VDEW

MATERIALIEN

M-17/2003

Aktionsplan WETTBEWERB

Umgang mit Schlüsselmaterial

V D E W

Verband der
Elektrizitätswirtschaft e.V.

Umgang mit Schlüsselmaterial

September 2003

Beate Becker, Telefon: 069/6304-302, Mail: beate_becker@vdew.net

Ergänzend zu den Gesetzen und Rechtsvorschriften für den Einsatz der elektronischen Signatur und der Verschlüsselung haben die Verbände eine gemeinsame Erklärung zu „Sicherheitsrahmenbedingungen für den elektronischen Geschäftsverkehr im deutschen Strommarkt" abgegeben. Diese stellt die Basis für die Bildung einer Vertrauensinfrastruktur der Marktteilnehmer beim elektronischen Datenaustausch dar und zeigt Maßnahmen zur Sicherheit auf. Dadurch wird das Sicherheitsniveau auf der technischen und organisatorischen Ebene nachhaltig gehoben.

Die weitere organisatorische und technische Ausgestaltung wird durch Dokumente, zu denen auch der „Umgang mit Schlüsselmaterial“ gehört, vorgenommen. Erst organisatorische und technische Mindestanforderungen an den Umgang mit Schlüsselmaterial garantieren, dass alle Marktteilnehmer sich auf die eingesetzten Methoden verlassen können, unabhängig davon ob das Schlüsselmaterial im Rahmen einer firmeneigenen PKI zertifiziert wurde (MAKE) oder durch Zertifizierungsdienstleister bereit gestellt wurde (BUY).

Das vorliegende Dokument beschreibt diese Mindestanforderungen aus Nutzersicht. Es stellt die Regeln zum sorgfältigen Umgang mit krytographischem Schlüsselmaterial auf, die im Rahmen des elektronischen Geschäftsverkehrs eingesetzt werden. Eine Verletzung dieser Regeln würde die Vertrauensinfrastruktur zwischen den Marktteilnehmern schwächen oder letztlich in Frage stellen. Unsachgemäßer Umgang mit Schlüsselmaterial ist ungleich schwerwiegender als etwa leichtfertiger Umgang mit Passwörtern, weil an kryptographisches Schlüsselmaterial höhere Sicherheitserwartungen geknüpft sind und den damit verbundenen geschäftliche Transaktionen in der geldwerten Höhe und im Automatisierungsgrad mehr vertraut wird.

Das gesamte Regelwerk wird als PKI-Policy bezeichnet. Das vorliegende Kerndokument gilt sowohl für ein MAKE- als auch für ein BUY-Vorgehen.

Der VDEW empfiehlt seinen Mitgliedsunternehmen beim Einsatz von elektronischer Signatur und Verschlüsselung beim elektronischen Datenaustausch einen Rahmenvertrag mit den Marktpartnern zu schließen, in dem die Berücksichtigung der gemeinsamen Erklärung sowie der Folgedokumente vertraglich verankert wird.

Management Summary

Umgang mit Schlüsselmaterial

Der elektronische Geschäftsverkehr der Mitgliedsunternehmen in der deutschen Elektrizitätswirtschaft per Electronic Data Interchange oder anderer Verfahren soll sicherer und verbindlicher werden. Dazu wird empfohlen, im Rahmen einer firmenübergreifenden Vertrauensinfrastruktur zertifiziertes kryptographisches Schlüsselmaterial im Rahmen von Public-Key-Infrastruktur einzusetzen.

Mit dem Begriff "Vertrauensinfrastruktur" soll hier die Summe an technischen und organisatorischen Maßnahmen bezeichnet werden, die zwischen den Marktteilnehmern sichere und verbindliche Kommunikation und damit verlässlichen Geschäftsverkehr ermöglicht. Den politischen Rahmen setzt dabei die gemeinsame Erklärung der Verbände. Die weitere organisatorische und technische Ausgestaltung wird durch Dokumente, zu denen auch der „Umgang mit Schlüsselmaterial“ gehört, vorgenommen.

Erst organisatorische und technische Mindestanforderungen an den Umgang mit Schlüsselmaterial garantieren, dass alle Marktteilnehmer sich auf die eingesetzten Methoden verlassen können, unabhängig davon ob das Schlüsselmaterial im Rahmen einer firmeneigenen PKI zertifiziert wurde (MAKE) oder durch Zertifizierungsdienstleister bereit gestellt wurde (BUY).

