduzierung der Kommunikations- und Informationsaustauschbeziehungen auf Basis des kleinsten gemeinsamen Nenners (Sprechfunk „offen“) führen oder eine Teilnahme an Missionsnetzwerken mit nationaler Ausrüstung vollständig ausschließen.

Unter dem absehbaren Wandel der IT-Landschaft in Missionsnetzwerken, nicht zuletzt bedingt durch das Federated Mission Networking der NATO (FMN) und die damit einhergehende Implementierung eines Service orientierten Ansatzes, bedarf es neuer Konzeptansätze zur Gestaltung von IT-Architekturen, die den oben genannten Anforderungen mit einem hohen Grad an Anpassungsfähigkeit an sich dynamisch ändernde Einsatzumgebungen gerecht werden.

Die Bausteine der zukünftigen IT-Architektur benötigen Standards, um im multinationalen Kontext zeitnah anschlussfähige Schnittstellen bereitstellen zu können, sodass eine grundlegende Interoperabilität in Missionsnetzwerken gewährleistet werden kann. Gleichzeitig muss die zugesicherte Interoperabilität durch eine anpasste Kommunikations- und Sicherheitspolitik für alle beteiligten Akteure der Mission festgelegt, durchgesetzt und abgesichert werden. Die Kommunikations- und Sicherheitspolitik bestimmt den funktionalen Handlungsrahmen und legt die Prinzipien für die sicherheitsrelevante Informationsverteilung innerhalb der Mission fest.

Nicht nur für nationale Vorgaben im Bereich der IT-Sicherheit, sondern insbesondere im multinationalen Verbund mit potenziellen Missionspartnern sind grundlegende Prinzipien für eine kooperative Zusammenarbeit und einen sicheren Informationsaustausch festzulegen und diese mittelfristig in nationale Projekte und Ausstattungsvorhaben umzusetzen. Vor dem Hintergrund unbekannter Einsatzszenare und wechselnder beteiligter Nationen ist dafür ein hinreichend flexibler Ansatz erforderlich, der den notwendigen „Handlungsspielraum“ und Anpassungsmöglichkeiten zur Sicherstellung der Interoperabilität betroffener Truppenteile bietet und dennoch dem Schutzbedarf von Missionsdaten gerecht wird.

Für die Erfüllung hoch dynamischer Interoperabilitätsanforderungen müssen weitergehende Eigenschaften für Schnittstellen zu anderen Sicherheitsdomänen beschrieben werden, sodass diese unter konkreten Einsatzbedingungen technisch angepasst bereitgestellt und vor allem kontrolliert eingesetzt werden können. Diese neue Form einer flexiblen Integrierbarkeit garantiert eine Abbildung der benötigten Informationsflüsse zwischen den jeweiligen Domänen und garantiert die ganzheitliche Bereitstellung eines Common Relevant Operational Picture (CROP) auf allen Führungsebenen.

Das vorliegende Dokument beschreibt die notwendigen Anforderungsparameter zur Herausarbeitung eines Konzepts zur Entwicklung einer adaptiven, funktionalen IT-Sicherheitsarchitektur. Der Begriff *adaptiv* drückt die Fähigkeit aus, neben den funktionalen Aspekten einer IT-Architektur auch die qualitativen Bedingungen ihrer Nutzung zur Erfüllung entsprechender Missionsaufgaben festzulegen und für alle Phasen der Einsatzführung sicherzustellen. Veränderungen in den Missionsrahmenbedingungen führen mit dieser Eigenschaft zeitnah auf eine neue Integrations-, Kommunikations- und Sicherheitspolitik unter Verwendung einer einheitlichen und zertifizierten IT-Sicherheitsarchitektur.

In den folgenden Abschnitten werden Anforderungen in Bezug auf einzelne Bausteine einer IT-Sicherheitsarchitektur beschrieben.

Das Dokument macht Vorgaben bzw. trifft Annahmen für eine mögliche funktionale Umsetzung einer solchen Integration und beschreibt schließlich aus funktionaler Sicht die Eigenschaften geforderter Einzelkomponenten, ohne auf konkrete Produkte oder Umsetzungen einzugehen. Die Eigenschaften stehen immer im Kontext der geforderten Flexibilität, die eine schnelle Anpassung bei Änderungen in der Kommunikations- und Sicherheitspolitik garantieren.

Die beschriebenen Bausteine wurden gemeinsam mit zivilen Firmen des IT-Sektors entwickelt und in einen Entwurf für eine zukünftige IT-Sicherheitsarchitektur überführt. Die Bausteine sind fachlich validiert und auf Machbarkeit hin verifiziert. Einzelne Bausteine sind ggf. derzeit noch nicht durch Produkte hinterlegt, jedoch mittelfristig absehbar durch vorhandene Technologien oder deren Weiterentwicklung bereitstellbar, sodass eine Integration insbesondere im Hinblick auf die deutsche Teilhabe am Federated Mission Networking der NATO – durch das German Mission Network, kurz GMN – als realisierbar eingeschätzt wird.

Die Konzeption zur Entwicklung einer adaptiven, funktionalen IT-Architektur berücksichtigt wesentliche Elemente von Ansätzen anderer Nationen, mit denen das Dokument nach nationaler Billigung ebenfalls erörtert und dann der NATO als konsolidierter Vorschlag für entsprechende Vorgaben im Bereich FMN angezeigt werden soll. Auch für das HERKULES Folgeprojekt kann das Dokument nach nationaler Abstimmung als Richtschnur dienen, um eine möglichst einheitliche Umsetzung der Bereitstellung von IT-Services sowohl im zivilen als auch im militärischen Bereich zu gewährleisten.

4 AUFBAU DER FUNKTIONALEN SICHERHEITSARCHITEKTUR

4.1 RAHMENPARAMETER

Die IT-Sicherheitsarchitektur aus Einsatzsicht basiert auf der Analyse des tatsächlichen Schutzbedarfes (Gefährdungsprofil) der in heutigen Einsätzen übertragenen/verarbeiteten Informationen und beschreibt die zur bestmöglichen technischen Absicherung der Informationen notwendigen Komponenten auf funktionaler Ebene. Sie abstrahiert von einer technischen Lösung in Form konkreter Produkte. Aus Sicht der IT-Sicherheitsarchitektur stellt die Umsetzung der beschriebenen funktionalen Forderungsbausteine der jeweiligen Einzelkomponenten einen ausreichenden Schutz der in Einsätzen zu verarbeitenden Informationen vor dem Hintergrund einer jeweils durchgeführten Risikobewertung (Anlage) dar und deckt damit einen Großteil der Gefährdungsprofile in heutigen Einsatzszenarien ab.

Ziel der Architektur ist eine weitestgehende Zentralisierung der Verarbeitung von Informationen in stationären und verlegefähigen Rechenzentren und eine damit einhergehende Bündelung der Funktionalitäten in einem möglichst eng umgrenzten Bereich. Lediglich für Systemanteile, die eine Autarkiefähigkeit (z.B. auf der mobilen Ebene) fordern, ist eine gesonderte Ausbringung von Einzelkomponenten der Architektur erforderlich. Dies steht im Einklang mit den architekturellen Vorgaben des IT-SysBw im Rahmen der Ausrichtung hin zu einer serviceorientierten Architektur.

Die Sicherheitsarchitektur bietet zudem die Möglichkeit zur Integration von Sicherheitsdomänen bis zu einem bestimmten Schutzbedarf und trägt damit zur effizienteren Ausgestaltung der Führungsunterstützung in heutigen Einsätzen insbesondere aus betrieblicher Sicht bei, da anders als bisher nicht komplette System-Stacks für die unterschiedlichen Sicherheitsdomänen ausgeprägt werden müssen. Die daraus resultierenden Anforderungen an die bereitzustellenden Core- und Community of Interest Services (CS und COIS gemäß NATO C3 Classification Taxonomy) sind gesondert herausgestellt und bei Rüstungsprojekten zu beachten. Nur so kann aus Sicht der Sicherheitsarchitektur der gemäß IT-Strategie des Geschäftsbereichs BMVg geforderten Einheitlichkeit der IT-Services über verschiedene Sicherheitsdomänen hinweg effizient Rechnung getragen werden.

Als Eingangsgrößen für die beschriebene Architektur werden die Erfahrungen und Anforderungsprofile heutiger Einsätze herangezogen. Die Architektur muss skalierbar, multinational interoperabel, hoch verfügbar und trotz der hohen Sicherheitsanforderungen einfach zu betreiben sein, um das sich schnell ändernde Anforderungsprofil heutiger Einsätze adäquat bedienen und die Anforderungen an das Betriebspersonal in einem handhabbaren Umfang halten zu können.

Im operativen Umfeld stellen sich hohe Herausforderungen durch den scheinbaren Widerspruch zwischen einer einsatzbedingten, zeitnahen Informationsverarbeitung bei gleichzeitiger Sicherstellung komplexer Prozesse für eine regulierte und nachweispflichtige Informationsverteilungspolitik.

Der Erfolg bzw. die Qualität eines Architekturentwurfs repräsentiert sich im erreichbaren Effizienzgrad von spezifischen Informationsprozessen und sollte sich daran bewerten lassen. Die Umsetzung der Architektur Mission Network sollte unter Bedingungen einer Multi-Level Security Datenverwaltung hocheffiziente Informationserzeugungs-, Verteilungs- und Anwendungsprozesse erlauben.

Erweiterte Anforderungen an die Instrumente für eine flexible Regulierbarkeit und damit zur Neuausrichtung von bestehenden Informationsprozessen sind zu berücksichtigen. Den Hauptgrund bildet eine hohe Dynamik sich ändernder Einsatzanforderungen. Der Zeitbereich kann dabei beliebige Größenordnungen beanspruchen.

Effiziente Informationsverteilungsprozesse sollen das kooperative Zusammenwirken unterschiedlicher Einsatzkräfte maßgeblich beeinflussen und transparent machen. Es darf zu keinem Zeitpunkt zu einer Verletzung kommunikativer und sicherheitsrelevanter Grundprinzipien im Informationsaustausch führen.

Trotz strenger Anforderungen an die Separierung von klassifizierten Datenbeständen bestehen hohe Anforderungen, zeitnah auf Informationsbestände verschiedener Datenbereiche der Gesamtarchitektur zugreifen zu können. Auf der einen Seite werden Daten im Zuge operativer Handlungen übernommen (initiale Bereitstellung), einsatzbezogen erhoben und verarbeitet, auf der anderen Seite werden Daten für die Informationsgewinnung verteilt, aggregiert und präsentiert. Im ersten Fall stehen Prozesse für die Übernahme, Erzeugung und Generierung von Daten im Vordergrund. Im zweiten Fall sind Prozesse für eine zeitnahe Informationsgewinnung und koordinierte Einsatzführung zu betrachten.

Damit kommt den Vorgaben für die Verteilung von Informationen sowie dem Umgang mit aggregierten Daten eine gesonderte Bedeutung zu, die zwar technisch durch die jeweilige Sicherheitsarchitektur unterstützt werden (z.B. dynamisch erzeugte Sicherheitszonen zur Separierung von aggregierten Informationen), aber abhängig von grundsätzlichen, einsatzbezogenen Vorgaben sind, welche nicht innerhalb der Sicherheitsarchitektur getroffen werden können.

Der Wandel des IT-Systems der Bundeswehr hin zu einer Serviceorientierten Architektur und die zukünftig zu erwartende verstärkte Abstützung auf die Leistungserbringung in der Basis Inland auch bei einsatzrelevanten IT-Services und die stringente Umsetzung des Prinzips „train and work as you fight“ bedingen eine durchgängige Umsetzung der Architektur nicht nur bei den in Einsätzen ausgebrachten IT-Komponenten, sondern auch innerhalb der Rechenzentren der Basis Inland.

4.1.1 ABZUBILDENDE SICHERHEITSDOMÄNEN

Primär adressiert die IT-Sicherheitsarchitektur den für die Bundeswehr in Einsatzumgebungen wichtigsten Anwendungsfall, die Sicherheitsdomänen von „Mission Networks“ – im Folgenden generisch als Sicherheitsdomäne „MISSION SECRET“ bezeichnet. Dabei bezieht sich der Terminus "Mission" derzeit noch auf eine konkrete operative Mission, welche im Bündnisrahmen durchgeführt wird und an der unterschiedlichste Nationen und Organisationen beteiligt sind. Der Terminus „Mission Secret” stellt nach heutigen Stand somit keine valide Sicherheitsklassifizierung dar, sondern bedarf eines konkreten Einsatzszenarios.

Während die Sicherheitsanforderungen an die in den Missionsnetzwerken eingesetzten IT-Systeme in der Vergangenheit jeweils im einsatzspezifischen Kontext festgesetzt wurden, oder der Anspruch eines durchgängigen „System High“-Ansatzes in Form der Sicherheitsdomäne „NATO SECRET“ zum Einsatz gekommen ist, soll die vorgestellte Sicherheitsarchitektur einen effizienteren Ansatz zur Abdeckung des Schutzbedarfes der Informationen in Missionsnetzwerken geben, der dynamisch während der Missionsdurchführung anpassbar ist. Notwendige Maßnahmen zur Absicherung des Systems bzw. der Systemanteile sollen angepasst an den tatsächlichen Schutzbedarf das tatsächliche notwendige Maß darstellen und Aspekte der multinationalen Interoperabilität berücksichtigen. Sicherheitsdomänen mit gleichem oder geringerem Schutzbedarf (OFFEN, VS-NUR FÜR DEN DIENSTGEBRAUCH) sind in die Sicherheitsarchitektur zu integrieren, wenn die getroffenen Maßnahmen den Vorgaben der jeweiligen Sicherheitsdomäne entsprechen bzw. diese abdecken. Die Sicherheitsarchitektur muss so gestaltet sein, dass sie nicht nur den Schutzbedarf vergangener und laufender Einsätze abdeckt, sondern auch zukünftig in Einsätzen zur Anwendung gebracht werden kann. Eine entsprechende Modularität und Integrierbarkeit neuer Technologien bzw. Weiterentwicklung von Standards ist daher zu berücksichtigen. Eine Harmonisierung mit den Vorgaben der NATO und anderen Bündnisorganisationen, die im Fokus der politischen Vorgaben für die Bundeswehr liegen, sind unabdingbar für die erfolgreiche Implementierung innerhalb einsatzrelevanter Anteile des IT-SysBw.

4.1.2 VORGABEN

Vorgaben für nationale Sicherheitsdomänen sind insbesondere bei deren Integration in eine Gesamtarchitektur zu berücksichtigen. Gleiches gilt für informationstechnische Übergänge zu Sicherheitsdomänen, die außerhalb einer funktionalen IT-Sicherheitsarchitektur für Einsatznetzwerke ausgebracht sind, mit denen aber ein durchgängiger, medienbruchfreier Informationsaustausch sichergestellt werden muss.

Resultierend aus den betrieblichen Anforderungen ist die Sicherheitsarchitektur in eine Gesamtbetriebsführung IT-SysBw zu integrieren und hat Beiträge zu einem gesamtheitlichen Lagebild IT/Führungsunterstützung zu liefern. Dabei ist auch das IT Service Management der Sicherheitsservices, unabhängig von der Anzahl der zu integrierenden Domänen, technisch nur einmal auszubringen, um den betrieblichen Aufwand insbesondere in Einsätzen auf das erforderliche Mindestmaß zu reduzieren.

Innerhalb der funktionalen IT-Sicherheitsarchitektur verarbeitete Informationen sind nachzuweisen. Eine einheitliche Nachweisführung des Zugriffs auf die gespeicherten Informationen ist sicher zu stellen. Die Anwender müssen innerhalb der Architektur identifizierbar sein, auch im multinationalen Kontext. Der Zugriff auf das System ist rollen- und rechtebasiert zu ermöglichen.

Bei der funktionalen Beschreibung und späteren Umsetzung der Komponenten ist zur Festlegung des geforderten Funktionsumfanges und der jeweiligen Ausprägung eine am Schutzbedarf der tatsächlich übertragenen/verarbeiteten Informationen ausgerichtete Risikobewertung durchzuführen und ein bei der jeweiligen Ausprägung verbleibendes Restrisiko zu identifizieren sowie ggf. mögliche Maßnahmen zur Risikominimierung zu beschreiben.

Auch hat die Sicherheitsarchitektur den gesamten Lebenszyklus von Informationen zu berücksichtigen. Hier sind die jeweiligen Phasen der Einsatzplanung und -durchführung als Maßstab heranzuziehen, und auch der Umgang mit Informationen nach einem Redeployment ist zu beschreiben.

