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 88 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. Zielgruppen 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 potentiell 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 wohlmöglich 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 noch keine vergleichbar leistungsfähige Virenscanner verfügbar, was mitunter darauf zurückzuführen ist, dass sie mit ihrer Energie haushalten müssen und sich daher den konstanten Stromverbrauch durch Hintergrundscans nicht leisten können.

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)

Bedrohungen gehen nicht nur von extern eingeschleuster Schadsoftware aus – auch legale, über offizielle Kanäle installierbare mobile Anwendungen, sogenannte „Apps“, können insbesondere im Umgang mit sensitiven Informationen ein Risiko darstellen.

Häufig verschicken sie auf den Endgeräten angefallene Daten an verschiedene Dienste 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, potentiellen 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.

Erarbeitung eines Sicherheitskonzeptes

Notwendige Konsequenz ist, dass im Umgang mit sensiblen Daten zunächst ein Sicherheitskonzept erarbeitet und im-

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)

plementiert 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 über eine sichere Verbindung zwischen Endgeräten und dem internen Netzwerk erfolgen. Hierzu kann das mobile Endgerät auf Lösungen zurückgreifen, die auch schon bei Notebooks zum Einsatz kommen, z.B. VPN[3] -Tunnel, 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 internen 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 5), geschützt werden.

3 Virtual Private Network

4 Sichere Netzübergreifende Sprachkommunikation

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, 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 zunächst wieder geprüft werden.

Weiterhin kann es ratsam sein, die Nutzung von Apps mit App- oder betriebssystemspezifischen 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.

5 Mobile Device Management

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.

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 Sichere Endgeräte für die Bundesverwaltung

2 Sichere Endgeräte für die 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 Mobiltelefone direkt aus dem Handel nicht geeignet, um eingestufte Daten zu verarbeiten.

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

2.1 Handlungsansatz

Aus diesem Grund wurde im Jahr 2012 eine Ausschreibung[6] sicherer mobiler Endgeräte für die Bundesverwaltung vorgenommen. Ziel waren Smartphones, die sowohl die Anforderungen modernen mobilen Arbeitens erfüllen, als auch die hohen Sicherheitsanforderungen, die sich aus der Verarbeitung sensibler Daten ergeben.

2.1.1 Anforderungen an sichere mobile Endgeräte

Um die Versorgungssicherheit für die Bundesverwaltung zu gewährleisten, legte die Ausschreibung Wert darauf, zwei separate

6 B 3.20 - 3613/12: „Rahmenverträge über Lieferung, Installation und Betrieb eines Systems für die sichere mobile Kommunikation“

Anbieter zu finden, die unabhängig voneinander jeweils die folgenden grundlegenden Anforderungen erfüllen mussten:

Ein Anspruch an die neuen mobilen Geräte war, dass sie multifunktional sein sollten. Separate Geräte – eines für sichere Sprache, eines für sichere Datenverarbeitung und letztlich eines für offenen Datenverkehr – sollten durch ein einzelnes multifunktionales Gerät ersetzt werden.

Dieses sollte sensitive dienstliche Daten und offene Daten sicher voneinander trennen, eine mobile Anbindung an das interne Behördennetz leisten und über eine Ende-zu-Ende Sprachverschlüsselung verfügen, mit der zusätzlichen Anforderung, dass die Sprachverschlüsselung beider Hersteller interoperabel sein musste.

Eine besondere Herausforderung an die Hersteller war es, diese Funktionen unter Berücksichtigung hoher Sicherheitsanforderungen bereitzustellen: So wurde 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 wurde eine Ablageverschlüsselung für persistente Daten verlangt.

Weiterhin wurde vorgeschrieben, dass eine sichere Datenübertragung zwischen dem Behördennetzwerk und dem Endgerät über einen VPN-Kanal erfolgen soll.

Da das Endgerät sowohl mit möglichst wenig Restriktionen (verschiedene Applikationen, freier Webzugriff, ...) einsetzbar sein soll, als auch eine Umgebung für die sichere Verarbeitung von dienstlichen Daten ermöglichen soll, waren Schutzmechanismen zur Separation dieser Funktionen gefordert.

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 meist gute Sprachqualität, Verfügbarkeit und geringer zusätzlicher Aufwand absolute Voraussetzung. Der Schutz der mobilen Telefonie sollte daher 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 Ergebnis der Ausschreibung

Erfüllt wurden die Anforderungen durch die beiden Produkte SecuSUITE und SiMKo3, die jeweils für die Bearbeitung von Daten, die bis zum Geheimhaltungsgrad VS-NfD[7] (Verschlusssache nur für den Dienstgebrauch) eingestuft sind, zugelassen wurden.

Das Produkt SecuSUITE vom Anbieter Secusmart basiert auf den Endgeräten des Herstellers BlackBerry mit dem Betriebssystem BB 10. In dieses wurde die microSD-Karte der Firma Secusmart mit BOS[8] -Chip integriert.

Die zweite Produktlösung wurde von T-Systems entwickelt und verwendet einen Virtualisierungsansatz. Auf dem verwendeten Smartphone Samsung Galaxy S3, sowie dem Tablet Samsung Galaxy Note 10.1, separiert ein L4 Mikrokernel mehrere Android Betriebssysteme.

Beide Produktlösungen benutzen eine SmartCard als Sicherheitsanker.

