Bundesamt
für Sicherheit in der
Informationstechnik

# Sicheres mobiles Arbeiten

Problemstellung, Technische Voraussetzungen und Lösungswege anhand der Anforderungen für mobile Endgeräte in der Bundesverwaltung

# Inhaltsverzeichnis

# Das BSI im Dienst der Öffentlichkeit

Das Bundesamt für Sicherheit in der Informationstechnik wurde am 1. Januar 1991 mit Sitz in Bonn gegründet und gehört zum Geschäftsbereich des Bundesministeriums des Innern.


Mit seinen derzeit rund 600 Mitarbeiterinnen und Mitarbeitern und ca. 80 Mio. Euro Haushaltsvolumen ist das BSI eine unabhängige und neutrale Stelle für alle Fragen zur IT-Sicherheit in der Informationsgesellschaft.

Als zentraler IT-Sicherheitsdienstleister des Bundes ist das BSI operativ für den Bund, kooperativ mit der Wirtschaft und informativ für den Bürger tätig.

Durch die Grundlagenarbeit im Bereich der IT-Sicherheit übernimmt das BSI als nationale IT-Sicherheitsbehörde Verantwortung für unsere Gesellschaft und ist dadurch eine tragende Säule der Inneren Sicherheit in Deutschland.

Ziel des BSI ist der sichere Einsatz von Informations- und Kommunikationstechnik in unserer Gesellschaft. IT-Sicherheit soll als wichtiges Thema wahrgenommen und eigenverantwortlich umgesetzt werden. Sicherheitsaspekte sollen schon bei der Entwicklung von IT-Systemen und -Anwendungen berücksichtigt werden.

Das BSI wendet sich mit seinem Angebot an die Anwender und Hersteller von Informationstechnik. Zielgruppe sind die öffentlichen Verwaltungen in Bund, Ländern und Kommunen sowie Privatanwender und Unternehmen.

Diese Broschüre beschreibt das Konzept des BSI bezüglich Smartphones in der Bundesverwaltung und den SNS-Standard zur Sicheren Netzübergreifenden Sprachkommunikation, der in den „Kryptohandys“ der Bundesverwaltung zum Einsatz kommt. Es wird ein Ausblick auf geplante und laufende Entwicklungen gegeben.

# 1 Einleitung – Sachlage

# 1 Einleitung – Sachlage

Smartphones und Tablets bieten sowohl im beruflichen als auch im privaten Bereich eine Reihe von Vorzügen und sind zum ständigen Begleiter in allen Lebenslagen geworden. Im Umgang mit sensiblen Informationen geschieht der Einsatz mobiler IT- und Kommunikationstechnologie allerdings häufig auf Kosten der Sicherheit.

Beim Design von mobilen Endgeräten legen die Hersteller zwar auch Wert auf Sicherheit, aber sie steht meist nicht im Fokus. Dieser liegt primär auf Benutzerfreundlichkeit, Erreichbarkeit und Entertainment. Zudem erfüllt die Umsetzung der Sicherheitsinteressen des jeweiligen Herstellers nicht unbedingt die Sicherheitsbedürfnisse des Nutzers.

Jedem Anwender sollten daher die Gefahren bewusst sein, die die Nutzung eines modernen Mobiltelefons, für die Verarbeitung sensitiver Daten, mit sich bringt.

**Risiko – Diebstahl und unbefugter Zugriff**

Mit zunehmender Speichergröße ist es verlockend, alle potenziell benötigten Daten griffbereit auf dem mobilen Begleiter

mitzuführen. So können im modernen Smartphone auch schon mal mehrere Gigabytes an Daten darauf warten, unfreiwillig den Besitzer zu wechseln.

Hat der vernetzte Nutzer über sein Smartphone auch noch Zugang zu seinem Firmennetzwerk, eröffnen sich dem „neuen Besitzer“ des Endgerätes womöglich zusätzlich gleich alle internen Unternehmensdaten.

**Risiko – Schädlinge**

So wie die mobilen Alleskönner ihren großen Brüdern (PC und Laptop) in Sachen Leistung und Funktionsumfang ebenbürtig werden, so werden sie auch als Angriffsziel attraktiver.

Doch PC und Laptop werden meist mit Firewall und Virenscanner gegen Schädlinge geschützt, und insbesondere bei Unternehmens-IT gelten für sie strenge Regelungen für die Installation von Programmen oder den internen und externen Datentransfer.

Für Smartphones hingegen sind die traditionellen Malware-Abwehrmaßnahmen nicht effektiv durchführbar: Smartphones müssen stetig mit ihrer Energie haushalten und können sich daher den Stromverbrauch durch konstante Hintergrundscans nicht leisten. Darüber hinaus sehen deren Betriebssysteme im konventionellen Betrieb (nicht „gerootet“) Applikationen mit derartig privilegierten Berechtigungen, wie sie solche Abwehrprogramme für einen effektiven Schutz benötigen, nicht vor.

Die leichtfertige Datenanbindung der Smartphones an das Unternehmens- oder Behördennetzwerk kann ein sorgfältig erarbeitetes Sicherheitskonzept auf gefährliche Weise untergraben, denn durch die Integration des Endgeräts in das Netzwerk stellt nun das Endgerät mit seinen Schnittstellen einen neuen Zugang zum Netzwerk dar. Über diesen können dann z. B. Daten abfließen oder Schadsoftware sowohl für das Endgerät, als auch das Netzwerk eingeschleust werden.

**Risiko – mobile Anwendungen (Apps)**

Mobile Endgeräte bieten potenziellen Angreifern durch ihre ständige Präsenz, ihrer Vielzahl von Sensoren und diversen Schnittstellen, das perfekte Infiltrationswerkzeug, mit dem sie sich Augen und Ohren im Einsatzumfeld der Endgeräte verschaffen können. Auch Benutzerverhalten, seine Aktionen und Bewegungen an jedem Ort und zu jeder Zeit, ist eine leichte Beute für die mobilen Begleiter und kann ggf. durch Dritte ausgewertet werden.

Der Übergang zwischen Schadsoftware und legitimen mobilen Anwendungen (sogenannten Apps) ist hier fließend, da Bedrohungen nicht nur von extern eingeschleuster Schadsoftware ausgehen. Auch legale, über offizielle Kanäle installierbare Apps können, insbesondere im Umgang mit sensitiven personenbezogenen Informationen oder in einem sensitiven Umfeld, ein Risiko darstellen. Häufig verschicken sie auf den Endgeräten angefallene Daten an Diensteanbieter im Internet, ohne dass die Verarbeitungswege dem Nutzer oder dem IT-Administrator offensichtlich sind.

### Risiko – Lauscher

Dass vor dem Austausch von Daten zwischen Netzwerk und mobilen Endgerät Maßnahmen ergriffen werden müssen, die ein Abgreifen dieser auf dem Übertragungsweg verhindern, ist im Allgemeinen bekannt.

Weniger bekannt ist, dass auch die mobile Telefonie, z. B. über die ungenügend abgesicherte Funkstrecke, potenziellen Mithörern eine Reihe von Möglichkeiten bietet, unbefugt an der Kommunikation teilzuhaben.

Die GSM-eigene Funkstreckenverschlüsselung ist beispielsweise mit Hilfe von Rainbow-Tables[1] überwindbar. Zudem kann die Verschlüsselung durch das Vortäuschen einer Basisstation mittels Einsatzes eines IMSI-Catchers[2] gleich vollständig umgangen werden, da Basisstationen dem Endgerät vorschreiben können, die Verschlüsselung auszuschalten. Neuere Mobilfunkstandards bieten zwar besseren Schutz, da aber in der Regel eine Abwärtskompatibilität zu GSM geboten wird, kann der IMSI-Catcher die Verwendung von GSM beim Endgerät erzwingen.

Weiterhin hat sich gezeigt, dass bei unverschlüsselten Telefonaten ein Abgreifen über die Telekommunikationsinfrastruktur nicht auszuschließen ist.

1 Passiver Angriff auf Mobilfunkstrecke

2 Aktiver Angriff auf Mobilfunkstrecke (Mehr Informationen dazu in der BSI-Publikation „Öffentliche Mobilfunknetze und ihre Sicherheitsaspekte“ Kapitel 1.3.1)

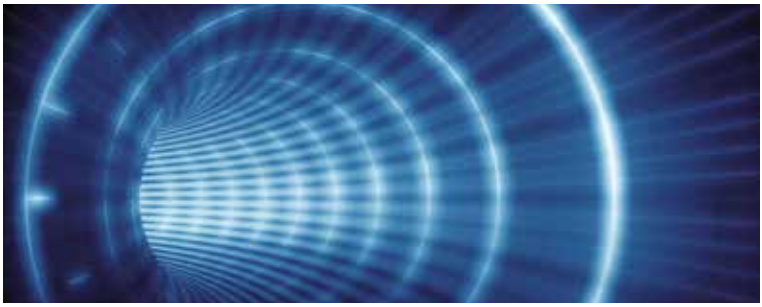
### Erarbeitung eines Sicherheitskonzeptes

Notwendige Konsequenz ist, dass im Umgang mit sensiblen Daten zunächst ein Sicherheitskonzept erarbeitet und implementiert werden muss, dass das jeweilige Gesamtsystem einschließlich mobiler, datenreicher Endgeräte berücksichtigt.

### Sicher ins Firmen-Netzwerk

Teil eines solchen Sicherheitskonzeptes muss eine Absicherung der Kommunikationswege sein.

Die Datenkommunikation sollte daher nur über eine sichere Verbindung zwischen den mobilen Endgeräten und dem internen Netzwerk erfolgen. Dazu kann auf bekannte Techniken, wie z. B. VPN[3]-Tunnel, zurückgegriffen werden, so dass der Datentransfer nur über einen authentisierten, verschlüsselten Kanal zwischen dem mobilen Client und dem heimischen Netzwerk erfolgt.



Das Endgerät wird damit zu einem Teil des internen Netzwerks des Unternehmens bzw. der Behörde. Es kann nun auf die inter-

3 Virtual Private Network

nen Daten zugreifen, ohne dass diese auf der Übertragungsstrecke abgegriffen werden können.

### Ende-zu-Ende-Sprachverschlüsselung

Um die Absicherung der Sprachkommunikation sicherzustellen, sollten sensible Mobilfunkgespräche auf der gesamten Kommunikationsstrecke zwischen Anrufer und Angerufenen, z. B. mittels SNS[4] (mehr dazu in Kapitel 6), geschützt werden.

Dadurch können sowohl Lauschangriffe über die Luftschnittstelle, als auch über die Telekommunikationsinfrastruktur abgewehrt werden.

### Restriktive Handhabung mobiler Anwendungen

Bevor eine App auf einem Gerät verwendet wird, welches auch sensible Daten beherbergt, oder das in einer Umgebung verwendet werden soll, in der sensible Daten verarbeitet werden, ist es angebracht, diese Applikation eingehend zu prüfen. Hierbei muss sichergestellt werden, dass keine unnötigen Daten anfallen bzw. an Unberechtigte weitergeleitet werden, und dass sensitive Daten keinen unnötigen Risiken ausgesetzt werden.

Auch Updates bereits installierter Apps müssen wieder geprüft werden.

4 Sichere Netzübergreifende Sprachkommunikation

Weiterhin kann es ratsam sein, die Nutzung von Apps mit App- oder betriebsystemspezifischen Einschränkungen so zu konfigurieren, dass ein angemessener Kompromiss zwischen Benutzerfreundlichkeit und Datensparsamkeit getroffen wird. Um solche Einschränkungen zentral durchzusetzen, können Administratoren MDM[5]-Systeme einsetzen (s. u.).

**Zentrales Management schützt Endgerät und Netzwerk**

Weiterhin muss das Sicherheitskonzept den Schutz der Integrität des Endgeräts und des Netzwerks berücksichtigen. Dazu gehört das Durchsetzen der bestehenden Sicherheitsrichtlinien des Netzwerks auch auf den mobilen Endgeräten.

Zu diesen Richtlinien gehören die Ablageverschlüsselung der Daten auf dem Endgerät, eine sichere 2-Faktor-Authentisierung am Endgerät mittels eines Hardwareankers oder auch das Erzwingen einer vorgegebenen Passwortkomplexität.

Zu diesem Zweck sollte die Rolle eines Geräteadministrators definiert werden, dessen Aufgabe die Festlegung, Verwaltung und Umsetzung von Einstellungen und Sicherheitsfunktionen auf den Endgeräten im Sinne der Sicherheitsrichtlinien ist. Dieser muss vor Inbetriebnahme eines Endgeräts eine initiale, sichere Konfiguration vornehmen. Optional ist, diese im laufenden Betrieb rekonfigurierbar zu gestalten, z. B. über ein MDM.

MDMs ermöglichen eine zentrale Administration der Endgeräte in Hinblick solcher Richtlinien und bieten häufig auch Optionen, wie das nachträgliche Löschen der Daten eines verlorenen oder gestohlenen Gerätes.

5 Mobile Device Management

Zu beachten bei der Verwendung eines MDMs ist aber, dass der zentralen Administration bei der Vielfalt erhältlicher Smartphones technische Grenzen gesetzt sind. Nicht jedes Endgerät ist von Haus aus im gleichen Umfang mit den notwendigen Mechanismen ausgestattet, daher müssen diese oft nachgerüstet werden. Ebenso unterstützt das Managementsystem auch nicht unbedingt jedes gewünschte Endgerät. Der Administrationsaufwand steigt somit mit jedem zu unterstützenden Endgerätetyp, da mit jedem neuen Endgerätetyp neuer Aufwand bei Planung, Konfiguration und technischer Umsetzung an den zentralen Systemkomponenten entsteht.

