Nationaler IT Gipfel

Arbeitsgruppe 2

Digitale Infrastrukturen als Enabler
für innovative Anwendungen

UAG Plattformen

Ergebnisbericht 2013

Projektgruppe Sichere IKT-Plattformen für Intelligente Netze

Inhalt

1 Einleitung

Mit den Empfehlungen für eine Nationale Strategie Intelligente Netze anlässlich des 7. Nationalen IT-Gipfels in Essen stellt sich die Frage, wie Intelligente Netze technologisch und sicher realisiert und betrieben werden können. Was verstehen wir konkret unter Intelligenten Netzen, und welche Rolle kommt den IKT-Plattformen bei der Realisierung von Intelligenten Netzen zu? Inwieweit sind Intelligente Netze als kritische Infrastrukturen anzusehen? Welche Möglichkeiten bestehen, dass Intelligente Netze verschiedener Domänen auf Basis bereits existierender IKT-Plattformen auch miteinander kommunizieren können? Mit diesen Fragen hat sich die Projektgruppe in den vergangenen Monaten intensiv beschäftigt und ihre Überlegungen im folgenden Dokument zusammengefasst.

Die Intelligenten Netze der Domänen Energie, Gesundheit, Verkehr, Bildung und Verwaltung sind Anwendungsbereiche von Intelligenten Netzen. Hier ist ein deutlicher Trend dahingehend zu beobachten, dass diese Netze immer stärker miteinander verschmelzen. Eine Intelligenz, die sich aus der Vernetzung von Sensoren, Aktoren, automatisierten Steuerungselementen sowie Verarbeitungslogiken ergibt, ist dazu zwingend erforderlich. Bei der Realisierung von Lösungen für Intelligente Netze der jeweiligen Domänen spielen IKT-Plattformen eine zentrale Rolle.

Das vorliegende Kapitel soll als erste Orientierungshilfe für alle Entscheidungsträger dienen, die sich mit der Umsetzung der Strategie Intelligenter Netze befassen. Es soll Gedankenansätze und Impulse aus technischer Sicht liefern. Dabei wird die Umsetzung neben dem zwingend erforderlichen Telekommunikationsnetz im Wesentlichen über bereits bestehende und neue IKT-Plattformen erfolgen.

2 Definitionen und Begrifflichkeiten

Intelligente Netze

Die AG2 hat sich für den IT-Gipfel 2012 auf folgende Definition Intelligenter Netze geeinigt:

> *„[...] Intelligente Netze beginnen/enden bei Sensoren/Aktoren, denen sie Daten entnehmen bzw. zuführen, werden über Kommunikationskanäle verschiedener, meist breitbandiger Accesstechnologien aggregiert und münden in zentralen Plattformen zur Speicherung bzw. Weiterverarbeitung über anwendungsbezogene Dienste."*[1]

In Erweiterung dieser Definition Intelligenter Netze definiert die Projektgruppe:

> *Ein Intelligentes Netz (IN) ist eine Infrastruktur, in der mindestens ein Teil der Infrastruktur mit Informations- und Kommunikationstechnologie derart verbunden ist, dass eine Regelung oder Koordination der gesamten Infrastruktur oder ihrer Teile mittels IuK-Technologie möglich ist.*

Als Intelligente Netze werden somit Lösungen bezeichnet, die als verteilte Anwendungen den Nutzen einer existierenden Infrastruktur verbessern bzw. optimieren, indem aus dieser Datenverarbeitung zielgerichtete Informationen zur rechten Zeit am rechten Ort für die richtige Person oder zur autonomen Umsetzung vorgegebener Aufgaben entstehen.

IKT-Plattformen

Die AG2 hat sich für den IT-Gipfel 2012 auf folgende Definition Intelligenter Netze geeinigt: Eine IKT-Plattform ist ein verteiltes System, das aus einer Menge von Komponenten der Informations- und Kommunikationstechnologien besteht, die

1. Dienste zur Verfügung stellt,
2. von Anwendungen genutzt werden kann,
3. ohne dass diese notwendigerweise sämtliche Bestandteile der Plattform kennt.

Intelligente Netze werden durch IKT-Plattformen realisiert. Eine IKT-Plattform besteht in der Regel aus Hardware, Software und Kommunikationsnetzen, mit deren Hilfe Daten übertragen, gespeichert oder verarbeitet werden können. Eine IKT-Plattform unterstützt eine Anwendung, indem sie Dienste, Daten und virtuelle wie physikalische Ressourcen über einheitliche Schnittstellen zur Verfügung stellt.

Beispiele für Intelligente Netze

Um besser nachvollziehen zu können, was konkret unter Intelligenten Netzen verstanden werden kann, werden in der Tabelle1 einige Beispiele anhand der fünf Domänen Energie, Gesundheit, Verkehr, Bildung und Verwaltung aufgeführt.

Festzustellen ist, dass Netz, Hardware, Software, Anwendungen und Dienste wiederkehrende Bestandteile sind, welche eine Zusammenarbeit zwischen den Domänen grundsätzlich ermöglichen.

[1] IT-Gipfel AG2: „Digitale Infrastrukturen. AG2-Jahrbuch 2011/2012", S. 295, URL: http://www.it-gipfel.de/IT-Gipfel/Navigation/archiv,did=460266.html (20.11.2013)

Tabelle 1: Beispiele für Intelligente Netze anhand der fünf Domänen

	Energie	Gesundheit	Verkehr	Bildung	Verwaltung
Bestehende Infra-struktur	Stromnetz	E-Health-Anwendungen	Telematik-Infrastruktur	Bildungsplatt-formen, Hochschulnetz	Neuer Personalaus-weis, eID
IKT-Kompo-nenten (IKT-Plattform)	Netz, Hardware, Software, Anwendungen und Dienste				
Anwendungsbeispiele für Nutzen	Verbraucher können „eigenen" Strom generieren und handeln	gezielte schnelle Hilfe im Notfall, effizientere Nutzung von Spezia-listen und kostspieli-gen Geräten	Möglichkeiten einer effektiven Auslas-tung der Verkehrsinf-rastruktur	E-Learning-Anwen-dungen, Video-Conferencing, Collaboration	Nutzung von gemein-samen IT-Infrastruk-turen auf Bundes-, Landes und kommuna-ler Ebene

Quelle: Projektgruppe Sichere IKT-Plattformen für Intelligente Netze der AG2 des Nationalen IT-Gipfels, 2013

Informationssicherheit

Informationssicherheit basiert nach der Definition des Bundesamtes für Sicherheit in der Informationstechnik auf Vertraulichkeit, Verfügbarkeit und Integrität.