---

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

8 BOS-Chip: Ein im Auftrag des BSI im Kontext des digitalen Polizeifunks u.a. für Sprachverschlüsselung entwickelter Smartcardchip.
BOS: Behörden und Organisation mit Sicherheitsaufgaben

2.2 Alternativer Ansatz

Da der Smartphone Markt sehr schnelllebig ist und die Evaluierung und Entwicklung sicherer Endgeräte viel Zeit in Anspruch nimmt, wird es immer schwieriger, sichere Endgeräte bereitzustellen, bevor die Geräte wieder als veraltet betrachtet werden.

Parallel zum traditionellen Ansatz der Zulassung sicherer Endgeräte wird daher derzeit ein neuer Ansatz erprobt:

Durch den Fokus auf zentrales Management und mittels strenger Restriktionen am Endgerät soll der Evaluierungsaufwand am mobilen Gerät reduziert werden, und so möglichst zeitnahe Freigaben für Smartphones erlauben.

Dieser Lösungsansatz wird vom BSI als Systemlösung bezeichnet. Dieser Begriff soll ausdrücken, dass nicht (nur) Sicherheitsvorkehrungen am Endgerät, sondern erst das Gesamtsystem hier die Sicherheit gewährleistet.

Vier Punkte stehen dabei im Vordergrund:

» Die Daten werden durch bestimmte Überwachungspunkte kanalisiert, die den Verkehr auf verdächtige Inhalte und auffälliges Verhalten analysieren,

» Es wird konsequent jeglicher Datenverkehr verschlüsselt, teilweise auf verschiedenen Ebenen.

» Eine 2-Faktor-Authentisierung am Endgerät wird verlangt.

» Strenge IT-Policy Regeln werden aufgestellt, die den Umgang mit dem Gerät festlegen.

Als Endgeräte könnten alle Systeme zum Einsatz kommen, auf die man die obigen 4 Punkte anwenden kann, die also z.B. zentrales Management und eine Smartcard-basierte 2-Faktor-Authentisierung unterstützen.

Das Jahr 2014 wird zeigen, ob sich dieser Ansatz der Systemlösungen als effiziente und hinreichend sichere Alternative zu den Produktlösungen bewähren kann.

2.3 Prüfung von mobilen Anwendungen (App-Testing)

Unabhängig vom jeweiligen Evaluierungsansatz des mobilen Endgeräts werden für die mobilen Clients Applikationen benötigt, um die auf ihm anfallenden Informationen zu bearbeiten und seine Funktionen zu nutzen. Die 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 wird im BSI derzeit ein geeigneter Prozess entwickelt, Applikationen für den Bedarf der Bundesverwaltung auf ihre Vertrauenswürdigkeit zu prüfen.

Apps, die auf den dienstlich eingesetzten Endgeräten freigegeben werden sollen, werden damit initial und für jedes ihrer Updates eine systematische, sicherheitstechnische Überprüfung durchlaufen. Diese Überprüfung wird für jedes Zielsystem vorgenommen und unter Berücksichtigung des jeweiligen Einsatzszenarios ausgewertet werden.

3 Produktlösungen

3 Produktlösungen

Die Hersteller T-Systems und Secusmart bieten mit den Produkten SiMKo3 und SecuSUITE jeweils mobile Endgeräte für sichere Sprache und Daten, die den Verschlusssachenanforderungen für „VS-Nur für den Dienstgebrauch“ genügen.

Mit SiMKo3 liegt das Nachfolgeprodukt zum Vorgänger SiMKo2 der Firma T-Systems vor.

SecuSUITE bietet mit der enthaltenen SecuVOICE Applikation einen Nachfolger der SecuVOICE SNS Sprachverschlüsselungsgeräte der Firma Secusmart.

3.1 SiMKo3

SiMKo3 ist eine sichere, mobile Erweiterung des Büroarbeitsplatzes auf Smartphones und Tablets um jederzeit und von jedem Ort aus sicher auf PIM[9] -Daten, also auf E-Mails, Kalender, Kontakte und Aufgaben, zugreifen zu können. SiMKo3 synchronisiert die PIM-Daten mit den Groupwaresystemen VPN geschützt mittels ActiveSync Protokoll. Die Nutzung des Internetzugangs der stationären Infrastruktur ist obligatorisch. Sichere verschlüsselte Sprachkommunikation über IP nach SNS-Standard steht in Kürze bereit.

Abbildung 1: SiMKo3

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 Geheimhaltungsgrad „VS – Nur für den Dienstge-

9 Personal Information Management

brauch“ 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 das Sicherheitskonzept des SiMKo3:

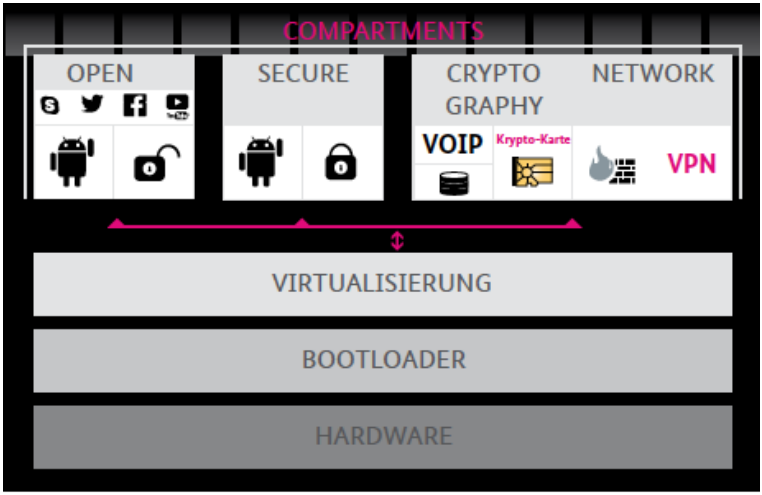


Abbildung 2: Sicherheitsarchitektur des SiMKo3 Endgerätes

Die wesentlichen Sicherheitsmerkmale des SiMKo3 Systems auf einen Blick:

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

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

» Sichere Datenkommunikation zwischen dem Endgerät und dem zugeordneten Server in der gesicherten, stationären IT-Infrastruktur über VPN.

