René Blaschke, Stefan Suhrer, Dominik Engel

Serviceorientierte Architekturen für Smart Grids

Die Energiewende ist gesellschaftlicher und politischer Konsens. Damit sie gelingen kann, ist eine Modernisierung der Energienetze notwendig, die die Einspeisung dezentraler Erzeuger ermöglicht. Dazu sind detaillierte Informationen zum aktuellen Netzzustand notwendig. Die Informations- und Kommunikationstechnologie (IKT) bietet die Methoden, über die diese Informationen in Smart Grids zur Verfügung gestellt werden können. Das reibungslose Zusammenspiel dieser Methoden bedingt eine geeignete Architektur, welche auch orthogonale Anforderungen wie Datenschutz und -sicherheit realisiert. Wir stellen eine serviceorientiere IKT Architektur vor, die neben der Integration der notwendigen Datenquellen und -senken, bewährte Designpatterns, auch im Bereich Datenschutz und -sicherheit, einsetzt. Der praktische Nutzen dieser Architektur zeigt sich in realen Anwendungsfällen der Smart Grids Modellregion Salzburg.

1 IKT als Wirbelsäule für Smart Grids

Die Zielvorgaben für Klimaschutz und Energie der Europäischen Union sehen eine Reduktion der Treibhausgase um 20%, eine Erhöhung der erneuerbaren Energien um 20% und eine Erhöhung der Energieeffizienz um 20% vor („20-20-20-Ziele“). Ohne Smart Grids kann diese Energiewende nicht gelingen [Appelrath, et al. 2012]. Der Begriff „Smart Grids“, oder intelligente Stromnetze, wird häufig als Synonym für die Herausforderungen, die sich den Energienetzen der Zukunft stellen, verwendet (Definition siehe [DKE 2012]). Historische Szenarien der Energieversorgung basieren auf einer zentralen Verteilung der Energie, von einem Erzeuger zu vielen Konsumenten, vgl. einem Broadcast in Computernetzwerken. Die sogenannte Energiewende führt nun zu einer Dezentralisierung der Energieproduktion, da z.B. private Photovoltaik (PV)-Anlagen in das Verteilernetz einspeisen, und Produzent (Producer) und Konsument (Consumer) zum „Prosumer“ amalgamieren. Zusätzlich zu diesem „Gegenverkehr“ im Verteilernetz stellt sich die Problematik, dass die erneuerbaren Energien in Ihrer Einspeisung stark fluktuieren, und Angebot und Nachfrage nicht immer konvergent verlaufen.

Hier kommt nun die „smarte“ Komponente der Verteilernetze ins Spiel. Durch Informations- und Kommunikationstechnologie (IKT) wird versucht, alle Beteiligten bzw. Komponenten, also Erzeuger, Verbraucher, Regelung, Markt und Speicherung, zu einem gemeinsamen Energiesystem zusammenzuschließen. So sollen die einzelnen Komponenten miteinander interagieren können, Angebot und Nachfrage ausgeglichen werden, und so letztlich die Verteilernetze entlastet werden. Ein entsprechendes Gesamtsystem stellt aufgrund seiner Komplexität hohe Anforderungen an die einzelnen Komponenten, aber vor allem auch an die zugrunde liegende IKT-Architektur. Die Architektur der IKT Infrastruktur, die damit sozusagen die Wirbelsäule der Smart Grids bildet, ist nicht nur entscheidend für die Qualität und Verfügbarkeit der notwendigen Daten, sie muss auch orthogonale Bedingungen wie Anforderungen an Datenschutz und Datensicherheit erfüllen.

Die Vorschläge für Smart Grids IKT-Architekturen in der Literatur spannen einen weiten Bogen, von klar dezentralen Ansätzen, z.B. [Kim et al. 2010], Architekturen die vorrangig Datenschutz berücksichtigen, z.B. [Wicker & Thomas 2011], bis hin zu Ansätzen, welche die

Kommunikationswege in den Vordergrund stellen, z.B. [Sood et al. 2009]. Eine Reihe von europäischen Forschungsprojekten widmet sich IKT Infrastrukturen in Smart Grids. Zum Beispiel hat das EU-Projekt „FINSENY“ die Erstellung einer nachhaltigen Infrastruktur für „Smart Energy“ basierend auf zukünftigen Internettechnologien zum Ziel. Das EU-Projekt „NOBEL“ entwickelt Ansätze einer dezentralen Energiebörse, während im inzwischen abgeschlossenen EU-Projekt „SmartHouse/SmartGrid“ die Rolle von intelligenten Gebäuden beleuchtet wurde. Neben den europäischen Initiativen sind IKT-Architekturen für Smart Grids Fokus eine Reihe von nationalen Projekten und Modellregionen. Der Beitrag in diesem Kapitel stellt die praktische Umsetzung einer auf SOA basierenden IKT-Architektur in der Smart Grids Modellregion Salzburg vor. Eine auf serviceorientierten Architekturen (SOA) basierende IKT-Architektur für Smart Grids wird zum Beispiel auch von [Jung et al. 2012] vorgeschlagen. Der hier präsentierte Ansatz unterscheidet sich von dieser verwandten Arbeit unter anderem durch die Orientierung am reverse Proxy Designmuster und der starken Berücksichtigung praktischer Aspekte, auch durch die Einbettung in die Smart Grids Modellregion Salzburg.