> *„Vertraulichkeit: Vertrauliche Informationen müssen vor unbefugter Preisgabe geschützt werden. Verfügbarkeit: Dem Benutzer stehen Dienstleistungen, Funktionen eines IT-Systems oder auch Informationen zum geforderten Zeitpunkt zur Verfügung. Integrität: Die Daten sind vollständig und unverändert."*[2]

Kritische Infrastrukturen

Als Ausgangspunkt der Projektgruppe dient die Definition kritischer Infrastrukturen[3] der Bundesregierung (KRITIS):

> *„Kritische Infrastrukturen sind Organisationen und Einrichtungen mit herausragender oder gar existenzieller Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden."*[4]

Viele Intelligente Netze in den Domänen Energie, Gesundheit, Verkehr und Verwaltung gehören demnach zu kritischen Infrastrukturen.

Eine immer bedeutendere Rolle bei den Kritischen Infrastrukturen kommt der IKT zu. Deshalb ist ein wichtiger Baustein zur Umsetzung der Ziele des Nationalen Plans zum Schutz der Informationsinfrastrukturen der Schutz dieser Informationstechnik.[5]

---

2 Bundesamt für Sicherheit in der Informationstechnik (BSI): Leitfaden Informationssicherheit, IT-Grundschutz kompakt, Februar 2012, Artikelnr. BSI-Bro12/311, URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Leitfaden/GS-Leitfaden_pdf.pdf?__blob=publicationFile (20.11.2013)

3 In diesem Dokument stehen im Mittelpunkt der KRITIS-Thematik die IT-Bedrohungen, also der Schutz von Kritischen Informationsinfrastrukturen. Siehe auch den Arbeitsbereich des BSI, URL: https://www.bsi.bund.de/DE/Themen/KritischeInfrastrukturen/kritischeinfrastrukturen_node.html (20.11.2013)

4 Internetplattform zum Schutz Kritischer Infrastrukturen (KRITIS) (http://www.kritis.bund.de)

5 Nationaler Plan zum Schutz der Informationsinfrastrukturen in Deutschland, URL: http://www.bmi.bund.de/cln_156/SharedDocs/Standardartikel/DE/Themen/OeffentlicheDienstVerwaltung/Informationsgesellschaft/NPSI.html (20.11.0213)

3 Sichere IKT-Plattformen für Intelligente Netze

Die rasch voranschreitende Vernetzung sowie die Möglichkeit, durch Intelligente Netze zuvor voneinander getrennte Systeme zu konvergieren, zu orchestrieren und transparent zu machen, schafft zugleich neue Herausforderungen für deren Absicherung.

Es geht dabei nicht nur um stationäre und mobile Endgeräte (z. B. Computer, Smartphone), sondern vor allem um eine stark wachsende Zahl von vernetzten Geräten – etwa im Haushalt, in einer Windkraftanlage, in einem Fahrzeug oder in einer Straßenlaterne –, die mit anderen Maschinen (M2M) oder Personen (P2M) über das Internet kommunizieren.

Die dabei erzeugten und genutzten Daten, die zwischen Geräten, Netzwerken und Cloud-Diensten ausgetauscht werden, müssen ausreichend geschützt sein.

Unsere digitale Gesellschaft benötigt deshalb nicht nur hochleistungsfähige Intelligente Netze, sondern auch Plattformen und Dienste, die eine vertrauenswürdige Nutzung ermöglichen, sodass sichere IKT-Plattformen unter anderem folgende Eigenschaften besitzen sollten:

- Schutz vor unbefugtem Zugriff (Lesen und Manipulation) bieten,
- stabil und ausfallsicher sein,
- personenbezogene Daten schützen und
- auf offenen Standards basieren.

Diese zu realisieren und mit Gefahren durch menschliche Fehlhandlungen, organisatorische Mängel, technisches Versagen oder höhere Gewalt[6] risikobewertend umzugehen, bedarf sowohl physischer als auch logischer Sicherheitsmaßnahmen, die von organisatorischen und personellen Regelungen flankiert sein müssen und in eine Gesamt-Sicherheitsarchitektur einfließen sollten.

Der Aufbau von Plattformen für Intelligente Netze sollte unter Sicherheitsgesichtspunkten erfolgen. Dabei ist darauf zu achten, dass die gesamte Einsatzumgebung in den Blick genommen wird. Ein grundsätzliches Misstrauen in derzeit als sicher geltende und überwiegend angewendete kryptographische Verfahren ist dagegen nicht angebracht. Dies belegen die derzeit genutzten Angriffsvektoren. Angreifer zielen nicht darauf ab, die eingesetzten kryptographischen Verfahren zu brechen, sondern Schwachstellen in der Implementierung der Einsatzumgebung zu finden, um so die Verschlüsselung und andere Sicherheitsmechanismen zu umgehen.

3.1 Physische Sicherheit

Die physische Absicherung einzelner Elemente der Plattformen Intelligenter Netze wie etwa Rechenzentren ist dabei der erste Schritt zu einer umfassenden Sicherheitsarchitektur. Diese Maßnahmen beinhalten aber weit mehr als gesicherte Türen und Fenster. Vielmehr müssen die Lage und auch der Schutz vor menschlichen Eingriffen wie etwa Diebstahl, Vandalismus sowie gezielte Sabotage beachtet werden.

Dabei dürfen Sicherheitserwägungen nicht allein von Extremsituationen ausgehen, sondern müssen sämtliche Beeinträchtigungen berücksichtigen, die Einfluss auf die verwendeten Komponenten nehmen können. Um die notwendige Verfügbarkeit und Datenintegrität zu gewährleisten, sind daher technische Maßnahmen für eine sichere, unterbrechungsfreie Energieversorgung, für Brandschutz sowie für ein gleichmäßiges Temperatur- und Feuchtigkeitsniveau unerlässlich.