4.1.3 OPERATIONELLE ANFORDERUNGEN

Zusammengefasst ergeben sich folgende operationelle Anforderungsbausteine an die funktionale IT-Sicherheitsarchitektur, die es in der Ausgestaltung zu berücksichtigen gilt:

- Einheitliches Identitäts- und Zugriffsmanagement für Friedensbetrieb und Einsatz

  Die Sicherheitsarchitektur muss ein durchgängiges, einheitliches Access Management für die Basis Inland und die Einsatzgebiete ermöglichen. Die Teilnahme an einem Einsatzkontingent muss seitens der IT durch eine „Freischaltung“ der jeweiligen Informationsdomäne erfolgen. Innerhalb der Informationsdomäne ist das „need to know“ Prinzip anzuwenden, d.h. der jeweilige Anwender erhält Zugriff nur auf die Informationen, die er zur Erfüllung seines jeweiligen Einsatzauftrages benötigt. Dafür notwendige Rollen- und Rechtekonzepte sind durch das Identitäts- und Zugriffsmanagement zu unterstützen. Da aber nicht für jede Information der korrekte und abschließende Kreis berechtigter Empfänger festgelegt werden kann, ist auch das „need to share“ Paradigma zu unterstützen und zumindest für eine ausreichende Metadatenstruktur eine rollen- und rechteübergreifende Publizierung zu integrieren. Dadurch muss es auch Nutzern außerhalb einer Rechtegruppe bei Bedarf möglich sein Informationen, die zur Wahrnehmung Ihrer Aufgabe erforderlich sind, anzufordern und eine anlassbezogene Freigabe erteilt zu bekommen.

- Modularität

  An die Sicherheitsarchitektur „Mission Network“ werden je nach Anwendungsebene unterschiedliche Auflagen bezüglich Kapazität, Verfügbarkeit und Absicherung gestellt. Auf der mobilen Ebene sind die Möglichkeiten zur Ausbringung einzelner Komponenten der Sicherheitsarchitektur wesentlich begrenzter als auf der Ebene verlegefähiger oder stationärer Einrichtungen. Ein modularer Aufbau der Sicherheitsarchitektur ist damit Grundvoraussetzung für eine adäquate Realisierung der benötigten Komponenten unterschiedlicher Mobilitätsdimensionen.

- Skalierbarkeit

  Die Sicherheitsarchitektur muss dynamisch an unterschiedliche Anforderungen (Qualität und Quantität) anpassbar sein und auch im laufenden Betrieb eine Anpassung der Nutzerzahlen erlauben, um den dynamischen Einsatzumgebungen unter Berücksichtigung eines effizienten Betriebes Rechnung zu tragen. Dabei sollte die Skalierbarkeit berücksichtigen, dass einzelne Module insbesondere bei kleineren Kontingenten in einzelnen Hardware Komponenten zusammengefasst werden können, um den logistischen Aufwand in ein vernünftiges Verhältnis zur Anwenderzahl zu setzen.

- Durchgängiger Informationsraum

  Die heutigen Informationsaustauschbeziehen sowie der Wegfall einer strikten Trennung zwischen Einsatz und Grundbetrieb, auch in Bezug auf die Bereitstellung von IT-Services z.B. durch Reach-Back, bedingen eine Durchlässigkeit sowohl aus geographischer als auch aus Sicht der Informationsbereitstellung. Informationen müssen möglichst verzugslos von der Basis Inland in die jeweiligen Einsatzgebiete und umgekehrt übertragen werden können. Gleichfalls muss es auch technisch möglich sein, entsprechend eingestufte Informationen zwischen den Informations- und Sicherheitsdomänen austauschen zu können. Die bisher oft verwendete Praxis von „Drehstuhlschnittstellen“ ist weder effizient noch zuverlässig. Eine möglichst zeitnahe und unterbrechungsfreie Informationsbereitstellung trägt maßgeblich zur Informationsüberlegenheit bei.

- Zentrale Leistungsbereitstellung/dezentrale Leistungskonsumierung

  Die dezentrale Bereitstellung von IT-Services als lokale Applikation auf Arbeitsplatz PCs erhöht den administrativen Aufwand des IT-Systems und führt zu zusätzlichen Fehlerquellen im Betrieb. Die Implementierung von Changes muss für eine große Anzahl von Komponenten geplant und zeitlich gestaffelt ausgeführt werden, was den Anforderungen der Einsätze widerspricht. Vielmehr gilt es durch eine zentrale IT-Service Bereitstellung den betrieblichen Aufwand vor Ort zu minimieren, die Systeme mit hoher Informationsdichte zu konzentrieren und Arbeitsplatzausstattungen wo immer möglich so minimalistisch und damit kostengünstig wie möglich zu gestalten – unter Berücksichtigung der operationellen Erfordernisse. Auch hier steht die Effizienz der Leistungserbringung, die es zu optimieren gilt, im Vordergrund. Die IT-Sicherheitsarchitektur hat diesen Vorgaben Rechnung zu tragen.

- Unterstützung von Autarkiefähigkeit

  Gleichwohl ist eine vollständige Verfügbarkeit informationsübertragender Systemanteile in der Realität nicht zu gewährleisten, insbesondere vor dem Hintergrund der militärischen Einsatzszenarien. Die Störung der rückwärtigen Anbindung ist in Einsätzen ein nicht unwahrscheinliches Szenario und in der Ausplanung der IT zu berücksichtigen. Die IT-Sicherheitsarchitektur hat daher insbesondere im mobilen Bereich eine (zeitlich begrenzte) Autarkiefähigkeit der Anwender für Anteile der Leistungserbringung im IT-SysBw zu ermöglichen. Anforderungen an den Schutzbedarf der autark vorgehaltenen Informationen sind dabei nicht zu vernachlässigen.

- Ausfallsicherheit

  Insbesondere für IT-Services, die die Kernführungsfähigkeit in laufenden Einsätzen sicherstellen, sind hohe Anforderungen an die Verfügbarkeit zu stellen. Da eine IT-Sicherheitsarchitektur und deren relevante Komponenten elementarer Bestandteil der Service Bereitstellung sind, ist ein gleich hohes Maß an Verfügbarkeit für diese Anteile des IT-SysBw zu fordern. Komponenten der IT-Sicherheit und für die Absicherung des IT-SysBw dürfen nicht die Verfügbarkeit des Gesamtsystems beeinträchtigen und sind entsprechend zu planen.

- Integration bestehender und zukünftiger IT-Services

  Da eine Sicherheitsarchitektur das Gesamtsystem zu betrachten hat, ist die Integration sowohl eingeführter, als auch geplanter IT-Services zu berücksichtigen. Gemäß den gültigen Vorgaben sind die gleichen IT-Services in unterschiedlichen Sicherheitsdomänen bereit zu stellen. Hierfür hat die IT-Sicherheitsarchitektur Lösungsmöglichkeiten aufzuzeigen, die einen möglichst ressourcenschonenden Betrieb der jeweiligen IT-Services ermöglichen. Auf eine Ausbringung der IT-Services in autarken Stacks für jede Sicherheitsdomäne soll nach Möglichkeit verzichtet werden.

4.2 ZIELBILD

4.2.1 KOMPONENTEN EINER FUNKTIONALEN IT-SICHERHEITSARCHITEKTUR

Allein aus einer funktionsorientierten Perspektive der Einzelbausteine lassen sich der Charakter bzw. die Arbeitsprinzipien einer IT-Sicherheitsarchitektur nicht ermitteln und bewerten. Erst die Informationsbewegungen, die Prozesse mit ihren Interaktionen und koordinierte Folgen nachvollziehbarer Entscheidungsketten der beteiligten Akteure visualisieren die zielorientierte Anwendung der IT-Sicherheitsarchitektur zur Lösung konkreter Missionsaufgaben. Die Präzision und Schnelligkeit, mit der die IT-Sicherheitsarchitektur dieser Dynamik im Rahmen einer laufenden Mission angepasst werden kann, bestimmt maßgeblich, neben allen funktionalen Aspekten, den Wert der zukünftigen IT-Sicherheitsarchitektur.

IT-Sicherheitsarchitekturen zukünftiger Einsatzumgebungen müssen daher die Fähigkeit besitzen, sich flexibel an konkrete Bedingungen und Risiken einzelner Einsätze anzupassen. Basierend auf qualifizierten, z.T. evaluierten Kernkomponenten, die elementar für eine ganzheitliche Abbildung der IT-Sicherheit in Einsatznetzwerken sind, ist deren Nutzungsausprägung abhängig von dynamischen Gefährdungsprofilen zu definieren, die für die einzelnen funktionalen Bausteine der IT/Führungsunterstützung und Hierarchieebenen des Einsatzszenarios individuell zu bestimmen sind.

Grundlage hierfür muss eine fortlaufende Bewertung der aktuellen Einsatzumgebung in Bezug auf Risiken des Standortes, der beteiligten Gruppen von Akteuren mit ihren Befugnissen und Kooperationen, notwendiger Informationsmengen mit ihren Verteilungsprinzipien und Klassifizierungen sein. Eine sich ständig ändernde Cyber-Gefährdungslage muss zwangsläufig Veränderungen an der Ausprägung einzelner Komponenten zur Folge haben. Das bedeutet, dass angemessen zur aktuellen Gefährdungsbewertung eine abgestimmte Integrations-, Kommunikations- und Sicherheitspolitik der IT-Sicherheitsarchitektur nachgeführt und eingestellt wird, die den Handlungsspielraum und damit die Dynamik kooperativer Prozesse weiter öffnet bzw. einschränkt.

Gleichfalls gilt es, die operativen Anforderungen an die in Einsätzen verwendete IT der potenziellen Bedrohungslage gegenüber zu stellen, um technische und organisatorische Maßnahmen der IT-Sicherheit mit den Anforderungen des Nutzers bestmöglich in Einklang zu bringen. Moderne IT-Sicherheitsarchitekturen benötigen Instrumente, um für den aktuellen Sicherheitskontext bestehende Restrisiken berechnen zu können, um diese zielorientiert durch ein regulatives Nachführen weiterer Sicherheitsfunktionen zu minimieren oder vollständig zu beseitigen. Die Steuerbarkeit der Bausteine einer IT-Sicherheitsarchitektur erlaubt die zeitkontinuierliche Erfassung und Abbildung des Sicherheitszustandes einer laufenden Mission durch die Anwendung qualifizierter, semantischer Auswertungsprozesse von Systemzustandsinformationen in einer Wissensdatenbank.

Eine moderne IT-Sicherheitsarchitektur stellt nicht nur Schnittstellen im Sinne einer funktionalen Interoperabilität bereit, sondern kontrolliert diese gemäß der eingestellten Sicherheitspolitik in Bezug auf autorisierte Endgeräteklassen. Die Datenflusskontrolle an den Schnittstellen bestimmt die Art und die Richtung von notwendigen Kommunikationen. Die Fähigkeit, kontrollierte Schnittstellen anzuwenden, erlaubt auch eine vollständige Änderung aktueller Kommunikationsbeziehungen durchzusetzen und im Ernstfall (nach Auswertung der Kriterien, die eine Verletzung der Kommunikationspolitik anzeigen), bestimmte Gruppen von Akteuren vom Missionsverbund auszuschließen und deren IT- Systeme von der IT-Sicherheitsarchitektur technisch abzukoppeln.

Dabei sind integrative Ansätze zur Abbildung mehrere Sicherheitsdomänen mit ähnlichen Schutzbedarf der Informationen genauso zu berücksichtigen, wie technische Randbedingungen im Bereich der Informationsübertragung (Bsp. Latenz, Bandbreite), was sich in verschiedenen Profilen relevanter Bausteine an den Schnittstellen ausdrückt. Generell sind aber auch die integralen Bestandteile der im Folgenden beschriebenen Architektur in Abhängigkeit der Anwendungsebene und des zu identifizierenden Gefährdungsprofils im jeweiligen Einsatzkontext unterschiedlich auszuprägen. Die beschriebenen funktionalen Forderungen sind dennoch sicher zu stellen.

4.2.2 EINZELBAUSTEINE DER FUNKTIONALEN IT-SICHERHEITSARCHITEKTUR

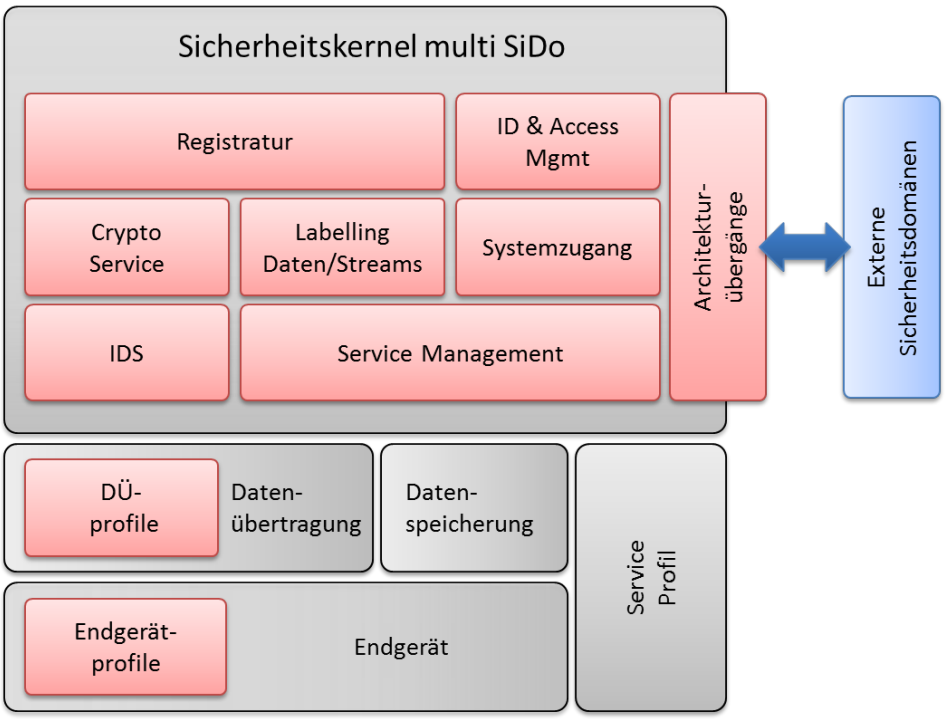

Abbildung 2: Bausteine der funktionalen IT-Sicherheitsarchitektur

Abbildung 2 zeigt das Zielbild der funktionalen IT-Sicherheitsarchitektur als reine Bausteinsicht, ohne ihre Beziehungen weiter zu spezifizieren.

Die Bausteine bilden Funktionsblöcke ab, die im Rahmen einer gesamtheitlichen Architektur als notwendige Bestandteile angesehen und im Folgenden näher beschrieben werden. Die Bausteine der Architektur werden in einem Sicherheitskernel zusammengefasst, der die Verwaltung/Integration mehrerer Sicherheitsdomänen ermöglicht.

Anforderungen, die aus IT-Sicherheitssicht an solche Komponenten gestellt werden, die direkt mit dem Kernel interagieren, sind in der Abbildung ebenfalls als Blöcke dargestellt und werden ebenfalls detailliert beschrieben. Um die Wirksamkeit der Gesamtarchitektur zu gewährleisten, müssen diese Anforderungen in entsprechenden Systembestandteilen berücksichtigt und umgesetzt werden. Gleiches gilt für das Service Profil, das die Anforderungen an IT-Services beschreibt, die in die Architektur integriert werden sollen. Dazu gehört auch die Datenspeicherung, die zwar nicht direkt durch die Sicherheitsarchitektur beeinflusst wird, aber sehr wohl über Datensicherungskonzepte zum gesamtheitlichen Ansatz beiträgt und durch die Trennung zwischen Funktionalität und Datenhaltung im Bereich der IT-Services einen wesentlichen Baustein für die Sicherheitsarchitektur darstellt.

Die vorgestellte funktionale IT-Sicherheitsarchitektur stellt mit dem Baustein „Domänen-Übergänge“ Übergänge in andere Sicherheitsdomänen (DEU GEHEIM, NATO SECRET, EU SECRET) bereit, die nicht in der vorgestellten IT-Sicherheitsarchitektur abzubilden sind. Zum einen stellt die vorgestellte Sicherheitsarchitektur Anforderungen an die funktionale Ausprägung dieser Übergänge, zum anderen sind gültige Vorschriften und Auflagen der anzubindenden Sicherheitsdomänen für diese Domänen-Übergänge heran zu ziehen.

5 EINZELBAUSTEINE DER ARCHITEKTUR

5.1 ENDGERÄTEPROFILE

Die multinationalen Einsätze der Bundeswehr sind durch unterschiedliche Rollen (Gefährdungsprofil, Rechte, Aufgaben, Applikationen) und Einsatzprofile (stationär, verlegefähig und mobil) gekennzeichnet. Die erforderlichen Endgeräte sind daher hinsichtlich Leistungsfähigkeit, Größe, Schnittstellen und Robustheitsgrad einsatz- und ebenengerecht individuell auszulegen. Die verfügbare Bandbreite zur Anbindung an die Informationsräume ist ebenfalls durch die jeweilige Einsatzumgebung festgesetzt bzw. begrenzt.

Die Anbindung hängt im Wesentlichen von der Ebene ab. Auf höheren Ebenen (z.B. stationäre und verlegefähige Gefechtsstände) kann von einer stabilen, breitbandigen Anbindung ausgegangen werden.