Die Salzburger Smart Grids Moedellregion wurde im Jahr 2009 vom Klima- und Energiefonds (KLIEN) der österreichischen Bundesregierung als erste “Smart Grids Modellregion” Österreichs geschaffen, auch zum Zwecke der Errichtung und Evaluierung eines IKT-Gesamtsystems. In diesem Leuchtturmprojekt werden einige der zahlreichen Herausforderungen, die sich den intelligenten Netzen stellen betrachtet, mit dem besonderen Augenmerk auf Kundenakzeptanz und Nutzerfreundlichkeit. Im konkreten Feldversuch in der Gemeinde Köstendorf sind u. a. die folgenden Komponenten beteiligt:

- 90 Gebäude
- regelbare Ladestationen (36 E-Autos)
- Wechselrichter (43 PV-Anlagen, ca. 192kWp)
- regelbarer Ortsnetztrafo (Leistung 250kVA)
- Smart Meter.

Diese Hauptkomponenten sind auch teilweise die Schwerpunkte entsprechender Forschungsfelder in der Modellregion (Elektromobilität, Stromnetze, Wärmenetze, etc.). Hauptaugenmerk in diesem Beitrag sind die technologischen Herausforderungen die sich der IKT in diesem Umfeld bieten. Einerseits muss die Kommunikation der einzelnen Komponenten und Akteure sichergestellt sein, um eine „intelligente Vernetzung“ zu bewerkstelligen, andererseits handelt es sich bei den zu übertagenden Daten in vielen Fällen um hochsensible Kundendaten bzw. Steuerungsparameter der Komponenten, die in ein entsprechendes Sicherheitsumfeld eingebettet werden müssen. Gerade der Security Aspekt spielt eine maßgebliche Rolle, da vermehrt neue Technologien einer gesunden Skepsis der Anwender gegenüberstehen. Darüber hinaus gibt es eindeutige gesetzliche Vorgaben, die Handhabung und Bereitstellung der benutzerspezifischen Daten regeln. Im Folgenden werden wir zwei sich daraus ergebende Anwendungsfälle genauer betrachten.

2 User-Stories

Die aktuellen gesetzlichen Vorgaben, die Veränderungen am Energiemarkt und die Neuordnung der Energiesysteme stellen die EVUs (Energieversorgungsunternehmen) vor neue, teilweise ungelöste, Probleme. Durch die Veränderungen entstehen einerseits neue komplexe

Anforderungen, aber auch Chancen und neue Geschäftsfelder. Eine exemplarische User-Story (Anwendungsfall) wird hier dargestellt. Diese resultiert aus den verpflichtenden gesetzlichen Anforderungen.

2.1 Bereitstellung der Verbrauchsdaten

Laut österreichischem Bundesgesetzblatt (BGBl. II Nr. 138/2012 Teil II) vom 24.04.2012 müssen bis 2019 mindestens 95% der an einen Netzbetreiber angeschlossenen Zählpunkte mit intelligenten Stromzählern (sog. Smart Meter) ausgestattet werden, d.h. die bestehenden herkömmlichen Stromzähler müssen ersetzt werden und eine Infrastruktur für die Datenübermittlung muss erstellt werden. Smart Meter sind eine der Schlüsselkomponenten im Smart Grid, da erst durch ihren Einsatz die zeitnahe Auswertung und Koordination von Angebot und Nachfrage ermöglicht wird. Daran geknüpft ist die sog. DAVID Verordnung (Datenformat- und VerbrauchsinformationsdarstellungsVO 2012, BGBl. II Nr. 313/2012), welche die Datenübermittlung vom Netzbetreiber zum Stromlieferanten und von Verbrauchsinformationen an den Endkunden regelt. Darin wird explizit die Kundeninformation über die Verbrauchsdaten in einer Website verordnet, inkl. der darzustellenden Werte. Ziel ist die Energieeffizienz durch zeitnahe Kundeninformation zu erhöhen und letztlich beim Endverbraucher eine Korrelation zwischen Verhalten und Verbrauch herzustellen.
Bezogen auf die Kundeninformation ergeben sich bei allen Netzbetreibern folgende Pflichten:

- Erstellung eines aktuellen Sicherheitsumfeldes,
- RollOut der Smart Meter,
- Datenerfassung und -speicherung,
- Datenvorratshaltung (drei Jahre) und
- Datenbereitstellung und -visualisierung über das Internet unter Berücksichtigung der datenschutzrechtlichen Bestimmungen bzgl. Zugriffsrechten,

die in Abbildung 1 aus Endverbrauchersicht als System-Use-Case-Diagramm visualisiert sind.

