Samsung Knox

Enterprise Security für Samsung Smartphones und Tablets

SAMSUNG

Mit der richtigen Lösungsplattform auf die wechselhaften Anforderungen an die Enterprise-Mobility reagieren

Chancen und Risiken von BYOD

Zu den aktuellen Trendthemen gehört „Bring your own device“, also der Einsatz privater Mobiltelefone und Tablets im Firmenumfeld. Nutzer möchten gerne in Ihrem Business-Alltag aktuelle Mobilgeräte nutzen, um sich bei Ihrer Arbeit unterstützen zu lassen und auch von unterwegs auf die Firmen-IT-Infrastruktur zugreifen zu können. Eine Steigerung der Produktivität kann das Ergebnis eines konsequenten Mobilgeräteeinsatzes sein. Doch besteht die große Herausforderung für Unternehmen darin, eine geschäftlich-private Mischnutzung der BYOD-Endgeräte zuzulassen, ohne die Enterprise IT-Sicherheitsinteressen oder die Privatsphäre der Nutzer zu verletzen. Möglich wird dies erst durch entsprechend vorbereitete Endgeräte.

Mobilitätsstrategien auf dem Prüfstand

Der enorme Zuwachs bei Smartphone- und Tablet-Auslieferungen und der Wandel in der Popularität verschiedener Herstellermarken zeigen deutlich, warum Unternehmen ihre Mobilitätsstrategien und -richtlinien laufend auf den Prüfstand stellen müssen. Noch vor zwei oder drei Jahren war nicht vorauszusagen, dass, laut dem Marktforschungsunternehmen IDG Enterprise*, fast 80 Prozent der 236,4 Millionen Smartphones, die im zweiten Quartal 2013 ausgeliefert wurden, Android™-basierte Geräte sein würden oder das Samsung allein bei Android™-Smartphones einen Marktanteil von fast 40 Prozent halten würde.

Mobilgeräteanbieter, die keine Innovationen liefern und die Anforderungen der Benutzer nicht erfüllen, können ganz schnell vom Marktführer zum Mitläufer werden. Eine solche Veränderung kann erhebliche Auswirkungen auf Unternehmen haben, vor allem angesichts der weitverbreiteten Anwendung des BYOD-Grundsatzes. Spiegelt die Mobility-Strategie eines Unternehmens nicht das sich wandelnde Profil der Mobilgeräte seiner Mitarbeiter wider, kann es schnell passieren, dass die Unternehmens-IT nicht mehr in der Lage ist, diese Geräte effektiv zu verwalten und zu steuern.

Festlegen eines Anforderungskonzepts

Nun, da frühere Mobilgerätegenerationen für Nutzer immer schneller irrelevant werden und sich die mobilen Technologien immer rasanter weiterentwickeln, brauchen Unternehmen für die Optimierung ihrer Mobility-Strategien einen gut durchdachten Ablauf. Bei diesem Ablauf, welcher in diesem Dokument beschrieben wird, ist es nicht damit getan, die Funktionalität jedes beliebigen Mobilgeräts zu beurteilen. Auch andere Aspekte – von den Präferenzen der Mitarbeiter bis hin zu Partner-Ökosystemen – sind wichtig, ganz zu schweigen von den Verwaltungs- und Sicherheitsanforderungen, die üblicherweise auf der Liste der Bedenken von CIOs und Geschäftsführern ganz oben stehen.

Mobilitätsanforderungen und Mitarbeiterpräferenzen ermitteln

Einsatzszenarien im Fokus

Bei jeglichen Bemühungen zur Einführung oder Feinabstimmung einer Mobility-Strategie sollten nicht zuallererst die Mobilgeräte im Fokus stehen. Der erste Schritt sollte vielmehr eine eingehende Analyse der bereits im Unternehmen vorhandenen Mobilitätspraktiken und -verfahren sein. Mit anderen Worten: Ehe ein Unternehmen ermitteln kann, wie es Mobilgeräte und -technologien der neusten Generation am besten nutzt, muss es zuerst verstehen, wie sich die Mobilität zu den zentralen Geschäftszielen verhält und wie die eigenen Mitarbeiter derzeit ihre Mobilgeräte nutzen.