Deshalb ist ein Kompromiss zwischen Gerätediversität und Administrationsaufwand zu treffen.

**Sicherheit vs. Nutzerakzeptanz**

Auch an anderen Stellen kollidiert die Sicherheit mit den Wünschen und der Akzeptanz der Nutzer. Insbesondere die Usability leidet häufig unter den Anforderungen der Sicherheitsmaßnahmen.

Schränkt der Administrator aus Sicherheitsgründen liebgewonnene Funktionalitäten der mobilen Geräte ein, scheitern Sicherheitsmaßnahmen oft schon an der mangelnden Kooperation der Nutzer.

Aus diesem Grund muss die Nutzerakzeptanz von Grund auf bei der Planung berücksichtigt werden.

# 2 Mobiles Arbeiten in der Bundesverwaltung

# 2 Mobiles Arbeiten in der Bundesverwaltung

Bei der Sicherheit gilt, dass die Kette, welche die Information bearbeitet, nur so sicher ist wie ihr schwächstes Glied. Eine noch so sichere Ende-zu-Ende-Verschlüsselung hilft nicht, wenn sie auf einer Umgebung ausgeführt wird, die die Informationen schon vor der Verschlüsselung abfangen kann oder eine angebliche Verschlüsselung dem Benutzer nur vortäuscht.

Da ein effektiver Schutz nur durch ein wohldurchdachtes Sicherheitskonzept erfolgen kann, das genau auf das Einsatzszenario abgestimmt ist, sind mobile Endgeräte direkt aus dem Handel nicht geeignet, um eingestufte Daten zu verarbeiten.

Eine der Aufgaben des BSI ist es, sichere Kommunikationslösungen für den Einsatz in der Bundesverwaltung bereitzustellen und deren Sicherheit zu gewährleisten.

## 2.1 Handlungsansatz

Konzepte für sichere mobile Endgeräte für die Bundesverwaltung müssen immer das Ziel verfolgen, sowohl die Anforderungen modernen mobilen Arbeitens zu erfüllen, als auch die hohen Sicherheitsanforderungen, die sich aus der Verarbeitung sensibler Daten ergeben.

Um die Versorgungssicherheit für die Bundesverwaltung zu gewährleisten, wird zudem Wert darauf gelegt, mehrere Anbieter zu finden. Diese müssen unabhängig voneinander jeweils die nachfolgenden grundlegenden Anforderungen erfüllen.

### 2.1.1 Anforderungen an sichere mobile Endgeräte

Die mobilen Geräte müssen multifunktional sein; separate Geräte – eines für sichere Datenverarbeitung, eines für offenen Datenverkehr und letztlich eines für sichere Sprache – können Endnutzern nur in Ausnahmefällen z. B. bei nochmals höheren Sicherheitsanforderungen zugemutet werden.

Daher muss ein sicheres Endgerät zuverlässig sensitive dienstliche Daten und offene Daten voneinander trennen, eine mobile Anbindung an das interne Behördennetz leisten und es sollte eine Ende-zu-Ende-Sprachverschlüsselung verfügen.

An die Ende-zu-Ende-Sprachverschlüsselung wird der Anspruch gestellt, dass Verschlüsselungslösungen unterschiedlicher Hersteller jeweils miteinander interoperabel sein müssen.

Eine besondere Herausforderung an die Hersteller ist es, diese Funktionen unter Berücksichtigung hoher Sicherheitsanforderungen bereitzustellen:


So wird immer ein hardwarebasierter Vertrauensanker für eine 2-Faktor-Authentisierung (Wissen: PIN und Besitz: Sicherheitskarte) gefordert. Dieser stellt eine vertrauenswürdige Implementierung kryptographischer Algorithmen und einen sicheren Schlüsselspeicher bereit und ist z. B. für die Authentisierung am Endgerät und an der Netzwerkinfrastruktur zuständig.

Eine Verschlüsselung der Daten auf dem Endgerät ist unerlässlich, damit ein direktes Abgreifen der Daten auf dem Endgerät durch Unbefugte verhindert werden kann. Daher wird eine Ablageverschlüsselung für persistente Daten verlangt.

Die Datenübertragung zwischen dem Behördennetzwerk und dem Endgerät hat über einen VPN-gesicherten Kanal zu erfolgen.

Da das Endgerät einerseits möglichst flexibel (verschiedene Applikationen oder Programme, freier Webzugriff, ...) einsetzbar sein soll, andererseits aber auch eine Umgebung für die sichere Verarbeitung von dienstlichen Daten anbieten soll, werden Schutzmechanismen zur Separation dieser Funktionen eingefordert.

Eine große Herausforderung insbesondere bezüglich der Nutzerakzeptanz stellt die Sprachverschlüsselung dar: Da Telefonie gewählt wird, wenn ein schneller und direkter Informationsaustausch gewünscht ist, sind für die Nutzerakzeptanz gute Sprachqualität, Verfügbarkeit und geringer zusätzlicher Aufwand absolute Voraussetzung. Der Schutz der mobilen Telefonie sollte über die Implementierung des SNS-over-IP-Standards (siehe Kapitel 5) erfolgen und somit auch eine Interoperabilität zu bisherigen und zukünftigen behördlichen Mobilfunkgeräten gewährleisten.

### 2.1.2 Anforderungen an die Infrastruktur

Da der Markt der mobilen Endgeräte sehr schnelllebig ist und die Komplexität der mobilen Endgeräte laufend zunimmt, ist ein ausschließlich auf das Endgerät ausgerichteter Schutzansatz nicht mehr genug.

Durch die Ergänzung des Endgeräteschutzes durch zentrale Management- und Monitoringmaßnahmen auf Seiten der Infrastruktur soll das Schutzniveau trotz veränderter Ausgangslage erhalten bleiben.

Die Sicherheit kann durch ein System von unterschiedlichen Maßnahmen ergänzt werden. Folgende Punkte stehen dabei im Vordergrund:

» Konsequente Verschlüsselung des Datenverkehrs, auch für nicht eingestufte Informationen, teilweise auf verschiedenen Ebenen.

» Zentrales Management der Endgeräte.

» Zentrales Monitoring und Analyse des Datenverkehrs hinsichtlich verdächtiger Inhalte und auffälligen Verhaltens.

» Aufstellen strenger IT-Policy-Regeln (technisch und organisatorisch), die den Umgang mit dem Gerät festlegen.

### 2.2 Aktuelle Lösungen und Produkte

Produkte, die für die sichere Kommunikation in der Bundesverwaltung eingesetzt werden sollen, werden zunächst durch das BSI einer Evaluierung unterzogen. Im Zuge dieser Evaluierung müssen Nachweise über die geforderten Sicherheitsfunktionen erbracht und geprüft werden.

Im folgenden Kapitel werden die Produkte aus dem Bereich „mobile Kommunikation“ vorgestellt, die aktuell durch das BSI zugelassen sind.

### 2.3 Prüfung von mobilen Anwendungen (App-Testing)

Grundsätzlich werden für die mobilen Clients Applikationen benötigt, um die auf ihm anfallenden Informationen zu bearbeiten und ihre Funktionen in vollem Umfang zu nutzen.

Diese Apps müssen in sensibler Umgebung, zuzüglich ihrer primären Aufgabe, vor allem nachweislich vertrauenswürdig sein.

Während man zwar für jede erdenkliche Funktion in öffentlichen App-Stores meist schnell eine geeignete Applikation finden kann, gestaltet sich der Nachweis deren Sicherheit oft schwieriger.

Vor diesem Hintergrund wurde im BSI ein Prozess entworfen, Applikationen für den Bedarf der Bundesverwaltung auf ihre Vertrauenswürdigkeit zu prüfen.

Apps, die auf den dienstlich eingesetzten Endgeräten eingesetzt werden sollen, werden damit initial und für jedes ihrer Updates einer systematischen, sicherheitstechnischen Überprüfung unterzogen. Diese Überprüfung wird separat für jedes Zielsystem vorgenommen und unter Berücksichtigung des jeweiligen Einsatzszenarios ausgewertet.

# 3 Sichere Endgeräte für die Bundesverwaltung

# 3 Sichere Endgeräte für die Bundesverwaltung

Das Produktportfolio für die Bundesverwaltung deckt diverse Einsatzszenarien ab.

Für den **Geheimhaltungsgrad VS-NfD**[6] (Verschlusssache nur für den Dienstgebrauch) realisiert:

» das **SINA Tablet** von *secunet* (Kapitel 3.1) den vollständigen mobilen Arbeitsplatz, der mittels Virtualisierung mehrere Betriebssysteme voneinander separiert,

» **SecurePIM** (Kapitel 3.4) von *Vitual Solution* sowie **SecuSUITE** (Kapitel 3.3) und **SecuTABLET** (Kapitel 3.2) von *Secusmart* hochmobile Endgeräte für dienstliche Datenkommunikation.

» Verschlüsselte mobile Telefonie ermöglicht die SecuVOICE (Kapitel 3.3.1) App für das SecuSUITE Gerät von *Secusmart.*

Für den Geheimhaltungsgrad bis zu VS-VERTRAULICH bietet das Portfolio schließlich noch das Sprachverschlüsselungsendgerät **TopSec mobile** (Kapitel 3.5) von *Rohde & Schwarz.*

6 Es gibt in der Bundesrepublik Deutschland vier Geheimhaltungsstufen (in aufsteigender Reihenfolge):
VS-NfD; VS-VERTRAULICH; VS-GEHEIM; VS-STRENG GEHEIM


### 3.1 SINA Tablet

Das in Kooperation mit der Firma secunet Security Networks AG entwickelte SINA Tablet stellt das Verbindungsglied zwischen der altbewährten IT und der mobilen IT dar und ist vom BSI für die Verarbeitung von Daten bis zum Geheimhaltungsgrad VS-NfD zugelassen.

Als Geräteplattform kommt eine Auswahl herkömmlicher Tabletcomputer mit leistungsstarken Prozessoren zum Einsatz. Als Betriebssystem dient SINA OS, eine abgesicherte Virtualisierungslösung, über die unterschiedliche Gastsysteme (z. B. aktuelle Windows und Linux-Versionen) ausgeführt werden können. Dies geschieht für den Nutzer transparent, d. h. er kann alle bekannten Anwendungen in seinem gewohnten PC-Betriebssystem einsetzen.

Durch die Virtualisierungstechnik von SINA OS ist die Nutzung mehrerer Gastsysteme mit unterschiedlicher VS-Einstufung

auf demselben Tablet möglich. Somit kann der Nutzer zwischen einem sicheren Arbeitsplatz zur Verarbeitung von VS-NfD-eingestuften Daten und einem offenen Arbeitsplatz wechseln. Hierbei ist eine strikte Trennung der Applikationen und Daten der verschiedenen Arbeitsplätze gewährleistet.

### 3.1.1 SINA Workstation als Basis

Die Softwarebasis des SINA Tablet ist identisch mit derjenigen der bereits langjährig in Behörden und Ministerien eingesetzten SINA Workstation[7]. Dadurch fügt sich das SINA Tablet nahtlos in bestehende SINA-Netzwerkinfrastrukturen ein.

Auch die bewährten Sicherheitsmechanismen der SINA Produktpalette stehen dem SINA Tablet zur Verfügung:

Hierzu gehören die Verschlüsselung aller lokalen Daten, die Verschlüsselung der Datenkommunikation über VPN-Tunnel, sowie die Kontrolle aller Peripheriegeräte und Schnittstellen. Als Vertrauensanker für die sichere 2-Faktor-Authentisierung dient ein kompakter USB-Token mit integrierter microSD-Karte.

7 Weitere Informationen finden Sie in der Broschüre „Sichere Inter-Netzwerk Architektur“

Abbildung 1: SINA Tablet

### 3.1.2 Tablet-spezifische Ausstattung

Sowohl SINA OS als auch die Gastsysteme lassen sich über (Multi-)Touch oder eine virtuelle Touch-Tastatur bedienen. Im Betrieb mit der ansteckbaren Tastatur oder weiteren Komponenten (z.B. externer Monitor) eignet sich das SINA Tablet auch als Desktop-Lösung.

Als Netzwerkschnittstellen stehen je nach Gerät WLAN, 3G/4G und Bluetooth zur Verfügung. Neben Video-Konferenzen und verschlüsselter IP-Telefonie (Voice-over-IP) ist auch der Betrieb als Thin-Client möglich.

Telefonie über das Mobilfunknetz oder über den SNS-Standard sind nicht möglich.


## 3.2 SecuTABLET

SecuTABLET ist eine Lösung für die sichere Verarbeitung von Daten bis zum Geheimhaltungsgrad „Verschlusssache – Nur für den Dienstgebrauch“ auf handelsüblichen Samsung Tablet-PCs.

Abbildung 2: SecuTABLET

Die Sicherheitsarchitektur des Produktes basiert auf dem Samsung Knox-Android Betriebssystem mit Sicherheitserweiterungen. Die zentralen Sicherheitsmerkmale werden auf die Secusmart Security Card (SSC) als kryptografischem Anker zurückgeführt.

### 3.2.1 Applikationen

Das Sicherheitskonzept des SecuTABLET sieht Applikationen für zwei Einsatzkategorien vor:

» Verarbeitung dienstlicher Daten (eingestuft bis zu VS-NfD)

» Offene Kommunikation und offene Datenverarbeitung

Beide Applikationsgattungen werden dem mobilen Endgerät über den EASE[8]-Server zur Verfügung gestellt.

Bevor Applikationen der ersten Kategorie zugeordnet werden können müssen sie zunächst einer Sicherheitsevaluierung unterzogen werden und eine Freigabe erhalten.