» 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 Kunden.

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

» Secure App-Store für kundenspezifische Applikationen - Hier werden überprüfte, sichere Apps zur Verfügung gestellt.

» Over-The-Air Updates – Installation vom BSI geprüfter und zugelassener Updates (über Mobilfunknetz oder WLAN)

» Sichere verschlüsselte Telefonie nach SNS-Standard (gemäß Ausschreibungsanforderungen in 2014)

Die Netzanbindung von SiMKo3 ist in Abbildung 6 auf Seite 24 abgebildet.

3.2 SecuSUITE

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

Abbildung 3: SecuSUITE

Die Perimeterseparation von BB10 ermöglicht eine Trennung dienstlicher und offener Daten.

Wie in Abbildung 4 dargestellt, nutzt das SecuSUITE Endgerät zwei unabhängige Daten-Kommunikationswege:

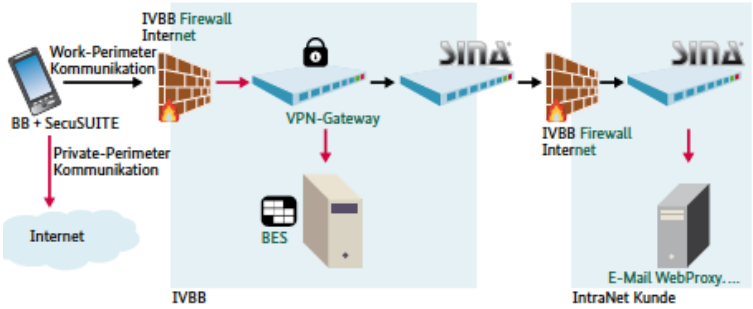


Abbildung 4: Die Architektur der Datenlösung von SecuSUITE mit zentralem BES

Aus dem privaten Perimeter kommt man direkt und ohne Umweg in das Internet. Dieses kann über das 3G/4G Netz des Providers oder auch über WLAN erfolgen.

Die Kommunikation aus dem Work-Perimeter wird durch ein vorinstalliertes VPN-Profil grundsätzlich durch einen SINA[10] -VPN-Zugang zum IVBB[11] geleitet.

Von dort aus erreicht das Endgerät sowohl den zentralen BES[12], der für die Administration der Endgeräte zuständig ist, und als auch sein zugehöriges Hausnetz. Erst dort werden die PIM-Daten mit den entsprechenden Servern synchronisiert oder auf hausinterne Verzeichnisse zugegriffen.

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

10 Weitere Informationen finden Sie in der Broschüre Sichere Inter-Netzwerk Architektur (BSI-Bro13/322)

11 InformationsVerbund Berlin - Bonn

12 BlackBerry Enterprise Service

Aufgrund der Ausschreibungsanforderungen wird bei SecuSUITE bereits seit 2013 Sprachverschlüsselung mittels SNS-over-IP unterstützt.

Anders als bei den bisherigen SNS Produkten benötigt SNS-over-IP eine zentrale Server-Infrastruktur, die dieses Jahr zentral aufgestellt wird. Abbildung 5 skizziert die Architektur dieses Systems.

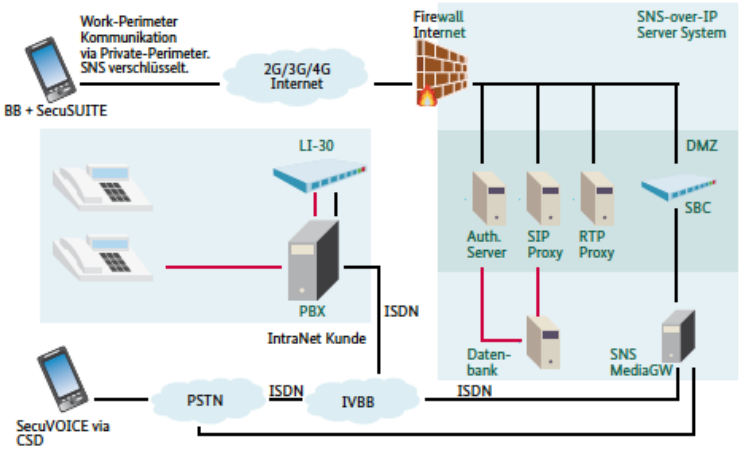


Abbildung 5: SecuSUITE Architektur für die Sprachverschlüsselung

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. Handelt es sich bei dem Zielgerät nicht um ein SNS-over-IP Endgerät, leitet es die Verbindung an das SNS-Media-Gateway, das daraufhin eine Protokollumsetzung von IP auf ISDN/V.110 durchführt.

Das SNS Media Gateway wird zusätzlich die Anbindung von SNS-Legacy Geräten ermöglichen.

Die folgende Abbildung 6 zeigt die Netzanbindungen der Produktlösungen noch einmal im Überblick.