Häufig wird bei solchen Evaluierungen auch die Generationenfrage eine Rolle spielen. Jüngere Mitarbeiter, die soziale Netzwerke und uneingeschränkte Mobilität gewohnt sind, könnten neue Anwendungsmöglichkeiten vorschlagen, durch die sie und ihre Arbeitgeber effizienter und produktiver arbeiten können. Tauscht man einfach nur die alten Geräte durch neue aus und verändert sonst kaum etwas, verpasst man möglicherweise eine Chance zur Optimierung der Mobility-Maßnahmen im Unternehmen auf Grundlage der Fähigkeiten der neuen Plattform sowie neuer Anwendungsmöglichkeiten und Abläufe.

Welche Mobilgeräte werden von Mitarbeitern genutzt?

Ein wesentlicher Baustein bei dieser Beurteilung auf der Makroebene ist die Ermittlung der durch die Mitarbeiter bevorzugten Mobilgeräte. Unternehmen, die BYOD-Programme eingerichtet haben, können einen guten Eindruck dieser Präferenzen gewinnen, indem sie einfach ermitteln, welche Mobilgeräte die Mitarbeiter mit an den Arbeitsplatz nehmen.

Selbst wenn Unternehmen das traditionelle Modell aus Einkauf, Ausgabe und Support unternehmenseigener Mobilgeräte nutzen, sollten sie die Vorlieben der Angestellten berücksichtigen, bevor sie sich für die Einführung einer bestimmten Plattform entscheiden. Gelingt es der IT-Abteilung und den Führungskräften nicht, die Mitarbeiterpräferenzen zu ermitteln, müssen sie unter Umständen feststellen, dass die von ihnen ausgewählten Geräte entweder ganz abgelehnt oder zu wenig genutzt werden.

Hat ein Unternehmen sich erst einmal ein genaues Bild seines eigenen Mobilitätsprofils und der Praktiken und Präferenzen seiner Mitarbeiter gemacht, kann es die nächsten Phasen des Evaluierungsprozesses in Angriff nehmen. Ein Scheitern bei diesem ersten, entscheidenden Schritt kann den letztendlichen Erfolg einer in der Entwicklung befindlichen Mobility-Strategie stark beeinträchtigen.

* 2013 Consumerization of IT in the Enterprise survey, IDG Eneterprise

Die Mobilfunkplattform muss die Sicherheits- und Kompatibilitätsanforderungen erfüllen

Nachdem sie sich einen Überblick über die Nutzung von Mobilgeräten verschafft und entschieden haben, wohin die Reise gehen soll, müssen Unternehmen als nächstes sicherstellen, dass sie aus der Erkenntnis die richtigen und nachhaltigen Entschlüsse ziehen.

Laut einer Untersuchung von IDG Enterprise* machten mehr als 1.600 IT-Manager, sowie Führungs- und Fachkräfte diese Erfahrung. Wie in Abbildung 1 dargestellt, gaben in dieser Umfrage aus dem Frühjahr 2013 88 Prozent der Befragten aus Unternehmen mit mehr als 1.000 Mitarbeitern an, dass die Fähigkeit, Gerätesicherheit zu bieten, ein wichtiger Faktor bei der Beurteilung von Mobilgeräteanbietern sei. Des weiteren sagten 69 Prozent dieser Befragtengruppe, dass sie von diesen Anbietern Unterstützung bei der Verwaltung der Verbreitung der Mobilgeräte benötigten.

Unternehmen sollten diese Phase ihrer Evaluierung nicht mit dem Fokus auf ein bestimmtes Gerät beginnen, sondern mit einer Beurteilung des Gesamtrisikoprofils ihres Unternehmens.