Diese Applikationen dürfen schützenswerte Daten (VS-NfD) verarbeiten und ihnen steht für die Anbindung an das dienstliche Hintergrundsystem ein exklusiver VPN-Tunnel zur Verfügung. In der Benutzeroberfläche sind sie durch ein kleines Schloss auf dem entsprechenden Icon gekennzeichnet.

Applikationen für offene Kommunikation und Datenverarbeitung erbringen keine Sicherheitsleistung. Sie müssen daher vor Einsatz auf den Endgeräten lediglich mittels des App-Checkers auf Schadwirkung untersucht werden.

Diese Applikationen sind strikt gegen die freigegebenen Applikationen abgeschottet. Sie können weder auf schützenswerte Daten zugreifen, noch mit den freigegebenen Applikationen kommunizieren. Ebenso ist ihnen die Nutzung des „dienstlichen“ VPN-Tunnels verwehrt.

8 EASE: Enterprise App Services Environment

### 3.2.2 Sicherheitsarchitektur

SecuTABLET wird langfristig in bestehende SecuSUITE-Infrastrukturen integriert. Das Hintergrundsystem besteht aus

» dem für VS-NfD zugelassenen SINA-VPN Gateway

» EASE-Server

» Standard IT-Komponenten, bspw. E-Mail-Server

» Mobile Device Management System, optional

Der EASE Server stellt dem mobilen Endgerät den SecuSTORE (App-Store) zur Verfügung und dient der sicherheitsrelevanten Endgeräte-Verwaltung:

Auf dem EASE-Server werden die applikationsspezifischen Container erzeugt. Dies wird als „App-Wrapping“ bezeichnet. Der Prozess des „App-Wrappings“ befähigt die jeweilige Applikation zum sicheren Umgang mit schützenswerten Daten.

Konkret bedeutet das

» Ablageverschlüsselung:
Sichere persistente Ablage der dienstlichen Daten mit applikationsspezifischem Schlüssel. Die SSC verhindert den unberechtigten Zugriff auf dieses Schlüsselmaterial.

» Transportverschlüsselung:
Sichere Datenkommunikation mit dem Hintergrundsystem über IPsec. Schutz des privaten Nutzerschlüssels und der Zertifikate mittels SSC.

» Sicherer Datenaustausch zwischen Applikationen: Gewährleistung, dass sichere Daten nur von dienstlichen Applikationen verarbeitet werden dürfen. Die hierfür erforderlichen Gruppenschlüssel sind gegen den unberechtigten Zugriff durch die SSC geschützt.

Zugriffsrechte für jede dienstliche Applikation werden im EASE-Server definiert und bieten einen zusätzlichen Schutz gegen unerlaubten Datenabfluss und -zufluss.

Die Sicherheitsmerkmale des App-Wrappings basieren auf Richtlinien (Policies). Nach dem Wrapping-Vorgang wird die Applikation vom EASE Server signiert und über den SecuSTORE dem Nutzer zur Verfügung gestellt.

Die Secusmart Security Card (SSC) stellt den Sicherheitsanker zum Schutz des kryptographischen Materials dar. Es handelt sich um die in Secusmart-Lösungen eingesetzte Micro SD Karte mit integriertem Krypto-Controller. Zugriff auf kryptographische Funktionen der SSC ist nur durch eine vom Nutzer festzulegende Smartcard PIN möglich. Für SecuTABLET dient sie der sicheren Erzeugung und Ablage von Schlüsselmaterial bzw. Zertifikaten.

SecuTABLET stellt die Integrität des Betriebssystems sowohl beim Start als auch zur Laufzeit des mobilen Endgeräts sicher. Über Samsung KNOX Funktionen wird gewährleistet dass das System nur mit vertrauenswürdiger Firmware bootet.

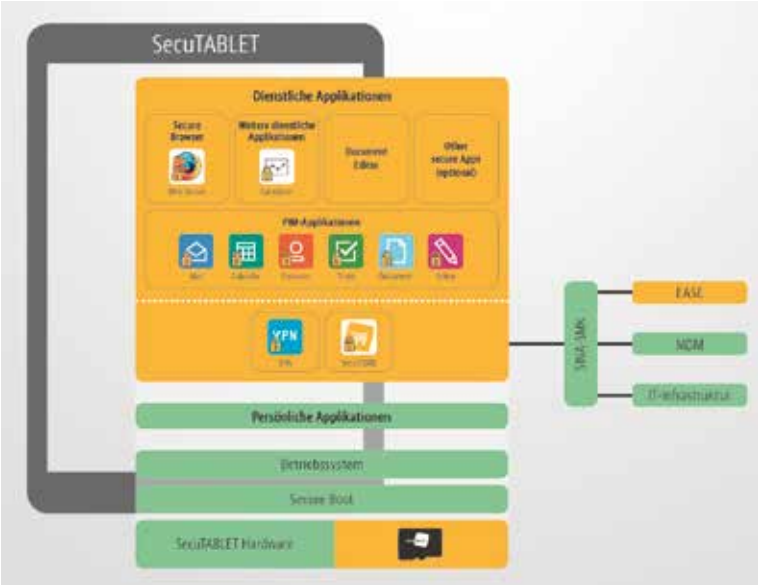
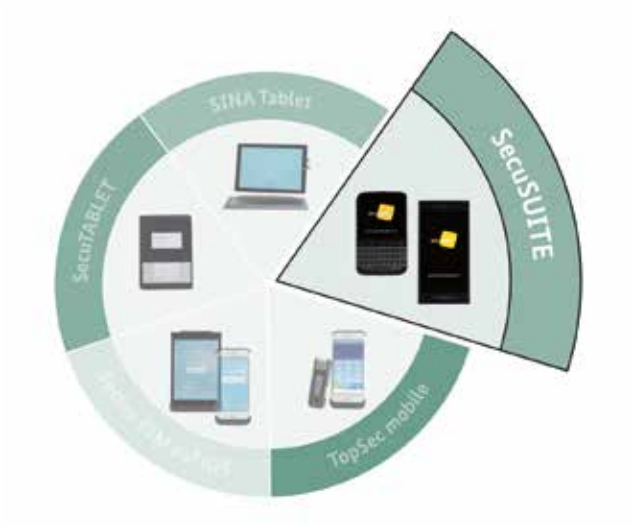



Abbildung 3: SecuTABLET Systemkomponenten




## 3.3 SecuSUITE

Das Produkt SecuSUITE der Firma Secusmart bietet eine Lösung für sichere Sprach- und Datenkommunikation basierend auf BlackBerry10-Endgeräten.

SecuSUITE integriert die microSD-Karte von Secusmart mit Sicherheitschip des BSI in das BlackBerry10-Betriebssystem und nutzt sie als zusätzlichen Sicherheitsanker für die nativen Sicherheitsmechanismen des BB10-Systems. Diese beinhalten u. a. VPN-Funktionalität, Verschlüsselung der Daten auf dem Endgerät und Funktionalität zum Remote-Management der Endgeräte.

Abbildung 4: SecuSUITE

### 3.3.1 Sicherheitskonzept des Endgeräts

Die Perimeterseparation von BB10 ermöglicht eine Trennung zu schützender und offener Daten. Daher sind auch zwei unabhängige Daten-Kommunikationswege vorgesehen:

Aus dem persönlichen Perimeter, der für die Verarbeitung offener Daten genutzt werden kann, kommt man direkt und ohne Umweg in das Internet.

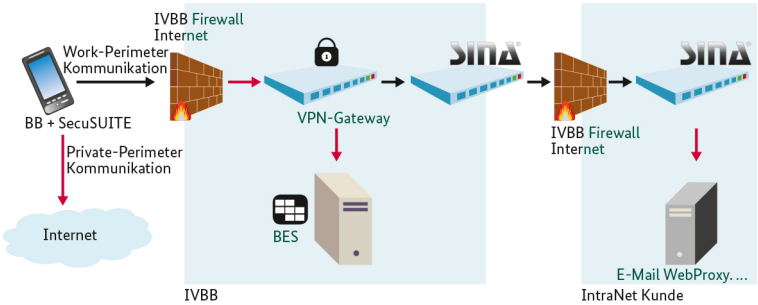



Abbildung 5: Die Architektur der Datenlösung von SecuSUITE mit zentralem BES

Die Kommunikation aus dem Work-Perimeter, der der Verarbeitung und dem Zugriff auf schützenswerte Daten dient, wird gemäß dem eingerichteten VPN-Profil grundsätzlich durch einen SINA-VPN-Zugang zum IVBB geleitet.

Von dort aus erreicht das Endgerät sowohl den zentralen BES[9], der für die Administration der Endgeräte zuständig ist, als auch sein zugehöriges Hausnetz. Erst dort werden die PIM-Daten mit den entsprechenden Servern synchronisiert oder auf hausinterne Verzeichnisse zugegriffen.

9 BlackBerry Enterprise Service

Die Kommunikationsstrecke zwischen dem IVBB in die Hausnetze der einzelnen Behörden und Ministerien wird ebenfalls mit SINA-VPN-Gateways verschlüsselt.

### 3.3.2 Applikationen

Über den BES können Applikationen in den Work-Perimeter ausgerollt werden. Dazu müssen sie zunächst einer Sicherheitsevaluierung unterzogen werden und eine Freigabe erhalten.

Im persönlichen Perimeter dürfen Applikationen durch die Anwender installiert werden, sofern sie vor Einsatz auf den Endgeräten mittels des App-Checkers auf Schadwirkung untersucht werden.

### 3.3.3 Sprachverschlüsselung

Mittels der SecuVOICE-App unterstützt SecuSUITE Sprachverschlüsselung mittels SNS-over-IP. Dazu wird eine zentrale SNS-Server-Infrastruktur benötigt.

Das SecuSUITE Endgerät meldet sich initial am Authentisierungsserver an, um die Zugangsberechtigung für das SNS-over-IP-System zu erhalten. Versucht es später, einen sicheren Anruf aufzubauen, stellt der SIP-Proxy den Kontakt zum Zielgerät her.

Dabei wird der SIP-Proxy durch einen Policy-Server unterstützt. Handelt es sich bei dem Zielgerät nicht um ein registriertes SNS-over-IP-Endgerät, entscheidet er auf Basis vorgegebener Regeln darüber, ob die Verbindung an das SNS-Media-Gateway oder an ein rot/schwarz Gateway, z. B. das IVBB Secure-Landing-Gateway (SecuGATE Z der Firma Secusmart) weitergereicht werden soll.

Das SNS-Media-Gateway führt eine Protokollumsetzung von IP auf ISDN/V.110 durch, wenn der Gesprächspartner ein ISDN/CSD-basiertes SNS-Legacy-Endgerät verwendet.

Verwendet der Gesprächspartner kein SNS-Endgerät, sondern ein „normales", nicht verschlüsselndes Telefon, stellt der Policy Server die Verbindung über ein rot/schwarz Gateway her, das daraufhin das Gespräch für die Gegenseite entschlüsselt.

Befindet sich der andere Gesprächsteilnehmer im IVBB wird die Verbindung hinter dem rot/schwarz Gateway durch den IVBB über VPN geschützt und ist trotz Entschlüsselung sicher.

Befindet sich der andere Gesprächsteilnehmer im öffentlichen Telefonnetz (PSTN) ist die Verbindung hinter dem rot/schwarz Gateway nach Verlassen des IVBBs ungeschützt. In diesem Fall bietet die SNS-Verschlüsselung lediglich einen Schutz vor dem Abgreifen des Telefonats auf der Mobilfunkschnittstelle.

Das SNS-Media-Gateway sowie die rot/schwarz Gateways des IVBB (SecuGATE Z, auch Secure-Landing-Gateway genannt, und SecuGATE C) gehen aus einer Kooperation zwischen Secusmart und Sirrix hervor. Die SNS-Infrastruktur ist eine Secusmart-Lösung.