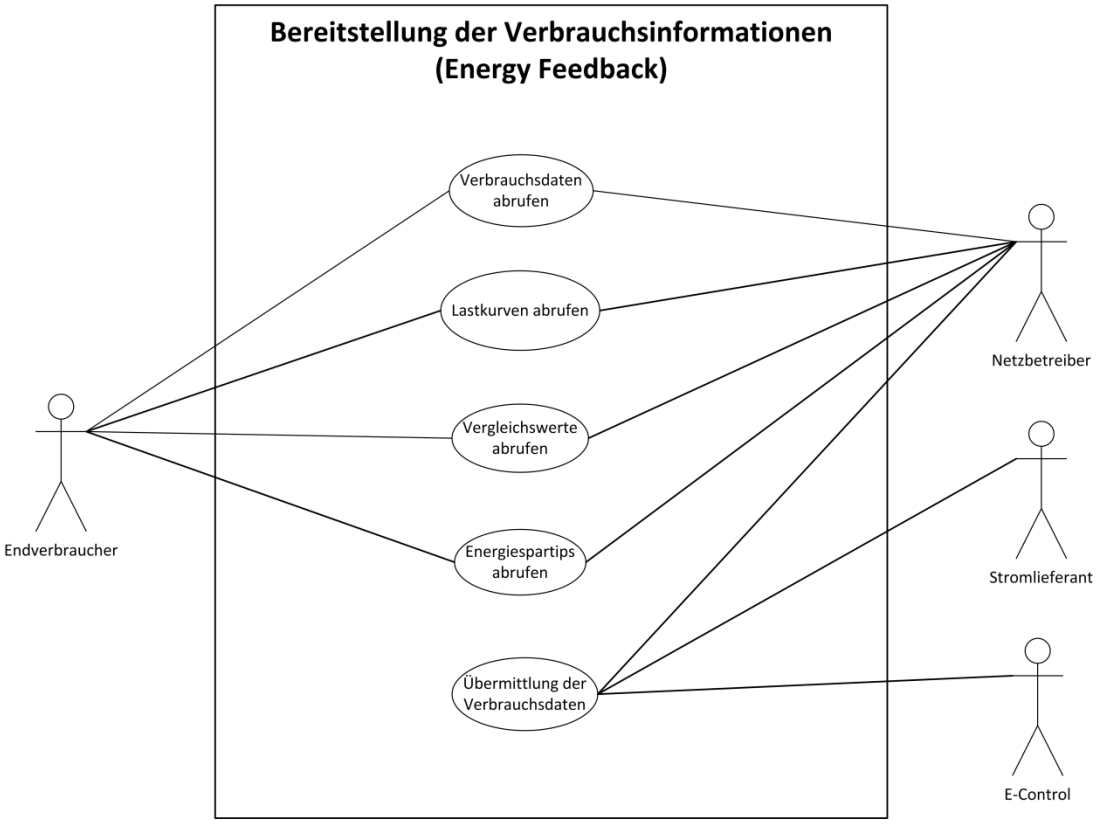

Abb. 1 System-Use-Case-Diagramm zur Beschreibung der User-Stories innerhalb des Systems Energy Feedback.

3 Grundbestandteile einer SOA für Smart Grids

In einer Systemlandschaft müssen sowohl Legacysysteme als auch moderne Systeme betrieben und unterstützt werden. Häufig werden einzelne Komponenten von unterschiedlichen Eigentümern, z.B. Teams, Abteilungen, Geschäftseinheiten oder Tochterunternehmen, auf unterschiedlichen Plattformen, Programmiersprachen und Programmierparadigmen implementiert. Hier besteht die Möglichkeit, dass jeder Eigentümer unterschiedliche Budgets, Zeitpläne, Ansichten oder Prioritäten hat. Diese Systeme haben in der Regel eine sehr lange Lebensdauer, da eine Abschaltung von existierenden Systemen meist mit hohen Kosten verbunden ist. Daher werden Komponenten oft nur bei schwerwiegenden

Fehlern ersetzt. Die auf diese Weise historisch gewachsenen Systeme führen zu einer heterogene Systemlandschaften in Unternehmen. Grundvoraussetzungen für Systeme im Unternehmenskontext sind die Skalierbarkeit und Flexibilität, weil sie wachsen und sich verändern.
Serviceorientierte Architekturen (SOA) ist ein Konzept um große verteilte Systeme warten und pflegen zu können. In dieser Arbeit wurde eine SOA-basierende IKT-Architektur für Smart Grids entwickelt.
Eine SOA besteht in der Regel aus drei Hauptakteuren:

- Dienstanbieter
- Dienstnutzer
- Dienstverzeichnis

Dienst
Ein Dienst fungiert als Zusammenschluss von Softwarekomponenten, welche von Teilnehmern verwendet werden kann. Um einen bestimmten Dienst nützen zu können, muss dieser über eine öffentlich beschriebene Schnittstelle verfügen. Die Teilnehmer können den Dienst nur über dessen Schnittstelle abfragen. Die Implementierungsdetails bleiben für die Servicekonsumenten verborgen.