Faktoren, die bei der Beurteilung von Mobilgeräteanbietern als entscheidend oder sehr wichtig angesehen werden:

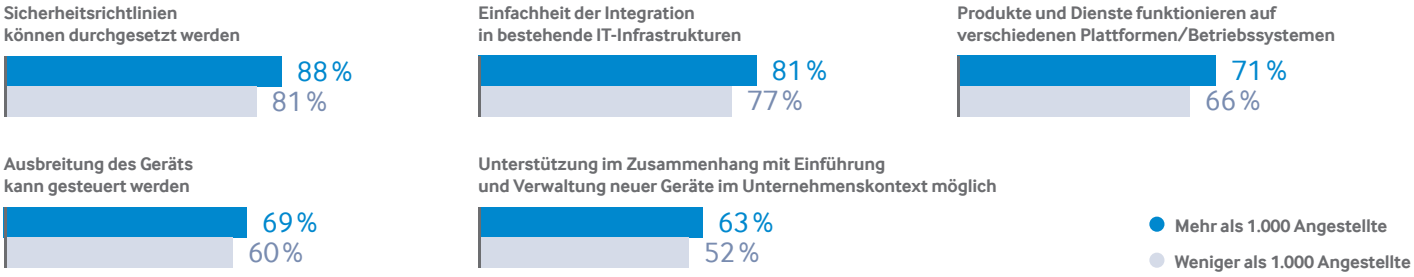

Abbildung 1: Beurteilung von Mobilgeräteanbietern

* 2013 Consumerization of IT in the Enterprise survey, IDG Eneterprise

Die wichtigsten Fragen, die ein Unternehmen beantworten muss, sind unter anderem:

- Welche Unternehmensdaten und -ressourcen sind besonders wertvoll und/oder sensibel?
- Wie kann das Unternehmen den Nutzen und die Risiken durch die Zugänglichkeit von Unternehmensdaten und -ressourcen für die Benutzer von Mobilgeräten am besten abwägen?
- Welche Unternehmensdaten können auf Mobilgeräte heruntergeladen werden und welche Daten müssen hinter der Unternehmensfirewall bleiben?
- Welche Arten von Sicherheitstechnologie und -verfahren gibt es für Mobilgeräte und deren Anwendungsmöglichkeiten?

Erst, wenn diese und andere Fragen zum Risikoprofil beantwortet wurden, können Organisationen belastbar ermitteln, welches Maß an Sicherheitsvorkehrungen sie auf den Mobilgeräten, innerhalb ihres Mobile-Management-Systems und in ihren Sicherheitsrichtlinien benötigen.

Anforderungen der Enterprise-Mobility gerecht werden

Samsung hat es sich als Ziel gesetzt, die vielfältigen Anforderungen zu erfüllen, die Firmenkunden mitbringen. Dieses Engagement geht über die Produktion von Smartphones, Tablets und anderen Mobilgeräten für den Unternehmenseinsatz hinaus. Es umfasst auch die gesamte Bandbreite an Programmen und Partnerschaften, die Enterprise-Mobility-Initiativen erfordern.

Samsung bietet ein umfangreiches Portfolio mobiler Endgeräte. Diese Smartphones und Tablets sind nicht nur mit verschiedenen Bildschirmgrößen und -formaten erhältlich, sie verfügen auch über eine große Palette an Leistungsmerkmalen und Funktionen. Folglich können Unternehmen für praktisch alle mobilen Anwendungsfälle das passende Samsung-Gerät finden.

Was die Mitarbeiterpräferenzen angeht, haben diese bereits beim Kauf ihres privaten Geräts eine Wahl getroffen. Wie sich anhand von Marktzahlen ablesen lässt, dominieren Android™-basierte Geräte den Smartphone-Markt. Samsung hält hierbei einen Marktanteil von fast 40 Prozent.

Ausgehend von dieser Prämisse kann daher angenommen werden, dass in Unternehmen mit BYOD-Programmen bereits eine große Anzahl von Samsung-Geräten genutzt wird. Unternehmen, die von älteren auf neuere Mobilgeräte umsteigen wollen, sollten sich genau anschauen, welche Geräte ihre Mitarbeiter bevorzugen.

Samsung bietet ein breites Spektrum an Sicherheits- und Managementfunktionen. So unterstützen die Geräte von Samsung beispielsweise Exchange ActiveSync® (EAS), ein Protokoll, mit dem Handynutzer produktiver sein können, indem sie einen sicheren Zugang zu ihren geschäftlichen E-Mail-Konten, Kalendern, Adressbüchern und Aufgaben erhalten. 2013 stellte Samsung eine neue umfassende Plattform für mobile Sicherheit vor: Samsung KNOX™.