## SiMKo3/SecuSUITE Netzanbindung

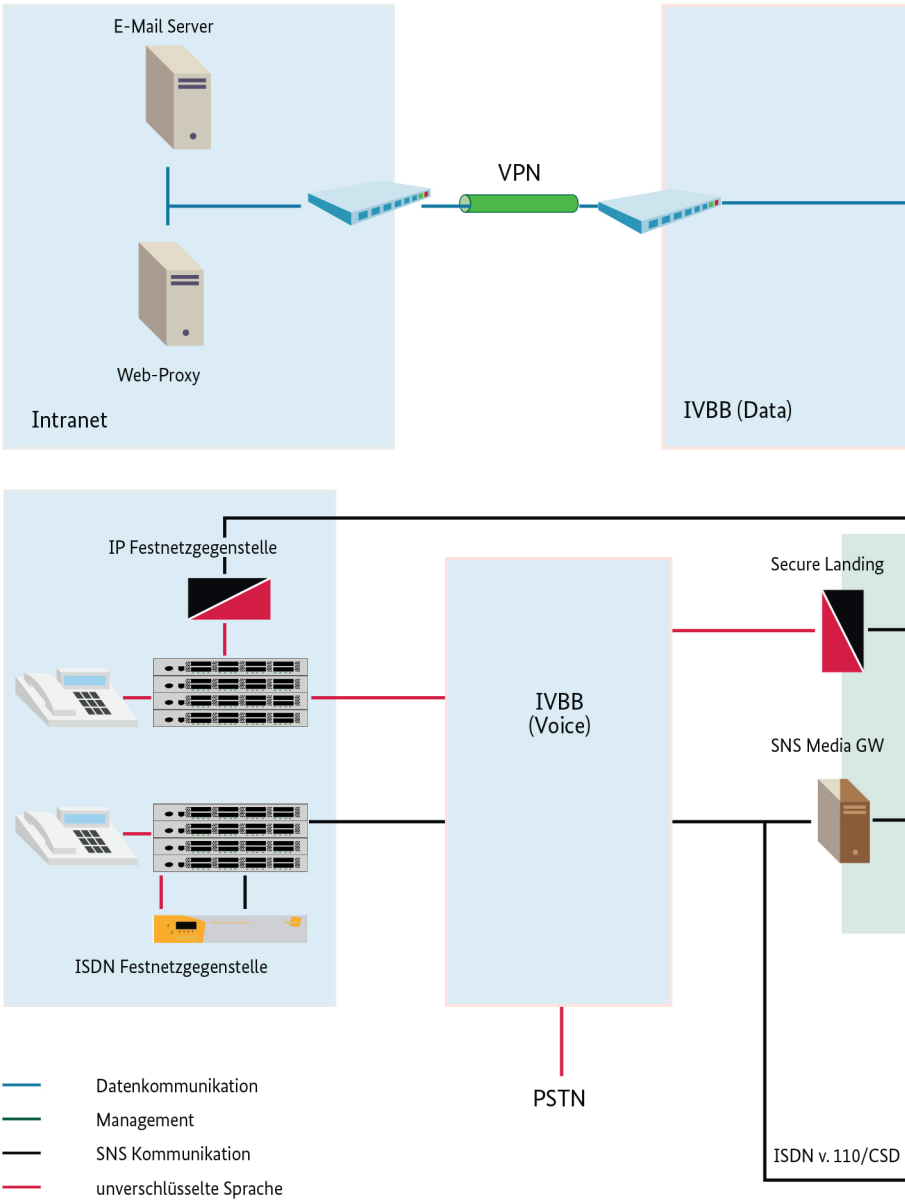
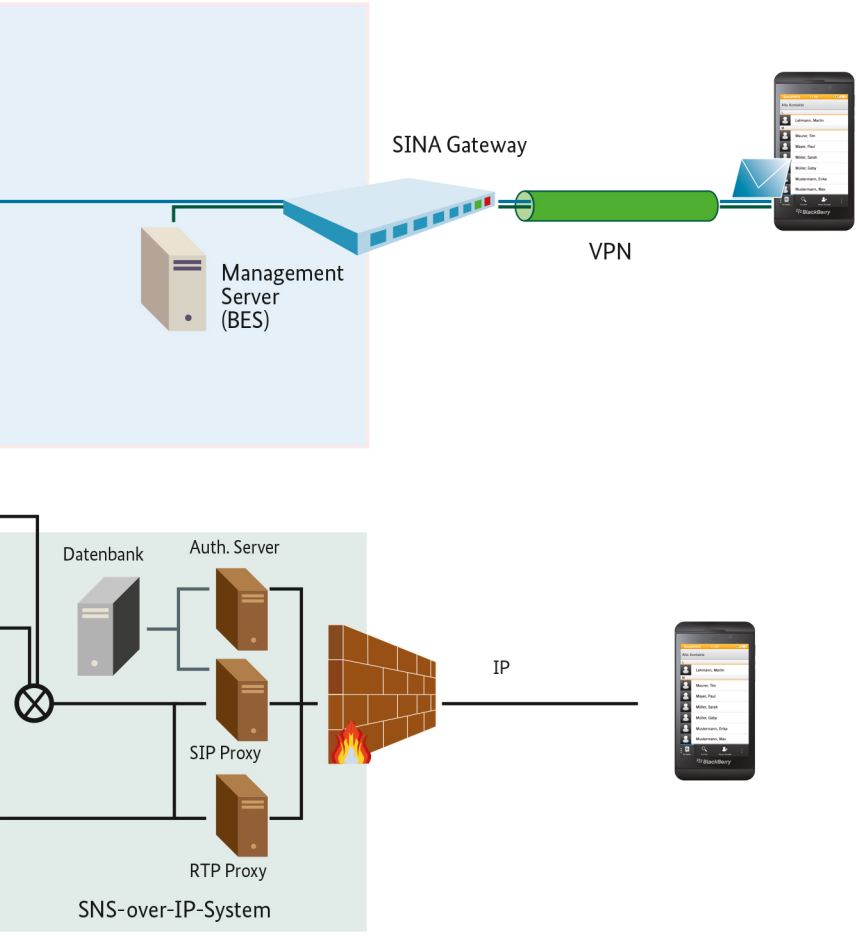



Abbildung 6: Netzwerkarchitektur SecuSUITE


SINA Gateway
VPN
Management
Server
(BES)
Datenbank
Auth. Server
SIP Proxy
RTP Proxy
SNS-over-IP-System
IP


### 3.4 SecurePIM

SecurePIM bietet behördlichen Nutzern die Möglichkeit, Daten mit mobilen Endgeräten (iPhone, iPad) über einen zentralen IVBB-Zugang mit Servern in ihren Hausnetzen zu synchronisieren.

Der Hersteller Virtual Solution bettet die mobile Datensynchronisationslösung SecurePIM in ein Gesamtsystem bestehend aus einer Infrastruktur mit dem genuscreen VPN-Gateway der Firma genua und zentralem Management und Monitoring ein.


Abbildung 7: SecurePIM auf iOS-Endgerät mit Sleeve.

SecurePIM ist eine Container Applikation, die auf dem Endgerät installiert wird, von anderen iOS-Apps aber durch Sicherheitsmechanismen gekapselt ist, um ungewollten Datenabfluss zu verhindern. Die Smartcard, die bei dieser Lösung zum Einsatz kommt wird mittels eines Sleeves mit dem Gerät verbunden.

### 3.4.1 SecurePIM auf iOS-Endgeräten im IVBB

SecurePIM bietet in diesem System dem Nutzer folgende Funktionen:

» Sichere Synchronisation mit Exchange-Servern: E-Mail, Kontakte, Kalender, Notizen und Aufgaben. Der SecurePIM-Client kann hierbei auf mehrere Postfächer zugreifen.

» Sicherer Download von Dokumenten (Office, PDF, Bilder) von Sharepoint-Servern

» Sicheres Browsing im Intranet

» Sichere lokale Speicherung und Bearbeitung der synchronisierten Daten auf dem iOS-Endgerät.

Eine App für verschlüsselte Telefonie ist langfristig geplant.

### 3.4.2 Applikationen

Neben der SecurePIM-App kann der Nutzer auf seinem iOS-Endgerät weitere öffentlich verfügbare Apps für die Verarbeitung von nicht eingestuften Daten, die für seine dienstlichen Belange erforderlich sind, installieren und verwenden, wie bspw. Apps für die Reiseplanung, Nachrichtenportale oder in-

House Apps[10], sobald sie mittels des App-Charakters auf Schadwirkung untersucht wurden.

### 3.4.3 Sicherheitskonzept

Das Sicherheitskonzept der SecurePIM-Lösung der Bundesverwaltung beruht auf folgenden Komponenten:

» *SecurePIM:* Als Kernkomponente der iOS-basierten Systemlösung wurde diese App und die zentralen Server des SecurePIM-Systems durch Virtual Solution im Auftrag des BSI um besondere Sicherheitsfunktionen für den behördlichen Einsatz erweitert.

» *Smartcard:* Der Betrieb von SecurePIM ist nur in Verbindung mit einer Smartcard als Sicherheitsanker möglich. Die Smartcard wird zur TLS-Verschlüsselung des Traffics zwischen dem mobilen SecurePIM-Client und den Servern im Hausnetz der Behörde und zur Verschlüsselung der lokal gespeicherten synchronisierten Daten auf dem Endgerät (Secure Data at Rest) verwendet. Ferner dient die Smartcard als Authentisierungstoken des Nutzers gegenüber der SecurePIM-App (2-Faktor-Authentisierung durch Wissen und Besitz).

» *Sleeve:* Die Smartcard wird über einen Adapterrahmen (Sleeve) mit dem iOS-Gerät verbunden. Sleeves sind verfügbar für alle aktuellen iOS-Geräte.

» *Bluetooth-Kartenleser:* Das BSI untersucht derzeit, ob statt des Sleeves ein Bluetooth Kartenleser verwendet werden kann, so

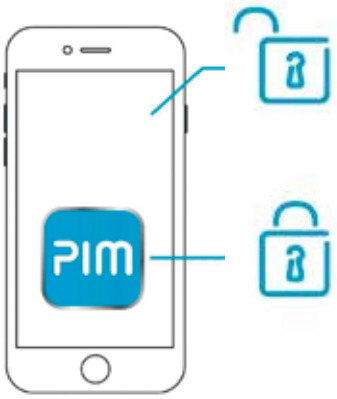
10 In-House-Apps sind Apps, die nicht im iOS-App-Store zu finden sind, sondern ausschließlich unternehmensintern ausgerollt werden.

dass eine geräteunabhängige Smartcardanbindung erfolgen kann.

» *App-Checking:* Sicherheitsüberprüfung mittels des App-Checkers aller weiteren Apps, die neben SecurePIM auf dem iOS-Endgerät installiert werden: Die Auswahl der Apps erfolgt durch den IT-Verantwortlichen der Behörde.

» *Zentrales Management:* Alle iOS-Endgeräte werden durch ein Mobile Device Management (MDM) und die SecurePIM-App durch ein Mobile Application Managment (MAM) konfiguriert und überwacht, das durch die jeweilige Behörde zu betreiben ist.

» *Betriebssystem:* Die iOS-Endgeräte werden ausschließlich unter einem sicheren Konfigurationsprofil im Supervised Mode betrieben. Im Rahmen der Evaluierung des Gesamtsystems führt das BSI eine Sicherheitsevaluierung der iOS-Funktionen durch, die die Sicherheitsziele von SecurePIM der Systemlösung unterstützen.




**Nicht eingestufte / nicht sicherheitsrelevante Daten:**
» Keine Veränderungen am Gerät selbst
» Kontrolle durch Nutzer
» Persönliche Nutzung freigegebener Apps möglich

**Eingestufte / sicherheitsrelevante Daten:**
» Secure Container als Teil des Behördennetzes
» Mail, Kontakte, Kalender, Aufgaben, Notizen, Browser und Dokumente auf SharePoint
» Volle Kontrolle durch interne IT
» Verschlüsselung für lokale Daten und Kommunikation durch SC-Integration

Abbildung 8: SecurePIM – Secure-Container-Konzept

» *Betrieb des iOS-Endgeräts innerhalb des IVBB:* Der gesamte Traffic des iOS-Endgeräts wird über den IVBB geroutet. Von dort erfolgt die Weiterleitung in das Internet oder in die Netze der Behörden. Die Verbindung des Endgeräts mit dem IVBB ist VPN-verschlüsselt. Innerhalb des IVBB werden alle Daten einem Sicherheitsmonitoring zur Erkennung der Signatur von möglicher Schadsoftware unterzogen. Die Einbindung der iOS-Clients in den IVBB ist in der folgenden Abbildung dargestellt:

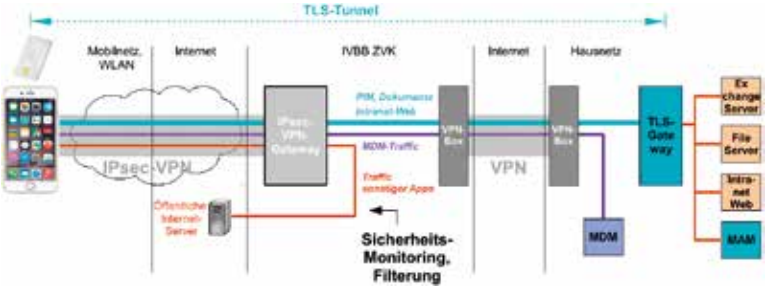



Abbildung 9: SecurePIM VPN-Anbindung


## 3.5 TopSec Mobile

Für höhere Sicherheitsansprüche, wie z. B. für die Verarbeitung von VS-VERTRAULICH (VS-V) eingestuften Daten, sind noch weiterreichende Maßnahmen zu treffen, als bei den Sicherheitslösungen für VS-NfD.

### 3.5.1 TopSec Mobile VS-V

Das TopSec Mobile des Herstellers Rohde & Schwarz ist ein solches mobiles Sprachverschlüsselungsgerät für Ende-zu-Ende gesicherte Telefonie. Bis zu VS-V eingestufte Informationen können über das TopSec Mobile mittels

Abbildung 10: TopSec mobile

VoIP-Verbindungen kommuniziert werden.

Als externes Verschlüsselungsgerät wird es über Bluetooth® an Smartphones, Tablets, PCs oder Satellitenterminals angebunden. Diese Basisgeräte haben dann nur noch die Funktion eines Netzadapters (im weitesten Sinne die eines Netzmodems), während alle entscheidenden Sicherheitsfunktionen für den Schutz der Sprache auf das externe TopSec Mobile ausgelagert sind.

Abbildung 11: TopSec mobile App

Die Aufnahme, Verschlüsselung und Wiedergabe erfolgt ausschließlich auf der vertrauenswürdigen Hardware des TopSec Mobile.

Damit ist die Sicherheitslösung TopSec Mobile in ihren wesentlichen Eigenschaften prinzipiell unabhängig von den Sicherheitseigenschaften des Basisgerätes und somit auch unabhängig von der Sicherheitsproblematik, die durch Viren, Trojaner, Spyware und der Zuverlässigkeit mobiler Plattformen entsteht.

Der Verbindungsaufbau erfolgt durch eine TopSec Mobile-App auf dem mobilen Endgerät. Diese verfügt über alle für Telefonie üblichen Funktionen, wie Telefonbuch, Kontaktlisten, Anrufliste und Tastenfeld. Das TopSec Mobile kann grundsätzlich mit iOS, Android, Blackberry und Windows-PCs verwendet werden.