Dienstbeschreibung
Jeder Dienst, der in einer SOA von anderen Benutzern verwendet werden kann, benötigt eine öffentlich beschriebene Schnittstelle. Diese Schnittstelle muss unabhängig von der Programmiersprache, der Plattform und der Implementierung sein. Eine solche Beschreibung ist beispielsweise die Interface Description Language (IDL) oder die Web Service Description Language (WSDL).

Dienstanbieter
Damit ein Dienstanbieter seine Service für andere Teilnehmer bereitstellen kann, muss er diese in einem Dienstverzeichnis registrieren. Diese Bereitstellung beinhaltet neben der Entwicklung des Dienstes dessen Betrieb und Wartung. Der Dienstanbieter ist somit für die Verfügbarkeit des Dienstes zuständig. Außerdem muss er sich um die Sicherheit der Plattform kümmern. Dies beinhaltet beispielsweise die Authentifizierung: Diese prüft die Identität möglicher Servicekonsumenten, oder die Autorisierung, welche die Berechtigung für den Aufruf des Dienstes sicherstellt.

Dienstverzeichnis
Wie erwähnt muss ein Dienstanbieter seine Dienste in einem Dienstverzeichnis registrieren. Die Teilnehmer können die angebotenen Dienste im Dienstverzeichnis durchsuchen. Für ein besseres Suchergebnis sollten die Dienste kategorisiert werden. Die stringente Zuordnung der angebotenen Dienste zu Kategorien zeichnet eine gute Klassifizierung aus.

Dienstnutzer
Der Dienstnutzer konsumiert angebotene Dienste von einem Dienstanbieter. Hierbei besteht die Möglichkeit, dass er im Dienstverzeichnis nach Diensten sucht und diese verwendet. Im Falle, dass der Nutzer den Anbieter kennt, ist eine Kommunikation ohne Dienstverzeichnis möglich. Dies kann Ressourcen schonen, da das Dienstverzeichnis in so einem Szenario nicht verwendet wird. Der Vorteil, dass das Dienstverzeichnis Änderungen des Dienstes verbreitet, geht dadurch verloren.

Interaktion
Damit ein Benutzer die Dienste eines Anbieters nutzen kann, muss der Anbieter diese zuvor veröffentlicht haben. Die Veröffentlichung beinhaltet die Installation des Dienstes auf einer Plattform und dessen Registrierung in einem Dienstverzeichnis. Danach kann der Nutzer den Dienst im Verzeichnis suchen und die Schnittstellenbeschreibung abfragen. Ein Austausch der Richtlinien für die

Nutzung des Dienstes, wie zum Beispiel eine benötigte Authentifizierung, findet daraufhin statt. Bei einem erfolgreichen Übereinkommen kann der Nutzer den Service abfragen [Melzer 2010].

4 SOA-Konzeption für Smart Grids

Auf Basis der eruierten Herausforderungen von Kapitel 2 „User-Stories“ wurde eine IKT-Architektur für Smart Grids entwickelt. Abb.2 zeigt das Ergebnis dieser Entwicklung.