Auf den unteren Ebenen werden der klassische Truppenfunk (VHF), Boden-Bord-Kommunikation (UHF), Weitverkehr (HF) Funkverbindungen oder taktische Satellitenkommunikation (TacSat) eingesetzt. Ergänzend werden in dem Projekt Mobile Taktische Kommunikation (MoTaKo) Technologien zur Breitbandübertragung für den militärischen Einsatz bewertet (z.B. SatCom on the Move, zellulare Netze). Die Anbindung der Endgeräte an die Funkterminals soll künftig über Standard LAN Schnittstellen erfolgen. Da die verfügbare Bandbreite von den Einsatzbedingungen abhängt, muss das System (Netzwerkkomponenten, Endgeräte, Applikationen, etc.) für schmalbandige Anbindung ausgelegt sein.

5.1.1 FUNKTIONALE FORDERUNGSBAUSTEINE

Die Endgeräte der unterschiedlichen Ebenen müssen in der Lage sein, die auf Basis der Gefährdungsprofile identifizierten, notwendigen Komponenten der Sicherheitsarchitektur zu unterstützen. Die Ausprägung der Komponenten ist dabei flexibel an die jeweilige Lage angepasst auszugestalten.

Wo gefordert müssen die Endgeräte eine (zeitlich begrenzte) Autarkiefähigkeit unterstützen, während bei den übrigen Anwendungsfällen auf eine zentralisierte Informationsverarbeitung zurückgegriffen werden kann. Das bedeutet eine weitestgehende Unterstützung des „Software as a Service“ Paradigmas.

Endgeräte müssen unabhängig von der Ausbringungsebene eine einheitliche Hardwareschnittstelle bereitstellen, um ggf. notwendige Anpassungen der implementierten Sicherheitsarchitektur an die jeweiligen Endgeräte mit geringem Aufwand zu unterstützen.

Unterschiedliche, integrierte IT-Services in Endgeräten (insbesondere im Bereich der Communication Services und Crypto Services) sind modular auszuprägen, sodass ein Austausch einzelner Services ohne ein Redesign des Endgerätes notwendig wird.

5.1.2 BESCHREIBUNG DES FUNKTIONALEN PROFILS

Die Endgeräte unterscheiden sich je nach den oben aufgeführten Rahmenbedingungen in folgenden Eigenschaften:

- Art der Anbindung (Funkanbindung, LAN),
- Zu unterstützende Applikationen und Services, z.B. Sprache, FüWES und/oder Datenverarbeitung,
- Formfaktor von Headset über Smartphone, Tablett, ZERO-Client, PC bis zur Server Workstation,
- Rechnerleistung (RAM / ROM / CPU / GPU),
- Betriebssysteme (Android / MS7 oder 10 / Server OS / Linux),
- On-/Offline Nutzungsbefähigung,
- Echtzeitfähigkeit,

- Fähigkeit zur sicheren Trennung und Priorisierung von Datenströmen,
- Mögliche Integration von PKI (z.B. mittels Smart-Card-Reader) in unterschiedlichen Klassen,
- Mögliche Integration von HW- und/oder SW-Krypto,
- Einstufung (BSI-Zulassung, NATO-Zulassung),
- Multi-Level-Security (MLS) Fähigkeit,
- Elektromagnetische Abstrahlsicherheit (Tempest Zone 2 bis Zone 0, SDIP 27 Level C bis Level A).

Zusätzlich ist zu beachten, dass sich die Umwelt- und Ergonomie-Anforderungen gerade auf mobilen Plattformen (z.B. Kabinen, Rad- und Kettenfahrzeuge, Boote und Flugzeuge) deutlich von denen im stationären und verlegefähigen Bereich unterscheiden. Zusammenfassend sollte der Systembediener über eine einzige, optimal gestaltete Mensch-Maschine-Schnittstelle sein gesamtes Aufgabenspektrum bearbeiten können.

Eine weitere Überlegung ist die Einführung von festen Produktlinien in unterschiedlichen Baureihen kombiniert mit modularen Erweiterungsmöglichkeiten. Hierzu das Beispiel Produktlinie Laptop stationär:

- Mobile Prozessoren (Atom, i3 bis mobilen XENON Prozessoren),
- Displaygröße 13“ / 15“ / 17“,
- Zulassung für GEHEIM, Mission SECRET oder VS-NfD mit Einfluss auf:
  - Tempestierung (SDIP Level A/B/C),
  - Kryptomodul (GEHEIM/Mission SECRET/VS-NfD),
  - Smart-Card-Reader,
  - Löschbare HDD / SSD.

Diese könnte sich von einer Produktlinie für den abgesessenen Einsatz mit Displaygrößen im Bereich 5‘‘ bis 7‘‘ abgrenzen.

Der Aufbau eines Warenkorbes mit entsprechenden Endgeräten dient der Reduzierung der Gerätevielfalt und der Vereinfachung des logistischen Footprints.

5.2 ANFORDERUNGEN AN DIE DATENÜBERTRAGUNG

5.2.1 FUNKTIONALE FORDERUNGSBAUSTEINE

Über geeignete Parametrisierung sind die verfügbaren Bandbreiten zwischen den einzelnen Bereichen (stationär – verlegefähig – mobil – hoch mobil) für die Übertragung von Informationen auszunutzen.

An die Datenübertragung sind verschiedene Anforderungen zu stellen. Die Basisanforderungen sind dabei durch die Sicherstellung der folgenden Punkte abzudecken:

- Vertraulichkeit der Daten,
- Integrität der Daten,
- Authentizität der Daten,
- Nachvollziehbarkeit der Übertragung,
- Prüfung des Empfangs.

Neben diesen Basisanforderungen sind die besonderen Rahmenbedingungen von Übertragungswegen in der militärischen Umgebung zu berücksichtigen:

- Verfügbarkeit von Übertragungswegen,
- Schmalbandige Übertragungswege,
- Schwankende Latenzen.

5.2.2 BESCHREIBUNG DES FUNKTIONALEN PROFILS

Vertraulichkeit der Daten

Durch eine ausreichend sichere Verschlüsselung der übertragenen Daten muss die Vertraulichkeit der übertragenen Daten gesichert werden. Auch bei einer Kompromittierung des Übertragungsweges, das heißt dem Abhören beziehungsweise Mitschneiden der zwischen Sender und Empfänger übertragenen Daten darf kein Rückschluss auf den Inhalt der übertragenen Daten möglich sein. Der Einsatz eines geeigneten Verschlüsselungsverfahrens und dazugehörigen Schlüsselmanagements mit regelmäßigem Wechsel des Schlüssels, oder besser des kompletten Verschlüsselungsverfahrens, ist dafür vorzusehen. Das Verschlüsselungsverfahren ist daher als eigenständiger IT-Service unabhängig von den Communication Services auszubringen.

Integrität der Daten

Bei der Übertragung von Daten muss durch den Einsatz geeigneter Übertragungsprotokolle sichergestellt werden, dass eine Erkennung von Datenveränderungen möglich ist und Verfälschungen der übertragenen Daten automatisch korrigiert werden können. Manipulationen von Daten auf dem Übertragungsweg durch Dritte müssen detektiert werden können. Um solche Manipulationen unmöglich zu machen, oder zumindest zu erschweren, sollten Daten nur signiert oder verschlüsselt übertragen werden. Dazu sind geeignete, entsprechend zertifizierte Systeme auf Sender- und Empfängerseite einzusetzen.

Authentizität der Daten

Neben der Integrität der Daten muss ebenfalls sichergestellt werden, dass die empfangenen Daten auch tatsächlich vom behaupteten Sender geschickt wurden, um sicherzustellen, dass die Kommunikation auch tatsächlich mit der beabsichtigen Gegenseite erfolgt. Dazu sind geeignete, entsprechend zertifizierte Systeme auf Sender- und Empfängerseite einzusetzen.

Nachvollziehbarkeit der Übertragung

Abhängig von der Einstufung der zu übertragenden Daten kann es notwendig sein die Übertragung zu protokollieren. Dazu sind Nachweise über den Ausgang von Daten auf Senderseite, ebenso wie Nachweise über den Eingang von Daten auf Empfängerseite notwendig. Diese Protokollinformationen sind in nicht manipulierbaren Systemen abzulegen, um eine nachträgliche Manipulation, auch durch Administratoren, zu verhindern.

Prüfung des Empfangs

Neben der Protokollierung des Ausgangs kann es notwendig sein, auch den Empfang auf der Gegenseite durch Quittungsmechanismen zu protokollieren. So kann nachgewiesen werden, dass Daten den adressierten Empfänger auch tatsächlich erreicht haben.

Verfügbarkeit von Übertragungswegen

Die Bedeutung von Übertragungswegen spielt eine Rolle bei der Festlegung der Verfügbarkeitsanforderungen des Übertragungsweges. Die bestmögliche Verfügbarkeit kann nur durch eine redundante Auslegung von Übertragungswegen mit unterschiedlichen Übertragungstechnologien sichergestellt werden. Diese müssen in Form einer Hot-Standby-Fähigkeit den sofortigen Wechsel von einem Übertragungsweg auf einen anderen ermöglichen. Für die diesen Übertragungsweg nutzenden Systeme muss der Wechsel des Übertragungswegs vollständig transparent erfolgen, also keine spezielle Behandlung im Falle des Ausfalls eines Übertragungsweges erfordern.

Systeme müssen gleichzeitig jederzeit damit umgehen können, dass der Übertragungsweg plötzlich nicht mehr zur Verfügung steht. Die Datenübertragungen sind in einem solchen Fall nach Möglichkeit zwischen zu speichern und nach Wiederherstellung der Verbindung nachzuholen.

Schmalbandige Übertragungswege

In einer militärischen Umgebung muss regelmäßig damit gerechnet werden, dass die Bandbreite von Übertragungswegen insgesamt gering oder zeitweise verringert ist. In der Auslegung von Systemen ist darauf zu achten, dass keine überflüssigen Daten übertragen werden. Es gilt das Prinzip der Datensparsamkeit. Bei jeder geplanten Datenübertragung ist zu berücksichtigen, dass diese einerseits Bandbreite auf dem Übertragungsweg, andererseits aber auch Systemleistung für die notwendigen Verschlüsselungsverfahren benötigt. Daher dürfen stets nur solche Daten übertragen werden, die auf der Empfängerseite für die Sicherstellung des geplanten Zweckes unbedingt erforderlich sind.

Schwankende Latenzen

Neben der Begrenzung in der Bandbreite ist regelmäßig mit hohen Latenzen in der Datenübertragung zu rechnen. Neben der Nutzung geeigneter Übertragungsprotokolle müssen auch auf Anwendungsebene entsprechende Vorkehrungen dafür getroffen werden, dass sich Nachrichten auf dem Übertragungsweg gegenseitig überholen, später gesendete Nachrichten also vor früher gesendeten eintreffen können. Die korrekte Behandlung auf Empfängerseite muss auch in diesem Fall sichergestellt sein. Hieraus ergeht eine direkt Forderung an die Latenzresistenz der im System ausgebrachten IT-Services (inkl. des Crypto Services).

5.3 REGISTRATUR

5.3.1 FUNKTIONALE FORDERUNGSBAUSTEINE

Die elektronische Registratur muss sicherstellen, dass klassifizierte Informationen gemäß den geltenden Vorschriften verarbeitet werden.

Die allgemeine Verwaltungsvorschrift des Bundesministeriums des Innern zum materiellen und organisatorischen Schutz von Verschlusssachen (Verschlusssachenanweisung VSA) setzt zusammen mit den Durchführungsbestimmungen einzelner Ressorts den Rahmen für die Behandlung von Verschlusssachen. Im Bereich der Bundeswehr dient die A-1130 als Durchführungsbestimmung, die im Schwerpunkt die Behandlung von physischer VS beschreibt. Die elektronische Registratur muss die nachfolgend aufgelisteten Gesetze bzw. Vorschriften erfüllen:

- VS-Anweisung – VSA (sofern nationale Einstufungsgrade abgebildet sind),
- A-1130/1 und A-1130/2 – Militärische Sicherheit in der Bundeswehr,
- A-960/1 – IT-Sicherheit in der Bundeswehr,
- Signatur-Gesetz – SigG,
- Vorgaben aus NATO/EU und anderen relevanten Bündnisorganisationen zum Umgang mit eingestuften Informationen in bündnisweiten Einsätzen.

Die elektronische Registratur hat primär das Ziel einer Nachweisführung gemäß den Anforderungen der geltenden Vorschriften. Es müssen alle Anwendungsfälle der VS-Bearbeitung im Nachweis festgehalten werden. Im Wesentlichen lassen sich die Anwendungsfälle wie folgt zusammenfassen:

- Vereinnahmung & Kenntnisnahme von klassifizierten Informationen,
- Informationsraumübergreifender elektronischer Austausch von klassifizierten Informationen (Anbindung Netzübergang),
- Anbindung/ Austausch mit der physischen Registratur,
- Vergabe bzw. Änderung des Geheimhaltungsgrades für ein Informationsobjekt,
- Löschen von elektronischen klassifizierten Informationen,
- Übergabe von Informationen bei mehreren zu integrierenden Sicherheitsdomänen.

Die Prozesse der elektronischen, wie auch der physischen Registratur müssen unterstützt werden. Dies muss in einer Form erfolgen, die für den Benutzer ein medienbruchfreies Zusammenarbeiten mit möglichst wenig zusätzlichem Aufwand ermöglicht.

Die elektronische Registratur übernimmt die Verwaltung klassifizierter Informationen in elektronischer Form und bietet einen Übergang zu einer physischen VS-Registratur an. Die Schnittstelle zwischen elektronischer und physischer VS-Registratur muss alle Prozesse (z.B. Vereinnahmung) in beiden „Welten“ unterstützen.

5.3.2 BESCHREIBUNG DES FUNKTIONALEN PROFILS

Die Registratur muss folgende Funktionen unterstützten:

- Verwaltung missionsbezogener Konfigurationen,
- Revisionssichere Speicherung klassifizierter Informationen,
- Nachweisführung,
- Auswertung (Audit),
- Separierung von Daten bei mehreren zu integrierenden Sicherheitsdomänen.

5.3.2.1 VERWALTUNG MISSIONSBEZOGENER KONFIGURATIONEN

Eine missionsbezogene Konfiguration dient zur Umsetzung funktionaler und sicherheitsrelevanter Prozesse in Bezug auf eine Zugriffssteuerung klassifizierter Informationen und Nachweisführung. Die genannten Aspekte sind kontextbezogen nachzuführen und durchzusetzen. Die missionsbezogene Konfiguration muss unterschiedliche Regulierungsaspekte unterstützen:

- Ermächtigungen des Nutzers (Clearances),
- Zugriffs-Paradigma „Kenntnis nur, wenn nötig“,
- Zugriffs-Paradigma „Responsibility to share“,
- Verwaltung von Wertevorräten mit VS-bezogenen Metadaten, die im Zusammenhang mit der Realisierung der VS-Registratur zur Anwendung kommen (Security Policy Information File, SPIF).

Ermächtigungen des Nutzers (Clearances)

Die Ermächtigung des Nutzers muss in der Registratur in elektronischer Form als Clearance abgebildet werden. Bei jeder Kenntnisnahme wird die Ermächtigung des Nutzers gegen die Einstufung des VS-Objektes abgeglichen. Nur wenn die Einstufung des Dokumentes zur Ermächtigung eines Nutzers passt, wird die Registratur nach Prüfung des Need-to-know ausliefern. Sollten diese Parameter nicht zusammen passen, erfolgt ein negativer Eintrag in der Nachweisführung.

Zugriffs-Paradigma „Kenntnis nur, wenn nötig“

Das Prinzip *„Kenntnis, nur wenn nötig“* (auch „Need-to-know“) beschreibt eine Zugriffs-Paradigma zur Verteilung klassifizierter Informationen. Als Ableitung dieses Grundsatzes ist der Kreis der Personen, denen klassifizierte Informationen zugänglich sind, auf das durch den Auftrag gegebene Minimum zu beschränken. Dies gilt allgemein, aber auch für jedes Dokument individuell. Darüber hinaus ist jeder, der klassifizierte Informationen weitergibt, verpflichtet zu prüfen, ob der Empfangende zur Annahme bzw. Kenntnisnahme berechtigt ist. Hier lässt sich ableiten, dass es dem Weitergebenden bzw. dem bereitstellenden System möglich sein muss, im Rahmen dieser Prüfung die Berechtigung des Empfängers zu prüfen. Die elektronische Registratur muss die Vergabe des Need-to-know auf drei unterschiedlichen Arten unterstützen:

- Zuweisung des Need-to-know an eine Person,
- Zuweisung des Need-to-know an berechtigte Mitglieder einer Organisationseinheit, sowie
- Zuweisung des Need-to-know an einen Inhaber eines Dienstpostens.

Zugriffs-Paradigma „Responsibility to share“

In einigen Anwendungsbereichen ist das *Prinzip „Kenntnis nur, wenn nötig“* für die benötigten Belange nicht anwendbar. Stattdessen wird oftmals das Zugriffs-Paradigma *„Responsibility to share – balanced with the principle of Need-to-know“* gefordert, das einen Paradigmenwechsel in der Zugriffskontrolle darstellt.