Die wichtigsten Vorteile von Samsung KNOX™:

MERKMALE	BESCHREIBUNG
Geräte- & Datensicherheit	Security Enhanced Android™ (SE for Android™) zur Sicherung von Container-Lösungen von Drittanbietern, ARM® TrustZone-basierte Integrity Measurement Architecture (TIMA) zum Schutz von Zertifikaten und Verschlüsselungscodes vor unerlaubtem Zugriff
Container-Usability	Durch Entfallen des Wrappings von Drittanbieter-Apps wird die Verfügbarkeit der Apps für die Benutzer erhöht; flexiblere Nutzung von Apps und Daten zwischen Containern und privatem Bereich; sofortige Container-Erstellung (bis zu zwei Container), um den Speicherbedarf gering zu halten
Einfache Anmeldung	Einfache Registrierung und Anmeldung bei MDM-Downloads von Drittanbietern über SEG und Universal MDM Client, der den Aufwand zur Erstellung eines KNOX™-Containers auf ein Minimum reduziert
Cloud-basiertes Mobile Device Control	Effektives und effizientes Management von Mobilgeräten und Inhalten mit verschiedenen Plattformen über umfassende cloud-basierte MDM-Dienste sowie ein einheitlicher Punkt für Einkauf und Abrechnung von KNOX™-Lizenzen und cloud-basierten Business-Anwendungen

Das Unternehmen mit einer umfassenden Mobilitätsplattform voranbringen und sichern

Samsung KNOX™ ist eine ganzheitliche Plattform, die Unternehmen eine optimierte Sicherheits- und Container-Lösung mit Cloud-basierten Enterprise-Mobility-Management-Diensten sowie einen Marketplace bietet, auf dem KNOX™-Produkte und Software-as-a-Service (SaaS)-Anwendungen erhältlich sind. Samsung KNOX™ ist eine sich weiterentwickelnde Plattform für die dynamischen Anforderungen an die Enterprise-Mobility.