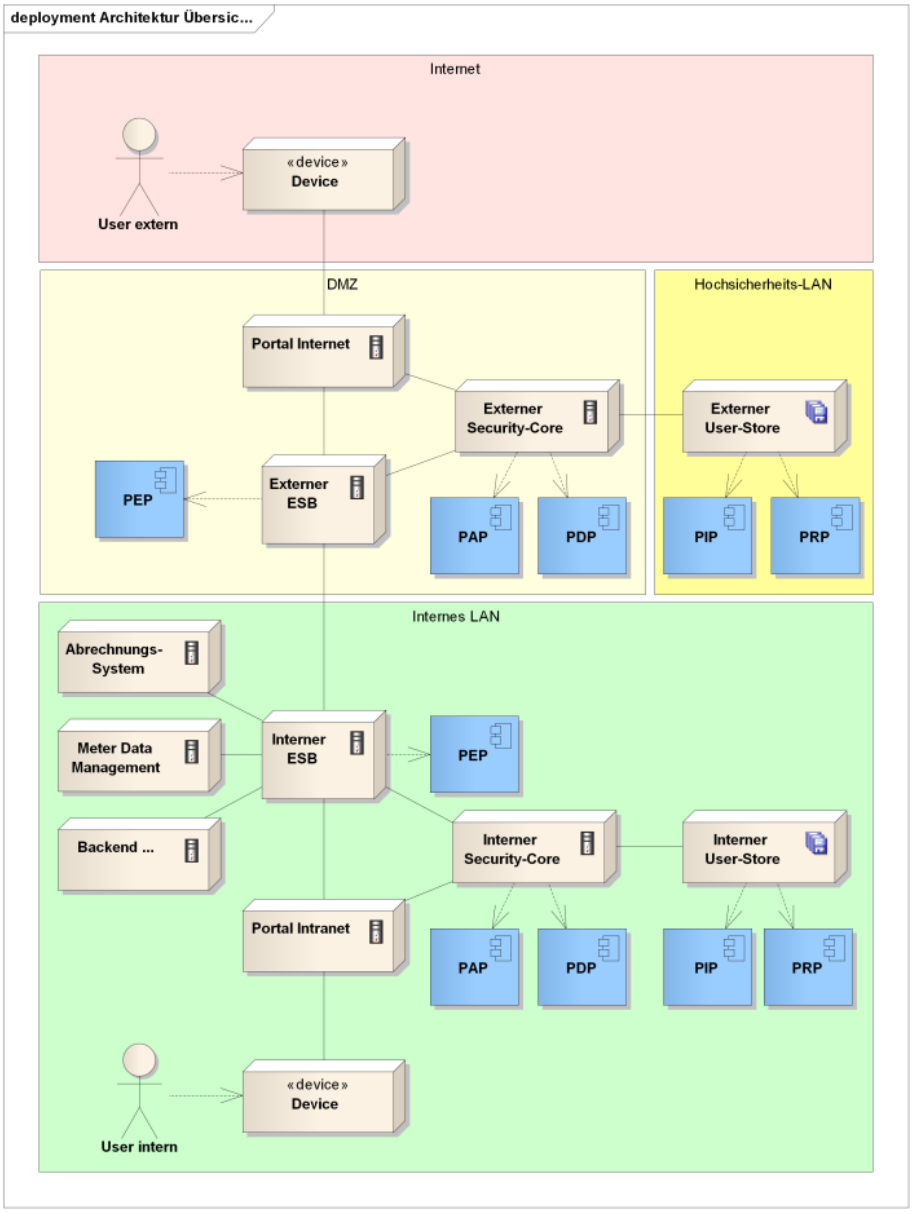

Abb. 2 Architekturübersicht

Systemkomponenten

Die in Abb. 2 dargestellte Architektur wurde nach dem PEP Framework entworfen. Für die Implementierung dieses Frameworks in die Architektur sind folgende Kernkomponenten essentiell.

Policy Enforcement Point (PEP): Der PEP fungiert als Softwareproxy, der je nach Laufzeitumgebung unterschiedlich ausgeprägt werden kann. Er sendet Autorisierungsanfragen an den PDP, ob ein Service aufgerufen werden darf. Im Anwendungsfall Energie Feedback wird beispielsweise der Request für das Beziehen der 15 Minuten Vortageswerte an den PDP und nicht an das Back-End mit den benötigten Daten umgeleitet. Ein bereits erfolgreich durchgeführter Authentifizierungsprozess wird hierbei vorausgesetzt.

Policy Decision Point (PDP): Auf die Autorisierungsanfragen des PEP antwortet der PDP mit einer Zugriffsentscheidung. Die Autorisierungsentscheidung erfolgt anhand von Sicherheitsrichtlinien. Der PDP kann die Sicherheitsrichtlinien beim PRP und PIP mittels eines eXtensible Access Control Markup Language (XACML) Request abfragen. Die Autorisierungs-Policy kann einen Zugriff erlauben oder verweigern. Der PDP ermöglicht zum Beispiel, dass einem Unternehmen nur der Zugriff auf Verbrauchsdaten der Sparte Strom und einer weiteren Institution der Zugriff auf sämtliche Verbrauchsdaten gestattet wird.

Policy Retrieval Point (PRP): Der PRP dient als Repository in dem die Sicherheitsregeln gespeichert werden. In der derzeitigen Implementierung handelt es sich hierbei um eine relationale Datenbank.

Policy Information Point (PIP): Informationen zu den Attributen können beim PIP abgefragt werden. Die Attribute können sich auf den gesamten Entscheidungskontext beziehen. Die Attributs-Informationen können folgende Aspekte umfassen:

- ein Subjekt, zum Beispiel das Alter oder eine Rolle (Nutzerattribute)
- die Umgebung, zum Beispiel der verwendete Webbrowser (Umgebungsattribute)
- die Ressource, zum Beispiel „beinhaltet Messdaten“ (Ressourcenattribute).

Mit diesen zusätzlichen Informationen können Attribut-basierende Abfragen erstellt werden, z.B. nur Nutzer mit einem speziellen Tarif dürfen den Service abfragen, der die Verbrauchsdaten im Minuten-Raster liefert.