Dieses Prinzip verpflichtet stets zu prüfen, ob eine Information oder ein Service aufgrund einer Klassifizierung zugänglich gemacht werden darf – dann würde sie auf jeden Fall geteilt –, im Gegensatz zu der mit dem Need-to-know-Prinzip einhergehenden Prüfung, ob der Zugriff erlaubt und auch erforderlich ist.

Ziel des Prinzips „*Responsibility to share – balanced with the principle of Need-to-know*“ ist die Einsicht, dass der Empfängerkreis einer Information vom Ersteller vorab nicht abgeschätzt werden kann. Ein Zugriff muss deshalb von einer unbekannten, aber authentifizierbaren Menge möglich sein. Dies ist immer eng verbunden mit der Schaffung von Vertrauen in die Nutzer.

Security Policy Information File (SPIF)

Die in einem Informationsraum gültigen Einstufungen werden in einem Security Policy Information File (SPIF) verwaltet. In einem SPIF werden die Geheimhaltungsgrade und Kategorien definiert und deren Beziehungen untereinander beschrieben. Die SPIF für den missionsbezogenen Informationsraum stellt eine Grundlage für die Konfiguration eines sicheren Netzübergangs dar.

5.3.2.2 REVISIONSSICHERE SPEICHERUNG KLASSIFIZIERTER INFORMATIONEN

Informationen im System werden bewertet und im Anschluss mit einem Geheimhaltungsgrad, der von öffentlich bis in die höchsten zulässigen, nationalen und NATO/EU Geheimhaltungsgrade gehen kann, belegt. Der Nachweis des Geheimhaltungsgrades unterliegt in Verbindung mit dem Labelling der Registratur. Die Informationen müssen entsprechend des Geheimhaltungsgrades in einem „Datentopf“ gespeichert werden. Die Beschaffenheit eines „Datentopfes“ kann von einzelnen Dateien auf physisch getrennter Hardware bis hin zu Einträgen innerhalb einer Datenbank mit logisch getrennten Zugriffsrechten gehen. Die genaue Ausprägung ist zu untersuchen.

Eine revisionssichere Speicherung gewährleistet den lückenlosen Nachweis über den Informationsbestand der Registratur.

5.3.2.3 NACHWEISFÜHRUNG

Ein grundlegendes Sicherheitsziel ist die Nicht-Abstreitbarkeit bezüglich der Kenntnisnahme von klassifizierten Informationen und ausgeführten Handlungen. Im Schadensfall muss eine sichere Identifizierbarkeit des Akteurs möglich sein, der entweder die Kenntnis über vertrauliche Sachverhalte besitzt oder eine sicherheitsrelevante Operation ausgeführt hat. Der Einsatz von elektronischen Signaturen im Zuge jeglicher Handlungsausführung bildet dafür eine notwendige Bedingung, so dass operative Entscheidungen als Willensbekundung des Akteurs im Protokollsatz kryptografisch hinterlegt werden können. Die Integration von Security-Token mit vertrauenswürdigen Protokollierungseinheiten ist Aufgabe eines verteilten Identitätsmanagements in Verbindung mit zugelassenen Endgeräteklassen.

Jeder Protokolleintrag innerhalb der Nachweisführung enthält mindestens folgende Informationen.

- Wer? – Bediener,
- Was? – Informationsobjekt,
- Wann? – Zeitstempel,
- Wo? – Client / Drucker / etc.,
- Wie? – Druck / Export / Kenntnisnahme.

Es ist somit sichergestellt, dass jederzeit nachvollzogen werden kann,

a) wer zu einem bestimmten Zeitpunkt Kenntnis über eine Verschlusssache hatte,
b) was der Inhalt der Verschlusssache war, und
c) wer im Sinne des Need-to-know unberechtigt versucht hat, auf die Verschlusssache zuzugreifen.

Ein zweiter Aspekt der Nachweisführung bezieht sich auf einen Nachweis über den Informationsbestand innerhalb der Registratur. Über die Nachweisführung der Registratur lässt sich als Bestandsnachweis ein Katalog vereinnahmter, klassifizierter Informationen aufbauen.

5.3.2.4 AUSWERTUNG (AUDIT)

Im Rahmen der Nachweisführung werden die Handlungen von Akteuren zusammen mit anderen Kontextinformationen verwaltet. Für die Überprüfung der Nachweisdaten stellt die Registratur Prozesse bereit, die unter Anwendung kryptografischer Verfahren sowohl die Integrität als auch die Authentizität der Nachweisdaten gewährleisten.

Die gespeicherten Protokolldaten sind einer Nachweispolitik unterzogen und können nur durch autorisierte Personen oder Personengruppen zugänglich gemacht werden. Neben den Bestandnachweisen lassen sich zum Beispiel Übersichten zu Datenimporten, Datenexporten oder auch Quittungsbücher oder Vernichtungsprotokolle als Report abrufen.

5.3.2.5 SEPARIERUNG VON DATEN BEI MEHREREN ZU INTEGRIERENDEN SICHERHEITSDOMÄNEN

Grundsätzlich sollen gemäß der generellen Anforderungslage Sicherheitsdomänen, die Informationen des gleichen oder geringeren Schutzbedarfes beinhalten, in die funktionale IT-Sicherheitsarchitektur integriert werden können.

Die hierzu erforderliche Steuerung und Durchsetzung der erforderlichen Separierung der Daten getrennt nach Sicherheitsdomänen hat durch die elektronische Registratur zu erfolgen. Hierzu greift die VS-Registratur unter anderem mittels verschiedener Schlüssel auf den Crypto Service zurück, der die Verschlüsselung der Informationen auf dem Storage getrennt nach Sicherheitsdomänen übernimmt.

Zusätzlich muss die Registratur Domänenübergänge innerhalb der Sicherheitsarchitektur für entsprechend eingestufte Informationen ermöglichen, um übergreifende Informationsflüsse zu unterstützen. Die Umsetzung muss sowohl die manuelle, durch den Nutzer initiierte Übergabe von Informationen, als auch den automatischen Transfer auf Basis entsprechender Labels und Policies gewährleisten.

5.4 IDENTITY & ACCESS MANAGEMENT

5.4.1 QUERSCHNITTLICHE ANFORDERUNGEN

Zur Etablierung eines Identity & Access Managements wird eine zentrale Governance zur übergreifenden Festlegung einer entsprechenden Strategie, von globalen Festlegungen (z.B. einem Namenskonzept), von Entitäts- und Objektklassen, von Identitäten, Rollen und Rechten und Sicherheitsdomänen benötigt. Diese Governance ist in multinationalen Einsätzen mit allen beteiligten Nationen abzustimmen und dem CONOPS (Contingency Operations Plan – Operationsplanung) als verbindliche Vorgabe in Form eines IAM Konzeptes beizufügen.

5.4.2 FUNKTIONALE FORDERUNGSBAUSTEINE

Für ein funktionierendes Identity & Access Management im Sinne einer Sicherheitsarchitektur, die den operativen Anforderungen heutiger Einsätze entspricht, bedarf es der Einrichtung folgender Einzelbausteine:

- Identity Management Directory IAMDir,
- Enterprise Single Sign On,
- Flexibles Access Management,
- Provisionierung von Informationen,
- Self-Service Unterstützung,
- Public Key Infrastructure.

5.4.3 BESCHREIBUNG DES FUNKTIONALEN PROFILS

Das Identity & Access Management unterteilt sich in einzelne, funktionale Bausteine, die im Folgenden dargestellt sind.

Identity Management Directory IAMDir

Das IAMDir fungiert als Metadirectory des Identity Management. Hier werden alle im Kontext IAM definierten Entitäten und diesen zugeordnete Identitäten logisch zentral hinterlegt, konsolidiert und gepflegt.

Der Baustein IAMDir wird befähigt, die Festlegungen zu Identitäten aus dem IAM-Konzept, insbesondere Typen von Identitäten, deren Lebenszyklus und die an die Identität gebundenen Informationen (Attribute) gemäß der IAM Governance zu administrieren.

Angeschlossene Systeme werden über Workflows mit Identitäten und zugehörigen Informationen versorgt und verwaltet.

Das IAMDir muss in der Lage sein, Informationen mit Instanzen anderer Nationen bzw. sonstigen Einsatzpartnern auszutauschen, sowie entsprechende Anfragen von außerhalb des eigenen Systems zu verifizieren und zu beantworten.

Enterprise Single Sign On (ESSO)

Als Baustein des IAM wird eine Komponente für ein Enterprise Single Sign On (ESSO) unter Nutzung einer einheitlichen PKI implementiert (soweit möglich auf Basis einer einheitlichen Smartcard als einheitlicher Token zur starken Authentifizierung.). Das ESSO muss sich im Bedarfsfall auch auf andere Option A Affilates in Einsatznetzwerken (vgl. Federated Mission Networking (FMN der NATO) erstrecken oder zumindest mit anderen ESSO Entitäten von Missionspartnern synchronisierbar sein, sodass der Nutzer transparent im gesamten Einsatznetzwerk Zugriff auf die für seine Berechtigungsebene zur Verfügung stehenden IT-Services und Informationen enthält.

Rollen und Berechtigungen (Access Management)

Im IAM System werden durch so genanntes Role-Mining identische oder gleichartige Rollen zusammengefasst und definiert. Grundlage bildet das Rollen- und Berechtigungskonzept des IAM Konzeptes.

Dazu sind alle zu berücksichtigenden IT-Systeme, IT-Verfahren, Anwendungen und Datenquellen aus den Einsatzvorgaben abzuleiten. Abhängig vom Ergebnis geht davon eine Bereinigung der Daten einher. Für alle Daten ist die führende Datenquelle zu identifizieren. Für alle Entitäten sind Identitätsmerkmale zu definieren.

Angeschlossene Systeme erhalten diese Rollen und Berechtigungen für deren Aufgabenerledigung über definierte Workflows, die pro angeschlossenes System definiert und implementiert werden.

Rollen und Berechtigungen sind an wahrgenommenen Rollen bzw. Funktionen im Home Base Betrieb bzw. in „Mission Threads“ für Einsatzgebiete auszurichten. Durch Rollenwechsel muss ein Nutzer mit wenig Verzug für die Aufgabenwahrnehmung in einer neuen Funktion bzw. Rolle berechtigt werden können und Zugriff auf die für die neue Aufgabenwahrnehmung benötigten IT-Services und Informationen erhalten, unabhängig davon, ob sich die Rolle in Prozessen des Friedens- oder Einsatzbetriebes befindet.

Provisioning

Als zusätzliche Komponente zu einer filegesteuerten Bereitstellung und in Eigenverantwortung des angeschlossen Systems zu implementierenden Datenübernahme aus dem IAM, ist die Möglichkeit einer zeit- oder eventgesteuerten Provisionierung der Informationen über Identitäten, zugehörigen Informationen, Rollen und Berechtigungen in die angeschlossenen (Teil-)Systeme zu schaffen. Je nach angeschlossenem System oder der Anforderung kann dies in Echtzeit wie auch zeit- oder eventgesteuert erfolgen. Änderungen am angeschlossenen System werden erkannt und mit dem IAM synchronisiert.

Self-Service

Den Nutzern wird über ein Webportal die Möglichkeit der Abfrage ihrer Identitäten gegeben. Weiterhin können die Nutzer definierte Attribute pflegen. Hierzu gehören insbesondere die Passwortvergabe, sofern kein ESSO implementiert ist, und die Beantragungen und Freigabe von Rollen und Rechten sowie z. B. die Namensänderungen. Darüber hinaus wird den Administratoren von Identitäten, Rollen und Berechtigungen die Möglichkeit eines erweiterten Administratorenmodells im Sinne von delegierter Administration bereitgestellt.

5.4.4 PUBLIC KEY INFRASTRUCTURE

5.4.4.1 FUNKTIONALE FORDERUNGSBAUSTEINE

- Automatisierte Erneuerung von Zertifikaten vor ihrem Ablauf, dabei Möglichkeit zur Authentisierung mit bestehendem Zertifikat.
- Interoperabilität innerhalb der NATO.
- Als verlegefähige PKI autarke Ausgabe von Zertifikaten und Ausgabe von Sperrlisten oder OCSP-Antworten.
- Nutzung des EDTA auch im Einsatz, dabei – je nach verfügbarer Infrastruktur im Einsatzland – Spiegelung der Sperrinformationen der V-PKI in der Einsatz-PKI und lokale Verteilung über LDAP oder Bereitstellung eines lokalen OCSP- Service als lokalem Trust-Provider.

5.4.4.2 BESCHREIBUNG DES FUNKTIONALEN PROFILS

Die Public Key Infrastructure (PKI) ermöglicht die Zuordnung von Identitäten oder Rollen zu kryptografischen Schlüsseln. Eine der Komponenten einer PKI ist die Certification Authority (CA). Die CA signiert mit ihrem privaten Schlüssel das Zertifikat eines PKI-Teilnehmers. Dem geht eine Prüfung der Identität und der Zuordnung zum Schlüssel voraus. Weiterhin signiert sie Informationen zum Widerruf von Zertifikaten, die Zertifikatswiderrufslisten (CRL). Neben dem öffentlichen Schlüssel können im Zertifikat Informationen zur Identität sowie potenziell zu (gegebenenfalls rollenbasierten) Rechten enthalten sein.

Neben der eigentlichen Certification Authority (CA) gehören auch Komponenten zur Verteilung von Sperrinformationen (z.B. über LDAP Server oder OCSP Responder) zur PKI.

Zertifikate kodieren auch die Einsatzfelder (Key Usage) der Schlüssel; nach Stand der Technik werden Zertifikate Einsatzfeldern wie Verschlüsselung oder digitale Signatur eindeutig zugeordnet. Ebenso kann und sollte auch bei Verschlüsselungszertifikaten die Verwendbarkeit für die Verschlüsselung eingestufter Informationen im Zertifikat kodiert werden.

Aktuell steht die PKIBw zur Verfügung, die zum Teil Zertifikate aus der Verwaltungs-PKI heraus nutzt, zum Teil aber auch eine eigene Root-CA betreibt. Für Einsätze der Bundeswehr ist eine verlegefähige PKI notwendig, welche als Sub-CA der Bw-eigenen Root-CA betrieben werden kann. Es ist dabei sicherzustellen, dass

- Zertifikate für nicht-deutsche Teilnehmer bzw. Gateways ausgestellt werden können,
- im Einsatzland selbst Sperrinformationen erzeugt werden können, sowie
- eine Registrierung von Nutzern und anderen Entitäten im In- und Ausland erfolgen kann.

Aufgrund der Personalsituation in Einsätzen ist ein möglichst automatisierter Betrieb zu ermöglichen.

Grundsätzlich ist zu beachten, dass im Einsatz die Verfügbarkeit der notwendigen Bandbreite unter Umständen eine erhebliche Herausforderung darstellt. Ebenso ist eine Anbindung an zentrale Stellen in Deutschland gegebenenfalls eingeschränkt. Daher ist der Umfang der notwendigen Kommunikation bei der Nutzung der PKI möglichst gering zu halten, und die Funktionalität sollte auch bei rein lokaler Anbindung an die verlegefähige Einsatz-PKI weitestgehend erhalten bleiben.

(Gegebenenfalls rollenbasierte) Berechtigungen können in der PKI durch ergänzende Attribut-Zertifikate ausgestellt werden. Im Einsatz erscheint es sinnvoll, diese und andere Informationen auf sicherem Weg auf dem EDTA austauschen zu können. Dies könnte durch Nutzung von Sicherheitsmechanismen nach BSI TR-03110 in zukünftigen Versionen des EDTA ermöglicht werden; diese fortgeschrittenen Sicherheitsmechanismen werden zum Beispiel in deutschen hoheitlichen Dokumenten (ePA) eingesetzt, welches die sichere Änderung von Datengruppen auf dem EDTA gemäß spezifischer Terminal Berechtigungszertifikate im Feld erlaubt.