Die vom BSI für VS-VERTRAULICH zugelassene Produktversion ist für VoIP-Telefonie innerhalb geschlossener Nutzergruppen konzipiert. Zum VoIP-Betrieb gehört auch ein VoIP-Server,

der die Verbindungen zwischen den TopSec Mobile-Clients aufbaut, und der durch die Nutzergruppe betrieben wird.

Das TopSec Mobile-System ist damit unabhängig von öffentlichen VoIP-Service-Providern und von nationalen Telefonnetzen. Die einzige netzseitige Voraussetzung für TopSec Mobile-gesicherte Telefonie ist ein hinreichend breitbandiger und Jitter-armer Internetzugriff, der in mobilen Netzen über EDGE, UMTS und LTE meist gegeben ist.

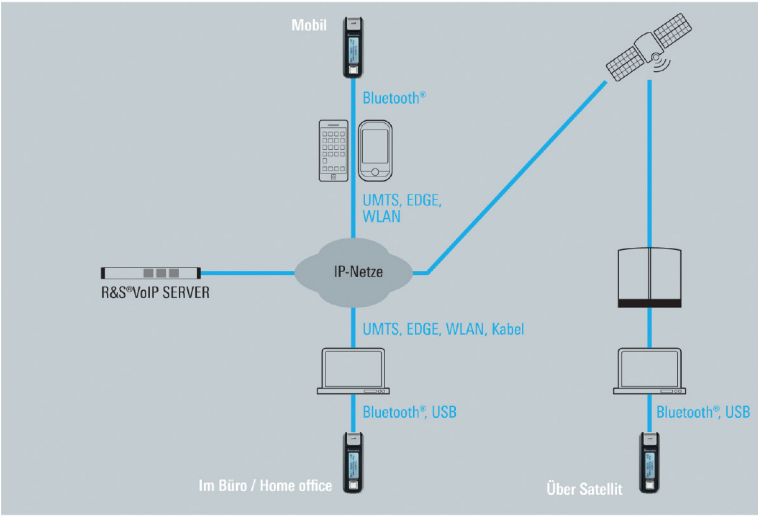



Abbildung 12: TopSec mobile – Anbindung verschlüsselte Sprache

Für VS-VERTRAULICH eingestufte Telefonie wird der VoIP-Service durch Rohde & Schwarz zentral für die Nutzergruppe aller Bundesbehörden angeboten. Darüber hinaus ist eine weitere Separierung von Nutzergruppen mit besonderen Sicherheitsanforderungen möglich, indem diese einen eigenen VoIP-Server betreiben.

# 4 SNS – Sichere Netzübergreifende Sprachkommunikation

# 4 SNS – Sichere Netzübergreifende Sprachkommunikation

Um unerwünschte Mithörer auszuschließen, müssen Sprachdaten von Mobilfunkgesprächen auf der gesamten Kommunikationsstrecke zwischen Anrufer und Angerufenen geschützt werden. Man spricht in diesem Zusammenhang von einer „Ende-zu-Ende"-Verschlüsselung, da das Sprachsignal auf seinem Weg von einem zum anderen Ende der Übertragungskette abhörsicher verschlüsselt bleibt. Ein Lauschangriff auf das GSM-Netz oder ein Abgreifen in der Netzinfrastruktur führen in diesem Fall ins Leere, da die Ende-zu-Ende-Verschlüsselung im Allgemeinen nicht so einfach zu überwinden ist, wie die veralteten Sicherheitsmechanismen des Mobilfunknetzes.

Für Anwendungsfälle, in denen ausschließlich die Mobilkommunikation einer geschlossene Benutzergruppe abgesichert werden soll, zum Beispiel im Rahmen der firmeninternen Kommunikation, existiert mittlerweile eine Vielzahl an Produkten mit diversen Verschlüsselungslösungen. Dabei reicht die Palette der weltweit verfügbaren Lösungen von der preiswerten Software bis hin zur teuren Spezialhardware.

Leider erweist sich gerade die Vielfalt an technischen Lösungen als zentrales Hindernis für die Verbreitung dieser wichtigen Sicherheitstechnologie:

Wer auch immer beabsichtigt, sein Telefonat durch den Einsatz von Ende-zu-Ende-Verschlüsselung abzusichern, muss nicht nur hoffen, dass der Angerufene auch über ein Telefon mit zusätzlicher Verschlüsselungsapplikation verfügt. Es muss darüber hinaus am anderen Ende der Leitung auch ein Produkt

vorhanden sein, welches mit dem des Anrufers kompatibel ist. Die Wahrscheinlichkeit für einen solchen Zufallstreffer ist praktisch gleich null, sodass sicheres Telefonieren heute de facto nur innerhalb geschlossener Benutzergruppen möglich ist.

Um die Sicherheitslücken des GSM-Netzes wirksam schließen zu können, muss somit zunächst eine Interoperabilität der vorhandenen Sicherheitslösungen herbeigeführt werden. Erst unter dieser Voraussetzung ist mit einer nennenswerten Zunahme von verschlüsselter mobiler Sprachkommunikation zu rechnen. Dabei liegt der Gedanke nahe, dass Interoperabilität schlicht durch eine technische Vereinheitlichung der Produkte zu erreichen ist. Die Erfolgsaussichten für die Etablierung eines einheitlichen Ende-zu-Ende-Verschlüsselungsstandards im Mobilfunkbereich sind jedoch eher gering, denn die Kosten- und Sicherheitsniveaus der vorhandenen Produkte sind zu unterschiedlich, die Interessen der einzelnen Firmen oder gar Nationalstaaten zu vielfältig.

**Lösungsansatz – Vielfältigkeit zulassen**

Mit dem im Jahr 2010 definierten SNS-Standard verfolgt das BSI einen alternativen Ansatz zur Lösung des Interoperabilitätsproblems, der nicht auf eine schwer zu erreichende allgemeine Vereinheitlichung zielt. Vielmehr werden Vielfalt und Unterschiedlichkeit der Systeme als unvermeidliche Randbedingung der Problematik akzeptiert.

Der SNS-Standard geht davon aus, dass mobile Endgeräte grundsätzlich verschiedene Betriebsmodi beherrschen können. Die Verschlüsselungssoftware eines Herstellers A könnte dann nicht nur in dem von Hersteller A selbst entwickelten Betriebsmodus funktionieren, sondern in einem weiteren

Betriebsmodus, der ursprünglich für die Lösung des Herstellers B entwickelt wurde. Die Endgeräte müssen sich lediglich beim Aufbau der Verbindung „einigen“, welcher der beiden Betriebsmodi und somit welches Verschlüsselungskonzept im weiteren Gesprächsverlauf zum Einsatz kommt.

Dazu stellt SNS der eigentlichen Kommunikation eine Aushandlungsphase voran, in welcher die Endgeräte über ein dafür bestimmtes Protokoll ohne Einflussnahme des Nutzers einen sicheren Betriebsmodus auswählen. Demnach muss lediglich das verwendete Aushandlungsprotokoll von allen Endgeräten umgesetzt werden.

Damit sichergestellt ist, dass die Endgeräte in der Aushandlungsphase immer einen gemeinsamen Modus vorfinden, liefert der SNS-Standard zusätzlich zwei Basis-Betriebsmodi. In diese können die Endgeräte zurückfallen, wenn sie mit einem Endgerät konfrontiert werden, das ansonsten keine der eigenen Modi kennt.

Da die Software moderner Smartphones ähnlichen Bedrohungen ausgesetzt ist wie die herkömmlicher Desktop-Rechner oder Laptops, sieht das Sicherheitskonzept der Basis-Betriebsmodi vor, dass eine externe Hardwarekryptokomponente, die **BOS-Sicherheitskarte,** den Vertrauensanker für die Kommunikation bildet. Zertifikate, Schlüssel und Verschlüsselungsalgorithmen sind somit sicher von angreifbaren Softwarekomponenten getrennt und eine Kompromittierung des Gesamtsystems über ein kompromittiertes Endgerät wird verhindert.

## 4.1 Aushandlungsprotokoll

Die von SNS zu Gesprächsbeginn vorgeschriebene Aushandlungsphase zwischen den Endgeräten verläuft für den Nutzer vollständig transparent. Es wird also weder gefordert, dass der Nutzer vorher weiß, ob sein Gesprächspartner mit dem Betriebsmodus XY zu erreichen ist und sein Gerät entsprechend einstellt, noch ist sein Einwirken erforderlich.

Die algorithmische Umsetzung der initialen Aushandlung ist sehr einfach (Abbildung 9). Das Verhandlungsverfahren besteht aus nur einem einzigen bilateralen Kommunikationsschritt, bei dem eine Liste der möglichen Betriebsmodi an das jeweils andere Gerät übertragen wird. Jeder aufgeführte Betriebsmodus repräsentiert dabei ein eigenes Paket bestehend aus Diensten, Sprachkodierung (Vocoder) und Sicherheitskonzept (Authen-

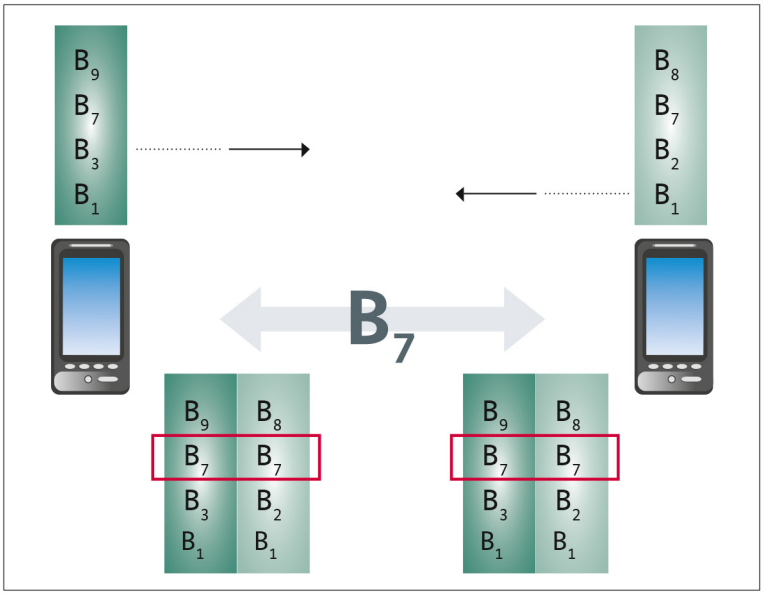



Abbildung 13: SNS-Betriebsmodusaushandlung

tisierung, Verschlüsselung ...), welches von dem jeweiligen Endgerät unterstützt wird.

Durch einen Vergleich der beiden Listen bestimmen beide Seiten unabhängig voneinander den ersten übereinstimmenden Eintrag (in Abbildung 9) und vollziehen anschließend den weiteren Verbindungsaufbau nach den Vorgaben dieses gemeinsamen Betriebsmodus.

Das Verhandlungsverfahren kann prinzipiell in alle bereits vorhandenen Produktlösungen integriert werden und dort die Funktion eines generischen Interoperabilitätsprotokolls erfüllen.

Ausgehend von dieser Basiseigenschaft lässt sich Interoperabilität flexibel und auf vielfältige Weise gestalten und weiterentwickeln, auch innerhalb der Produktlinie eines Herstellers.

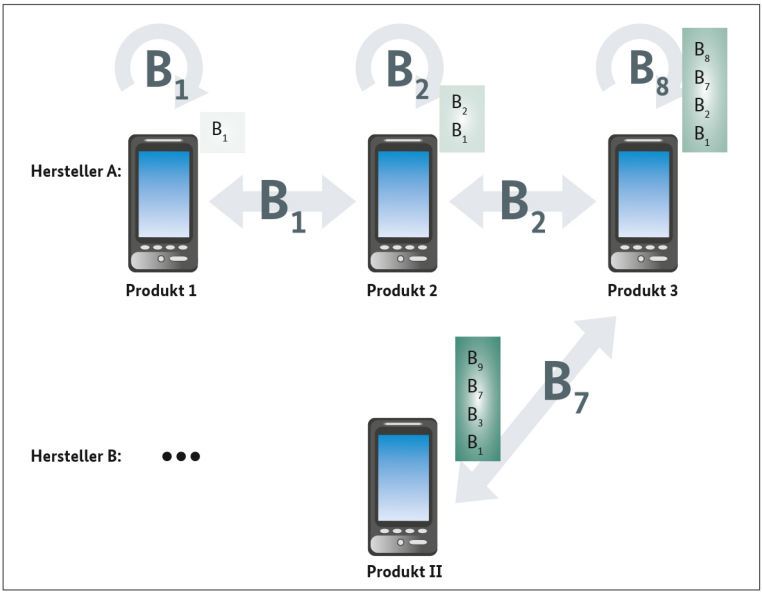



Abbildung 14: SNS-Betriebsmodusaushandlung - Interoperabilität

Das Beispiel in Abbildung 10 zeigt die Produktlinie des Herstellers A, in der nacheinander im Zuge der technischen Weiterentwicklung die Produkte 1 bis 3 entstehen. Durch den Einsatz des Verhandlungsverfahrens gelingt es, im Verbindungsaufbau den jeweils geeigneten Betriebsmodus auszuwählen. So wird der Betriebsmodus B1 nur bei Verbindungen zu älteren Geräten (Produkt 1) benutzt. Neuere Geräte wählen den jeweils aktuellsten auf beiden Geräten verfügbaren Betriebsmodus aus (B2, B8), um damit verbundene Vorteile nutzen zu können.

Die Interoperabilität zu den Produkten eines Herstellers B kann im Zuge Weiterentwicklung der Produktlinie ebenfalls realisiert werden (B7).