Policy Administration Point (PAP): Die Verwaltung der Policies erfolgt über den PAP [Blasch et al. 2012].

Systeme

Folgend werden die Funktionen der Systeme aus Abb. 2 beschrieben.

Portal Internet / Intranet: Bei den Portalen handelt es sich um Webserver. Diese Webserver dienen für User als Einstiegspunkte über browserfähige Endgeräte. Beim Aufruf des Portals wird im ersten Schritt eine gecachte Webseite angezeigt. Dort hat der Anwender die Möglichkeit sich zu authentifizieren. Die Authentifizierung kann beispielsweise über Username und Passwort erfolgen.

Security-Core: Nachdem sich der Anwender mit seinen Anmeldeinformationen im Portal angemeldet hat, wird diese Authentifizierungsanfrage an den Security-Core weitergeleitet. Der Security-Core hat die Aufgabe, die Anmeldeinformationen zu überprüfen und den User zu authentifizieren. Des Weiteren trifft der Security-Core die Zugriffsentscheidungen und fungiert somit als PDP. Die PAP Komponenten des Security-Cores dienen der zentralen Verwaltung von Policies.

User-Store: Sämtliche sicherheitsrelevante Userdaten, die Policies und die Attributsinformationen sind im User-Store gespeichert. Der User-Store fungiert ausschließlich als Datenspeicher. Die Verwaltung dieser Daten passiert über den PAP des Security-Cores. Über den PDP können die im User-Store gespeicherten Authentifizierungs- und Autorisierungs- Informationen abgefragt werden.

ESB: Der Enterprise Service Bus ermöglicht die Vermittlung von Anfrage- und Antwortnachrichten. Alle Ressourcen-Anfragen passieren über den ESB, der somit als Reverse Proxy fungiert. Über den ESB werden Daten aus dem Backend Systemen bezogen und als Service zur Verfügung gestellt. Vor jedem zur Verfügung gestellten Service ist ein PEP. Bevor ein Anwender einen Service abfragen darf, wird eine Autorisierungsanfrage vom PEP an den PDP gesendet. Erst wenn der PDP die Erlaubnis erteilt, kann ein Anwender einen Service nutzen.

Netzsegmente

Die in Abb. 2 dargestellte Zielarchitektur für Smart Grids Anwendungen teilt sich in mindestens vier unterschiedlichen Netzsegmente auf. Diese werden folgend beschrieben.

Internet: Das Internet ist der öffentliche Bereich, wo ein User mit einem browserfähigen Endgerät Webseiten aufrufen kann. In diesem Netzsegment lässt sich die Sicherheitsstufe nicht beeinflussen.

DMZ: In der demilitarisierten Zone (DMZ) befinden sich der Portalserver, der externe ESB und der externe Security-Core. Der Portalserver fungiert als Einstiegspunkt für externe User. Der externe ESB ermöglicht einen Nachrichtenaustausch innerhalb der DMZ und übermittelt die Ressourcen-Anfragen für interne Backend Systeme an den internen ESB. Der externe Security-Core übernimmt die Berechtigungsverwaltung für externe User.

Hochsicherheits-LAN: Da in der DMZ schwächere Sicherheitsbestimmungen gelten, die Daten vom externen User-Store jedoch sehr sensibel sind, gibt es ein stark abgesichertes Netzsegment, welches in der Architektur als Hochsicherheits-LAN bezeichnet wird. Ausschließlich dem externen Security-Core ist ein Zugriff auf dieses Netzsegment gewährt, welcher somit auf den externen User-Store zugreifen darf.

Internes LAN: Das interne LAN repräsentiert ein unternehmensinternes Netzwerk. In diesem Netzwerksegment befinden sich sämtliche Backend Systeme, der interne ESB, ein Portalserver für das Intranet, ein interner Security-Core und ein interner User-Store.
Sowohl der Security-Core als auch der User-Store wurden aus Sicherheitsgründen doppelt ausgeführt. Dadurch existiert eine physikalische Trennung von Mitarbeiterdaten und beliebig externen Userdaten.

Authentifizierung

Das Sequenzdiagramm in Abb. 3 zeigt eine exemplarische Authentifizierung eines User gegenüber einem Portalserver.
Im ersten Schritt gibt der Anwender seine Authentifizierungsinformationen im Portal Login Fenster ein. Aus diesen Anmeldedaten generiert der Portalserver eine Security Assertion Markup Language (SAML) konforme Anfragenachricht. SAML ist ein XML-basierter Standard zum Austausch von Authentifizierungsinformationen im Single-Sign-On (SSO) Kontext. Mit dieser Nachricht stellt der Portalserver eine Authentifizierungsanfrage an den Security-Core. Der Security-Core bezieht die für die Authentifizierungsüberprüfung relevanten Daten aus dem User-Store. Mit den bezogenen Daten kann der Security-Core die Authentifizierung des Anwenders kontrollieren. Nachdem der Security-Core die Überprüfung durchgeführt hat, erstellt das System eine SAML Assertion und übermittelt diese dem Portalserver. Diese Security Assertion beinhaltet die Information, dass der User erfolgreich

authentifiziert wurde. Mit dem ausgestellten SAML Token ist dem Anwender auf allen Systemen ein Zugriff gewährt, für welche er die dementsprechenden Berechtigungen besitzt.