Ein Ansatz zur Anbindung einer Einsatz-PKI an die vorhandene Infrastruktur ist folgender:

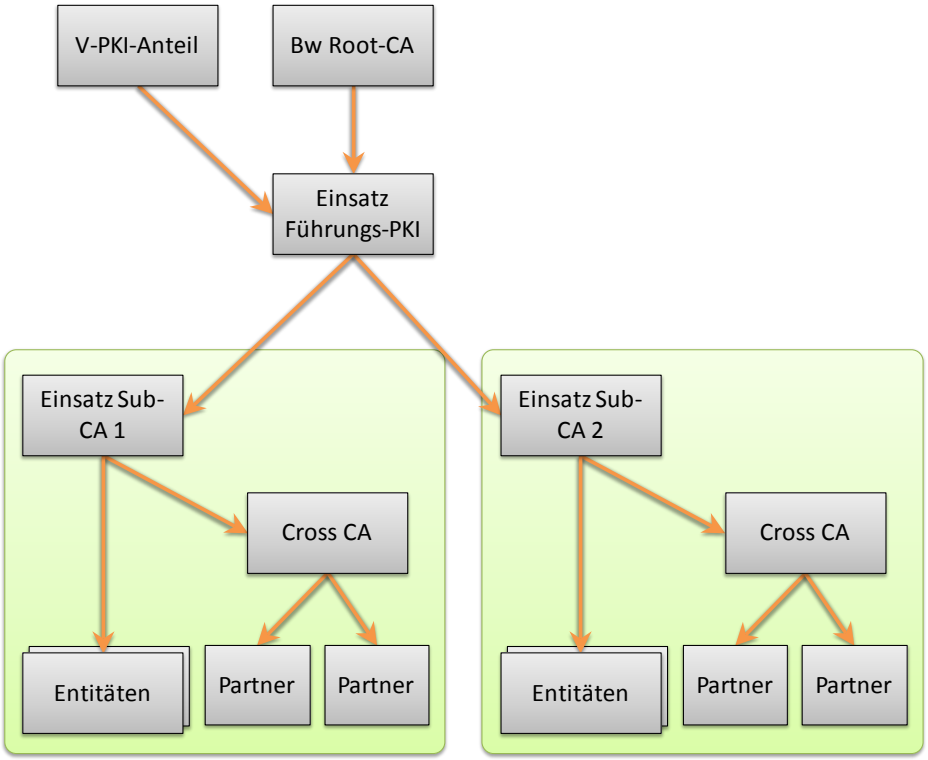

Abbildung 3: Anbindung einer Einsatz-PKI an die vorhandene Infrastruktur

Die Einsatz-PKI wird dabei durch V-PKI und die PKIBw zertifiziert. Diese stellt dann die Sub-CA-Zertifikate für die jeweiligen Einsätze aus. Neben den internen Aufgaben der Einsatz-Sub-CA (hier nicht im Detail dargestellt) können auch Zertifikate für Partner (NATO-Partner, aber gegebenenfalls z.B. auch NGOs) ausgestellt werden.

5.5 CRYPTOSERVICE

5.5.1 FUNKTIONALE FORDERUNGSBAUSTEINE

- Zugriff auf den Cryptoservice über eine definierte Schnittstelle. Diese Schnittstelle muss ebenfalls kryptographisch abgesichert werden. Beide Module müssen sich an dieser Schnittstelle gegenseitig sicher authentifizieren können.
- Unterstützung der Verschlüsselung von Daten bei der Informationsübertragung, bei der Informationsverarbeitung und -speicherung durch die VS-Registratur.
- Skalierbare Ausprägung
- Verwendung möglichst quelloffener Bibliotheken
- Abstützung auf softwarebasierte Verschlüsselung wo immer möglich
- Anbindung eines physikalischen Zufallsgenerators
- Modularisierte Einbindung von Pseudozufallsgeneratoren
- Unterstützung mehrerer asymmetrischer Verfahren und Auswahl der Algorithmen entlang der „Suite B“ des NSA
- Migrationsfähigkeit auf neue kryptographische Verfahren und Schlüssellängen

5.5.2 TECHNISCHE FORDERUNGSBAUSTEINE

Der Cryptoservice muss mindestens folgende symmetrischen Blockchiffren unterstützen:

- AES-128
- AES-192
- AES-256
- AES-384

Triple-DES gilt als zukünftig nicht mehr ausreichend sicher und sollte daher vom Cryptoservice nicht verwendet werden. Als Betriebsmodi für diese Blockchiffren kommen Cipher-Block Chaining (CBC), Counter Mode (CTR), sowie der Galois-Counter-Mode (GCM) in Betracht.

Der Cryptoservice muss folgende asymmetrischen Kryptoalgorithmen unterstützen:

- RSA mit einer Schlüssellänge von mindestens 2048 Bit
- ECIES mit einer Schlüssellänge von mindestens 256 Bit (optional)
- DLIES mit einer Schlüssellänge von mindestens 2048 Bit (optional)

Der Cryptoservice muss folgende Hashfunktionen unterstützen:

- SHA2 mit mindestens 256 Bit
- SHA3

Die Hash-Funktionen MD5 und SHA1 gelten als nicht mehr ausreichend kollisionsresistent und sollten daher vom Cryptoservice nicht verwendet werden.

Der Cryptoservice muss so ausgelegt werden, dass sich jederzeit neue kryptographische Verfahren und Schlüssellängen modular integrieren lassen.

Wenn der Cryptoservice symmetrische Schlüssel nicht nur zur Verschlüsselung, sondern auch zur symmetrischen Datenauthentisierung verwendet, so muss sichergestellt sein, dass es sich um verschiedene, nicht voneinander ableitbare Schlüssel handelt. Eine Ausnahme hiervon bildet der GCM-Mode, bei dem eine implizite Datenauthentisierung stattfindet.

5.5.3 BESCHREIBUNG DES FUNKTIONALEN PROFILS

Der Cryptoservice ist hinsichtlich

1. der zu erwartenden Informationsdichte,
2. des zu erwartenden Risikoprofils, und
3. des Schutzbedarfs der Informationen

einsatz- und ebenengerecht innerhalb eines Einsatznetzwerkes individuell auszulegen. Dabei muss die Stärke der gewählten Verschlüsselung dem Informationsgefälle in Richtung der taktischen Ebene Rechnung tragen, um den „Spagat“ zwischen steigenden Interoperabilitätsanforderungen in Richtung der taktischen Ebene, limitierter Hardware, Hardwareinhomogenität bei vorhandenem Appliances (insbesondere im Bereich der Communication Services), und der Schnelllebigkeit des operativen Anforderungsprofils berücksichtigen.

Der Zugriff auf den Cryptoservice sollte wo sinnvoll über das Identity & Access Management erfolgen, da hier sowohl symmetrische Schlüssel als auch asymmetrische Schlüssel zur sicheren Authentifizierung verwendet werden und eine zentrale Schlüsselablage gewährleistet wird. Diese Schnittstelle muss es ermöglichen, dass der symmetrische Schlüssel zur Wirkverschlüsselung überschlüsselt mit einem oder mehreren asymmetrischen, öffentlichen Schlüsseln aus dem Modul Identity & Access Management zusammen mit der kryptierten Information abgelegt werden kann.

Um Interoperabilität im Koalitionsrahmen unterstützen zu können, sollte sich die Auswahl der Algorithmen an den „Suite B“ Empfehlungen des NSA orientieren. Mehrere asymmetrische Verfahren zur Verschlüsselung sollten unterstützt werden.

Um sowohl aktuellen als auch künftigen Anforderungen gerecht zu werden, sollte der Cryptoservice über eine ausreichende Skalierbarkeit verfügen und modular aufgebaut sein.

Hierdurch sind das Hinzufügen von weiterer geeigneter Hardware und die Integration von neuen kryptographischen Verfahren und neuen Schlüssellängen möglich.

Zudem muss der Crypto Service neben der Absicherung von Informationen im Rahmen der Informationsübertragung auch eine Absicherung der Informationen auf Datenspeichern erlauben und somit das Back End der IT-Services schützen. Dabei hat der Crypto Service ebenfalls unterschiedliche Hardware seitige Voraussetzungen in Abhängigkeit seiner Einsatzumgebung (Bsp. Mobile Endgeräte) zu berücksichtigen und muss entsprechend adaptierbar sein.

Grundsätzlich sind die verwendeten privaten Schlüssel vor Missbrauch und Verlust zu schützen. Das höchste Schutzniveau bieten dabei dedizierte Hardware-Security-Module (HSM). Für Umsetzungen in Software werden durch die Verwendung von geeigneten quelloffenen Bibliotheken Risiken (z.B. Seitenkanalattacken, Implementierungsfehler oder Einsatz von Pseudozufallsgeneratoren, PRNG) minimiert. Eine Schnittstelle zur Anbindung eines physikalischen Zufallsgenerators sollte verfügbar sein.

Falls ein Pseudozufallsgenerator (PRNG) eingesetzt wird, so ist zum einen durch zusätzliche Maßnahmen sicherzustellen, dass dieser stets über genügend Entropie verfügt, zum anderen ist dieser PRNG so als Modul zu implementieren, dass er bei Verfügbarkeit besserer Algorithmen oder auch bei Bekanntwerden von Designschwächen jederzeit ausgetauscht werden kann.

Die symmetrischen Schlüssel sollten entweder zur Verschlüsselung oder zur symmetrischen Datenauthentifizierung verwendet werden. Eine Mehrfachnutzung ist zu vermeiden. Gleiches gilt für asymmetrische Schlüssel, die möglichst einer Funktion (Signatur, Verschlüsselung) sowie einem Protokoll

(z.B. RSASSA_PKCS#1 v1.5 oder RSASSA_PSS) zugeordnet sein sollten, sofern nicht organisatorische Gründe dagegen sprechen.

Sofern das Identity & Access Management zum Zugriff auf den Crypto-Service im Einsatz auf den eDTA zur Nutzer-Authentifizierung zurückgreift, sollte für zukünftige Versionen des EDTA die Verwendung fortgeschrittener Sicherheitsprotokolle angelehnt an die technische Richtlinie BSI TR-03110 geprüft werden. Hiermit lassen sich Informationen (wie Rollenzuordnungen, Berechtigungen oder entsprechende Attributzertifikate) im Feld durch einen sicheren Kanal zwischen eDTA und lokaler Infrastruktur ergänzen, ohne dass der eDTA hierzu zu einer Registrierungsstelle gebracht werden muss.

Der Overhead des Cryptoservices in Bezug auf Latenz und Bandbreitenbedarf muss ebenfalls mit der zu erwartenden Einsatzumgebung skalieren. Insbesondere in taktischen Umgebungen mit Communication Services, die reduzierte Kapazitäten aufweisen, muss der Crypto Service wenig „overhead“ produzieren. Gleiches gilt für den Anwendungsfall der Informationsverschlüsselung auf Storage Ebene, auf der die zusätzliche Latenz nicht die Leistungserbringung des IT-Services beeinträchtigen darf.

Der Cryptoservice muss Schnittstellen zum Identity & Access Management, dem IT-Service Profil, dem Systemzugang und den Endgeräteprofilen vorsehen.

5.5.3.1 VERSCHLÜSSELUNG AUF APPLIKATIONSEBENE

Die Verschlüsselung auf Applikationsebene verfolgt die Zielstellung, die Vertraulichkeit von Informationen auf Prozessebene abzusichern. Sie ist unabhängig von Verschlüsselungsmechanismen der Transportebene und erlaubt den Schutz von Informationsobjekten mit Mitteln der Kryptografie als eine erweiterte Form der Zugriffssteuerung.

Benutzerautorisierung auf Basis von Objektschlüsseln

Die Autorisierung für ein Informationsobjekt erfolgt durch die Vergabe eines kryptografischen Schlüssels, der genau einem Informationsobjekt zugeordnet ist. Der kryptografische Schlüssel wird als *Objektschlüssel* bezeichnet. Subjekte, die im Besitz des *Objektschlüssels* sind, erhalten den Zugriff auf das entsprechende Informationsobjekt.

Der Besitz eines *Objektschlüssels* stellt eine notwendige Bedingung dar, um den Inhalt einer vertraulichen Information lesen zu können. Diese Bedingung muss jedoch nicht hinreichend sein, wenn der Aspekt berücksichtigt wird, dass die Vergabe von Zugriffsrechten im militärischem Bereich unterschiedlichen Prinzipien der Informationsverteilung folgen muss (Need-to-Share, Need-to-Know).

Die Verschlüsselung auf Applikationsebene erweitert die Konzepte zur kryptografischen Schlüsselverwaltung. Die Erzeugung von *Objektschlüsseln* und die Verschlüsselung von Informationsobjekten über den Cryptoservice gestalten sich als Teil der operativen Erzeugung und Verteilung von Informationen. *Objektschlüssel* sind symmetrische Schlüssel und dienen der blockweisen Verschlüsselung (z.B. AES-256 im Cipher Block Chaining Mode) von Dateien, unabhängig von ihrem konkreten Dateiformat.

Das Kryptokonzept für die Verschlüsselung auf Applikationsebene setzt voraus, dass alle beteiligten Akteure innerhalb der Informationsdomäne im Besitz eines benutzerbezogenen privaten Schlüssels sind (Hardware- oder Softwaretoken).

Die Erzeugung und Verteilung von Schlüsselpaaren für Akteur-Identitäten ist Aufgabe des Cryptoservice im Zusammenspiel mit einer PKI Lösung und dem Identitäts-Management. Das Identitäts-Management ist für die sichere Zuordnung und Bereitstellung der zugehörigen Public-Keys für Akteur-Identitäten zuständig.

Verteilungsprozesse auf Applikationsebene

Im Bereich der Vertraulichkeit werden die Prinzipien „Kenntnis nur, wenn nötig" *(Need-to-Know*) oder „Kenntnis an eine Gruppe, dass ein Informationsobjekt existiert“ (*Need-to-Share*) diskutiert. Für beide Prinzipien gilt, dass eine hinreichende Bedingung erst durch einen der Kryptografie nachgelagerten Prozess geschaffen wird, um in den Besitz des *Objektschlüssels* zu kommen.

Für die Umsetzung z.B. des Prinzips „Kenntnis nur, wenn nötig" wird eine auf den Akteur zurückführbare Willensbekundung eingefordert. Erst im Fall einer Zustimmung gelangt ein Akteur nachweislich in den Besitz eines *Objektschlüssels*. Diese Vorgehensweise dient dem Sicherheitsziel einer nicht abstreitbaren Kenntnisnahme.

Für die Verteilung eines Informationsobjektes wird der zugehörige *Objektschlüssel* mit dem öffentlichen Schlüssel des adressierten Empfängers (Public-Key des ausgewählten Akteurs) durch den Cryptoservice asymmetrisch verschlüsselt.

Der öffentliche Schlüssel kann über eine Schnittstelle des Identity Managements abgerufen werden. Die nachgelagerten Verteilungsprinzipien entscheiden darüber, wie der verschlüsselte *Objektschlüssel* in den Besitz des entsprechenden Akteurs (Subjekt) gelangt.

Im Prozess der Informationsverteilung können autorisierte Akteure unter Verwendung ihres privaten Schlüssels den für sie bereitgestellten verschlüsselten *Objektschlüssel* unter eigener Kontrolle entschlüsseln.
Der *Objektschlüssel* wird gesichert an den Cryptoservice übermittelt, der das entsprechende Informationsobjekt im Auftrag des Akteurs anschließend entschlüsselt.

5.6 LABELLING

5.6.1 FUNKTIONALE FORDERUNGSBAUSTEINE

Der Funktionsbaustein Labelling muss einen Service liefern, der das Kennzeichnen von digitalen Informationsobjekten mit VS-bezogenen Metainformationen ermöglicht. Die so digital gekennzeichneten Informationsobjekte schaffen eine Grundlage für die elektronische VS-Verwaltung und Nachweisführung sowie zur Prüfung am Netzübergang.

5.6.2 BESCHREIBUNG DES FUNKTIONALEN PROFILS

Unter Labelling ist das Kennzeichnen von digitalen Informationsobjekten mit VS-bezogenen Metainformationen zu verstehen. Es schafft eine Grundlage für die elektronische VS-Verwaltung und Nachweisführung. Es ermöglicht die Zugriffskontrolle für unterschiedlich berechtigte Bediener durch Vergleich von Security Label und persönlicher Identifizierung des Bedieners. Darüber hinaus dienen Security Labels zur Prüfung am Netzübergang, ob die Weiterleitung in einen anderen Informationsraum erlaubt ist.

Unter Verwendung von Security Labels ist eine automatische Filterung von gelabelten Informationsobjekten am Netzübergang möglich. Nach einer Gültigkeitsprüfung der digitalen Signatur entscheidet der Netzübergang anhand des Geheimhaltungsgrads und ggf. weiterer im Label enthaltener Warn- und Zusatzvermerke (Metadaten) sowie der am Netzübergang gültigen Security Policy über die Weiterleitung in einen anderen Informationsraum.

Die von einem Labelling Service erzeugten Security Labels müssen der NATO Spezifikation IST-068/RTG-031 entsprechen. Zukünftig sind die sich im Standardisierungsprozess der NATO befindlichen STANAGs 4774 und 4778 zu berücksichtigen.

Der Labelling Service muss nach Common Criteria gegen das Nationale Schutzprofil Labelling (NPP Labelling) evaluiert sein. Auf dieser Basis muss für den einzusetzenden Labelling Service ein projektbezogener Zulassungsantrag beim BSI gestellt werden.

Je nach Menge von verschiedenen „neuen“ Informationen, muss die Performance des Labelling Services sehr hoch sein. Hierzu muss der Labelling Service in der Lage sein zu skalieren, z.B. mittels Aufbau und Erweiterung eines Clustersystems.