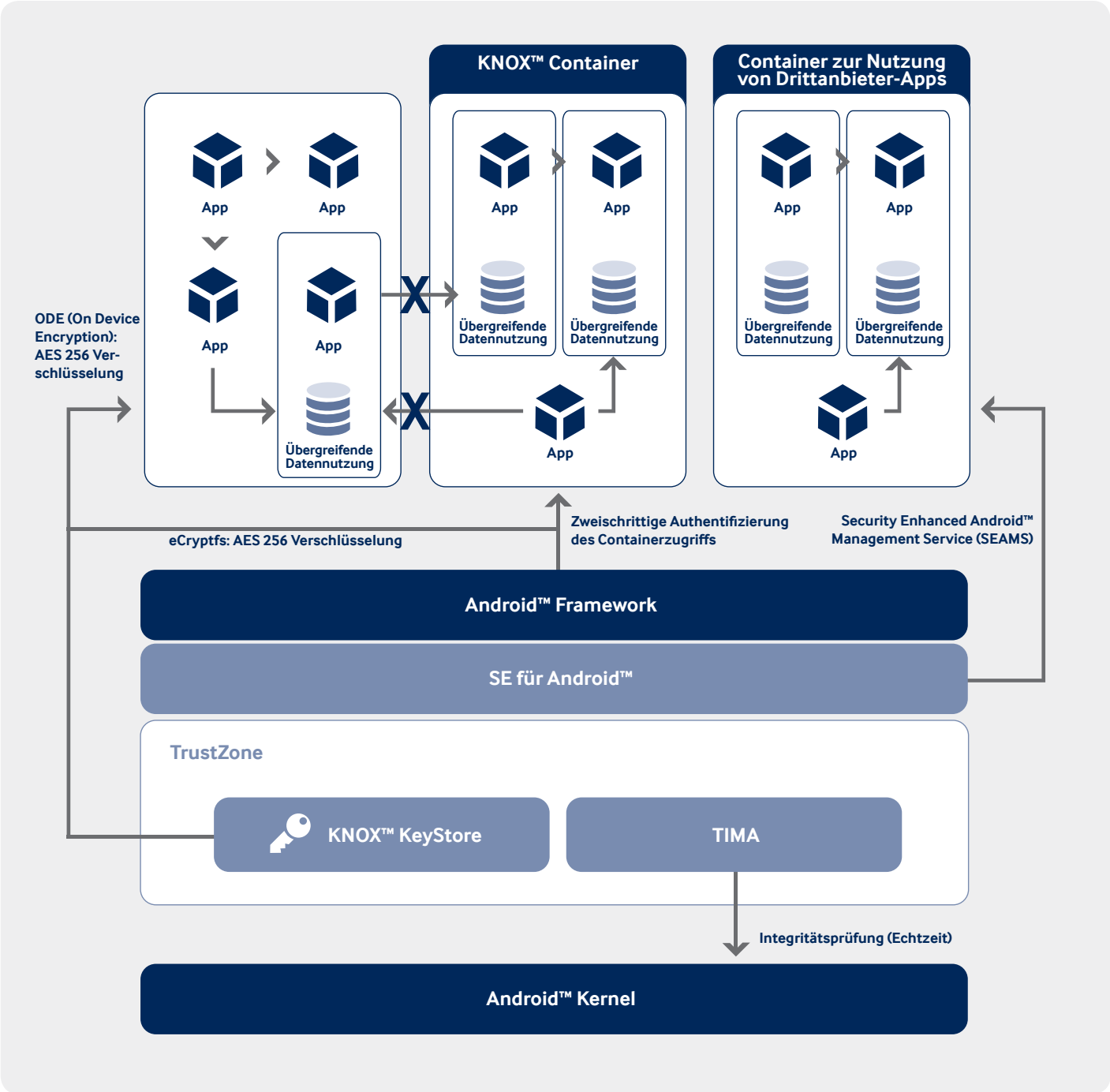

Abbildung 2: Darstellung der erweiterten Funktionen von Samsung KNOX™

Eine sichere, flexible Enterprise-Mobility mit verbesserter Sicherheitstechnologie

Mehr Schutz durch erhöhte Sicherheit

Samsung KNOX™ erfüllt dank eines mehrstufigen Sicherheitsmodells sowie branchenführender Device-Management-Funktionen und dem dadurch möglichen, umfassenden Schutz vor Schadprogrammen und missbräuchlichem Zugriff, die Bedürfnisse anspruchsvoller Unternehmensumgebungen.

- **Trusted Boot.** Trusted Boot ist auf Geräten mit KNOX™-Lösung eine der Hauptkomponenten und die erste Verteidigungslinie gegen potentiell schädliche Angriffe. Trusted Boot gewährleistet, dass nur verifizierte und autorisierte Software auf dem Gerät ausgeführt werden kann.
- **ARM®TrustZone-basierte Integrity Measurement Architecture (TIMA).** TIMA wird in der sicheren Umgebung ausgeführt und gewährleistet eine nicht kompromittierbare, ständige Überwachung der Integrität des Linux®-Kernels. Stellt TIMA fest, dass die Integrität des Kernels oder Bootloaders verletzt wurde, wird die Unternehmens-IT über das MDM benachrichtigt, damit sie eine Reaktion basierend auf ihren Richtlinien einleitet. Eine dieser auf Richtlinien basierenden Aktionen deaktiviert den Kernel und schaltet das Gerät umgehend ab.
- **Security Enhanced Android™ (SE for Android™).** Durch die Optimierung mittels SE for Android™ fördert Samsung KNOX™ die Plattformsicherheit von Container-Lösungen von Drittanbietern, die neben dem KNOX™-Container betrieben werden.