Das vorliegende Dokument beschreibt diese Mindestanforderungen aus Nutzersicht. Das Dokument beschreibt die Regeln zum sorgfältigen Umgang mit krytographischem Schlüsselmaterial, die im Rahmen des elektronischen Geschäftsverkehrs eingesetzt werden. Eine Verletzung dieser Regeln würde die Vertrauensinfrastruktur zwischen den Marktteilnehmern schwächen oder letztlich in Frage stellen. Unsachgemäßer Umgang mit Schlüsselmaterial ist ungleich schwerwiegender als etwa leichtfertiger Umgang mit Passwörtern, weil an kryptographisches Schlüsselmaterial höhere Sicherheitserwartungen geknüpft sind und den damit verbundenen geschäftliche Transaktionen in der geldwerten Höhe und im Automatisierungsgrad mehr vertraut wird.

Das gesamte Regelwerk wird als PKI-Policy bezeichnet. Das vorliegende Kerndokument gilt sowohl für ein MAKE- als auch für ein BUY-Vorgehen.

- Umgang mit Schlüsselmaterial bedeutet dabei, wie ein Marktteilnehmer (juristische Person) und wie ein Anwender (natürliche Person) das Personal Security Environment (PSE) und damit den privaten Schlüssel behandelt
- und wie ein Anwender Zertifikate, also Beglaubigungen der öffentlichen Schlüssel und damit öffentliche Schlüssel behandelt.
- Thematisierung von Zuständigkeiten und Risiken
- ein Minimum an gemeinsamen Begrifflichkeiten, welches dem gemeinsamen Verständnis dienen soll. Dies setzt aber kein technisches Verständnis bei den Anwendern voraus.

Nicht Inhalt des Kerndokuments ist
- die Erzeugung und Verteilung von Schlüsselmaterial im Rahmen der gemeinsamen Vertrauensinfrastruktur (PKI)
- die Definition und Realisierung von Vorgängen oder Prozessen, in denen Schlüsselmaterial eingesetzt wird.

Dies wird in den weiteren Policy-Dokumenten PKI-Policy und Certification Practice Statement, die sich an einem MAKE-Vorgehen orientieren, behandelt.

Weitere organisatorische Aspekte, wie Vertretungsregelungen bei verschlüsselten Dokumenten, werden ebenfalls in der Ausarbeitung PKI-Policy angesprochen, aber als firmeninterne Maßnahme nicht näher behandelt.

Umgang mit Schlüsselmaterial

Sicherheit beim elektronischen Geschäfts-verkehr in der deutschen Elektrizitätswirtschaft

Empfehlungen für die Marktteilnehmer

Stand: 1. September 2003

Version: 1.0

INHALT

1 Allgemeine Bemerkungen

Die VDEW-Projektgruppe „Sicherheit beim elektronischen Datenaustausch“ hat zur Gewährleistung einer sicheren Kommunikation zwischen den Marktteilnehmern in der deutschen Elektrizitätswirtschaft die gemeinsame Erklärung zu "Sicherheitsrahmenbedingungen für den elektronischen Geschäftsverkehr im deutschen Strommarkt“ zwischen den beteiligten Verbänden angeregt. Die Erklärung wird von folgenden Verbänden getragen:

Bundesverband der Deutschen Industrie e. V. - BDI, Berlin
VIK Verband der Industriellen Energie- und Kraftwirtschaft e. V., Essen
Verband der Elektrizitätswirtschaft - VDEW - e.V., Berlin
Verband der Netzbetreiber – VDN – e.V. beim VDEW, Berlin
Verband der Verbundunternehmen und Regionalen Energieversorger in Deutschland – VRE - e. V., Berlin
Verband kommunaler Unternehmen – VKU – e.V., Köln

Diese Erklärung bildet die gemeinsame Basis, damit die Sicherheitsbelange im Geschäftsverkehr in der Branche angemessen berücksichtigt werden.

Die gemeinsame Erklärung auf der verbandspolitischen Ebene wird durch entsprechende Dokumente im organisatorischen und technischen Umfeld ergänzt und ausgestaltet werden.

Diese Dokumente werden vom VDEW erarbeitet und veröffentlicht.

Allgemein definiert haben die organisatorischen Teile den Anspruch, ein einheitliches organisatorisches Sicherheitsniveau bei der Verschlüsselung und Signatur von unternehmensübergreifenden Transaktionen zwischen den Marktteilnehmern zu gewährleisten.

Ebenso allgemein definiert sollen die technischen Teile der Dokumente auch beim Einsatz unterschiedlicher Produkte oder Dienstleistungen die Interoperabilität auf der technischen Ebene sicherstellen.