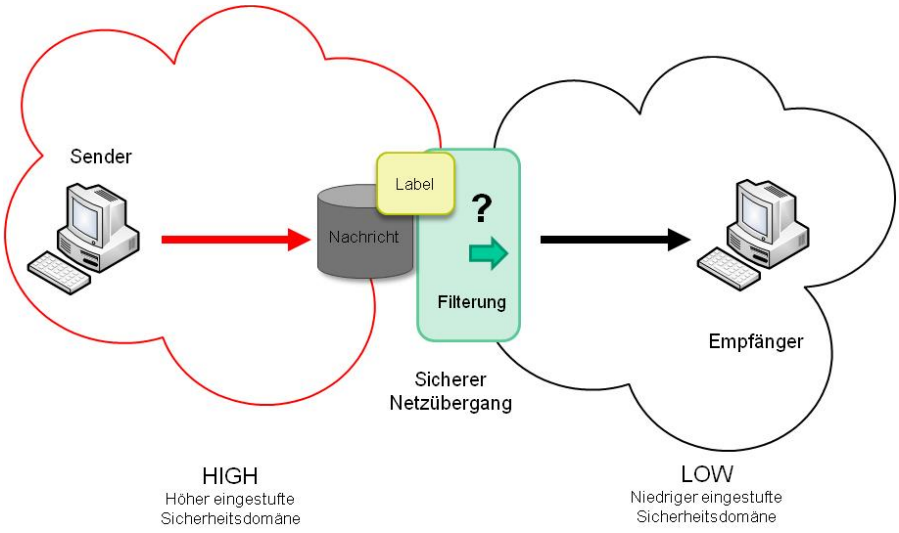

Abbildung 4: Informationsflusskontrolle anhand von Security Labels

Beim Labelling wird zwischen verschiedenen Binding-Möglichkeiten unterschieden. Die gängigste Art ist das sog. Detached Binding, bei dem der Labelling-Service für jeweils ein Informationsobjekt ein XML Security Label als separate Datei erzeugt. Das XML Security Label basiert stets auf den VS-bezogenen Metainformationen des jeweiligen Informationsobjektes und ist über eine digitale Signatur sicher an das Informationsobjekt gebunden, sodass die Integrität und Authentizität der Daten gewährleistet ist.

Die VS-bezogenen Metadaten müssen auf Basis eines im Labelling Service konfigurierbaren Wertevorrates erzeugt werden können. Beim Aufruf des Labelling-Service muss die jeweils anzuwendende Security Policy über einen entsprechenden Parameter (Security Policy ID) vorgegeben werden. Die über diesen Parameter referenzierte SPIF-Datei (Security Policy Information File) muss flexibel konfigurierbar sein.

Der Labelling Service muss die Attribute eines Security Labels eines gelabelten Informationsobjektes auslesen können. Dabei wird die Integrität und Gültigkeit des Security Labels durch Verifizierung der digitalen Signatur und Validierung gegen vorgesehene Security Policies (XML SPIF) geprüft.

Mit dem Begriff Informationsobjekt wird im Folgenden das zu labelnde Objekt als Träger von (potenziell vertraulichen) Informationen bezeichnet. Hierbei werden die folgenden Klassen von Informationsobjekten unterschieden:

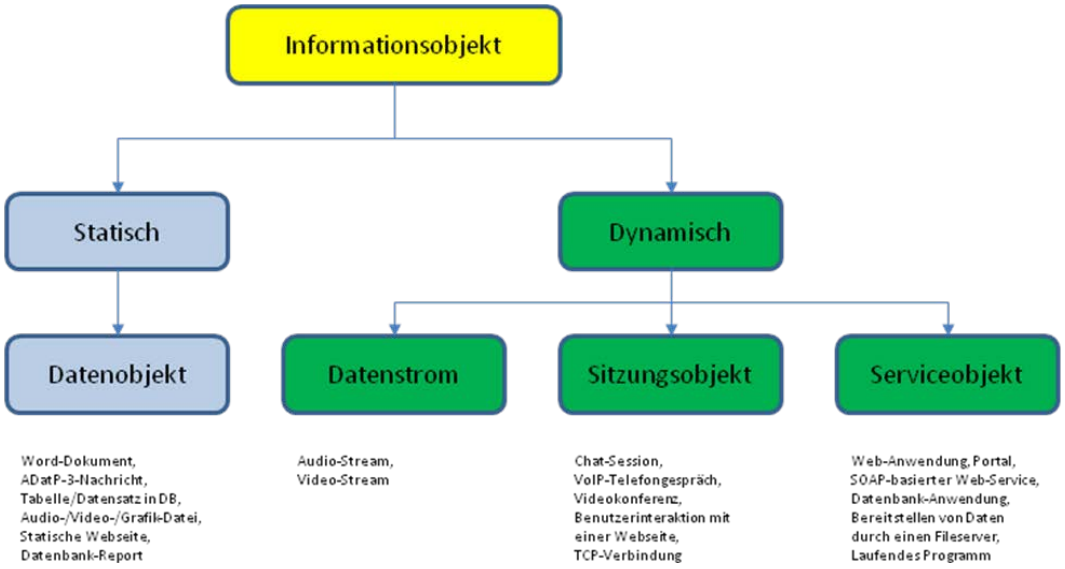

Abbildung 5: Klassen von Informationsobjekten

5.6.2.1 LABELLING VON STATISCHEN INFORMATIONSOBJEKTEN

Bei statischen Informationsobjekten handelt es sich um Informationsobjekte, die zum Zeitpunkt des Labelling-Vorgangs in ihrer endgültigen Form vorliegen. Nach der in Abbildung 5 angegebenen Klassifizierung ist bei statischen Informationsobjekten ausschließlich die Klasse der Datenobjekte zu betrachten. Ein statisches Datenobjekt ist eine abgegrenzte Menge von digitalen Daten, die mit einem Label versehen werden soll. Im Rahmen der NATO Labelling-Dokumentation wird dies auch als finite Informationsobjekte bezeichnet.

Die Inhalte des Datenobjekts liegen zum Labelling-Zeitpunkt vollständig vor, so dass alle enthaltenen Daten bei der Labelling-Entscheidung berücksichtigt werden können. Nachträgliche Änderungen sind hierbei nicht ausgeschlossen; sie führen jedoch zu einer neuen Version des Datenobjekts, die dann wiederum neu zu labeln ist.

5.6.2.2 LABELLING VON DYNAMISCHEN INFORMATIONSOBJEKTEN

Bei dynamischen Informationsobjekten handelt es sich um Informationsobjekte, die zum Zeitpunkt des Labelling-Vorgangs nicht in ihrer endgültigen Form vorliegen. Um dynamische Informationsobjekte zu labeln sind folgend beschriebene Schritte notwendig, die allerdings derzeit noch von keinem marktverfügbaren Produkt unterstützt werden:

1. Labelling der Datenquelle

   Da die Daten eines dynamischen Informationsobjektes fließend sind und nicht in abgeschlossener Form zur Verfügung stehen, bietet es sich an, zunächst die Datenquelle des dynamischen Informationsobjekts zu labeln, also bei Datenströmen die Quelle, bei Sitzungsobjekten die Sitzung und bei Serviceobjekten den Service. Die identifizierenden Merkmale der Datenquelle werden im Security Label gespeichert und mit einer digitalen Signatur versehen (sichere Bindung des Security Label an die Datenquelle). Die Datenquelle wird dabei vorab mit der höchsten im Anwendungsfall denkbaren VS-Einstufung versehen (SYSTEM HIGH-Prinzip). Dieses Security Label kann anschließend verwendet werden, um z.B. die implizite Zuordnung der VS-Einstufung aus dem Security Label zu dem betreffenden dynamischen Informationsobjekt zu nutzen.

2. Hybrides Labelling-Verfahren

   Bei dem hybriden Labelling-Verfahren werden die dynamischen Informationsobjekte (Datenstrom, Sitzungsobjekt, Serviceobjekt) zeitlich oder volumenbezogen partitioniert und die entstehenden Segmente einzeln gespeichert. Der eigentlich transiente Datenfluss wird somit segmentweise persistiert.

   Die einzelnen Segmente stellen abgeschlossene Datenobjekte dar, d.h. statische Informationsobjekte, auf die das statische Labelling-Verfahren anwendbar ist. Bei einem automatischen Labelling-Verfahren kann dabei auf das Security Label der Datenquelle zurückgegriffen werden, also insbesondere Übernahme der VS-Einstufung beim Labelling (siehe oben).

   Alle weiteren Schritte (Speicherung der gelabelten Daten inkl. Security Label sowie Übertragung über den sicheren Netzübergang) können damit grundsätzlich analog zur Behandlung statischer Informationsobjekte durchgeführt werden.

   Die folgenden Randbedingungen sind bei der Anwendung eines hybriden Labelling-Verfahrens zu beachten:

   - Die durch die zeitliche oder volumenbezogene Partitionierung hervorgerufene Verzögerung der Datenverfügbarkeit muss bei der betreffenden Datenquelle in operativ akzeptablen Grenzen liegen.
   - Die Nutzbarkeit der Daten darf durch die Partitionierung nicht erschwert oder sogar verhindert werden. Alternativ muss die Partitionierung vor der Nutzung wieder rückgängig gemacht werden und das ursprüngliche Informationsobjekt wiederhergestellt werden.
   - Für jedes relevante Datenstromformat/ Kommunikationsprotokoll muss ein (vermutlich) spezifischer Daten-Partitioner verfügbar sein.
   - Der Daten-Partitioner muss den Labelling-Service verwenden, um jedes abgeschlossene Segment automatisch mit einem Security Label zu versehen.

Das hybride Labelling-Verfahren ist einfacher umzusetzen als andere, theoretisch denkbare Ansätze für das dynamische Labeln von Informationsobjekten, da dieses Verfahren sich enger an das bereits umgesetzte Labelling von statischen Informationsobjekten anlehnt.

Aufgrund der Vielzahl unterschiedlicher Datenstromformate, Kommunikationsprotokolle und Datenraten ist zu erwarten, dass für jede Klasse dynamischer Informationsobjekte spezifische Umsetzungen pro Anwendung erforderlich sein werden. Insbesondere sind dabei Abhängigkeiten der Partitionierung und des Streaming von Datenstromformaten, Kommunikationsprotokollen und Datenraten zu beachten. Folglich müssen die operativ relevanten Anwendungen in diesen Punkten noch detaillierter analysiert werden.

5.7 INTRUSION DETECTION SYSTEM

5.7.1 FUNKTIONALE FORDERUNGSBAUSTEINE

Ein IDS (Intrusion Detection System) ist ein Gerät oder eine Software-Anwendung, die einen Administrator im Falle einer Security- oder Policy-Verletzung benachrichtigt. Das System wird auch aktiv, sollte das administrierte IT-Netzwerk in irgendeiner anderen Form kompromittiert sein.

Das IDS überwacht und analysiert die Aktivitäten in einem Netzwerk. Weiterhin werden die Konfigurationen und Schwachstellen analysiert und die Datei-Integrität bewertet. IDS können typische Angriffs-Muster erkennen, abnormale Aktivitäts-Muster analysieren und Verletzungen der Anwender-Policies identifizieren.

IDS-Produkte der Enterprise-Klasse sind üblicherweise auch in der Lage, auf entdeckte Bedrohungen zu reagieren.

Ein IDS folgt in der Regel einem zweistufigen Prozess. Der erste, passive Schritt ist Host-basiert. Das System inspiziert die Konfigurations-Dateien des Netzwerks, um nicht zu empfehlende Einstellungen und Policy-Verletzungen zu erkennen. Der zweite, aktive Schritt ist Netzwerk-basiert. In diesem Schritt stellt das System Angriffs-Methoden nach und zeichnet die Reaktionen auf, um im Angriffsfall schnelle Reaktionen sicherzustellen. Das IDS muss den gesamten relevanten Datenverkehr echtzeitnah auch unter Hochlast erfassen, analysieren und ggf. zur späteren Analyse speichern können. Da die Bandbreiten im Sicherheitskernel skalierbar sein müssen, muss auch das System die Möglichkeit einer entsprechenden Skalierung bieten.

5.7.2 BESCHREIBUNG DES FUNKTIONALEN PROFILS

Das IDS unterstützt verschiedene Erkennungsverfahren, so insbesondere:

- Mustervergleich für Netzpakete (Pattern Matching),
- Abweichen von Normalprofilen für Verkehrsparameter (Traffic-based Anomaly Detection).

Es bietet die Möglichkeit, Normalprofile durch Verkehrsflussanalyse über einen bestimmten Zeitraum zu „erlernen“. Da sich das Verkehrsprofil einsatzbezogen ändern kann, muss es möglich sein, zwischen verschiedenen Normalprofilen zu wechseln, so dass auch einsatzbezogene Normalprofile erstellt werden können. Weiterhin muss sich die Traffic-based Anomaly Detection auch komplett abschalten lassen, ohne dass dadurch die Funktionalität des IDS beim Mustervergleich beeinträchtigt wird. Für die Paketanalyse sind mindestens die aktuell für netzbasierte IDS/IPS marktgängig vorhandenen technischen Möglichkeiten zu unterstützen, z.B.

- Erfassung und Analyse von IPv4- und IPv6-spezifischem Verkehr,
- Erkennung von paketübergreifenden Angriffen (durch intelligente Reassemblierung der höheren Protokollebenen),
- protokollabhängige Analyse der Datenpakete auf Layer 3 bis Layer 7.

Die Signaturdatenbasis muss hinsichtlich der Erkennungsleistung dem aktuellen Stand der Technik entsprechen und folgenden Anforderungen genügen:

- Die Signaturdatenbasis muss sich jederzeit durch Signaturen für neu bekanntgewordene Schwachstellen ergänzen lassen.
- Die Signaturdatenbasis muss sich auch um frei definierbare Signaturen ergänzen lassen.

In der Signaturdatenbasis enthaltene Referenzen speichern die Herkunft der jeweiligen Signatur sowie die mit ihr assoziierten Angriffen und Schwachstellen. Dort enthalten sind Referenzen auf einen (geschätzten) relativen Schweregrad (Severity) bei erfolgreichem Angriff, auf konkrete Voraussetzungen für einen erfolgreichen Angriff (z.B. Software-Versionen, Patch-Stände) und auf Informationen zu Gründen für mögliche Falschmeldungen (False Positives), um die indizierten Ereignismeldungen und damit die Sicherheitslage besser bewerten zu können.

Das IDS muss auch offline (d.h. ohne jegliche Verbindung zu einer zentralen Signaturbasis) mit hinreichendem Funktionsumfang betrieben werden können. Dazu muss das IDS auch durch ein Offline-Update, d.h. durch authentisiertes, verschlüsseltes und integritätsgeschütztes Herunterladen von Signaturen und Konfigurationsparametern, Anwendungssoftware- und Betriebssystem-Patches, Überprüfung von Authentisierungs- und Integritätsparametern und Einbringen über Datenträger jeweils auf den neuesten Stand gebracht werden können.

Bei allen Signaturübereinstimmungen sowie Unter-/ Überschreitungen von Schwellenwerten für die Anomalie-erkennung erfolgen folgende Aktionen:

- Ereignismeldungen (Security Information Event Messages) erzeugen,
- unter einstellbaren Bedingungen Alarmierungsfunktionen aktivieren (z.B. E-Mail, SMS, Pager),

- Ereignismeldungen sowie relevante ursächliche Rohdaten (Verkehrsmitschnitte) einschließlich Nutzlast (Payload) in konfigurierbarem Umfang und für einen konfigurierbaren Zeitraum für eine spätere Analyse zwischenspeichern sowie
- an optionale weitere Analysekomponenten (z.B. ein SIEM-System) in offenen bzw. standardisierten Formaten (z.B. Syslog) weiterleiten können.

Die Ereignismeldungen müssen mindestens folgende Informationen beinhalten:

- Datum und Uhrzeit,
- Quelladresse oder -netz,
- Zieladresse oder -netz,
- Protokolle (Ebenen 2-4),
- Assoziierter Dienst bzw. Anwendung,
- Kategorisierung und geschätzter Schweregrad des Angriffs,
- Grundlage, auf der ein Angriff identifiziert wurde (bspw. Signatur, Anomalie).

Über eine mittels Rollen- und Berechtigungskonzept zugriffsgeschützte grafische Benutzerschnittstelle (GUI) werden die wesentlichen Betriebsparameter des Systems intuitiv dargestellt und die Konfiguration der Signaturdatenbasis und andere Laufzeitparameter erlaubt.

Die GUI unterstützt eine interaktive Analyse der mit Angriffen assoziierten, temporär gespeicherten Rohdaten. Das kann z.B. durch kontextsensitive Browsing-Funktionen geschehen, die zu Ereignismeldungen entsprechenden Meldungsbestandteile sowie relevante Zusatzinformationen (z.B. Statistiken über das Vorkommen in der Datenbank, korrespondierende DNS-Einträge und Who is-Records) auf Anforderung ein- und ausblenden können. Aus den protokollierten Ereignismeldungen können Berichte (Reports) mit statistischen Kennzahlen für entsprechende Zeitperioden generieren werden.