[6] Bundesamt für Sicherheit in der Informationstechnik (BSI): Leitfaden Informationssicherheit, IT-Grundschutz kompakt, Februar 2012, Artikelnr. BSI-Bro12/311, URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Leitfaden/GS-Leitfaden_pdf.pdf?__blob=publicationFile (20.11.2013)

Wie Informationssicherheit allgemein, kann auch physische Sicherheit nur über ein mehrstufiges Konzept erzielt werden. Dieses umfasst präventive bauliche Maßnahmen ebenso wie aktive Abwehr- und Schutzvorkehrungen sowie eine Kontrolle der Prozesse und Abläufe und nicht zuletzt klare Regelungen für den Zugang des Personals.

Verschiedene Organisationen auf nationaler und internationaler Ebene[7] haben hierzu Richtlinien, Architekturen und Qualitätskriterien erarbeitet.

3.2 Netzwerk-Sicherheit

Bereits heute greifen Mitarbeiter seltener lediglich von stationären Geräten, dem „klassischen" Desktop-Arbeitsplatz, mit einer IP-Adresse, einem Netzwerk-Anschluss und einem Protokoll auf Daten im Netzwerk zu. In einer zunehmend mobilen und damit entgrenzten Arbeits- und Lebensumwelt, die durch Plattformen für Intelligente Netze geschaffen wird, und ihre Freiheitschancen und Effizienzgewinne gerade hieraus schöpft, können Nutzer von jedem Ort aus und mit jedem Gerät über jede beliebige Instanz eines Netzwerks die für sie notwendigen Daten bearbeiten. Hier sind Benutzername und Kennwort als Mittel der Authentifizierung sowie als alleinige Zugangskontrolle nicht mehr ausreichend. Eine rein endpunktbasierte Sicherheitsverwaltung wird daher von mehrstufigen Ansätzen abgelöst werden müssen, die sämtliche sicherheitsrelevanten Aktivitäten in Netzwerken und Einsatzumgebungen umfassen.

Das bedeutet jedoch vor allem proaktiv vorzugehen, Sicherheit nahtlos in die Architektur einzufügen, bereits bei der Konstruktion einzuplanen und bestehende Sicherheitstechnologien zu integrieren.

Insbesondere in Intelligenten Netzen sollten Maßnahmen gegen Bedrohungen sich nicht auf einzelne Elemente fokussieren, sondern perspektivisch auf das gesamte Netzwerk mit seinen Kommunikationsverbindungen ausgerichtet sein, beispielsweise durch den Einsatz von Verschlüsselung per Voreinstellung.

3.3 Plattform- und Dienste-Sicherheit

Der Schutz der Plattform- und Diensteebene ist ein wesentlicher Aspekt der Sicherheitsarchitektur. Gerade auf diesen Ebenen aufgrund ihrer Komplexität der Strukturen, Datenmodelle und Schnittstellen sind unternehmenskritische Informationen und schützenswerte Zugriffsberechtigungen den größten Gefahren ausgesetzt. Traditionelle Sicherheitskonzepte zeigen hier immer weniger Wirkung, da virtualisierte Anwendungen kaum mit physischen Ressourcen identisch sind. Wichtig ist deshalb, dass Maßnahmen wie Security by Design[8], ein transparentes und stringentes Identity- und Accessmanagement, die Nutzung von IDS/IPS-Systemen und CERT-Services sowie notwendige Sicherheitsprozesse wie Incident-, Vulnerability- und Patch-Management für ein risikobasiertes, verlässliches und vertrauenswürdiges Sicherheitsmanagement etabliert werden.

Vertrauen kann durch einen risikobewertenden Ansatz erzielt werden. Dieser setzt auf einem einheitlichen, technologieneutralen Verfahren zur Risikoanalyse von Plattformen für Intelligente Netze unter Berücksichtigung nationaler und internationaler Sicherheitsstandards auf. Unterschiede und Kriterien sind hinsichtlich der Kritikalität für Betreiber und Nutzer festzulegen.

---

[7] z. B. eco – Verband der deutschen Internetwirtschaft (http://www.eco.de) oder Uptime Institute (http://uptimeinstitute.com/)

[8] Im Rahmen der Anwendungskonzeption und -entwicklung (Entwurfsprinzip) werden Sicherheits- und Datenschutzmaßnahmen berücksichtigt.

[9] z. B. die Common Criteria (http://www.commoncriteriaportal.org)

Wichtig für die Risikobewertung einzelner Elemente der Plattformen Intelligenter Netze ist darüber hinaus die Evaluierung und Zertifizierung sowohl bestimmter Einzelkomponenten als auch des gesamten Systems. Um mit den gerade in der IT sehr kurzen Innovationszyklen Schritt halten und gleichzeitig den Anwendern einen Bewertungsrahmen bieten zu können, sind möglichst internationale Standards und „Frameworks" für die Risikobewertung[9] zu nutzen. Dies sollte in einem weltweit abgestimmten Rahmen je nach Kritikalität abgestuft erfolgen.

3.4 Datenschutz

Die Einhaltung des Datenschutzes ist für die Umsetzung und Akzeptanz von Intelligenten Netzen von großer Bedeutung. Da die domänen-, firmen- und organisationsübergreifende Datenverarbeitung ein besonders wichtiges – wenn auch nicht ausschließliches – Merkmal Intelligenter Netze ist, ist der Abgleich der Datenmodelle zwischen verschiedenen Domänen Intelligenter Netze eine wesentliche Aufgabe Intelligenter IKT-Plattformen.

Die vorhandene Technik kann die Datenschutzbestimmungen heute im Wesentlichen abbilden bzw. darauf angepasst werden. Wenn allerdings Datenschutz in einzelnen Bundesländern Deutschlands schon unterschiedlich interpretiert wird, wird dieses durch unterschiedliche Datenschutzniveaus in 28 EU-Mitgliedsstaaten noch zusätzlich erschwert.

Eine Chance auf Rechtssicherheit und Harmonisierung bietet deshalb die EU-Datenschutz-Grundverordnung. Bei einem domänenübergreifenden Datenschutz müssen aber auch Regelungen und Compliance über den reinen Datenschutz hinaus Berücksichtigung finden.

Verarbeiten Intelligente Netze Daten von bzw. über Endverbraucher, muss stets nachvollziehbar sein, wie diese Daten genutzt werden. Endverbraucher müssen die Option (Opt-in, Opt-out) haben, Dienste Intelligenter Netze zu nutzen – oder eben auch nicht.