Die politischen, organisatorischen und technischen Aussagen in der gemeinsamen Erklärung und seinen Folgedokumenten haben Empfehlungscharakter und sollen in der Solidargemeinschaft der Marktteilnehmer eine verlässliche Vertrauensinfrastruktur ermöglichen.

Die Maßnahmen sollen als Leitlinie bei der Umsetzung im eigenen Unternehmen und der nachfolgenden Anwendung an den Marktschnittstellen dienen. Allerdings sollen gegenüber den Verbandsempfehlungen geänderte Vorgehensweisen begründbar sein und das allgemeine Sicherheitsniveau nicht beeinträchtigen.

Die Marktteilnehmer sollten aus wirtschaftlichen Gründen daran interessiert sein, dass die Vertrauensinfrastruktur nicht ausgehöhlt wird. Nur dadurch ist die sichere elektronische Abwicklung der Geschäfte mittelfristig gewährleistet und kann so ausgebaut werden, dass auch weitere Automatisierungsschritte beherrschbar bleiben.

2 Die Vertrauensinfrastruktur der deutschen Stromwirtschaft

2.1 Ziele

Der elektronische Geschäftsverkehr der Mitgliedsunternehmen in der deutschen Elektrizitätswirtschaft per Electronic Data Interchange oder anderer Verfahren soll sicherer und verbindlicher werden. Dazu wird im Rahmen einer firmenübergreifenden Vertrauensinfrastruktur zertifiziertes kryptographisches Schlüsselmaterial im Rahmen von Public-Key-Infrastruktur eingesetzt.

Mit dem Begriff "Vertrauensinfrastruktur" soll hier die Summe an technischen und organisatorischen Maßnahmen bezeichnet werden, die zwischen den Marktteilnehmern sichere und verbindliche Kommunikation und damit verlässlichen Geschäftsverkehr ermöglicht.

Den Rahmen setzt dabei die oben genannte gemeinsame Erklärung der Verbände.[1]

Erst organisatorische und technische Mindestanforderungen an den Umgang mit Schlüsselmaterial garantieren aber, dass alle Marktteilnehmer sich auf die eingesetzten Methoden verlassen können, unabhängig davon ob das Schlüsselmaterial im Rahmen einer firmeneigenen PKI zertifiziert wurde (MAKE) oder durch Zertifizierungsdienstleister bereit gestellt wurde (BUY).

Das vorliegende Dokument beschreibt diese Mindestanforderungen.

Das Dokument beschreibt die Regeln zum sorgfältigen Umgang mit kryptographischem Schlüsselmaterial, das im Rahmen des elektronischen Geschäftsverkehrs eingesetzt wird. Eine Verletzung dieser Regeln würde die Vertrauensinfrastruktur zwischen den Marktteilnehmern in Frage stellen.

Das gesamte Regelwerk wird als PKI-Policy bezeichnet. Das vorliegende Kerndokument gilt sowohl für ein MAKE- als auch für ein BUY-Vorgehen.

Umgang mit Schlüsselmaterial bedeutet dabei die Art und Weise, wie

- ein Marktteilnehmer (juristische Person) und wie ein Anwender (natürliche Person) das Personal Security Environment (PSE) und damit den privaten Schlüssel behandelt
- ein Anwender Zertifikate, also Beglaubigungen der öffentlichen Schlüssel und damit öffentliche Schlüssel, behandelt.

Nicht Inhalt des Kerndokuments ist

- die Erzeugung und Verteilung von Schlüsselmaterial im Rahmen der gemeinsamen Vertrauensinfrastruktur (PKI)
- die Definition und Realisierung von Vorgängen oder Prozessen, in denen Schlüsselmaterial eingesetzt wird.

In Punkt (3) der „Weiterführenden Informationen“ sind ausführliche organisatorische Anforderungen an ein MAKE-Vorgehen dokumentiert. Diese sind für Marktteilnehmer, die Schlüsselmaterial von externen Zertifizierungsdienstleistern („Trustcenter“) beziehen, nicht relevant.

---

1 Gemeinsame Erklärung zu Sicherheitsrahmenbedingungen für elektronischen Geschäftsverkehr im deutschen Strommarkt Siehe unter Weiterführende Informationen

2.2 Verantwortlichkeiten

Jede Person bei dem Marktteilnehmer, der an der firmenübergreifenden Vertrauensinfrastruktur teilnimmt, trägt Verantwortung für den regelgerechten Umgang mit Schlüsselmaterial während des gesamten Lebenszyklus dieses Schlüsselmaterials.

Der Besitzer von Schlüsselmaterial ist verantwortlich, dass dieses gemäß dieser Policy eingesetzt, geschützt und behandelt wird.