SiMKo3/SecuSUITE Netzanbindung

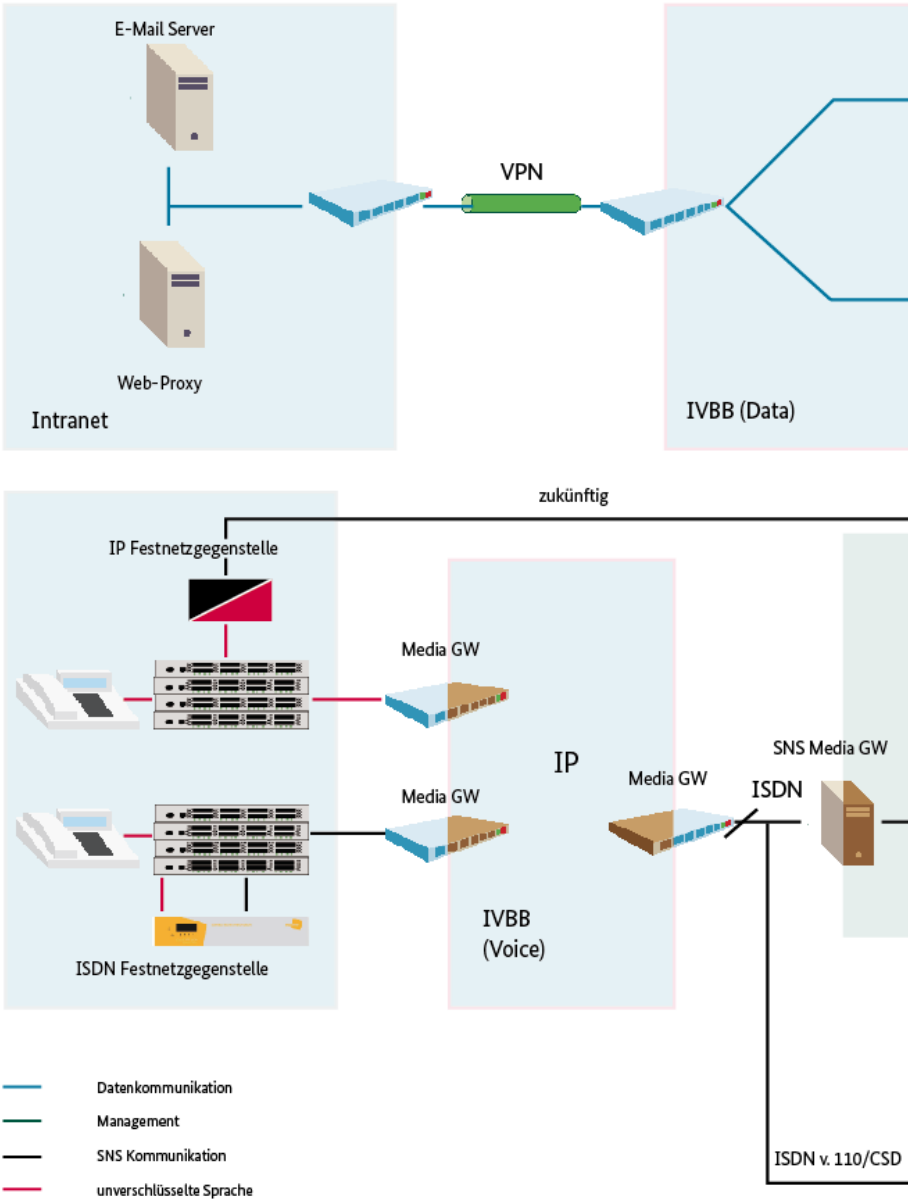
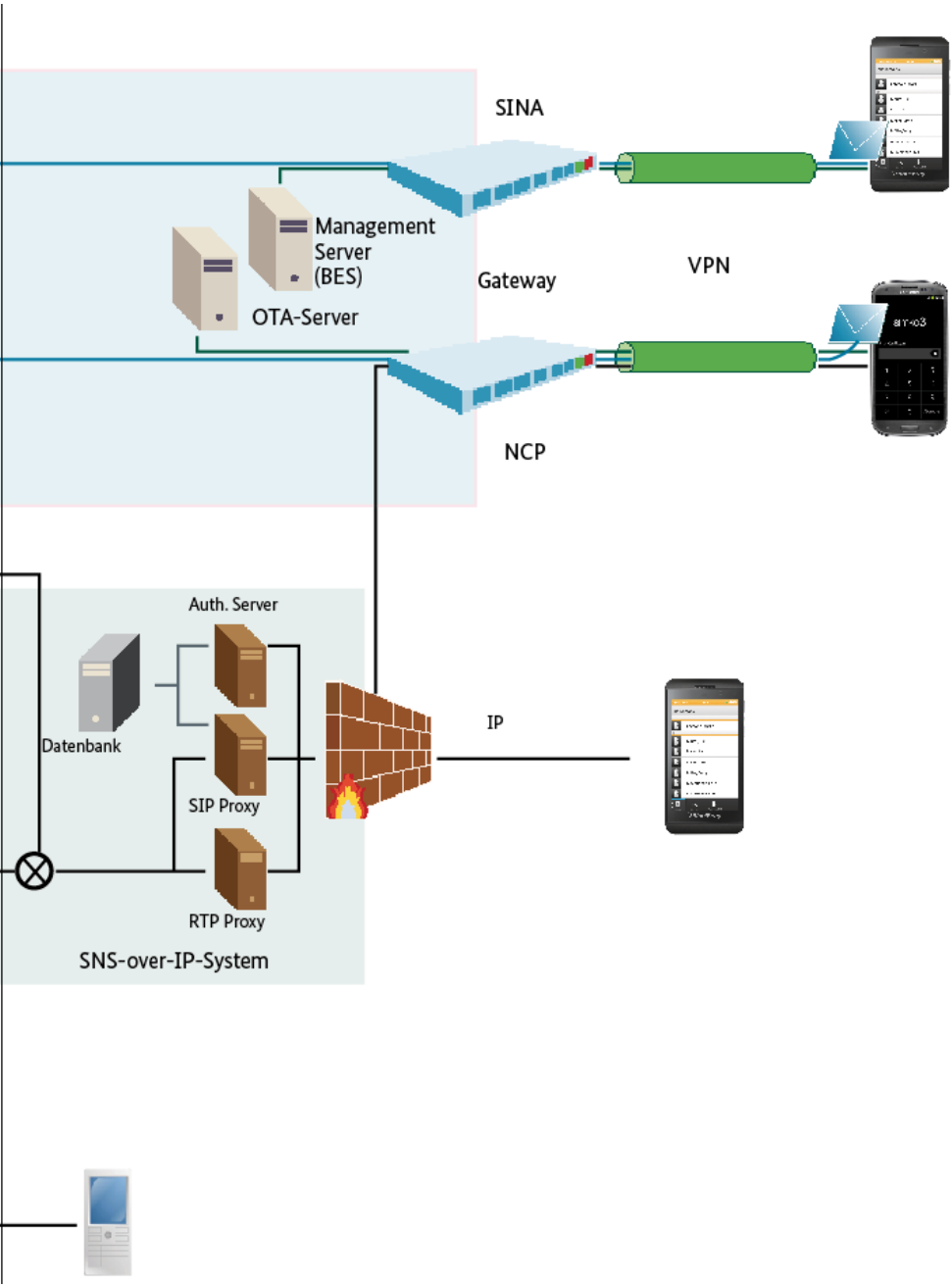