Als Beispiel seien die Ortungsdienste auf Smartphones oder Tablets genannt. Aktiviert der Nutzer diese Ortungsdienste und zieht unmittelbaren Nutzen daraus, muss ihm gleichzeitig bewusst sein, dass diese Daten gesammelt, ausgewertet und ggf. auch zu einer Profilerstellung genutzt werden können.

3.5 Offene Standards und Interoperabilität

IKT-Plattformen für Intelligente Netze müssen sicher und zuverlässig im Betrieb und gleichzeitig offen für Innovationen sein. Mit der Zusammenführung von Daten aus unterschiedlichen Intelligenten Netzen kann die Qualität der Information und Entscheidung in jeder einzelnen Domäne verbessert werden. An einem rasanten Zuwachs an Bedeutung für die weltweite IKT-Wirtschaft haben offene Standards[10], die die Grundlage für interoperable IKT-Plattformen liefern, einen maßgeblichen Anteil.

Da für kritische Infrastrukturen die Zuverlässigkeit und eindeutige Interpretierbarkeit von erhobenen Daten sowie die verifizierbare Ausführung gewünschter Aktionen im Mittelpunkt stehen, müssen offene, standardisierte Schnittstellen und Datenmodelle diesen Anforderungen besonders Genüge tun.

Neben der Möglichkeit der Analyse der Datenflut aus verschiedensten Quellen (Big Data), stellt sich aufgrund der Sensibilität von Daten aus Intelligenten Netzen die Anforderung nach Anonymisierung von Datenquellen unter Beibehaltung der Verifizierbarkeit.

[10] Angelehnt an die Genfer Erklärung der OpenForumEurope Conference (PDF, Englisch) Februar 2008; URL: http://www.openforumeurope.org/library/geneva/declaration/manifesto-with-logos-final.pdf (20.11.2013)

3.6 Weitere Aspekte

Für die Entwicklung und den sicheren Betrieb Intelligenter Netze sind auch Aspekte der Betriebssicherheit wichtig, die zur verlässlichen Bereitstellung von Informationen und Diensten beitragen.

IKT-Plattformen sind verteilte Anwendungen und müssen folglich die Verteilung von Informationen in geeigneter Weise unterstützen bzw. selbst diesen Anforderungen genügen. Grundsätzliche Ansatzpunkte sind die Verbesserung der Qualität oder die Diversifikation von Informationen und technischen Komponenten.

Ganz wesentliche Bestandteile aus technischer Sicht sind die Zugangsnetze (leitungsgebundenes Netz, Mobilfunk, WLAN, u. a.). Ohne diese ist ein Zugang zu Informationen und Diensten über das Internet oder der Aufbau gesicherter Verbindungen zu geschlossenen Netzen schlicht unmöglich.

4 Technisches Referenzmodell von IKT-Plattformen für Intelligente Netze

Die Vielfalt möglicher Kombinationen Intelligenter Netze führt schnell dazu, dass eine einzelne Referenzarchitektur entweder zu abstrakt und damit als Muster nicht aussagekräftig genug zur Entwicklung spezifischer Modelle ist oder zu spezifisch, um als allgemeines Muster für eine hinreichend große Menge Intelligenter Netze zu dienen. Daher ist ein schrittweiser Ansatz sinnvoll, für den im Folgenden die Grundlagen dargestellt werden.

Entsprechend der Definition handelt es sich bei Intelligenten Netzen aus technischer Sicht um verteilte Systeme. Als Ansatz, um derartige Systeme systematisch und strukturiert zu beschreiben und zu entwickeln, bietet sich das Architekturmuster der diensteorientierten Architektur (SOA, Service-oriented Architecture) an. Bei diesem Ansatz werden IT-Ressourcen (wie Sensoren/Aktoren und Verarbeitungslogiken)11 nicht direkt angesprochen, sondern der Zugriff wird über Dienste ermöglicht.

Eine Anwendung wird über die Nutzung und Kombination verschiedener Dienste realisiert, wobei die Dienste selbst wiederum aus anderen Diensten bestehen können. Die interne Steuerung zum Angebot der Dienste bzw. das interne Management einer Plattform sind für den Nutzer des Dienstes verborgen. Insgesamt bietet dieses Architekturmodell eine abstrakte Sicht auf die Nutzung von Diensten, was die Wiederverwendbarkeit von Diensten, die Kombination von einfacheren zu höherwertigen Diensten und die Orientierung der Implementierung an vorgegebenen Prozessen erleichtert.

Abbildung 1 stellt dar, wie eine Anwendung auf Basis von Diensten verschiedener Plattformen realisiert ist.

Beispielsweise könnte eine Anwendung „Daten-Safe“ auf der Nutzung zweier Dienste aufgebaut sein: Identifikation des Nutzers und Speicherung von Dokumenten. Dabei können beide Dienste von verschiedenen Plattformen stammen bzw. es können alternative Dienste von weiteren Plattformen parallel für die gleichen Funktionen genutzt werden.