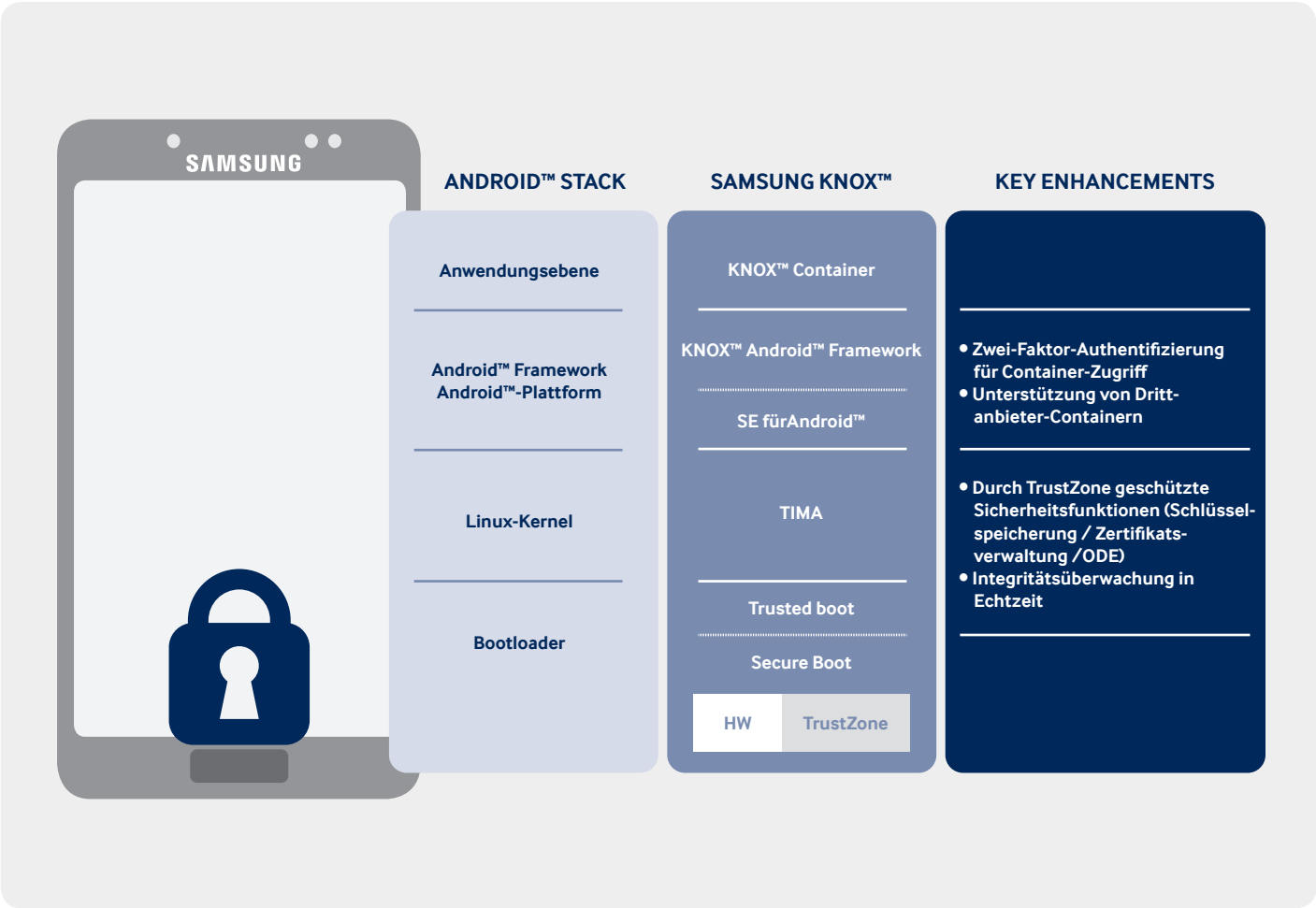

Abbildung 3: Optimierte Plattform-Ebenen von Samsung KNOX™

Samsung KNOX™ bietet wichtige Verbesserungen für eine höhere Hard- und Softwaresicherheit

- **Optimierungen für SE Android™.** Durch die Sicherheitsoptimierungen von SE for Android™ unterstützt Samsung KNOX™ die Plattformsicherheit von Container-Lösungen von Drittanbietern, die neben dem KNOX™-Container zum Einsatz kommen. Durch diese Flexibilität kann Samsung KNOX™ Unternehmen eine hohe Sicherheit für Container führender Drittanbieter bieten.