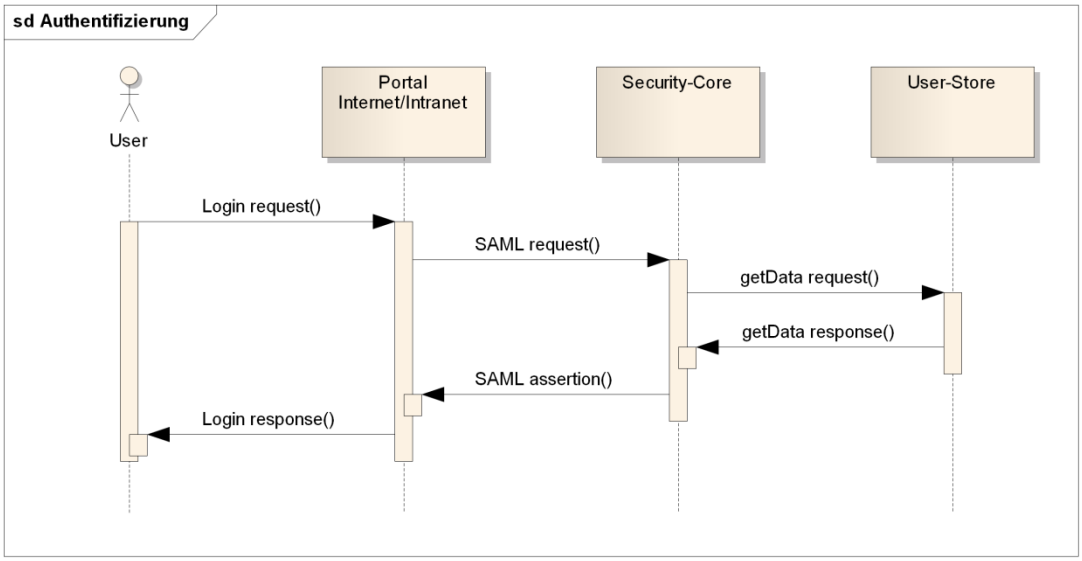

Abb. 3 Sequenzdiagramm: Authentifizierung

Autorisierung

Nachdem der User erfolgreich authentifiziert wurde, kann er weitere Interaktionen im Portal durchführen. Ein Beispiel hierfür ist der Aufruf der Energiefeedback Webseite. Sobald der Anwender versucht die Webseite aufzurufen, wird ein Service Request an den ESB gesendet. Jeder Service hat einen zugehörigen PEP, der eine Autorisierungsanfrage im XACML Format an den PDP stellt. Der Security-Core beinhaltet die PDP Komponente und bezieht die autorisierungsrelevanten Daten aus dem User-Store. Mithilfe dieser Daten kann der Security-Core prüfen, ob der Anwender für den Serviceaufruf berechtigt ist. Sofern der User für den Serviceaufruf berechtigt ist, erfolgt ein Request vom ESB zum Serviceprovider. Die Antwortnachricht vom Provider gelangt über den ESB zum User. Das Sequenzdiagramm in Abbildung 4 visualisiert diesen Autorisierungsablauf.