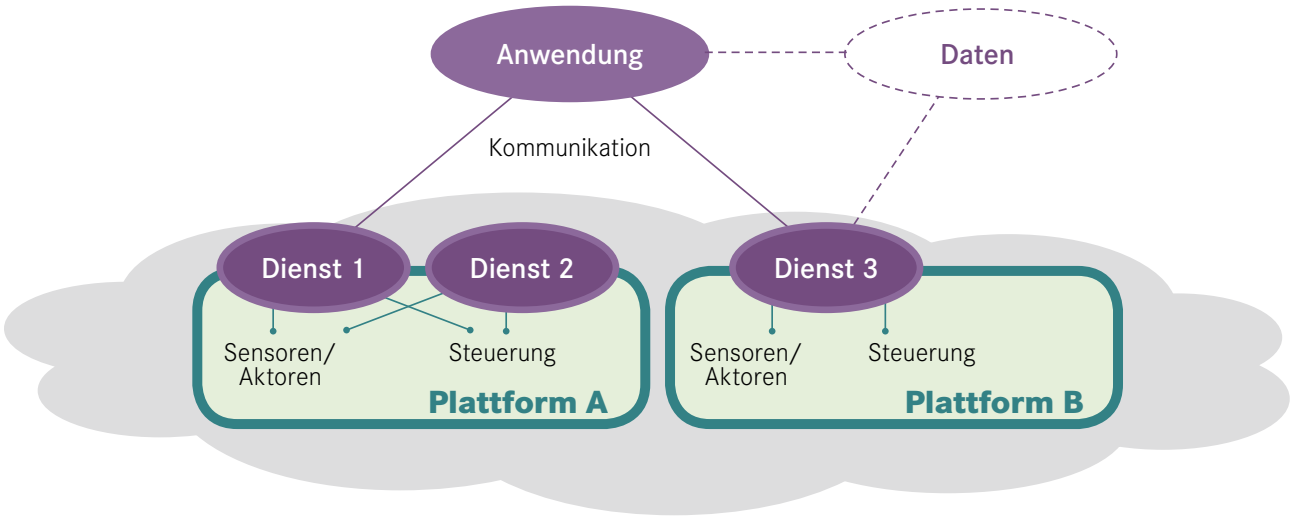

Abbildung 1: IKT-Plattfomen zum Aufbau Intelligenter Netze
Quelle: Projektgruppe Sichere IKT-Plattformen für Intelligente Netze der AG2 des Nationalen IT-Gipfels, 2013

Folgende Vorteile ergeben sich aus technischer Sicht aus der Nutzung eines diensteorientierten Ansatzes als einheitlichem Ansatz zur Beschreibung und Entwicklung Intelligenter Netze:

- Fokussierung auf die Schnittstellen, Verzicht auf Vorgaben zur Implementierung,
- Erleichterung der Erstellung von bereichsübergreifenden Anwendungen durch die Verwendung ähnlicher Plattformansätze in verschiedenen Bereichen,
- Einbeziehung bestehender Infrastrukturen und Dienste, die schon diesem Architekturmuster folgen bzw. Kapselung anderer, bereits bestehender Funktionselemente.

Zur Illustration zeigt Abbildung 1 zudem exemplarisch, welche Komponenten eines Intelligenten Netzes Informationen bzw. Daten beinhalten, die evtl. auch in anderen Intelligenten Netzen (z. B. in anderen Domänen) für eine Weiterverwendung von Interesse sein könnten. Zum besseren Verständnis grundlegender Anforderungen, die sich aus technischer Sicht ergeben, wird ein stark vereinfachtes Modell einer IKT-Plattform vorgestellt. IKT-Plattformen stellen Dienste zur Verarbeitung der Informationen eines Intelligenten Netzes zur Verfügung. Der Zugriff auf diese Dienste erfolgt über eine geeignete Schnittstelle, die konkrete Eigenschaften und Anforderungen der Dienste verbirgt und so nach außen einheitliche, dienstkonforme Zugriffsmöglichkeiten auf die Dienste anbietet.

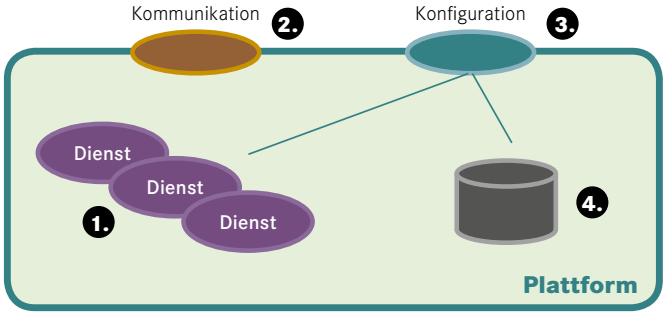

Abbildung 2: Vereinfachte Darstellung einer IKT-Plattform
Quelle: Projektgruppe Sichere IKT-Plattformen für Intelligente Netze der AG2 im Nationalen IT-Gipfel, 2013

Abbildung 2 zeigt minimale technische Bestandteile von Plattformen. Die Ressourcen sind in dieser Darstellung nicht sichtbar, da sie für den Nutzer verdeckt sind und für den direkten Zugriff nicht zur Verfügung stehen. Plattformen haben weitere Bestandteile, wie internes Management, die in dieser vereinfachten Darstellung nicht dargestellt sind.

Folgende Bestandteile von Plattformen sollen genannt werden:

1. Dienste
Dienste stellen Ressourcen bereit, wie den Zugriff auf Sensoren/Aktoren, Kommunikationsverbindungen, Datenspeicher, Identifikation von Nutzern usw. Ein Dienst ist in sich abgeschlossen und erfüllt eine genau definierte Aufgabe.

2. Kommunikation
Der Datenaustausch mit und zwischen Diensten erfordert Kommunikation, basierend auf standardisierten Schnittstellen zur Datenübertragung und zur Beschreibung von Datenobjekten. In diesem vereinfachten Modell steht diese logische Schnittstelle für den Austausch von Nutzdaten zur Erfüllung der vorgesehenen Aufgabe.

3. Konfiguration
Die Nutzung der Plattform bzw. von Diensten erfordert die Steuerung der Dienstnutzung wie das Auslesen der Beschreibungen der Plattformen und von einzelnen Diensten. Standardisierte Schnittstellen hierfür sind, verglichen mit dem Austausch von Nutzerdaten, komplexer, aber essenziell für ein Angebot vergleichbarer und interoperabler IKT-Plattformen.

4. Beschreibung von Diensten und Schnittstellen
Dienste können nur genutzt werden, wenn ihr Zweck und ihre Nutzung genau beschrieben sind. Gerade für den universellen Einsatz in verschiedenen Anwendungsbereichen ist eine eindeutige, weithin verständliche Beschreibung notwendig. Für eine weitgehend automatisierte Nutzung von Plattformen werden maschinenlesbare Beschreibungen benötigt.

Die Beschreibungen gehen über rein technische Angaben hinaus, beispielsweise gehören auch Service Level Agreements und Nutzungsbedingungen dazu.

Die in diesem vereinfachten Modell vorgenommene Trennung von Kommunikation und Konfiguration soll darauf hinweisen, dass für ein erfolgreiches Zusammenwirken von verschiedenen Diensten mehr nötig ist als der reine Datenaustausch.