Abbildung 6: Netzwerkarchitektur der Produktlösungen


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

4 Systemlösungen

4 Systemlösungen

4.1 Anforderungen

Neben der Bereitstellung von Produktlösungen, die gemäß den Kriterien des BSI untersucht werden, erprobt das BSI einen weiteren Ansatz zur Bereitstellung mobiler Lösungen:

Kommerziell verfügbare mobile Endgeräte, bei denen eine Untersuchung nicht in der Tiefe der Produktlösungen möglich ist, werden durch zusätzliche technische Maßnahmen ergänzt. Eine solche sogenannte Systemlösung enthält verschiedene Sicherheits-Komponenten und -Maßnahmen, die einen Betrieb innerhalb des IVBB ermöglichen sollen.

Bei den kommerziell verfügbaren Endgeräten soll es sich zunächst um iPhones und iPads des Herstellers Apple handeln.

Diese sind zusammen mit einer starken Nutzerauthentisierung, eID-Management, mit VS-NfD-geeignetem VPN-Tunnel, Browsing über Proxies, innerhalb eines „sicheren Datensynchronisationsdienstes“ oder mittels eines Thin-Clients zu betreiben.

Die Systemlösung zielt einzig darauf ab, eine sichere Datenlösung zu bieten. Sichere Telefonie ist nicht angestrebt.

4.2 Konzept

Die genannten Maßnahmen und Komponenten verteilen sich auf Endgeräte, Infrastruktur und Nutzereinschränkungen.

4.2.1 Endgeräte

Die mobilen Endgeräte sind in Verbindung mit einer sicheren Hardwarekomponente (Smartcard) zu betreiben. Entsprechende Adapter für iPhone und iPad werden zur Verfügung gestellt (Abbildung 7).

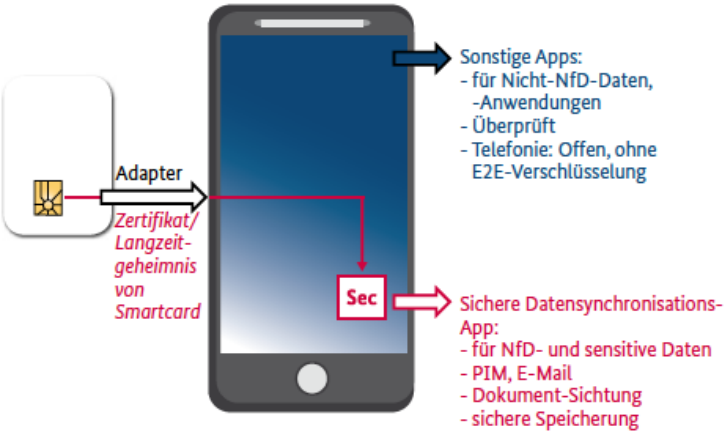


Abbildung 7: Systemlösung: Konzept

Die Smartcard ermöglicht eine starke 2-Faktor Nutzerauthentisierung. Im Zusammenspiel mit einer App für den sicheren Datensynchronisationsdienst bildet sie den Sicherheitsanker, sowohl für die sichere Verarbeitung und Speicherung, als auch für den Empfang und Versand von eingestuften und sensitiven Daten. Parallel dazu ist auch der Betrieb als Thin Client in Verbindung mit der Smartcard denkbar.

4.2.2 Infrastruktur

Zur Gewährleistung der Sicherheit des IVBB/NdB[13] Netzwerks müssen zusätzliche Sicherheitsmaßnahmen in den zentralen Infrastrukturkomponenten innerhalb des IVBB/NdB Netzwerks und innerhalb der Hausnetze implementiert werden. Dazu gehören

» ein zentraler VS-NfD geeigneter Netzübergang (VPN-Gateway für den gesamten Datenverkehr des mobilen Geräts)

» zentrales Sicherheitsmonitoring des ein- und ausgehenden Datenverkehrs.

13 Netze des Bundes

» Management der mobilen Endgeräte durch die Administratoren der Ressorts über Mobile Device (MDM).

» Bereitstellung untersuchter, zugelassener und freigegebener Apps für den dienstlichen Gebrauch.