Die auf dem IDS erhobenen und zwischengespeicherten Verkehrsdaten sowie weitere personenbezogene oder -beziehbare Informationen müssen entsprechend den geltenden Bestimmungen zum Datenschutz behandelt werden. Dazu gehört die automatisierte Löschung nach einem konfigurierbaren Zeitraum.

Das IDS muss an einen zentralen NTP-Dienst angeschlossen sein und darüber seine Systemzeit synchronisieren.

5.8 SERVICE MANAGEMENT

Die innerhalb der funktionalen IT-Sicherheitsarchitektur ausgebrachten bzw. adressierten Bausteine haben sich in ein ganzheitliches IT-Service Management zu integrieren, der sowohl die Anteile der Architektur als auch andere IT-Services/-Systeme eines Einsatznetzwerkes umfasst. Dieser ganzheitliche Ansatz liegt allerdings außerhalb des Geltungsbereichs dieses Dokumentes, so dass im Folgenden nur die für die Sicherheitsarchitektur relevanten Anforderungen in Form eines System Management Anteils beschrieben werden.

5.8.1 FUNKTIONALE FORDERUNGSBAUSTEINE

- Aufbau eines zentralen System Managements mit der Möglichkeit Events, Incidents und Requests aus unterschiedlichen Sicherheitsdomänen automatisiert zusammenführen zu können, sodass eine zentrale Bearbeitung stattfinden kann.
- Zentrales System Management kann sowohl innerhalb der missionsbezogenen Sicherheitsdomäne als auch alternativ im Reach Back-Element im Heimatland angesiedelt sein.
- Das Systemmanagement für nationale Anteile an multinationalen Einsatznetzwerken muss in der Lage sein, strukturierte Informationen über Schnittstellen anderen System Management Entitäten bereit zu stellen und Informationen von diesen zu empfangen und zu verarbeiten.
- Das System Management liefert ein standardisiertes betriebliches IT Lagebild, das multinational austausch- und erweiterbar ist.

5.8.2 BESCHREIBUNG DES FUNKTIONALEN PROFILS

Das System muss in der Lage sein, ausgewählte Services der operationellen Umgebung – insbesondere alle ausgeprägten Bausteine der IT-Sicherheitsarchitektur – zu überwachen und zu steuern.

Für ein einheitliches System Management ist eine Nutzung von gleichen Services, Prozessen und Tools in den zu überwachenden Informationsräumen anzustreben. Nur dadurch wird eine Skalierbarkeit über beliebige Sicherheitsdomänen hinweg ermöglicht, wodurch eine missionsbezogene Sicherheitsdomäne auch beispielsweise vom Heimatland aus überwacht werden kann. Hierfür muss eine Übergabe von Betriebsdaten über ein Information Exchange Gateway zwischen Sicherheitsdomänen ermöglicht werden.

Ist eine Harmonisierung der Tool Landschaft nicht möglich, müssen Informationen des System Managements über standardisierte Schnittstellen austauschbar sein.

Das System Management hat zur Gewährleistung der IT-Sicherheit den Konfigurationsstand aller angeschlossenen Configuration-Items (CIs) zu überwachen und bei Vorliegen genehmigter Changes möglichst ohne großen Zeit- und Ressourcenaufwand die Umsetzung des Changes zu ermöglichen. Insbesondere die Umsetzung von Emergency Changes ist systemseitig zu unterstützen, um Sicherheitslücken bei Bekanntwerden schnellstmöglich schließen zu können, ohne die Missionsdurchführung über einen längeren Zeitraum zu beeinträchtigen.

Es müssen Filtereigenschaften und Übertragungswege für die Übergabe von Betriebsdaten und weiterer Datensammlungen definiert werden. Hierzu zählen die Übertragung von aktuellen Statusdaten, Daten über Incidents, Eventmeldungen, etc. an eine zentrale Stelle. Das zentrale System Management kann innerhalb der missionsbezogenen Sicherheitsdomäne angesiedelt sein und/oder in einem Reach Back-Element im Heimatland. In letzterem Fall ist aber eine lokale Instanz zur Sicherstellung der Autarkiefähigkeit im Einsatzgebiet bei Bedarf einzurichten.

Die generierten Daten sind in einem betrieblichen IT-Lagebild zusammenzuführen, dass auch Aussagen über Anomalien oder Sicherheitsvorkommnisse im Einsatznetzwerk erlaubt. Die betriebliche IT-Lage ist somit eng an ein Cyberlagebild zu koppeln und wechselseitig mit Informationen zu versorgen.

Generierte Daten wie Events sind über ein standardisiertes Format auch anderen System Management-Entitäten im Einsatznetzwerk zugänglich zu machen, um übergreifende Anomalien oder Sicherheitsvorkommnisse bewerten zu können.

Zur Unterstützung des System Managements muss eine Inventarisierungsdatenbank implementiert werden. Zur Befüllung der Inventarisierungsdaten muss ein entsprechendes Inventarisierungstool ausgerollt werden.

5.9 SYSTEMZUGANG

5.9.1 BEGRIFFSDEFINITIONEN

Beim Systemzugang ist zwischen dem Zutritt, dem Zugang und dem Zugriff zu unterscheiden. Diese Begriffe sind durch das „Bundesamt für die Sicherheit in der Informationstechnik“ (BSI) wie folgt definiert:

Mit Zutritt wird das Betreten von abgegrenzten Bereichen wie z. B. Räumen oder geschützten Arealen in einem Gelände bezeichnet.

Zutrittsberechtigungen erlauben somit Personen, bestimmte Umgebungen zu betreten, also beispielsweise ein Gelände, ein Gebäude oder definierte Räume eines Gebäudes.

Der Zutritt wird mit organisatorischen und infrastrukturellen Maßnahmen geregelt. Die Zutrittskontrolle kann unter anderem mittels Protokollierung und Überwachungstechniken (z.B. Kamera) erfolgen.

Mit Zugang wird die Nutzung von IT-Systemen, System-Komponenten und Netzen bezeichnet.

Zugangsberechtigungen erlauben somit einer Person, bestimmte Ressourcen wie IT-Systeme bzw. System-Komponenten und Netze zu nutzen. Die Zugangskontrolle, die Identifikation und Authentisierung wird unter anderen mittels User ID und Password gesteuert. Ebenso sind organisatorische Regelungen maßgebend (Wer darf was nutzen?).

Mit Zugriff wird die Nutzung von Informationen bzw. Daten bezeichnet.

Über Zugriffsberechtigungen wird geregelt, welche Personen im Rahmen ihrer Funktionen oder welche IT-Anwendungen bevollmächtigt sind, Informationen, Daten oder auch IT-Anwendungen, zu nutzen oder Transaktionen auszuführen. Die Zugriffskontrolle beinhaltet die Rechtevergabe bezüglich Lesen, Ändern und Schreiben von Daten nach erfolgten Zugang (Wer darf auf was zugreifen?).

Eine Person, der der Zugang zu Systemressourcen (Netze, Komponenten) erlaubt wird, kann unterschiedliche Zugriffsrechte zur Nutzung einzelner IT-Anwendungen und Daten besitzen (siehe Kap. 5.4 Identity & Access Management). Dennoch werden die beiden Begriffe im Folgenden unter dem Begriff "Systemzugang" zusammengefasst.

Das BSI betrachtet in seinen Definitionen ausschließlich Personen. Personen sind Administratoren, Superuser/ Notfallnutzer, Auditoren, normale und technische sowie funktionale Nutzer.

Im Sinne eines Service-orientierten Systems, das in einem Teilstreitkraft-übergreifenden (joint) und multinationalen (combined) Rahmen den Informationsaustausch und die Bereitstellung des handlungsleitenden Lagebildes gewährleisten soll, ist darüber hinaus auch der Systemzugang durch andere Services und/oder Systeme zu betrachten. Im Weiteren wird der Begriff Systemzugang in dieser umfassenderen Bedeutung verstanden.

5.9.2 FUNKTIONALE FORDERUNGSBAUSTEINE

Der Systemzugang bietet einen einheitlichen Einstiegspunkt in das System und muss in gleicher Weise im Grundbetrieb, bei Ausbildungen, bei Übungen sowie bei Einsätzen und einsatzgleichen Verpflichtungen möglich sein

Der Systemzugang muss sicherstellen, dass

- nur autorisierte Nutzer,
- von diesen gestartete Prozesse und in Anspruch genommene Dienste (Services) und Systeme,
- mit definierten Rechten

am System arbeiten können.

5.9.3 BESCHREIBUNG DES FUNKTIONALEN PROFILS

Beim Systemzugang ist der Zugang durch Personen und durch andere Systeme sowohl nationaler als auch internationaler Ebene (hier insbesondere NATO) zu betrachten. Daher sind über die nationalen Bestimmungen hinaus auch internationale Bestimmungen zu beachten. Prinzipiell sind Systeme mit ihren zugehörigen Systemzugängen durch eine zuständige Stelle zu genehmigen.

Die Vertraulichkeit, Verfügbarkeit und Integrität der Informationen sowohl im nationalen als auch im multinationalen Rahmen muss in einem Umfang gewährleistet sein, der dem Schutzbedarf der Informationen entspricht. Dazu können auf den Endgeräten je nach Einstufung mehrere Arbeitsumgebungen eingerichtet werden, deren Zulassung je nach Anwendungsfall durch das BSI oder die DEUmilSAA erfolgt. Ist dies aus technischen oder organisatorischen Gründen nicht möglich, sind die Arbeitsumgebungen auf jeweils einem System einzurichten. Der Zugriff auf nicht öffentliche Informationen darf nur authentisiert und autorisiert erfolgen. Es sind entsprechende Schutzmaßnahmen zu implementieren (z. B. Verlängerung der Wartezeit nach jedem Anmelde-Fehlversuch, Sperrung nach einer definierten Anzahl von Fehlversuchen). IT-Systeme, die den Zugang Unbefugter ungehindert zulassen, dürfen nicht eingesetzt werden.

Bewährte Authentifizierungsmethoden sind:

- Wissen (Passwort),
- Besitz (Smartcard, Token, elektronischer Truppenausweis einschließlich „Public Key Infrastructure“ (PKI),
- biometrische Merkmale (Fingerabdruck, Venenmuster, Iris).

Bei der Auswertung von biometrischen Merkmalen ist zu beachten, dass ein Gerät regelmäßig durch mehrere Nutzer genutzt werden kann. Daher werden die Nutzer mit dem für sie vorgesehenen Endgerät über ein für sie vorgesehenes Rechteprofil verknüpft. Ausgehend von der Identität bzw. der Rolle der angemeldeten Nutzer wird der Zugriff auf Anwendungen, Services und Daten gewährt.

Ein Nutzer, der einen Systemzugang erhält, ist darüber zu informieren, dass

- er auf ein System der Bundeswehr zugreift,
- die Systemnutzung überwacht, aufgezeichnet und geprüft werden kann,
- die unbefugte Benutzung verboten ist und als Dienstvergehen/ Wehrstraftat geahndet werden kann.

Diese Informationen sind mittels eines modalen Hinweises bzw. Dialogs anzuzeigen.

Unabhängig von der Einstufung des Systems sind, bezogen auf den Systemzugang, mindestens folgende Sicherheitsauflagen zu erfüllen:

- Zutrittskontrolle:
  Wenngleich im Kontext dieses Dokumentes nicht weiter zu erörtern, ist eine wirksame Zutrittskontrolle zu implementieren und zu überwachen. Das betrifft sowohl die Liegenschaft als Ganzes als auch die Teile, in denen sich die Systeme bzw. Systemanteile befinden.

- Zugangskontrolle:
  Durch geeignete Maßnahmen ist sicher zu stellen, dass nur berechtigte Nutzer einen Systemzugang erhalten. Dazu müssen die Nutzer, Geräte, Systeme, Prozesse und Services identifiziert und bekannt sein. Nutzer müssen für den Zugriff auf eingestuften Informationen entsprechend sicherheitsüberprüft sein. Insbesondere der Entzug einer Berechtigung muss unmittelbar im System bekannt gemacht werden können. Nach gewährtem Zugang stellen Sicherheitsmaßnahmen im System sicher, dass die Nutzer nur erlaubte Handlungen durchführen oder anstoßen können.

- Ausbildung:
  Um die Sicherheitsrisiken des Systems zu verringern (z. B. Ausfall, Manipulation oder Ausspähen), ist den Nutzern in regelmäßigen Abständen zu verdeutlichen, welche Sicherheitsrisiken bestehen und welche entsprechenden Verhaltensregeln einzuhalten sind.

- Systemüberwachung:
  Das System muss Protokolle führen, die die Überwachung des Systems erlauben und bei einem Sicherheitsverstoß die Identifikation des Verursachers erlauben. An den wesentlichen internen Schnittstellen ist die Kommunikation zu überwachen, zu protokollieren und ggf. zu auditieren.

- Systemausgaben:
  Ausgaben von eingestuften Informationen, sowohl als Druck als auch als Dateien auf Medien, sind zu dokumentieren (siehe „VS-Nachweisführung“). Ebenso sind die Informationen zu kennzeichnen (siehe „Labelling“).

- Risikoüberwachung:
  Das aus den Regeln zum Systemzugang entstehende Restrisiko ist periodisch zu bewerten.

5.10 ARCHITEKTURÜBERGÄNGE

5.10.1 QUERSCHNITTLICHE ANFORDERUNGEN

Architekturübergänge werden durch Information Exchange Gateways (IEGs) abgesichert. Diese kontrollieren am Netzübergang zum Beispiel die Integrität und die Sicherheitseinstufung der transferierten Daten.

5.10.2 POLICY ENGINE

5.10.2.1 FUNKTIONALE FORDERUNGSBAUSTEINE

Verwaltung der Wertevorräte mit VS-bezogenen Metadaten, die im Zusammenhang mit der Realisierung der Architekturübergänge Extern/Intern zur Anwendung kommen.

5.10.2.2 BESCHREIBUNG DES FUNKTIONALEN PROFILS

Die Policy Engine für die Realisierung der Architekturübergänge muss zwei verschiedene Wertevorräte verwalten:

- Security Policy Information File (SPIF) sowie
- Network Security Label (NetSL).

Das SPIF verwaltet die in einem Informationsraum gültigen Einstufungen. In einem SPIF werden die Geheimhaltungsgrade und Kategorien definiert und deren Beziehungen untereinander beschrieben. Das SPIF für den missionsbezogenen Informationsraum stellt eine Grundlage für die Konfiguration des Sicherheitsfilters dar.

Der Sicherheitsfilter führt außer den netzwerkbezogenen Informationen auch Angaben zur Einstufung der verbundenen Informationsräume. Diese Informationen werden in Form von Network Security Label (NetSL) für die jeweilige Informationsdomäne mitgeführt. Die Einstufung des Netzes wird dabei durch folgende Attribute beschrieben:

- Sicherheitsrichtlinie,
  Beispiel: DEU, NATO.

- Geheimhaltungsgrad,
  Beispiel: VS-VERTRAULICH, SECRET.

- Zusätzliche Kategorien,
  Beispiel: Nur Deutschen zur Kenntnis, Releasable to Internet.
  Die zusätzlichen Kategorien können in drei Untermengen aufgeteilt werden:
  - Restrictive
    Einschränkung der Einstufung. Die Daten in dem Netzwerk dürfen nur angegebene Kategorien betreffen. Beispiel: Nur Deutschen zur Kenntnis.
  - Permissive
    Aufweichung der Einstufung. Durch diese Angabe wird die Freigabe der Daten in dem Netzwerk an weitere Informationsdomänen geregelt, wie etwa Releasable to Internet.
  - Informative
    Die Kategorien haben rein informativen Charakter und beeinflussen die Einstufung nicht.

5.10.3 INFORMATION EXCHANGE GATEWAY (IEG)

5.10.3.1 FUNKTIONALE FORDERUNGSBAUSTEINE

Ein IEG muss an den Architekturgrenzen feststellen, ob die Übertragung einer Information, unabhängig der Speicherart (Datei, Stream, DB Eintrag), zulässig ist.

Hierzu ist eine Identifikation von Quell- und Ziel-Domäne, Authentifizierung von Personen, Authentifizierung von Systemen und die Authentifizierung von Services notwendig.

5.10.3.2 BESCHREIBUNG DES FUNKTIONALEN PROFILS

Um die Datenaustauschbeziehungen zwischen Systemen unterschiedlichen Schutzbedarfs (Netzgrenzen mit Sicherheitsgefälle) abbilden zu können und die nationalen IT-Sicherheitsvorgaben zu wahren, ist es erforderlich, zugelassene Information Exchange Gateways einzusetzen.

Das aus den Komponenten Sicherheitsfilter und Firewall bestehende Information Exchange Gateway realisiert an einem Netzübergang zwei Sicherheitsfunktionen:

- Der Sicherheitsfilter verhindert das Abfließen von eingestuften Informationen aus dem höher eingestuften Netz (HIGH) in das niedriger eingestufte Netz (LOW).
- Das Firewall-System schützt das höher eingestufte Netz vor netzwerkbasierten Angriffen. Das Firewall-System sollte mindestens aus Application Level Gateway und Paketfilter bestehen, um durchgängige Verbindungen zu verhindern. Die so mögliche Content-Analyse erhöht das Sicherheitsniveau an dieser kritischen Stelle.