Verschiedene Plattformen – gerade aus unterschiedlichen Anwendungsbereichen – gehen von unterschiedlichen Vorrausetzungen zur Nutzung von Diensten aus. Beispielsweise wird in allen Bereichen verschlüsselte Kommunikation bekannt sein und daher von Diensten angeboten bzw. von einer Anwendung nachgefragt. Allerdings sind unterschiedliche Verschlüsselungsverfahren bzw. -parameter im Gebrauch. Daher muss Verschlüsselung konfiguriert werden, um tatsächlich genutzt werden zu können.

In den verschiedenen Bereichen Intelligenter Netze werden einzelne Komponenten aus technischer Sicht auf ganz unterschiedlichen Ebenen gesehen. Daher ist es schwer, alle möglichen Komponenten und Bestandteile Intelligenter Netze in einer Übersicht zusammenzufassen und hierarchisch zu strukturieren.

Mithilfe eines diensteorientierten Modells bietet sich eine Sichtweise an, die nicht von der Komplexität eines Dienstes oder dessen Implementierung abhängig ist, sondern Dienste zur beliebigen weiteren Verwendung in den Mittelpunkt stellt.

Dieser erste Entwurf des Referenzmodells umfasst vier Ebenen und die Sicherheit als technische Querschnittsaufgabe (siehe folgende Abbildung 3):

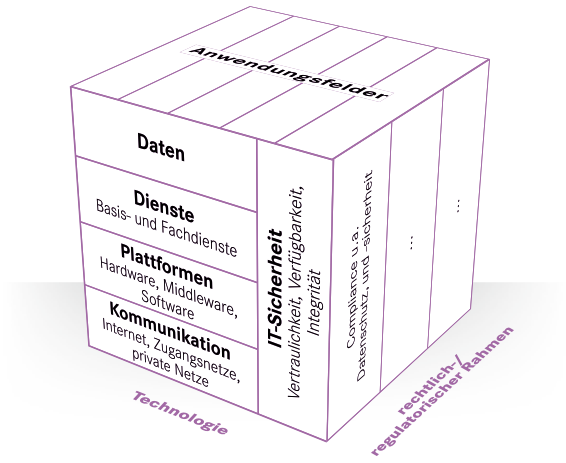

Abbildung 3: Komplexitätsrahmen Intelligenter Netze aus technischer Sicht auf IKT-Plattform
Quelle: Erweiterung der Abbildung „Komplexitätsrahmen Intelligenter Netze“ aus dem AG2-Jahrbuch 2012/2013, S. 39, wobei die Seite „Technologie“ aus Sicht von IKT-Plattformen ersetzt wurde.

- **Daten**
  Die Datenebene enthält die Inhalte und Informationen, die für ein Intelligentes Netz relevant und typisch sind. Sie entstehen z. B. über Sensoren und Aktoren, über Konfigurationseingaben, oder auch als Ergebnis von Anwendungen. In diesem Referenzmodell werden sie explizit ausgewiesen, da ihre domänenübergreifende Nutzung zu neuen Anwendungsmöglichkeiten führt und somit einen Mehrwert generiert. Sie stellen einen besonders schützenswerten Teil dar, da nicht nur die Informationssicherheit zu gewährleisten ist, sondern u. U. weitere rechtliche Aspekte, beispielsweise urheberrechtliche Punkte, zu beachten sind.[11]

- **Dienste**
  Die Dienste können in verschiedene Klassen aufgeteilt werden. Hervorgehoben werden hier Basisdienste, die aufgaben- und bereichsübergreifend genutzt werden können (wie Verarbeitungslogiken, Speicher, Identifikation, ...) und Fachdienste oder fachspezifische Dienste, die anwendungsspezifische Lösungen bereitstellen und nicht – oder nur in speziellen Bereichen – wiederverwendet werden.

  Besondere Beachtung verdienen Basisdienste, von deren Funktionieren andere Dienste und mehrere Anwendungen abhängen. Zur Lösung dieses Problems tragen die weitgehende Standardisierung von Schnittstellen und der Wettbewerb zwischen verschiedenen Anbietern bei.

- **Plattformen**
  Diese Ebene umfasst die Infrastruktur, um Dienste und Anwendungen anbieten zu können. Dazu gehört das Zusammenspiel von Hardware, Middleware und Software.

- **Kommunikation**
  Kommunikation als Grundlage umfasst das Internet als Backbone der Kommunikation, Zugangsnetze zum Internet (wie feste Anschlüsse, Mobilfunk), private bzw. geschlossene Netzinfrastrukturen (beispielsweise zur Steuerung von Stromnetzen).

  Private Netzinfrastrukturen können auf Basis des Internets realisiert oder davon unabhängig sein (z. B. VPN-basiert oder auf eigener physikalischer Infrastruktur).

  Das Internet in der jetzigen Form ist eine weit verbreitete Basistechnologie. Sicherheitsprobleme sind gut bekannt. Besondere Beachtung verdienen die Zugangsnetze, die für konkrete Verfügbarkeit von Kommunikation vor Ort entscheidend sind. Daher sollten Plattformen und Nutzer über redundante Netzzugänge verfügen.

- **Sicherheit**
  Der Querschnittsbereich Sicherheit umfasst die Sicherstellung von Vertraulichkeit, Verfügbarkeit und Integrität. Die Darstellung im obigen Modell deutet an, dass die in Kapitel 2.1.3 beschriebenen ganzheitlichen technischen Sicherheitsmodelle zum Einsatz kommen müssen, entsprechend des zugrunde liegenden rechtlich/regulatorischen Rahmens.

[11] Anmerkung: Bei diensteorientierten Architekturen findet der Datenzugriff über Dienste statt. Damit sind die Daten gekapselt. Im hier dargestellten Modell werden die Daten explizit dargestellt, da sie insbesondere für Sicherheitsbetrachtungen und den Austausch zwischen verschiedenen Intelligenten Netzen eine wichtige Rolle spielen.

5 Zusammenfassung und Fazit

IKT-Plattformen werden beim Aufbau Intelligenter Netze eine entscheidende Rolle spielen. Durch sie wird ein Abgleich von Datenmodellen zwischen verschiedenen Domänen erst möglich.

Sicherheit ist dabei nicht nur für die Akzeptanz ein entscheidender Faktor, sondern auch für die Funktionsfähigkeit, Verfügbarkeit und Integrität von Intelligenten Netzen. Dabei reicht es für die umfassende Sicherheit eines Intelligenten Netzes nicht aus, auf rein technischer Ebene Sicherheitsmaßnahmen zu implementieren. Vielmehr sind neben einem Sicherheitskonzept für IKT-Plattformen des Intelligenten Netzes auch Sicherheitskonzepte für die betrieblichen Prozesse und Abläufe der kritischen Infrastrukturen notwendig.