- **Optimierungen für TIMA.** TIMA führt aus der TrustZone heraus eine fortwährende Echtzeit-Überwachung des Systems durch, um unbefugte Änderungen am Kernel und an der Systempartition zu verhindern. Es schützt vor schädlichen Änderungen am Kernel-Code und der Einschleusung von Schadcode.

- **SmartCard Framework.** Smartphones werden immer häufiger auch zur zusätzlichen Authentifizierung mittels Kartenleser genutzt. Anstatt ein Kartenlesegerät bei sich zu tragen, können die Benutzer einfach ihr Telefon an einen Bluetooth®-Kartenleser halten. Mit der KNOX™-Plattform kann das Smartphone nun als sichere, authentifizierte SmartCard genutzt werden.

Umfassender Schutz vor Datenlecks, Schadsoftware und Angriffen

Erhöhte App-Sicherheit

- Anwendungsebene
- VPN pro App
- On-Device Datenverschlüsselung

Hervorragende Handhabbarkeit

- Unterstützung von mehr als 500 IT-Richtlinien
- Unterstützung von mehr als 1.000 MDM-APIs
- Management über Active Directory
- Kompatibel zu existierenden MDM/VPN/EAS-Infrastrukturen

Sichere Plattform

- Erhöhte Android™-Sicherheit
- TrustZone-basierte Integritätsüberwachung
- Trusted boot

Bereit für Einsatz im Militär- und Regierungsumfeld

- US DoD Mobile OS SRG*'
- US DoD CAC/PIV*
- Root of Trust-Management

* Zurzeit in Umsetzung

Komfortabel und sicher

Flexible Container-Usability

Der Samsung KNOX™ Container gewährleistet die Sicherheit der Unternehmensdaten durch die Erstellung eines abgesichterten Bereichs für Firmenanwendungen innerhalb des Mobilgerät des Mitarbeiters. Die Daten werden hierbei sowohl beim Speichern als auch bei Übertragungen verschlüsselt. Der Samsung KNOX™ Container stellt im Mobilgerät eine isolierte und sichere Umgebung mit eigenem Startbildschirm und Launcher sowie eigenen Anwendungen und Widgets dar. Anwendungen und Daten innerhalb des Containers sind von Anwendungen außerhalb des Containers getrennt. Dadurch bietet Samsung KNOX™ eine komfortable Container-Nutzbarkeit.

Unterstützung zahlreicher Apps

Benutzer können auf eine große Vielfalt von Anwendungen zugreifen, einschließlich KNOX™- und Google Play™-Apps, ohne dass ein App-Wrapping erforderlich ist. Durch den in KNOX™ integrierten Malware-Scan wird die Verfügbarkeit von Anwendungen erhöht, ohne dabei auf App-Sicherheit verzichten zu müssen. So können Unternehmen Firmenanwendungen ganz einfach und sicher im Container nutzen.

Flexible Nutzung von Apps und Daten

Der KNOX™-Container ermöglicht die anpassungsfähige, flexible Nutzung von Anwendungen, Daten sowie einer Zwischenablage zwischen dem privaten Bereich des Benutzers und dem Container. Unternehmen können die Nutzungsflexibilität von Apps und Daten innerhalb des Containers und zwischen persönlichem Bereich und Container steuern, indem sie die Richtlinien für den Container erstellen, anwenden und verwalten.

Mehr Komfort dank geringem Registrierungsaufwand und einer einheitlichen Benutzeroberfläche

Die Benutzer können ihre Mobilgeräte über den Cloud-Server des Samsung Enterprise Gateway (SEG) und den Universal MDM Client (UMC) registrieren und anmelden, was die Anzahl der erforderlichen Schritte für die Erstellung eines KNOX™-Containers auf ein Minimum senkt. Der MDM-Server registriert das Unternehmensprofil im SEG. UMC, eine auf Samsung-GALAXY-Geräten vorinstallierte Anwendung, kommuniziert mit dem SEG, um die MDM-Anwendung herunterzuladen und zu installieren. Nach der Installation authentifiziert die MDM-Anwendung die Anmeldedaten des Benutzers automatisch, indem sie mit dem MDM-Server kommuniziert.