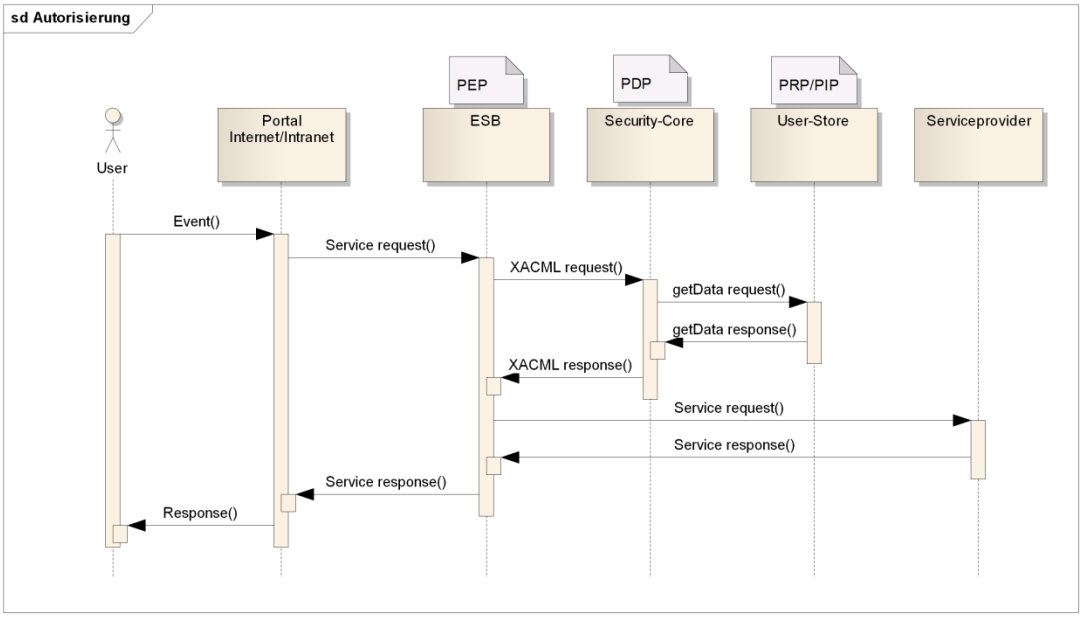

Abb. 4 Sequenzdiagramm: Autorisierung

5 Durchdachte Architekturen bewähren sich in der Praxis

Eine wohlüberlegte Konzeption der im Smart Grids zum Einsatz kommenden IKT-Architekturen ist auf mehreren Ebenen hilfreich. Die einheitliche und systematische Integration aller Datenquellen und –senken hebt Modularität und Austauschbarkeit. Die Erfüllung orthogonaler Kriterien wie Datenschutz und Datensicherheit kann bereits in der Konzeption, also in Erfüllung der Anforderungen „privacy by design“, bzw. „security by design“ [Cavoukian 2012], erfolgen. Die hier beschriebene, serviceorientierte, Architektur, die sich bewährter Design Patterns bedient, wurde erfolgreich als Prototyp umgesetzt und erfüllt aktuell alle Anforderungen der Salzburg AG in den beschriebenen Anwendungsfällen. Für die Smart Grids Modellregion Salzburg wurden erste prototypische Applikationen entwickelt, die bereits Daten über die IKT-Architektur abfragen. Die Applikationen visualisieren zum Beispiel Energieverbräuche, basierend auf Smart Meter Daten aus Back-End Systemen der Salzburg AG. Dem Anwender wird die Möglichkeit geboten, dass er nach einmaliger Anmeldung sämtliche Applikationen der Salzburg AG nutzen kann, für welche er die dementsprechenden Berechtigungen besitzt (Single-Sign-On). Durch den modularen Aufbau ist die Erweiterung auf andere Anwendungsfälle rasch und stringent möglich. Der umfassende Einsatz für den Großteil aller benutzerorientierten Anwendungsfälle eines EVU ist mit Ende 2015 geplant.

6 Literatur

[Appelrath et al. 2012] Appelrath, H.-J.; Kagermann, H. & Mayer, C. Future Energy Grid – Migrationspfade ins Internet der Energie. *Springer,* **2012**

[Blasch et al. 2012] Blasch, E.; Bossé, É. & Lambert, D. High-Level Information Fusion Management and System Design (Artech House Intelligence and Information Operations). *Artech House,* **2012**

[Cavoukian et al. 2010] Cavoukian, A.; Polonetsky, J. & Wolf, C. SmartPrivacy for the Smart Grid: embedding privacy into the design of electricity conservation. *Identity in the Information Society, Springer Netherlands,* **2010***, 3*, 275-294

[DKE 2012] DKE. Deutsche Normungsroadmap E-Energy / Smart Grids 2.0. *VDE VERBAND DER ELEKTROTECHNIK ELEKTRONIK INFORMATIONSTECHNIK e.V., Frankfurt am Main,* **2012**

[Jung et al. 2012] Jung, M.; Hofer, T.; Döbelt, S.; Kienesberger, G.; Judex, F. & Kastner, W. Access control for a Smart Grid SOA. *International Conferece For Internet Technology And Secured Transactions, 2012,* **2012**, 281-287

[Kim et al. 2010] Kim, Y.-J.; Thottan, M.; Kolesnikov, V. & Lee, W. A secure decentralized data-centric information infrastructure for smart grid. *Communications Magazine, IEEE,* **2010***, 48*, 58-65

[Melzer 2012] Melzer, I. Service-orientierte Architekturen mit Web Services: Konzepte - Standards - Praxis (German Edition). *Spektrum Akademischer Verlag,* **2010**

[Sood 2009] Sood, V.; Fischer, D.; Eklund, J. & Brown, T. Developing a communication infrastructure for the Smart Grid. *Electrical Power Energy Conference (EPEC), 2009 IEEE,* **2009**, 1 -7

[Wicker & Thomas 2011] Wicker, S. B. & Thomas, R. A Privacy-Aware Architecture for Demand Response Systems. *Proceedings of the 44th Hawaiian Conference on System Science (HICSS-44), Kauai, Hawaii,* **2011**