Standardisierung wird bei der Realisierung von Intelligenten Netzen auf technischer Ebene ein grundlegender Erfolgsfaktor sein. Auf Basis offener Standards werden IKT-Plattformen größtmöglich interoperabel mit unterschiedlichen Technologien kommunizieren können und dabei gleichzeitig Vielfalt und Wettbewerb fördern. Proprietäre Insellösungen sollten vermieden werden. Sie sind nicht evolutionär und in der Regel auch nicht modular weiterzuentwickeln.

Bei alldem gilt es festzuhalten: Dieser Beitrag gibt den aktuellen Diskussionsstand der Projektgruppe wieder. Über die bisher betrachteten Aspekte hinaus müssen im Weiteren Konzepte erarbeitet werden, wie die dargestellten diensteorientierten Ansätze weiterentwickelt werden können, um die gewünschte domänen-, firmen- und organisationsübergreifende Wertschöpfung zu ermöglichen. In diesem Zusammenhang müssen insbesondere folgende Punkte eingehend untersucht werden:

- Art und Weise einer kooperativen Governance bezüglich Architektur und Betrieb Intelligenter Netze, darunter insbesondere der IKT-Plattformen,
- Diensteübergreifende Ausgestaltung von Trust-Beziehungen und Identity-Management-Konzepten,
- Konzepte zur Monetarisierung einer Dienste- und Datennutzung in Intelligenten Netzen, insbesondere im Zusammenhang verschachtelter bzw. zusammengesetzter Dienste, also dann, wenn sich Anwendungen auf Dienste Dritter abstützen und entsprechende Verrechnungen von über Intelligente Netze erbrachte oder vermittelte Dienstleistungen zwischen Dienstenutzer und Diensteanbieter erforderlich werden,
- Konzepte zur Abbildung und Überwachung von Service Level Agreements auf Diensteebene.

Darüber hinaus sind in Abstimmung mit anderen Arbeitsgruppen die sich durch Intelligente Netze ergebenden Anforderungen an den rechtlich/regulatorischen Rahmen auszuarbeiten – nicht nur in Bezug auf Datenschutz/Datensicherheit, sondern auch auf darüber hinausgehende Anforderungen an kritische Infrastrukturen. Dies bedeutet insbesondere die Erarbeitung eines Kriterienkatalogs „Kritische Infrastrukturen“ zur Einordnung von Intelligenten Netzen und deren Bestandteilen als kritische Infrastrukturen sowie die Ableitung der diesbezüglichen Sicherheitsanforderungen für deren Entwicklung/Aufbau, Betrieb und Nutzung.

Klar geworden ist der Projektgruppe in der Erarbeitung, dass kritische Infrastrukturen in immer mehr Lebensbereichen eine existenzielle Rolle spielen und deren Verbreitung und Bedeutung rasant zunehmen wird. Zur Sicherung der anerkannten zahlreichen und umfassenden gesellschaftlichen und volkswirtschaftlichen Vorteile bedarf es der aktiven Befassung mit den vorgenannten Kriterien rechtlich/regulatorischer Rahmen sowie Datenschutz und -sicherheit – auf politischer, gesellschaftlicher und wirtschaftlicher Ebene.

6 Politische Handlungsempfehlungen zur Förderung von sicheren IKT-Plattformen für Intelligente Netze

6.1 Ausgangssituation und Zielsetzung

Alle Lebens-, Wirtschafts-, Verwaltungs- und Politikbereiche sind heute von IKT durchdrungen. Dabei hat sich IKT zu einem wichtigen Standortfaktor entwickelt. Sowohl in öffentlichen als auch privaten Netzwerken steigt der Datenverkehr in den kommenden Jahren aufgrund von mobilem und festnetzgebundenen IP-Datenverkehr, der zunehmenden Verbreitung internetfähiger Geräte, der Vernetzung physikalischer Objekte mit dem Internet (Industrie 4.0 und Internet der Dinge) und der das Internet intensiver nutzenden Weltbevölkerung signifikant.[12]

Ziel der Arbeitsgruppe 2 des Nationalen IT-Gipfel ist zu beschreiben, wie und in welcher Form „Digitale Infrastrukturen als Enabler für innovative Anwendungen" dienen können. In der Weiterführung der Empfehlungen für eine nationale Strategie Intelligente Netze anlässlich des 7. Nationalen IT-Gipfels befasst sich die Projektgruppe mit deren sicherer technologischer Realisierung. Das Dokument referenziert auf die Ergebnisse der Arbeitsgruppe 2 des Nationalen IT-Gipfels 2012 in Essen und gibt Handlungsempfehlungen aus Sicht von Wirtschaft und Wissenschaft für sichere Informations- und Kommunikations-Plattformen (IKT) an die Politik.

Ein Intelligentes Netz ist eine Infrastruktur, die den Nutzen einer existierenden Infrastruktur durch den Einsatz von IKT optimiert,[13] wobei Komponenten der bestehenden Infrastruktur mit Komponenten der Informations- und Kommunikationstechnologie verbunden werden. Intelligente Netze sind somit Lösungen, die als verteilte Anwendung eine Regelung oder Koordination unterschiedlicher technischer Geräte und/oder Dienste ermöglichen. Intelligente Netze helfen, gesellschaftliche Herausforderungen besser zu lösen und bieten große volkswirtschaftliche Chancen.

Realisiert werden Intelligente Netze durch den Einsatz von IKT-Plattformen, d.h. eine Menge von Komponenten der IKT, die

- Dienste zur Verfügung stellt,
- die von mindestens zwei Anwendungen genutzt werden können,
- ohne dass diese notwendigerweise die Elemente der Plattform kennen müssen.

Die zügige Einführung und Nutzung von intelligenten Netzinfrastrukturen und IKT-Plattformen erfordern ein Handeln insbesondere in Bezug auf Sicherheit und Akzeptanz.