Mobilgeräte mithilfe einer komfortablen, Cloud-basierten Lösung effizient verwalten

Das MDM wird durch eine Cloud-basierte Enterprise-Mobility-Management-Lösung, die keine interne Infrastruktur erfordert, vereinfacht. Die Lösung hilft mögliche Probleme bei der Umsetzung der Unternehmensmobilität zu beheben, wie z. B. Budgetbeschränkungen, begrenzte IT-Kenntnisse oder die Integration verschiedenartiger Geräte. Die Geräte können über ein Admin-Portal mit optionalem, lokalem Active-Directory-Support verwaltet werden, sodass das Mitarbeiterverzeichnis für das interne MDM nicht mehr regelmäßig aktualisiert werden muss, sobald das Unternehmen wächst. Über dieses Portal können IT-Administratoren die Geräte und Anwendungen der Mitarbeiter steuern und überwachen. Dank einer Vielzahl verfügbarer IT-Richtlinien können die IT-Administratoren die Unternehmensrichtlinien ganz einfach anwenden, z.B. Fernlöschung, Passwortzurücksetzung, Fernsperrung, Verschlüsselung der Daten im Gerätespeicher, Einschränkungen für freigeschaltete („jailbroken“)/gerootete Geräte, Einschränkungen bei der Kameranutzung, Standortmeldung usw. Darüber hinaus bietet die Lösung mit plattformübergreifendem Support für Android™- und iOS®-Geräte echte Unterstützung von BYOD (Bring Your Own Device) und CYOD (Choose Your Own Device). Auch ein komfortabler Schnellzugriff auf verschiedene webbasierte Mobile Apps wird mittels Single Sign-On (SSO) ermöglicht.

Mit Samsung als Partner auf zukünftige Mobilitätsbedürfnisse reagieren

Samsung für eine zukünftige Enterprise-Mobility

In der Welt der Spitzentechnologie gibt es nur weniges, das sich langsam entwickelt und der Mobilitätsmarkt gehört zu den aktivsten und sich am schnellsten weiterentwickelnden Technologiesparten. Durch die Präsenz modernster Smartphones, Tablets und anderer Mobilgeräte in der Geschäftswelt, hat sich der Status quo für Unternehmen drastisch gewandelt. Unternehmen, die wettbewerbsfähig bleiben und maximale betriebliche Effizienz erreichen wollen, müssen mit dem zunehmenden Funktionsreichtum der verschiedenen Mobilgeräte schritthalten. Um dieses Ziel bestmöglich zu erreichen, müssen sie nicht nur die Fähigkeiten der Geräte an sich betrachten, sondern auch eine Vielzahl anderer Faktoren, die für den Gesamterfolg des Enterprise-Mobility-Programms ausschlaggebend sind.

Samsung bietet ein variantenreiches und weit verbreitetes Angebot an Mobilgeräten, um ein passendes Modell für nahezu jeden Bedarf bieten zu können. Neben seinen innovativen Produkten hat Samsung eine sichere Enterprise-Mobility-Plattform der Zukunft geschaffen, die den hohen Anforderungen von Firmenkunden gerecht wird.

Dank einer breiten Palette an Mobilgeräten, ausgeklügelter Technologie und umfangreichen, unternehmensorientierten Partnerschaften und Programmen ist Samsung schon heute einer der führenden Akteure im Bereich der Enterprise-Mobility. Ausgehend von seinem Engagement für diese anspruchsvolle Kundschaft strebt das Unternehmen an, diese Rolle auch über die nächsten Jahre erfolgreich zu bekleiden.

Mehr Informationen zu Samsung Produkten und Samsung KNOX™ finden Sie unter

www.samsung.at
www.knox.samsung.at
www.samsungknox.com/de

www.knox.samsung.at

/SamsungAustria
/SamsungAT
/SamsungAustria

Kontaktdaten:
Samsung Electronics Austria GmbH
Praterstraße 31
1020 Wien

Service:
0800 72 67 864
Montag bis Freitag: 8 bis 18 Uhr
Samstag: 8 bis 15 Uhr
service@samsung.at

Stand Mai 2014 · Alle in diesem Dokument erwähnten Produkt- oder Firmenbezeichnungen sind Marken ihrer jeweiligen Eigentümer. Irrtümer und Änderungen vorbehalten.