4.2.3 Nutzereinschränkungen

Die Smartphones müssen unter bestimmten Restriktionen betrieben werden. Nur vertrauenswürdige und dienstlich erforderliche Apps sind auf dem Endgerät erlaubt.

Die Nutzer der Systemlösung sind zu sensibilisieren und ihr Risikobewusstsein, insbesondere für die auf den mobilen Endgeräten vorliegenden Daten, ist zu schärfen.

5 SNS – Sichere Netzübergreifende Sprachkommunikation

5 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.

5.1 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 8). 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 (Authentisierung, Verschlüsselung ...), welches von dem jeweiligen Endgerät unterstützt wird.

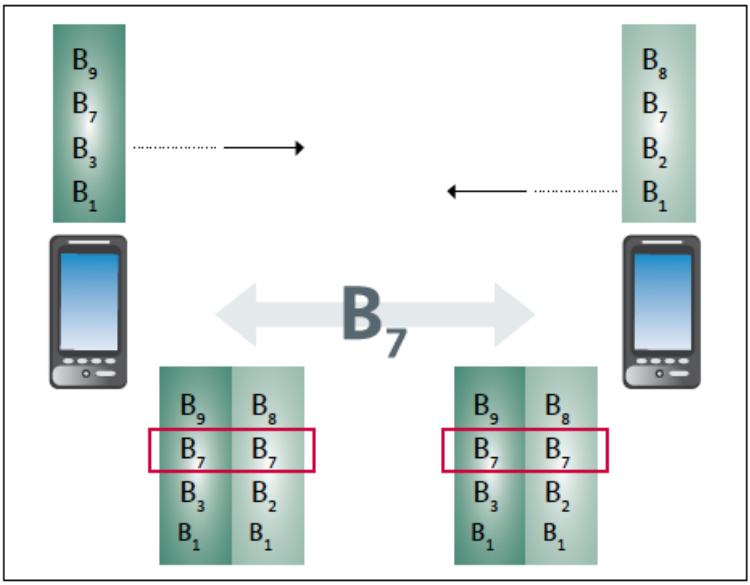


Abbildung 8: SNS-Betriebsmodusaushandlung

Durch einen Vergleich der beiden Listen bestimmen beide Seiten unabhängig voneinander den ersten übereinstimmenden Eintrag (in Abbildung 8) 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.

Das Beispiel in Abbildung 9 zeigt die Produktlinie des Herstellers A, in der nacheinander im Zuge der technischen Weiterentwicklung die Produkte 1 bis 3 entstehen. Durch den Einsatz

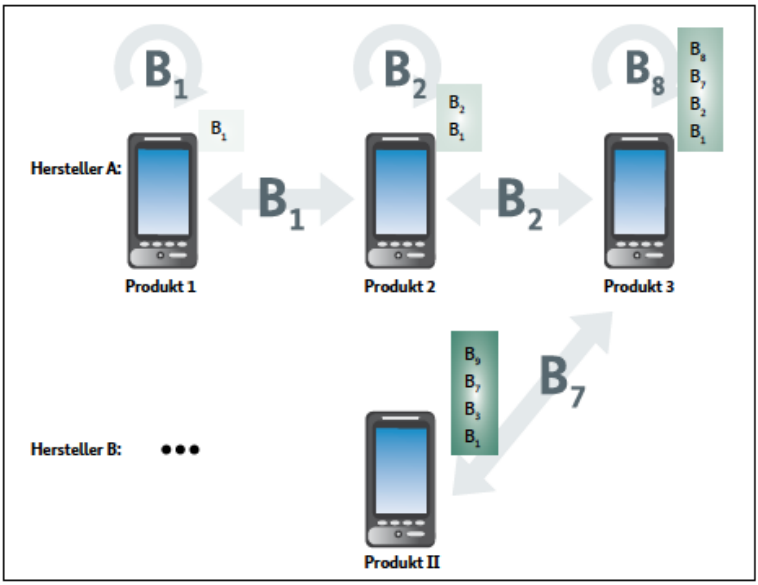


Abbildung 9: SNS-Betriebsmodusaushandlung - Interoperabilität

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.

5.2 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[14] -210-Protokolls auch die Möglichkeit geschaffen werden, zukünftig Endgeräte mit dualer SNS- und SCIP-Funktionalität zu entwickeln. So ist es schon jetzt den Endgeräten anhand der jeweiligen Protokoll-ID möglich, bei der Signalisierung den Partner als SNS- oder als SCIP-Endgerät zu identifizieren.

5.3 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

14 SCIP: Secure Communications Interoperability Protocol

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.

5.4 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.

5.5 SNS-over-IP

Durch die anfängliche Wahl von CSD als Kanal wurde eine gute Abdeckung innerhalb Deutschlands erzielt und somit ein zuverlässiges Kommunikationsmedium gewählt. Zunehmend sind allerdings auch IP-basierte Netze verfügbar. Insbesondere firmeninterne WLANs und UMTS bieten sich als Medium an. Über größere verfügbare Datenraten und geringes Delay bieten sie 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 ist eine initiale Version der SNS-over-IP Erweiterung für den SNS-Standard. Dieser initiale Entwurf „SNS over IP“ kann zusammen mit den bisherigen Teilen des SNS-Standards beim BSI angefordert werden.

Die Produkte SiMKo3 und SecuSUITE werden die ersten SNS-over-IP fähigen Endgeräte sein. Im Laufe der Produktentwicklung wird der Standard in Kooperation mit beiden Herstellern auf die Probe gestellt und verfeinert werden.

5.6 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.

5.6.1 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.[15]:

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 stören-

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

der 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.