Zwingende Voraussetzung zur Realisierung Intelligenter Netze ist ein flächendeckender Ausbau von Netzinfrastrukturen, um IKT-Plattformen für Intelligente Netze zu betreiben, zu nutzen und einen sinnvollen Austausch von Informationen zu gewährleisten. Hierzu bedarf es der weiteren Beschleunigung und Förderung des Breitbandausbaus. Die Entwicklung von IKT-Infrastrukturen sollte mindestens einen vergleichbaren Stellenwert wie beispielsweise der Ausbau konventioneller Verkehrsinfrastrukturen erhalten.

[12] The Global Information Technology Report 2013 / http://www3.weforum.org/docs/WEF_GITR_Report_2013.pdf. An dem nach Datenvolumen derzeit weltweit größten Internetknoten DE-CIX zeigt sich eine Verdreifachung des Internetverkehrs über einen Zeitraum von drei Jahren. (http://www.de-cix.net/about/statistics/)

13Referenz auf Jahrbuch 2012/2013 der AG2

6.2 Handlungsempfehlungen

Angesichts der gesellschaftlichen Bedeutung Intelligenter Netze sind die nachstehend zusammengestellten Handlungsempfehlungen breit angelegt und gehen über die rein technische Betrachtung hinaus. Dabei gilt, dass Sicherheit in Form von Vertraulichkeit, Integrität, Verfügbarkeit und Datenschutz stets integraler Bestandteil von IKT-Plattformen sein muss.

1. **Datenpolitik und rechtliche Rahmenbedingungen innovativ gestalten**
   Die Verknüpfung und Nutzung von Daten mit unterschiedlichern Schutzniveaus von einem Intelligenten Netzes in ein anderes, bereichs- und branchenübergreifend kann für die Gesellschaft von hohem Mehrwert sein. Um die Möglichkeiten dieser Verknüpfungen in neuen Formen von Pilotprojekten auszuloten, sollte ein entsprechender rechtlicher Rahmen geschaffen werden. Darüber hinaus sollte die zum Betrieb Intelligenter Netze notwendige Informationstechnik sowenig wie möglich reguliert werden. Grundsätzlich gilt es darauf zu achten, möglichst viel Innovation in Intelligenten Netzen zuzulassen.

2. **IKT-Plattformen durch finanzielle Anreizsysteme für Anwender schneller etablieren**
   Die Marktdurchdringung und flächendeckende Nutzung intelligenter und sicherer IKT-Plattformen ließe sich durch finanzielle Anreize für den Anwender schneller durchsetzen. Als Orientierung dafür kämen entsprechende Beispiele, etwa aus dem Energie-, Verkehrs-, Gesundheits- und Telekommunikationsbereich infrage.

3. **Internationale Standardisierungsbemühungen intensiver begleiten**
   Deutschland sollte sich stärker in Standardisierungsbemühungen auf europäischer Ebene sowie international einbringen und hierfür den entsprechenden Dialog in Deutschland vorantreiben.

4. **Einsatz offener Standards unterstützen**
   Aufgrund der schnellen technologischen Entwicklung ergibt sich beim Aufbau von langlebigen, sich technisch und wirtschaftlich evolutionär entwickelnden Infrastrukturen, die Anforderung nach Vermeidung proprietärer Gestaltung von Technologien. Der Einsatz offener Standards sollte unterstützt werden, da damit eine größtmögliche Interoperabilität zwischen verschiedenen Komponenten ermöglicht wird.

5. **Sicherheitsmodelle und Datenschutz in Intelligenten Netzen besser erforschen**
   Es besteht Forschungsbedarf zu Fragen der Sicherheit und des Datenschutzes in Intelligenten Netzen. Dabei sollten insbesondere Qualitätsanforderungen für Entwicklung und Betrieb von IKT-Plattformen in Intelligenten Netzen, in Abhängigkeit von der Kritikalität des jeweiligen Intelligenten Netzes untersucht werden. Die Bundesregierung sollte dies gezielt fördern.

6. **Vertrauensvolle Kooperation zwischen Politik und Wirtschaft stärken**
   Die vertrauensvolle Kooperation zwischen Politik und Wirtschaft auf allen Ebenen bei kritischen Informationsinfrastrukturen ist zu intensivieren. Dies hält die Sicherheit in Form von Vertraulichkeit, Integrität, Verfügbarkeit und Datenschutz in Deutschland auch weiterhin auf hohem Niveau.

Nationaler IT Gipfel

Herausgeber
Arbeitsgruppe 2 des Nationalen IT-Gipfels (AG2)
„Digitale Infrastrukturen als Enabler für innovative Anwendungen“

Ergebnisbericht 2013
Projektgruppe Sichere IKT-Plattformen für Intelligente Netze

Das Jahrbuch 2013/2014 „Digitale Infrastrukturen – Schwerpunkte und Zielbilder für die Digitale Agenda Deutschlands“ sowie weitere Dokumente der AG2 sind als Download frei erhältlich unter

www.it-gipfel.de

Mitglieder der Projektgruppe Sichere IKT-Plattformen für Intelligente Netze

Claudia Mrotzek (Leitung)
ORACLE Deutschland B.V. & Co. KG

Prof. Dr. Radu Popescu-Zeletin (Leitung)
Fraunhofer Institut für Offene Kommunikationssysteme FOKUS

Dr. Christoph Bach
Ericsson GmbH

Günther Diederich
ifib: Institut für Informationsmanagement Bremen GMBH

Peter Domschitz
Alcatel-Lucent Deutschland AG

Martin Falenski
Initiative D21 e. V.

Peter H. Ganten
Univention GmbH

Dr. Jörg-Michael Hasemann
T-Systems International GmbH

Lutz Märker
DVZ Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH

Jens Mühlner
T-Systems International GmbH

Caroline Neufert
BearingPoint GmbH

Dr. Norbert Niebert
Ericsson GmbH

Percy Ott
Cisco Systems GmbH

Stefan Pechardscheck
BearingPoint GmbH

Dr. Johannes Prade
Nokia Solutions and Networks GmbH & Co. KG

Dr. Matthias Renken
T-Systems International GmbH

Boris Schmidt
Deutscher Verband für Telekommunikation und Medien e. V.

Jens Tiemann
Fraunhofer Institut für Offene Kommunikationssysteme FOKUS

Dr. Gerhard Tobermann
ORACLE Deutschland B.V. & Co. KG

Johannes Wust
Hasso-Plattner-Institut für Softwaresystemtechnik GmbH