Durch den Einsatz des Verhandlungsverfahrens lässt der Standard also zu, dass jeder Hersteller seine eigene Produktlinie anbieten und weiterentwickeln und so seinen Kunden eine maßgeschneiderte Lösung nach deren Bedarf anfertigen kann. Die Interoperabilität zum bereits vorhandenen Gerätebestand geht dabei nicht verloren.

## 4.2 SCIP-Interoperabilität

Das gewählte Aushandlungsprotokoll orientiert sich in großen Teilen an SCIP1-210. SCIP ist ein im NATO-Umfeld verwendeter Standard für sichere Sprach- und Datenkommunikation, wobei SCIP 210 den Signalisierungsplan definiert.

Neben den bereits genannten Vorteilen des Aushandlungsprotokolls soll durch die Wahl des SCIP[11]-210-Protokolls auch die Möglichkeit geschaffen werden, zukünftig Endgeräte mit dualer SNS- und SCIP-Funktionalität zu entwickeln. So ist es

11 SCIP: Secure Communications Interoperability Protocol

schon jetzt den Endgeräten anhand der jeweiligen Protokoll-ID möglich, bei der Signalisierung den Partner als SNS- oder als SCIP-Endgerät zu identifizieren.

### 4.3 Basis-Betriebsmodi

Damit in jedem Fall ein gemeinsamer Modus gefunden werden kann, hat das BSI für den SNS-Standard zwei Basis-Betriebsmodi definiert, die von allen SNS-Endgeräten der Bundesverwaltung unterstützt werden müssen.

Diese unterscheiden sich nur geringfügig voneinander:

» Betriebsmodus 1 ist der TETRA-BOS-Kompatibilitätsmodus (→ BOS-Interoperabilität). Er berücksichtigt die TETRA-spezifischen Anforderungen an die Datenstrukturen, um eine Ende-zu-Ende-verschlüsselte Sprachkommunikation zwischen TETRA-Netz und GSM-Netz zu ermöglichen.

» Betriebsmodus 2 wurde für die Verwendung im CSD-Kanal optimiert und kann so eine bessere Sprachqualität erzielen.

Gemeinsam sind beiden Betriebsmodi hingegen die unterstützten Dienste, der Vocoder und das Sicherheitskonzept.

Primär bietet SNS den Schutz von Sprachkommunikation, also verschlüsselte Telefonie. Derzeit werden ausschließlich Duplex-Rufe, also Telefonie im herkömmlichen Sinn, unterstützt. Es wurden aber bereits Vorkehrungen getroffen, die später eine Integration von Halbduplex-Rufen erlauben soll. Dies sind Gespräche, bei denen immer nur im Wechsel gesprochen werden kann, beispielsweise nach Drücken einer PTT-Taste. Dadurch können Gruppenrufe wie im Sprechfunkverkehr bzw. Konferenzschaltungen realisiert werden.

Weiterhin wird ein Dienst zur parallelen Datenübertragung während des Telefonats geboten. Dazu wird ein zuverlässiger Datenkanal ( → reliable transport) bereitgestellt, der sowohl verschlüsselte als auch unverschlüsselte Daten innerhalb des Sprachkanals übertragen kann.

Darüber hinaus bietet der Standard einen Dienst zur Aushandlung von SMS-Schlüsseln während eines laufenden Telefonats (→ Sicherheitseigenschaften und -dienste).

Als Vocoder kommt der TETRA-CODEC zum Einsatz. Dieser verwendet für die Sprachkodierung ein ACELP-Kodierungsmodel (Algebraic Code Exited Linear Prediction) mit einem eigenem Codebook [1]. Er benötigt eine Datenrate von 7,2 kbit/s. Weitere Informationen zum TETRA-CODEC können dem ETSI-Standard entnommen werden.

SNS verwendet für die Basis-Betriebsmodi die BOS-Sicherheitskarte, die auch im digitalen Behördenfunk zum Einsatz kommt. Diese externe Hardwarekryptokomponente bildet den Vertrauensanker des Systems. Die BOS-Karte wurde im Hinblick auf eine verlustbehaftete Funkstrecke konzipiert und bietet daher ein entsprechend robustes Verschlüsselungssystem. Weiterhin ist durch ihre Verwendung eine Kompatibilität auf kryptographischer Ebene zu den sich im Einsatz befindenden TETRA-BOS-Funkgeräten gegeben.

### 4.4 Sicherheitseigenschaften und -dienste

Auf jeder BOS-Sicherheitskarte ist ein Nutzerzertifikat hinterlegt, das dem jeweiligen Besitzer über eine Teilnehmerkennung eindeutig zugeordnet ist und dessen **Authentizität** durch die BOS-PKI (Public-Key-Infrastruktur) gewährleistet wird. Jede BOS-Karte kann sich somit über ihr Zertifikat anderen

BOS-Karten gegenüber als **authentisch** ausweisen. Diejenigen Karten, die für die SNS-Geräte der Bundesverwaltung personalisiert wurden, enthalten in ihrem Zertifikat, in Form des Domänen-Namens der Behörde, auch die Information, welchem Organisationsbereich der Nutzer angehört.

Diese Nutzerzertifikate werden direkt nach der Aushandlungsphase zu Beginn der Gesprächsphase zwischen den Endgeräten ausgetauscht. Die Karten prüfen jeweils die Authentizität des eingegangenen Zertifikats und geben dem Nutzer bei erfolgreicher Verifikation den Domänen-Namen der Behörde des Gesprächspartners zurück.

Zusätzlich wird über das Zertifikat unterschieden, ob es sich bei der Karte um eine SNS-Karte für mobile Endgeräte, eine Multi-Krypto-Komponente, wie sie in Festnetzgegenstellen eingesetzt wird, oder um eine Karte für mobile Endgeräte aus dem BOS-Umfeld handelt. Auch diese Information wird von der Karte an die Endgeräte geliefert und von diesen ausgewertet und dem Nutzer angezeigt.

Parallel zur Authentisierung findet die Schlüsseleinigung statt. Über das Elliptic Curve Diffie-Hellman-Verfahren handeln beide Karten einen individuellen Gesprächsschlüssel aus. Dieser Schlüssel wird nur für dieses Gespräch verwendet und ist nur den beiden BOS-Sicherheitskarten bekannt. Im weiteren Verlauf des Gesprächs wird der Schlüssel als Input bei der Erzeugung des Schlüsselstroms, welcher die Sprachdaten verschlüsselt, verwendet.

Auch SMS können mit SNS sicher ausgetauscht werden. Eine wie bei der Sprachverbindung vorgeschaltete Schlüsseleinigung direkt vor Versand der SMS wäre allerdings unpraktisch, da bei Versand von SMS keine direkte Verbindung zwischen den

Teilnehmern besteht. So kann eine SMS auch versandt werden, wenn das Gerät des Empfängers ausgeschaltet ist.

Daher handeln die SNS-Endgeräte präventiv SMS-Schlüssel für die spätere Verwendung während SNS-Telefonaten aus. Diese Aushandlung geschieht ohne Interaktion durch den Nutzer und für den Nutzer vollständig transparent. Die ausgehandelten Schlüssel werden, mit einem eigens dafür vorgesehenen Schlüssel verschlüsselt, abgelegt.

Soll zu einem späteren Zeitpunkt eine SMS verschlüsselt an den entsprechenden Nutzer versandt werden, so bietet das Endgerät selbstständig die Verwendung des ausgehandelten SMS-Schlüssels an.

Ist kein Schlüssel vorhanden, weil noch kein Telefonat zwischen den entsprechenden Teilnehmern stattgefunden hat, so kann auf einen Default-Schlüssel zurückgegriffen werden. In diesem Fall wird der Nutzer vor Versand der SMS gewarnt.

### 4.5 SNS-over-IP

Durch die anfängliche Wahl von CSD als Kanal wurde zunächst eine gute Abdeckung innerhalb Deutschlands erzielt und somit ein zuverlässiges Kommunikationsmedium gewählt. Mittlerweile lösen aber zunehmend IP-basierte Netze die alten GSM Netze ab. Auch firmeninterne WLANs bieten sich als Medium an. Sie alle bieten durch ihre größeren verfügbaren Datenraten und geringes Delay mehr Gesprächskomfort.

Um SNS für den IP-Einsatz weiterzuentwickeln, hat das BSI im Jahr 2011 die Hersteller von Sprachverschlüsselungssystemen zu mehreren Workshops eingeladen. 13 nationale und

internationale Hersteller und Dienstleister haben die Einladung angenommen und wertvollen Input bei der Erarbeitung von SNS-over-IP geliefert. Der Fokus des Workshops war es, zunächst ein firmen-/behördeninternes SNS-over-IP-Konzept zu entwickeln, das die hausinterne mobile Kommunikation absichert und damit veraltete DECT-Einrichtungen durch SNS-over-IP-Systeme ersetzen kann. Aber auch externe Kommunikation mit IP-fähigen SNS-Endgeräten in öffentlichen Netzen war gefordert. Dass darüber hinaus die Kompatibilität mit den existierenden CSD-Geräten erhalten bleibt, war eine Auflage an das Konzept.

Das Ergebnis der Workshops war eine initiale Version der SNS-over-IP Erweiterung für den SNS-Standard. Dieser initiale Entwurf „SNS over IP“ wurde im Zuge der Inbetriebnahme der SNS-over-IP-Infrastruktur und der Produkte SecuSUITE und SiMKo3 weiterentwickelt und kann zusammen mit den bisherigen Teilen des SNS-Standards beim BSI angefordert werden.

Die Produkte SiMKo3 und SecuSUITE sind die ersten SNS-over-IP-fähigen Endgeräte.

### 4.6 Netze

Der SNS-Standard ist ein Sitzungsschicht-Protokoll und somit grundsätzlich unabhängig von den unterliegenden Protokollen und Netzen. Der Datenstrom wird durchgereicht, so wie er ist. Zwischen getrennten Netzen oder unterschiedlichen Protokollen kann durch Gateways eine Protokollumsetzung durchgeführt werden, ohne dass die Ende-zu-Ende-Verschlüsselung durch eine Umschlüsselung aufgebrochen werden muss.

Da allerdings zunächst kein Gespräch zustande kommen kann, wenn beide Teilnehmer in physisch getrennten Netzen oder mit verschiedenen Protokollen senden, musste zunächst ein Übertragungskanal und ein Übertragungsprotokoll gewählt werden.

### 4.6.1 CSD-Kanal/ISDN V.110

Zu Anfang (2010) wurde der CSD-Kanal (Circuit Switched Data) von GSM für SNS ausgewählt, der eine Datenrate von 9,6 kbit/s zur Verfügung stellt.[12]

Innerhalb Deutschlands liefert GSM immer noch die beste Abdeckung, dadurch konnte zum einen überall dort wo GSM Netzabdeckung besteht auch verschlüsselt telefoniert werden. Zum andern weist der CSD-Kanal geringen Jitter (Änderungen des Delays) auf, der bei Sprachkommunikation weit störender ist als Delay (Verzögerungen). Weiterhin findet netzintern bereits eine Protokollumsetzung zwischen CSD und dem ISDN V.110 Datenkanal statt. Dadurch müssen keine zusätzlichen Gateways für Kommunikation zwischen Festnetz und Mobilfunknetz installiert werden.

### 4.6.2 SNS-over-IP (3G/4G)

Mit SNS-over-IP wurden auch modernere Übertragungskanäle (3G/4G) für SNS erschlossen. Die für SNS-over-IP notwendigen Signalisierungs- und Kommunikationskonventionen sind im Teil 6 des Standards festgehalten worden.

12 Benötigt werden lediglich 7,2 kbit/s für den verwendeten ACELP-Vocoder.

Die Interoperabilität der CSD-basierten und 3G/4G basierten Endgeräte wird dadurch gewährleistet, dass die SNS spezifischen Protokollschichten (beschrieben in SNS Teil 2-5) unverändert geblieben sind. Es muss also lediglich eine Protokollumsetzung zwischen ISDN V.110 und IP (mit Secure SIP und RTP) erfolgen.

#### 4.6.2.1 Anbindung an offene Telefonnetze / Break-out-Modus

Ein von Anwendern vielfach bemängeltes Problem von Sprachverschlüsselungen ist der Mehraufwand bei der Bedienung, der auch dadurch zustande kommt, dass nicht in jedem Fall von Vornherein klar ist, ob der Gesprächspartner ebenfalls „verschlüsselungsfähig“ ist.

Rot/schwarz Gateways stellen hier ein nützliches Bindeglied dar, die es den Anwendern erlauben grundsätzlich verschlüsselte Telefonie zu verwenden und die Verbindungsherstellung vollständig der Infrastruktur zu überlassen: Kann der Gesprächspartner nicht verschlüsselt erreicht werden, so entschlüsselt das rot/schwarz Gateway die Kommunikation und stellt das Telefonat, nach voriger Warnung an den Anwender, über das öffentliche Telefonnetz her. Dieses Telefonat ist dann lediglich auf der mobilen Luftschnittstelle geschützt und nicht für den Austausch von VS-NfD eingestuften Informationen geeignet.

Damit dieses Verfahren bei einer großen Anzahl Anwender entsprechend skaliert, wurde in Absprache zwischen Secusmart und dem BSI ein weiterer Operationsmodus definiert, der, anders als die für VS-NfD geeignete Kommunikation, die BOS-Sicherheitskarte nicht während des gesamten Gesprächs in Anspruch nimmt.