5.6.2 3G/4G (SNS-over-IP)

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.

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.

5.6.3 BOS-Interoperabilität (BOS-TETRA Netz)

Da mit der BOS-SKE[16] 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 10 stellt die aktuellen Möglichkeiten netzübergreifender SNS Kommunikation dar.

16 SKE: Sicherheitskarte Typ E

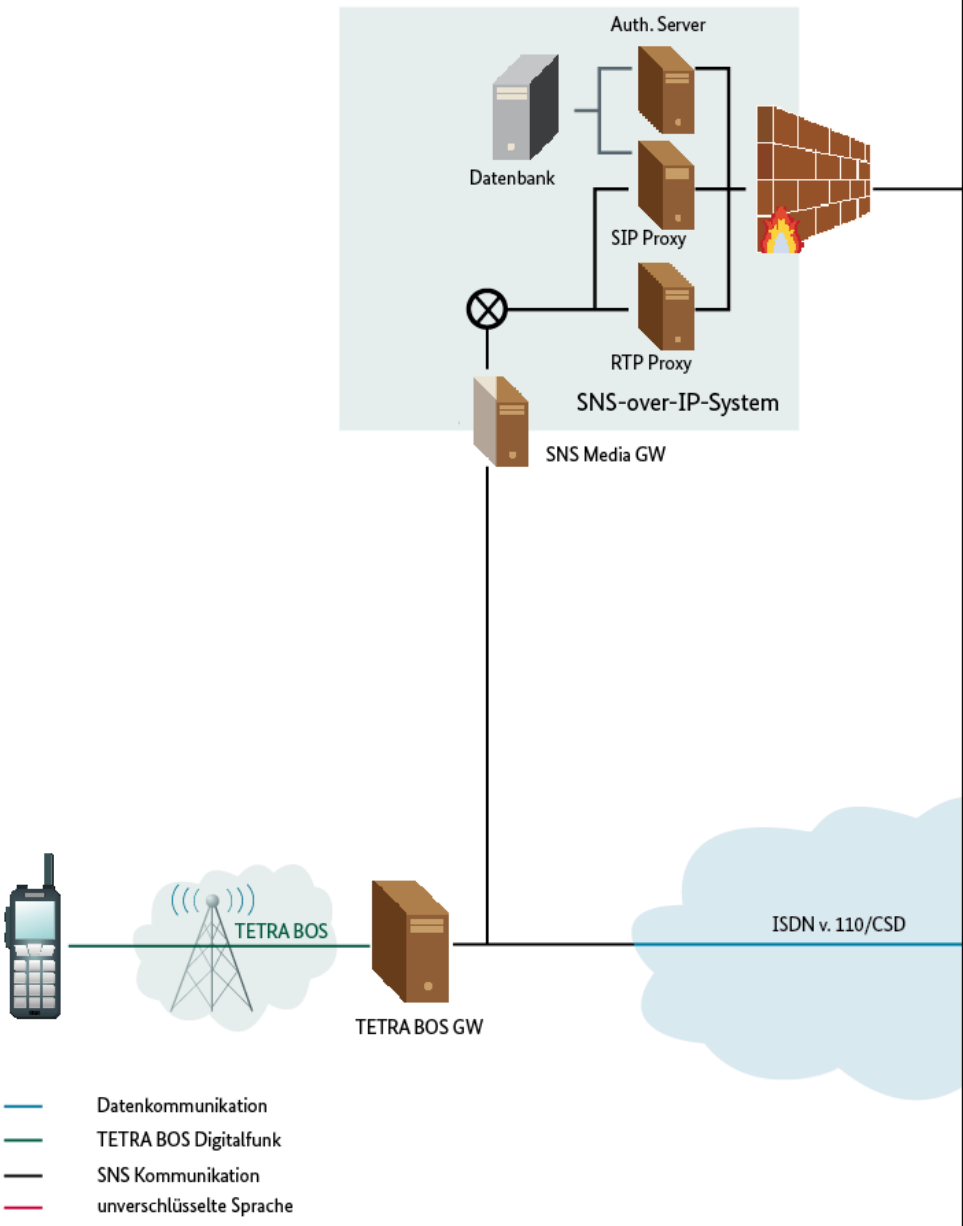
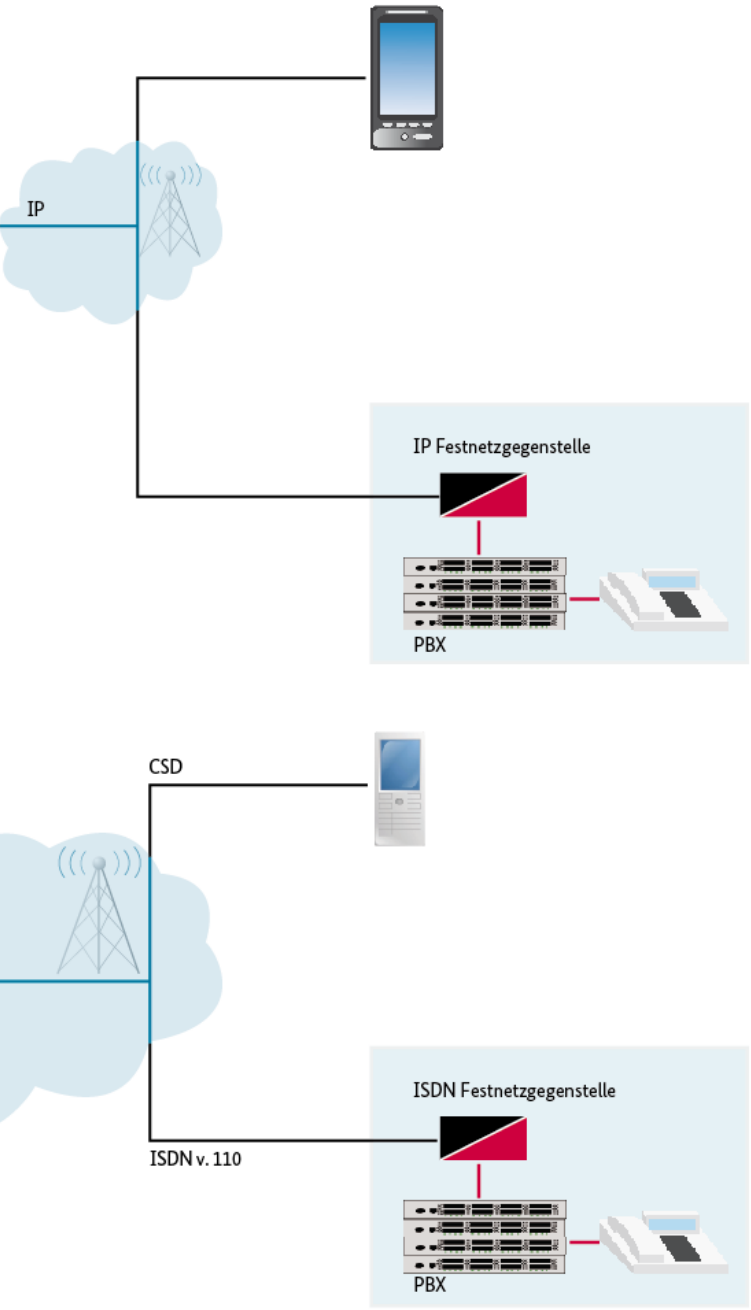