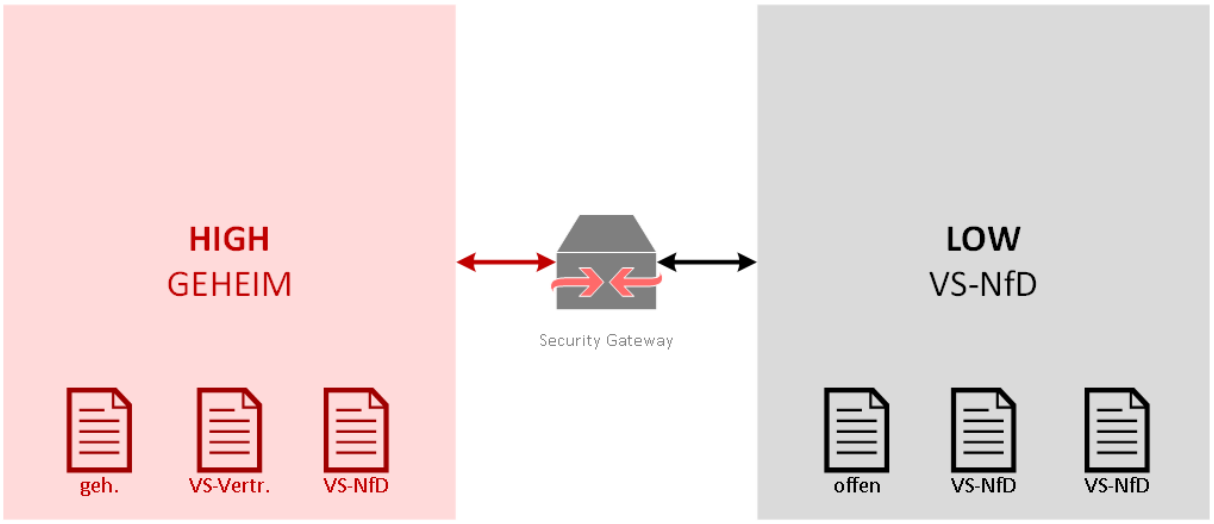

Abbildung 6: Schematische Darstellung des Sicheren Netzübergangs

Logisch gehört das Information Exchange Gateway zur Informationsdomäne HIGH, die Grenze zwischen zwei Informationsdomänen verläuft jedoch innerhalb des Filters. Es bedarf keinerlei Benutzerinteraktionen um die Informationsobjekte über den sicheren Netzübergang zu übertragen. Die Auswertung des XML Security Labels und die damit verbundene Freigabe zum Transfer laufen automatisch ab. Der Sicherheitsfilter kontrolliert die Integrität der gelabelten Informationsobjekte und trifft eine Entscheidung basierend auf der Einstufung der Daten und des jeweiligen Netzes. Informationsobjekte ohne gültiges XML Security Label werden abgewiesen und nicht über die Architekturgrenze transportiert. Ebenfalls werden keine Informationsobjekte mit einer für das Zielnetz zu hohen Einstufung übertragen. Des Weiteren untersucht und sanitarisiert der Sicherheitsfilter die protokollspezifischen Anteile der Kommunikation.

Neben der Label-basierten Prüfung, ob ein Informationsobjekt transportiert werden darf oder nicht, gibt es alternativ noch die Möglichkeit der sogenannten regelbasierten Filterung. Hierbei werden Regeln hinterlegt, die eine festgelegte Struktur beschreiben. Entsprechen die zu transportierenden Informationsobjekte dieser Struktur, so werden diese von Information Exchange Gateways in die Zielarchitektur transportiert. Andernfalls wird der Transport in die Zielarchitektur unterbunden.

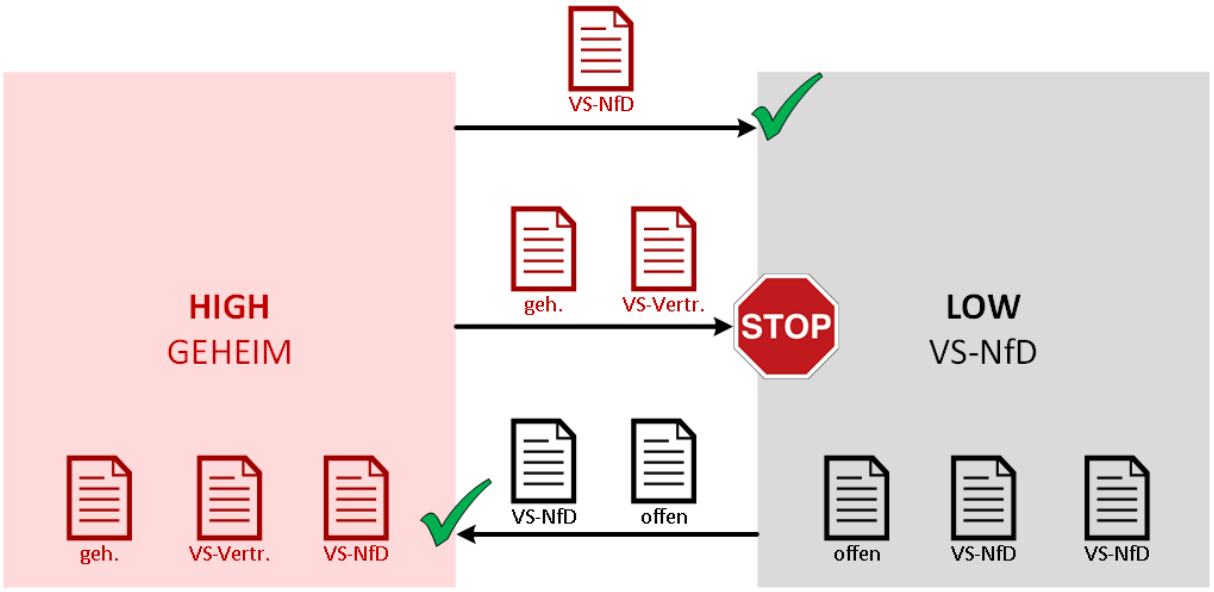

Abbildung 7: Architekturübergreifender Austausch von Informationsobjekten

Das Information Exchange Gateway muss nach Common Criteria gegen das Nationale Schutzprofil „Sichere Netzübergänge“ (NPP Sichere Netzübergänge) evaluiert sein. Auf dieser Basis muss für den einzusetzenden Labelling Service ein projektbezogener Zulassungsantrag beim BSI gestellt werden.

Derzeit am Markt verfügbare Information Exchange Gateways unterstützen nur den Austausch von statischen Daten, d.h. Dokumente/Dateien. Der Austausch von dynamischen Daten ist noch nicht möglich. Ein Lösungsansatz zum Austausch dynamischer Daten (Streams, etc.) kann dem Funktionsbaustein „Labelling“ entnommen werden und ist in zukünftigen Ausprägungen von IT-Sicherheitsarchitekturen in Einsätzen auszuprägen.

5.11 ANFORDERUNG AN IT-SERVICES

5.11.1 FUNKTIONALE FORDERUNGSBAUSTEINE

- Flexibilität und Anpassbarkeit an Laufzeitumgebungen/ Endgeräteprofile
- Standardisierte „Sandbox“-Definitionen
- Front-End/ Back-End Separation
- Unterstützung für lokales Caching bei geforderter Autarkiefähigkeit
- SaaS Support
- Einheitliche, externe Authentisierung, Autorisierung
- Integration von Replikationsmechanismen
- Portierbarkeit
- Fehlertoleranz, Wiederherstellbarkeit
- Latenztoleranz
- Standardisierte APIs
- Quellcodehoheit/ -reviews
- Unterstützung von Rollencontainern (Need to Know)
- Labelling Support

5.11.2 BESCHREIBUNG DES FUNKTIONALEN PROFILS

Zur Integration in den Sicherheitskernel müssen IT-Services ein Service Profil erfüllen, wodurch einheitliche Mindeststandards für mittelbare oder unmittelbare Anforderungen der IT-Sicherheit verbindlich umgesetzt werden. Das Service Profil gliedert sich in architekturbedingte, funktionale und nichtfunktionale Forderungsbausteine, die in ihrer Gesamtheit die Anforderungen der IT-Sicherheitsarchitektur an den Einzelaspekt IT-Services umsetzen und im Folgenden beschrieben werden.

IT-Services müssen in ihrer Implementierung zwischen Front- und Backend – i.e. zwischen Verarbeitung/ Anzeige der Daten und der Datenhaltung – unterscheiden. Der IT-Service muss in der Lage sein, seine Daten über einen Cryptoservice an einen dahinter liegenden Datenspeicher zu übergeben, unabhängig von dessen technischer Realisierung. Nur so kann eine sicherere und gleichzeitig effiziente Datenablage im Sinne der Architektur gewährleistet werden.

Das Front-End des IT-Services ist in einer standardisierten „Sandbox“ lauffähig zu gestalten, wobei diese für jede zu integrierende Sicherheitsdomäne innerhalb der Architektur betreibbar sein muss. Die „Sandbox“ ist dabei so zu gestalten, dass sie nur für den IT-Service notwendige und beschriebene Übergabepunkte/ Datenaustauschbeziehungen erlaubt und diesen ansonsten sowohl von der darunter liegenden Plattform als auch von den übrigen IT-Services separiert. Damit wird im Falle einer Kompromittierung eines IT-Services eine Ausbreitung auf andere IT-Services erschwert.

Bezüglich der Autorisierung von Nutzern müssen die IT-Services in der Lage sein, durch eine externe Entität vorgenommene Autorisierungen innerhalb ihrer Funktionalität umzusetzen. Gemäß dem Need to Know Prinzip, dem Nutzer nur Zugriff auf Informationen zu gewähren, die er für seine Aufgabenwahrnehmung benötigt, müssen IT-Services ein generisches Rollenprofil unterstützen und verarbeitete Informationen zwischen den verschiedenen Rollen abgrenzen. Entsprechende Schnittstellen zu einem zentralen Identity & Access Management sind entsprechend auszuprägen.

Das Paradigma „Software as a Service“ als zu erreichendes Ziel ist durch die IT-Services innerhalb der Architektur aus dem Blickwinkel der IT-Sicherheit heraus umzusetzen. Der zentralisierte Datenspeicher, die Informationsverarbeitung und -bereitstellung sowie die damit einhergehende Reduzierung der Systemanteile mit hoher Informationsdichte auf möglichst kleine Bereiche, ist wesentlich für eine Risikominimierung. Gleichzeitig ist durch die Abstraktion von der Ebene des Betriebssystems und der Hardware eine leichtere Wiederherstellbarkeit im Fehlerfall und einfachere Migration bei Veränderung der Infrastruktur gegeben.

Aufgrund der Forderung nach Autarkiefähigkeit insbesondere auf der mobilen Ebene, müssen einzelne IT-Services zudem in der Lage sein, auf unterschiedlichen IT-Plattformen bzw. mit abgestuften Ressourcen umgehen und ihre Leistungen bereitstellen zu können. Dabei müssen die in der Sicherheitsarchitektur ausgeprägten Endgeräteprofile durch die relevanten IT-Services beachtet und umgesetzt werden. IT-Services müssen für verschiedene Formfaktoren (Desktop, Tablet, Handheld) skalierbar sein.

Die durch IT-Services verarbeiteten Daten müssen im Rahmen der funktionalen IT-Sicherheitsarchitektur ein zentrales, sicherheitsdomänenübergreifendes Labelling unterstützen. Die durch die IT-Services implementierten Datenstrukturen müssen entsprechende Labels vorsehen, der IT-Service muss eine standardisierte Schnittstelle für den Labelling Service bereitstellen bzw. implementieren können.

Die Informationsdomäne „MISSION“ muss durchgängig von der Basis Inland bis auf die unterste taktische Ebene in den Einsatzgebieten bereitgestellt werden können. Dabei können IT-Services sowohl in der Basis Inland bereitgestellt und in die Einsatzgebiete verlängert, als auch vor Ort in den Einsatzgebieten unmittelbar erbracht werden. In beiden Fällen müssen IT-Services jedoch in der Lage sein, ihre Daten zwischen den verschiedenen Rechenzentren (sowohl in der Basis Inland als auch im Einsatzgebiet) möglichst synchron vorzuhalten. Dies wird zum einen durch die Forderung nach einer Autarkiefähigkeit in Einsatzgebieten und zum anderen durch Redundanzforderungen bedingt. Alle IT-Sicherheitsmechanismen der Architektur haben die durchgängige Bereitstellung des Informationsraums zu unterstützen.

IT-Services müssen insbesondere bei der Verwendung/ beim Betrieb in militärischen IT-Umgebungen eine spezifizierte Fehlertoleranz aufweisen, um den hohen Anforderungen an die Verfügbarkeit der IT-Services Rechnung tragen zu können. Ein Mittel hierzu ist die Umsetzung einer Multi-Session-Fähigkeit für den jeweiligen IT-Service, wobei Fehler oder Abstürze einzelner Sessions oder Instanzen nicht zu einem kompletten Ausfall des IT-Services führen dürfen. Sollte es dennoch zu einem Ausfall des IT-Services kommen, muss der Service die Fähigkeit zu einer schnellstmöglichen Wiederherstellbarkeit vorhalten.

Aufgrund der heterogenen IT-Service Landschaft bei Kommunikationsservices müssen IT-Services eine hohe Latenztoleranz bei der Informationsbereitstellung zu Nutzern oder anderen IT-Service Instanzen aufweisen. Ein schnelles Antwort-Zeit-Verhalten ist bei schmalbandigen oder hoch latenten Kommunikationsmitteln nicht immer gegeben – dies darf die Leistungserbringung der IT-Services nicht beeinträchtigen.

Um den Abhängigkeiten zwischen IT-Services auch über einem langen Betrachtungszeitraum Rechnung zu tragen, d.h. IT-Services beispielsweise beim späteren Erkennen struktureller IT-Sicherheitslücken flexibel austauschen zu können, muss die Interaktion der IT-Services untereinander und gegenüber externen Entitäten im System über standardisierte Schnittstellen (Application Programming Interface – API) erfolgen.

Auch bei zentralisierter Informationsverarbeitung und Umsetzung des Cloud Gedankens in zukünftigen Einsatznetzwerken müssen ausgewählte IT-Services in der Lage sein, lokales Caching bzw. lokale

Informationsverarbeitung für einen begrenzten Zeitraum zu ermöglichen und lokal verarbeitete Daten bei Wiederherstellung der Übertragungswege in den zentral gehaltenen Datenbestand zu integrieren.

6 AUSBLICK

Die reine Erfassung der Anforderungen an die Einzelkomponenten einer zukünftigen IT-Sicherheitsarchitektur für Einsatznetzwerke ist für eine Realisierung in den Streitkräften noch nicht ausreichend. Es gilt im Folgenden, die aufgestellten Anforderungen in einer Architektur „formal“ zu beschreiben, die dargestellten Entitäten entsprechend auszuprägen und das Wechselspiel der Komponenten bzw. deren logische Abhängigkeiten zu beschreiben.

Zusätzlich sind generische Anwendungsfälle zu definieren, die eine Ausprägung der einzelnen Komponenten der Sicherheitsarchitektur auf verschiedenen Führungsebenen unter Berücksichtigung zu definierender Gefährdungsprofile erlauben. Insbesondere die Implementierung von Mission Network Elementen sowie Mission Network Extensions im Kontext des Federated Mission Networking (FMN) der NATO sollten bei der Definition generischer Anwendungsfälle im Mittelpunkt stehen. Dadurch wird der flexible Ansatz der funktionalen Sicherheitsarchitektur deutlich und die Verfügbarkeit notwendiger Technologien kann auf der Zeitachse evaluiert werden.

Die identifizierten, produktunabhängigen Technologien bilden in der Summe eine Referenzarchitektur, die im Rahmen von heutigen und zukünftigen Rüstungsprojekten als Zielgröße für zu rüstende Anteile einer gesamtheitlichen IT-Sicherheitsarchitektur in einzelnen Projekten dienen kann. Damit kann der einheitlichen, übergreifenden und bedarfsgerechten Abbildung der IT-Sicherheit Rechnung getragen werden. Zugleich gilt es entlang der Referenzarchitektur eine weitestgehende Standardisierung der entsprechenden Komponenten im multinationalen Bereich zu erwirken, um die Interoperabilität in Einsätzen zu erhöhen und die durchgängige Gewährleistung von IT-Sicherheit auch im multinationalen Umfeld zu ermöglichen.

Die hierzu notwendigen Arbeitspakte sind als Folgetätigkeiten zu definieren, und das vorliegende Dokument ist bei Voranschreiten derweiteren Bearbeitung fortzuschreiben und um entsprechende Inhalte zu ergänzen.