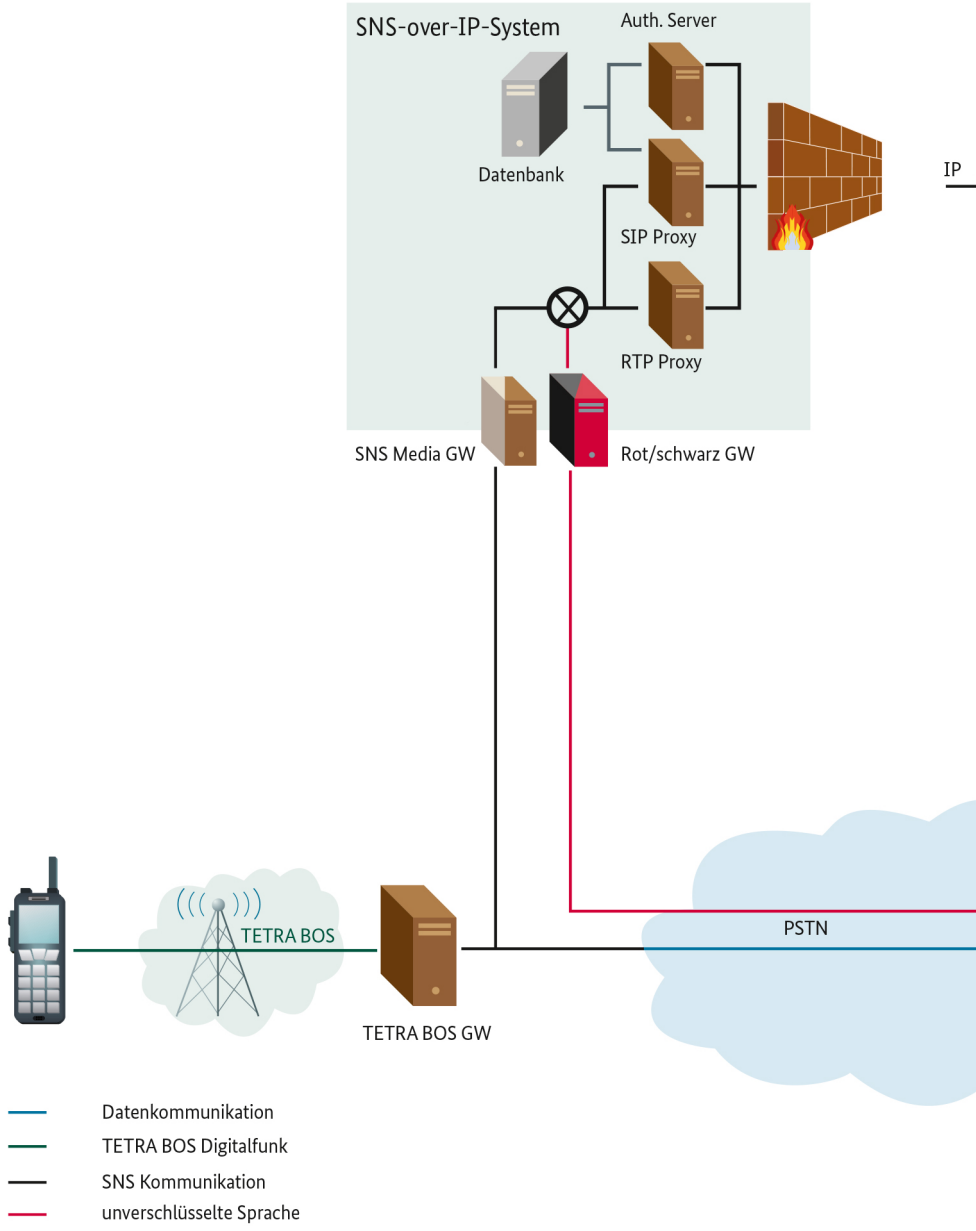
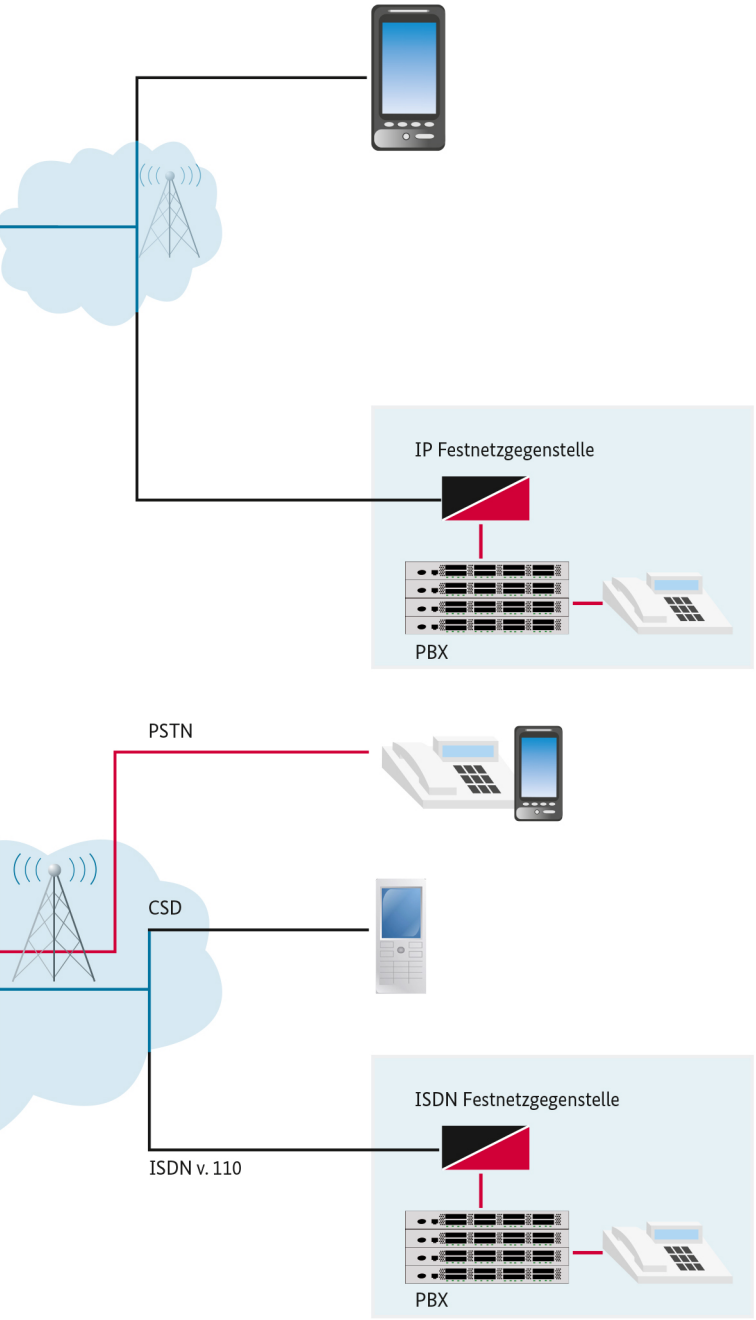



Abbildung 15: SNS – bisher unterstützte Netze


IP Festnetzgegenstelle
PBX
PSTN
CSD
ISDN v. 110
ISDN Festnetzgegenstelle
PBX

### 4.6.3 BOS-Interoperabilität (BOS-TETRA-Netz)

Da mit der BOS-SKE[13] die kryptographischen Algorithmen des TETRA-BOS-Systems für SNS übernommen wurden, ist SNS auf kryptographischer Ebene kompatibel zu BOS.

Weiterhin wurden bei der Definition des Betriebsmodus 1 die TETRA-BOS-spezifischen Protokollvorgaben übernommen, beispielsweise Framelängen und Framestealing-Vorgaben. Dadurch lässt sich mittels eines Gateways, welches ausschließlich eine Protokollumsetzung durchführt, ein Ende-zu-Ende verschlüsselter Ruf zwischen Teilnehmern im TETRA-BOS-Netz und GSM-Netz aufbauen.

Abbildung 15 stellt die aktuellen Möglichkeiten netzübergreifender SNS Kommunikation dar.

## 4.7 SNS-Starter-Kit

Um Entwicklern den Einstieg in SNS zu erleichtern, hat das BSI das „SNS-Starter Kit“ entwickeln lassen.

Das Starter-Kit enthält mehrere ID-000-Karten der BOS-Test PKI und die Software für ein „Golden Device“. Das „Golden Device“ implementiert den SNS-Standard, einschließlich diverser Testfälle, und kann Entwicklern als Referenzsystem dienen. So kann ein erstes Ausprobieren mit wenig Aufwand stattfinden und der Schritt zur vollständigen SNS-Implementierung erleichtert werden.

Derzeit unterstützt das Golden Device SNS auf Basis von CSD und ISDN V.110.

13 SKE: Sicherheitskarte Typ E

# 5 Legacy-Produkte

# 5 Legacy-Produkte

## 5.1 Sprachkommunikation

Im Zuge des IT-Investitionsprogramms[14] wurde die Bundesverwaltung mit Endgeräten für sichere Sprachkommunikation ausgerüstet.

### 5.1.1 Mobile Endgeräte

Es wurden zwischen 2010 und 2013 ca. 5600 mobile Endgeräte für die Bundesverwaltung angeschafft. Dabei handelt es sich um 3600 SecuVoice SNS Geräte der Firma Secusmart und 2000 TopSec mobile SNS Geräte der Firma Rohde & Schwarz.

#### 5.1.1.1 SecuVoice SNS

Die Firma Secusmart hat eine Lösung entwickelt, die auf micro-SD-Karten basiert. Der BOS-Chip ist hier auf einer micro-SD-Karte aufgebracht und wird von dieser intern angesteuert. Die SNS-Software befindet sich auf der micro-SD-Karte, deren Treiber sich bei Stecken der Karte auf dem Endgerät installieren. Die micro-SD-Karte bietet zusätzlich eine verschlüsselte Partition zur sicheren Ablage von Daten.

Abbildung 16: SecuVOICE SNS

14 http://www.bmi.bund.de/DE/Themen/OeffentlDienstVerwaltung/Informationsgesellschaft/IT-Investitionsprogramm/it_investitionsprogramm_node.html

SecuVoice SNS implementiert sowohl sichere Sprache als auch sichere SMS.

Verwendbar ist diese Lösung mit Nokia-Handys mit dem Symbian-Betriebssystem.

#### 5.1.1.2 TopSec mobile SNS

Die Lösung der Firma Rohde & Schwarz SIT verwendet ein separates Bluetooth-Gerät, das die Original BOS-SKE in SIM-Format enthält. Der Nutzer spricht direkt in das TopSec mobile SNS, welches daraufhin die Verschlüsselung vornimmt. Über Bluetooth hält das TopSec mobile SNS Kontakt zum Handy und übermittelt die verschlüsselten Daten.

Abbildung 17: TobSec mobile SNS

TopSec mobile SNS dient ausschließlich der Sprachverschlüsselung.

Die vollständige Liste der kompatiblen Handys kann der Webseite des Herstellers Rohde & Schwarz entnommen werden.

### 5.1.2 Festnetzgegenstellen

Nicht überall dürfen mobile Endgeräte verwendet werden. Besonders in sicherheitskritischen Bereichen ist die Mitnahme von Handys oft untersagt. Damit diejenigen, die in solchen Bereichen arbeiten, ebenfalls über SNS erreichbar sein können und um generell eine Anbindung von Anwendern im Festnetz zu ermöglichen, wurden 2011 Festnetzgegenstellen gekauft.

Mit den ca. 800 einkanaligen (ISDN S0) SecuGate LI1 und 56 mehrkanaligen (ISDN S2M) SecuGate LI30 der Firma Secusmart ist die Bundesverwaltung seit Herbst 2011 auch für SNS im Festnetz gerüstet.

#### 5.1.2.1 SecuGate LI1

Die Firma Secusmart hat in Kooperation mit TipTel das SecuGate LI1 entwickelt.

Abbildung 18: SecuGate LI1

Dabei handelt es sich um eine Festnetzgegenstelle zu SNS für ISDN-S0 Anschlüsse. Das SecuGate LI1 wird vor dem ISDN-Telefon angeschlossen und terminiert somit die Ende-zu-Ende-Sprachverschlüsselung direkt auf dem Schreibtisch. Dem Nutzer wird über Sprachansage und Displayanzeigen, die an das ISDN-Telefon gesendet werden, die sichere Verbindung signalisiert.

#### 5.1.2.2 SecuGate LI30

Abbildung 19: SecuGate LI30

Das SecuGate LI30, das von der Firma Secusmart in Kooperation mit Sirrix entwickelt wurde, ist eine mehrkanalige Festnetzgegenstelle für den Anschluss an eine Telefonanlage. Das LI30 kann bis zu 30 parallele Kanäle verarbeiten und terminiert die Verschlüsselung direkt an der Telefonanlage, die die Gespräche dann an die jeweiligen Endgeräte leitet. Auch hier wird dem Nutzer über Sprachansage und

Displayanzeigen, die an das ISDN-Telefon gesendet werden die sichere Verbindung signalisiert.

### 5.1.3 TETRA-BOS-Gateway (Prototyp)

Ein Prototyp für ein Gateway zwischen dem BOS-TETRA-Netz und dem PSTN-Netz wurde im Auftrag des BSI von T-Systems entwickelt. Das Gateway wird über die LS1-Schnittstelle an das TETRA-Netz angeschlossen und ermöglicht verschlüsselte Telefonie und verschlüsselte SMS zwischen Teilnehmern der beiden Netze.

Bevor ein Rufaufbau aus dem PSTN-Netz in das BOS-Netz zustande kommt, wird die Berechtigung des Teilnehmers aufgrund seiner BOS-Kartenidentität geprüft.

## 5.2 Datenkommunikation

Im Zuge des IT-Investitionsprogramms wurde die Bundesverwaltung auch mit Endgeräten für sichere Datenkommunikation ausgerüstet.

### 5.2.1 SiMKo2

Zwischen 2010 und 2013 wurden mehr als 4000 SiMKo2-Smartphones für die Bundesverwaltung angeschafft.