Abbildung 10: SNS – bisher unterstützte Netze


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

5.7 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.

6 Legacy Produkte

6 Legacy Produkte

6.1 Sprachkommunikation

Im Zuge des IT-Investitionsprogramms[17] wurde die Bundesverwaltung mit Endgeräten für sichere Sprachkommunikation ausgerüstet.

6.1.1 Mobile Endgeräte

Es wurden ca. 5600 mobile Endgeräte für die Bundesverwaltung angeschafft. Diese befinden sich seit Herbst 2010 im Einsatz. Dabei handelt es sich um 3600 SecuVoice SNS Geräte der Firma Secusmart und 2000 TopSec mobile SNS Geräte der Firma Rohde & Schwarz.

6.1.1.1 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.

SecuVoice SNS implementiert sowohl sichere Sprache als auch sichere SMS.

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

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

6.1.1.2 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.

TopSec mobile SNS dient ausschließlich der Sprachverschlüsselung.

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

6.1.2 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.

6.1.2.1 SecuGate LI1

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

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 Sprach-

verschlüsselung direkt auf dem Schreibtisch. Dem Nutzer wird über Sprachansage und Displayanzeigen, die an das ISDN-Telefon gesendet werden, die sichere Verbindung signalisiert.

6.1.2.2 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.

6.1.3 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.

6.2 Datenkommunikation

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

6.2.1 SiMKo2

Seit 2010 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 Ort aus sicher auf seine PIM-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.

» 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 wird von T-Systems auf Basis von verschiedenen HTC-Smartphones angeboten.

7 Weiterentwicklung & Ausblick

7 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 Bundesverwaltung und darüber hinaus zu gestalten.

Die erste Version des SNS-Standards wurde im März 2010 veröffentlicht. Durch die Fortschreibung im Jahr 2011 wurde diese auf SNS-over-IP erweitert. Um weiterhin auf dem Stand der Technik zu bleiben und den Anforderungen der Nutzer gerecht zu werden, entwickelt das BSI den Standard kontinuierlich weiter und fügt neue Komponenten hinzu.

Auf der SNS Roadmap für die nähere Zukunft befindet sich zunächst die Finalisierung von SNS-over-IP. Dies erfolgt in Zusammenarbeit mit den Herstellern der Produkte SecuSUITE (Secusmart) und SiMKo3 (T-Systems) im Zuge der Einführungsphase der neuen SNS Endgeräte.

Weiterhin ist geplant, diejenigen Teile des Standards, die das Aushandlungsprotokoll betreffen, zukünftig in einer Open-SNS Variante des SNS-Standards zur Verfügung zu stellen. Anders als der vollständige SNS-Standard wird diese Version dann nicht mehr VS-NfD (Verschlusssache – Nur für den Dienstgebrauch) eingestuft sein. Dadurch wird eine Aushändigung – beispielsweise per Download – ohne vorherige Vertraulichkeitsvereinbarung möglich, was die Einstiegshürde zu SNS verringern soll.

Sowohl Open-SNS als auch der vollständige SNS-Standard werden in Kürze auch auf Englisch erhältlich sein.

8 Kontaktinformationen

8 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 K15
Postfach 20 03 63
53133 Bonn
E-Mail: mobilfunksicherheit@bsi.bund.de
sns@bsi.bund.de

9 Literatur

9 Literatur

[1] ETSI EN 300 395-1Terrestrial 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
Februar 2014

Druck
WM Druck + Verlag
53359 Rheinbach

Bildnachweis
BSI, Seite: 3, 14, 19, 20, 21, 22, 23, 24, 28, 34, 35, 42, 46, 47, 48, 49
Fotolia, Seite: 6, 7, 8, 9, 10

Texte und Redaktion
Bundesamt für Sicherheit in der Informationstechnik – BSI

Artikelnummer
BSI-Bro14/323

www.bsi.bund.de