SiMKo2 ist ein Smartphone-basiertes System des Herstellers T-Systems für das mobile Arbeiten. Der Nutzer kann jederzeit und von jedem

Abbildung 20: SiMKo2

Ort aus sicher auf seine PIM[15]-Daten (Personal Information Management) zugreifen, also auf Kalender, E-Mails, Kontakte und Aufgaben. Außerdem kann er den Internetzugang seiner stationären IT-Infrastruktur sowie klassische Office-Programme sicher nutzen. SiMKo2 kann mit den verbreiteten Groupwaresystemen wie Microsoft Exchange, Novell Groupwise oder Lotus Notes/Domino synchronisieren; auch eine Adaption an die Open Source Groupware Kolab ist erfolgt.

Wesentliche Sicherheitsmerkmales des Systems SiMKo2 sind:

» „Digitale Identität". Jedes SiMKo2-Endgerät erhält ein durch eine vertrauenswürdige Zertifizierungsstelle (Trustcenter) ausgestelltes Zertifikat. Alle Sicherheitsoperationen wie Verschlüsselung der Nutzerdaten oder Berechnung der kryptografischen Schlüssel für die drahtlose Anbindung werden auf Basis dieser digitalen Identität durchgeführt. Die Erteilung des Zertifikats erfolgt pseudonymisiert, die Zuordnung eines SiMKo2-Nutzers zu einem SiMKo2-Zertifikat erfolgt erst durch den IT-Administrator des Nutzers.

» Sichere 2-Faktor-Authentisierung durch Besitz (Endgerät mit Kryptokarte) und Wissen (PIN).

» Verschlüsselung aller lokal gespeicherten Daten. Diese sind nur nach Eingabe der Geräte-PIN zugänglich.

» VPN-gesicherte Datenkommunikation zwischen dem Endgerät und dem zugeordneten Server innerhalb der gesicherten stationären IT-Infrastruktur.

15 Personal Information Management

» Abgesicherter Boot-Prozess. Dieser stellt sicher, dass die Gerätesoftware gegenüber dem evaluierten Zustand nicht verändert werden kann.

» Kontrollierter Prozess zur Installation von Zusatzsoftware. Software benötigt zur Ausführung eine digitale Signatur, die nur mit Zustimmung des BSI erteilt wird.

SiMKo2 wurde von T-Systems auf Basis von verschiedenen HTC-Smartphones angeboten und betrieben und ist mittlerweile durch SIMKo3 abgelöst worden.

### 5.2.2 SiMKo3

SiMKo3 ist das Nachfolgeprodukt zum Vorgänger SiMKo2 er Firma T-Systems. Es ist eine sichere, mobile Erweiterung des Büroarbeitsplatzes auf Smartphones (Samsung Galaxy S3) und Tablets (Samsung Note 10.1) um jederzeit und von jedem Ort aus sicher auf PIM-Daten, also auf E-Mails, Kalender, Kontakte und Aufgaben, zugreifen zu können.


Abbildung 21: SiMKo3

SiMKo3 synchronisiert VPN geschützt die PIM-Daten mit den Groupwaresystemen mittels ActiveSync-Protokoll.

SiMKo3 verwendet Separations- und Virtualisierungstechnik um das Konzept eines „Dual-Face-Devices“ umzusetzen: Grundlage ist ein Microkernel (L4-Kernel), auf dem verschiedene Android Gast-Betriebssysteme aufsetzen.

So steht dem Benutzer neben dem sicheren Compartment mit Zulassung für die Verarbeitung von Daten bis zum Geheimhal-

tungsgrad „VS – Nur für den Dienstgebrauch“ auch ein offenes Compartment zur Verfügung.

Während das sichere Compartment abgesicherte Verbindungen in das heimische Netzwerk gewährleistet, bietet das offene Compartment direkten Zugang zum Internet und größtmögliche Freiheitsgrade für den Nutzer. Die Applikationen und Daten bleiben zwischen den beiden Bereichen strikt voneinander getrennt. Die Kommunikation kann sowohl via Mobilfunknetz als auch über WLAN erfolgen.

Die folgende Abbildung skizziert die Sicherheitsarchitektur des SiMKo3-Endgerätes:

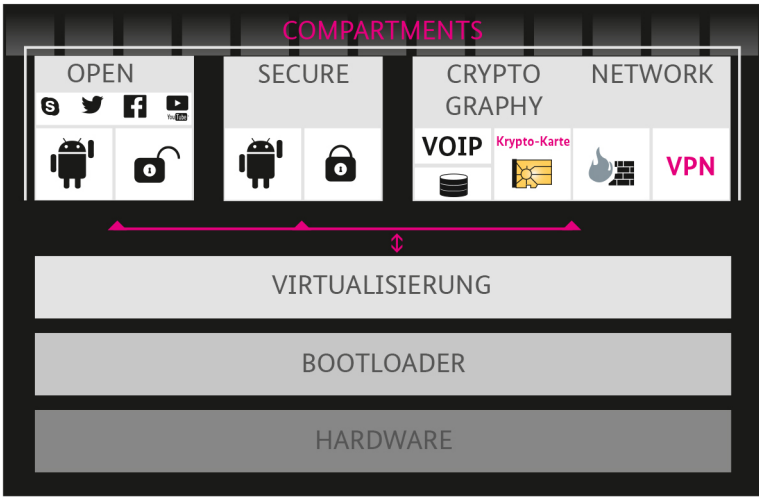



Abbildung 22: Sicherheitsarchitektur des SiMKo3-Systems

Die wesentlichen Sicherheitsmerkmale des SiMKo3-Systems sind:

» Sichere 2-Faktor-Authentisierung durch Besitz (Endgerät mit Kryptokarte) und Wissen (PIN) durch Einbindung einer

µSD Kryptokarte als Schlüssel- und Zertifikatsspeicher sowie Sicherheitsanker.

» Starke Verschlüsselung aller lokal gespeicherten Daten – Diese sind nur nach Eingabe der korrekten Geräte-PIN zugänglich.

» VPN-gesicherte Datenkommunikation zwischen dem Endgerät und dem zugeordneten VPN-Gateway (NCP) in der gesicherten, stationären IT-Infrastruktur.

» Abgesicherter Boot-Prozess – Dieser stellt sicher, dass das Gerät mit der evaluierten Software arbeitet.

» „Digitale Identität" – Alle Sicherheitsoperationen werden auf Basis der digitalen Identität von Zertifikaten einer vertrauenswürdigen PKI durchgeführt. Die Zuordnung eines SiMKo3-Nutzers zu einem SiMKo3-Zertifikat erfolgt durch den IT-Administrator des Nutzers.

» Personalisierung durch den Nutzer – Verbleib aller nutzerbezogenen Daten beim Nutzer.

» Kontrollierter Prozess zur Installation von Zusatzsoftware Software benötigt zur Ausführung eine digitale Signatur, die nur mit Zustimmung des BSI erteilt wird.

» Over-The-Air-Updates – Installation vom BSI geprüfter und zugelassener Updates.

» Sichere verschlüsselte Telefonie nach SNS-Standard.

Die Anbindung von SiMKo3 an die IT-Infrastruktur im IVBB ist in Abbildung 23 illustriert.

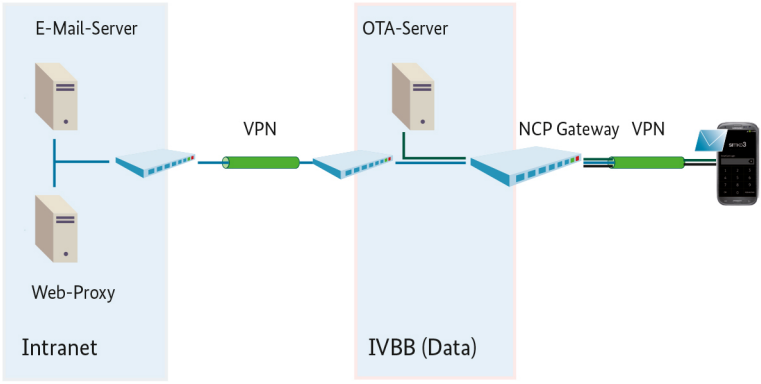



Abbildung 23: Netzwerkanbindung des SiMKo3-Systems

# 6 Weiterentwicklung & Ausblick

# 6 Weiterentwicklung & Ausblick

Mobiles Arbeiten bringt große Veränderung in die angestammten Arbeitsabläufe. Diesen Prozess sicher zu gestalten erfordert große Anstrengungen, auch über die reinen technischen Aspekte hinaus. Das BSI wird auch zukünftig dazu beitragen, nutzerfreundliche und sichere Lösung für die Bundesverwaltung und darüber hinaus zu gestalten.

## 6.1 Weitere mobile Endgeräte

Das BSI bereitet derzeit ein Evaluierungsverfahren vor, um die Sicherheitseigenschaften des Produkts BizzTrustTM für Android der Firma Rohde & Schwarz zu untersuchen und zu prüfen, ob BizzTrustTM zukünftig die Basis einer weiteren Lösung für die Bundesverwaltung bilden könnte.

BizzTrust für Android ist eine Plattform für Smartphones und Tablets, die mit einem gehärteten Sicherheitskern für Android das System in zwei Bereiche unterteilt: Einen persönlichen Bereich („Personal“) und einen Unternehmensbereich („Business“).

Anwendungen und Daten in den jeweiligen Bereichen sollen streng voneinander getrennt werden, um beispielsweise zu verhindern, dass eine vom Benutzer installierte App auf sensitive Unternehmensdaten zugreifen kann.

Der „Business“-Bereich ermöglicht einen Zugriff auf Unternehmensressourcen: So können Anwendungen aus dem Business-Bereich über einen VPN-Tunnel auf Ressourcen des Unterneh-

mens, wie E-Mail, Kontakte, Kalender und Intranet zugreifen und untereinander Daten austauschen. Der Zugriff auf externe Webseiten erfolgt im Business-Bereich über die Unternehmensfirewall, die potenziell gefährliche Inhalte ausfiltern kann.

BizzTrust integriert darüber hinaus eine einfach zu nutzende E-Mail-Verschlüsselung nach dem S/MIME-Standard.

Durch die Trennung der persönlichen Daten von Unternehmensdaten in separaten Bereichen bleibt die Flexibilität des Smartphones erhalten.

BizzTrust ist derzeit auf Sony-Geräten der Xperia-Z3-Serie verfügbar sowohl auf dem Tablet, als auch auf dem Mobiltelefon.

Voraussetzung für die Nutzung von BizzTrust ist der Trusted Objects Manager (TOM) der Firma Sirrix. Dabei handelt es sich um ein zentrales Management. Der TOM ermöglicht die Verteilung von Software und Firmware-Updates, von Sicherheitsprofilen sowie die Remote-Konfiguration der Geräte. Auch Apps, die von der Behörde freigegeben sind, können über den TOM zentral verteilt werden.

# 7 Kontaktinformationen

# 7 Kontaktinformationen

Das BSI stellt den SNS-Standard und die darin enthaltene technische Spezifikation des Verhandlungsverfahrens interessierten Firmen auf Anfrage zur Verfügung.

Weitere Informationen finden Sie auf der Webseite des BSI unter
www.bsi.bund.de

Kontakt:
Bundesamt für Sicherheit in der Informationstechnik
Referat KT14
Postfach 20 03 63
53133 Bonn
E-Mail: bsi@bsi.bund.de
sns@bsi.bund.de

## 7.1 Kontakte zu den Herstellern

Um Näheres über die zugelassenen Produkte zu erfahren wenden Sie sich bitte an die jeweiligen Hersteller:

» SINA Tablet – secunet Security Networks AG
  Web: https://www.secunet.com
  E-Mail: info@secunet.com

» SecuTABLET, SecuSUITE – Secusmart GmbH
  Web: https://www.secusmart.com
  E-Mail: info@secusmart. com

» SecurePIM:

  » Virtual Solution:
    Web: https://www.securepim.com
    E-Mail: kontakt@virtual-solution.com

  » Computacenter:
    Web: http://www.computacenter.de
    E-Mail: marcus.meister@computacenter.com

» TopSec Mobile – Rohde & Schwarz
  Web: www.cybersecurity.rohde-schwarz.com
  E-Mail: martin.wilske@rohde-schwarz.com

# 8 Literatur

# 8 Literatur

[1] ETSI EN 300 395-1 Terrestrial Trunked Radio (TETRA); Speech codec for full-rate traffic channel; Part 1: General description of speech functions, 2004-09

# Impressum

**Herausgeber**
Bundesamt für Sicherheit in der Informationstechnik – BSI
Godesberger Allee 185–189
53175 Bonn
E-Mail: bsi@bsi.bund.de
Internet: www.bsi.bund.de
www.bsi-fuer-buerger.de · www.facebook.com/bsi.fuer.buerger

**Bezugsquelle**
Bundesamt für Sicherheit in der Informationstechnik – BSI
Godesberger Allee 185–189
53175 Bonn
E-Mail: mobilfunksicherheit@bsi.bund.de
sns@bsi.bund.de
Internet: www.bsi.bund.de
Telefon: +49 (0) 22899 9582-0
Telefax: +49 (0) 22899 9582-5400

**Stand**
Oktober 2016

**Druck**
Druck- und Verlagshaus Zarbock GmbH & Co. KG
60386 Frankfurt am Main

**Bildnachweis**
Fotolia: Titelbild, Seiten 8, 9, 11, 12 und 13
Sonstige: BSI

**Texte und Redaktion**
Bundesamt für Sicherheit in der Informationstechnik – BSI

**Artikelnummer**
BSI-Bro16/323

www.bsi.bund.de