Das Unternehmen ist verantwortlich, dass dies angeordnet, überprüft und ggf. Missbrauch so bestraft wird, wie es die Unterschriftsrichtlinien für handschriftliche Unterschriften revisionssicher vorsehen. Korrumpiertes oder auch nur möglicherweise unsicheres Schlüsselmaterial muss unverzüglich gesperrt werden.

2.3 Risiken

Bei Nichtbeachtung der vorliegenden Regeln können folgende Schäden entstehen

- Vertraulichkeitsverlust: Bei Offenlegung des privaten Verschlüsselungsschlüssels, z. B. durch Zugriff auf das Personal Security Environment (PSE), können Daten durch Unbefugte gelesen und verwertet werden.
- Verlust an Originalität: Bei Offenlegung des privaten Schlüssels, z. B. durch Zugriff auf das Personal Security Environment, können Daten, die nicht verändert werden dürfen (z. B. Fahrpläne) und deshalb signiert wurden, durch Unbefugte unbemerkt verändert werden.
- Verfügbarkeitsverlust: Bei Verlust des Personal Security Environment und damit der privaten Schlüssel gehen Daten, die verschlüsselt gespeichert und als unverschlüsseltes Original gelöscht wurden, unwiederbringlich verloren, da die Stärke der Verschlüsselung jeden Entschlüsselungsversuch verhindert, wenn der private Schlüssel nicht mehr verfügbar ist.
- Verlust der Verbindlichkeit: Durch Offenlegung oder Zweckentfremdung des privaten Schlüssels in der PSE kann die Gültigkeit einer Transaktion oder eines Geschäftsvorgangs in Frage gestellt werden. Dadurch steht der Ruf des Marktteilnehmers als verlässlicher Partner auf dem Spiel.

Je nach Tragweite der Verwendung geschützter Daten kann der Schaden die Tragweite von gering bis katastrophal annehmen. Der Schaden kann ein finanzieller Schaden und/oder ein Imageverlust oder ein existenzieller Schaden (z. B. Unternehmenswert einer Aktiengesellschaft) sein.

2.4 Geltungsbereich und Zielgruppen

Diese Ausarbeitung ist Teil des politischen, organisatorischen und technischen Regelwerks zur Gewährleistung der Informationssicherheit bei den Marktteilnehmern in der deutschen Elektrizitätswirtschaft und richtet sich an alle natürliche Personen/Anwender, die als Mitarbeiter oder im Auftrag der Verbandsmitglieder im Sinne der gemeinsamen Erklärung zu "Sicherheitsrahmenbedingungen für elektronischen Geschäftsverkehr im deutschen Strommarkt“ firmenübergreifende Transaktionen durchführen.

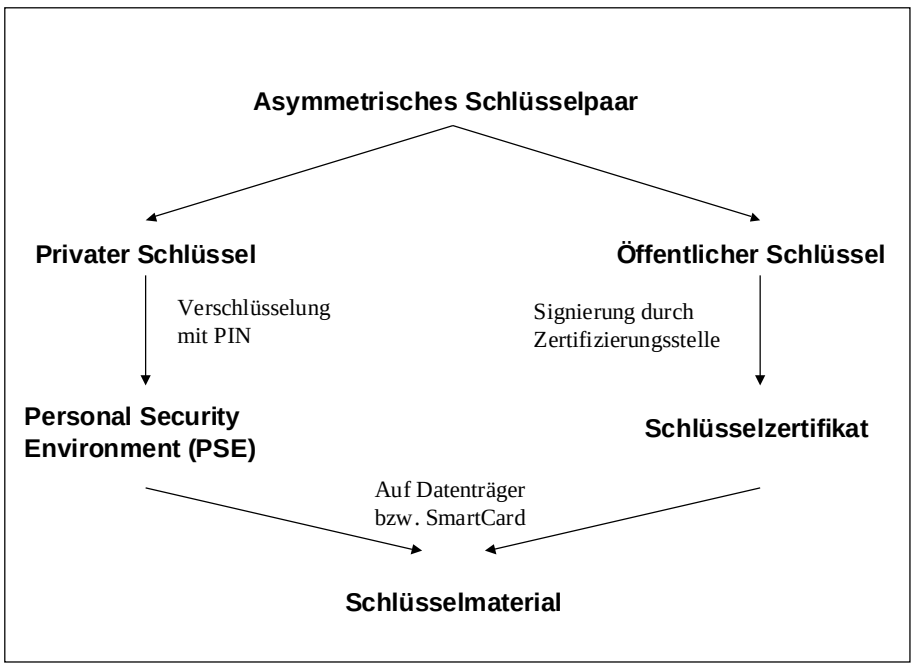
Anwender können sein:

1. Eigentümer eines persönlichen Schlüssels
2. Eigentümer eines Schlüssels ohne explizite Personenbindung (z. B. eines Gruppenverschlüsselungsschlüssels)
3. Besitzer eines Zertifikates

Für Anwender gemäß 1. – 2. gelten die Regeln bzgl. der Anwendung privater Schlüssel.
Für Anwender gemäß 3. gelten die Regeln bzgl. der Anwendung öffentlicher Schlüssel.
Führungskräfte haben informierende und kontrollierende Aufgaben.

2.5 Begriffe

Zur Leseerleichterung, zur verbindlichen Begriffsdefinition und zum Zusammenhang der Begriffe sind nachfolgende Diagramme und nachfolgendes, alphabetisch geordnetes Begriffsverzeichnis erstellt worden. Das Begriffsverzeichnis enthält die Begriffe, die für alle Verfahrensteilnehmer relevant sind. Die PKI-Policy (siehe weiterführende Literatur) (3) enthält darüber hinaus Begriffe, die besonders für MAKE-Teilnehmer relevant sind, also Marktteilnehmer, die sich eine eigene Public-Key-Infrastruktur, insbesondere mit einem eigenen Trustcenter, aufbauen möchten und das zertifizierte Schlüsselmaterial im Rahmen der marktweiten Vertrauensinfrastruktur einsetzen möchten.



Dieses Kerndokument der Policy enthält in ausführlicher und möglichst allgemein verständlicher Form die für alle notwendige Begriffswelt. Je nach Verbreitung wird die deutsche oder englische Bezeichnung gewählt.

Diagramm 1: Struktur des Schlüsselmaterials

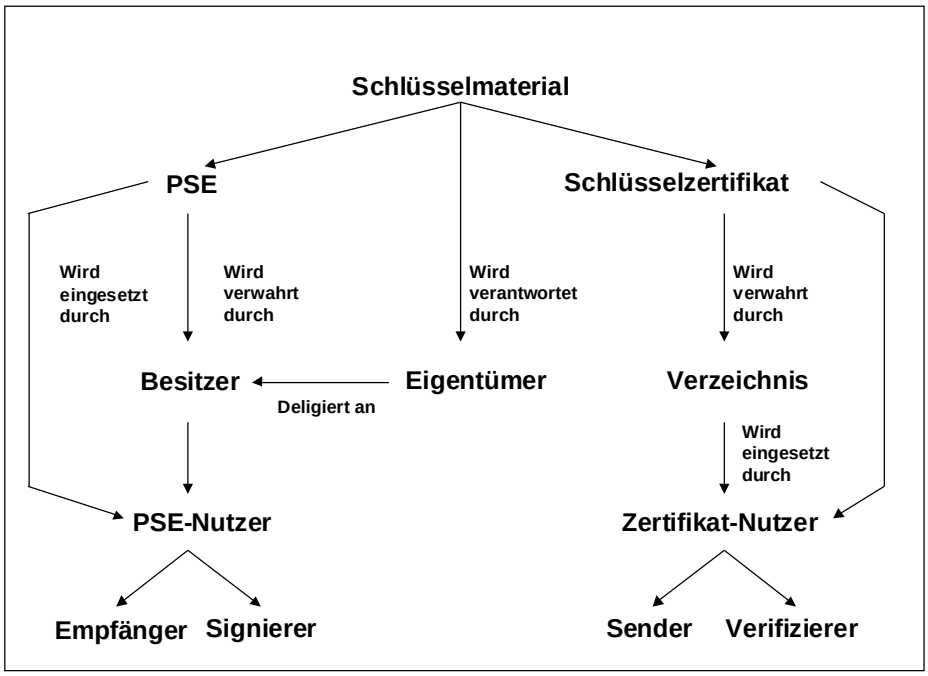


Diagramm 2: Verwendung des Schlüsselmaterials

Besitzer, Eigentümer und PSE-Nutzer sind bei persönlichem Schlüsselmaterial identisch [2]

[2] Die Unterscheidung ist lediglich für unpersönliche PSE relevant.

Mit „Eigentümer“ sollte nicht das Schlüsselmaterial ausgebende und verantwortende Unternehmen verwechselt werden (englisch issuer).

Dies kann ein externer Zertifizierungsdienstleister sein oder ein Marktteilnehmer, der selbst Schlüsselmaterial (zum firmenübergreifenden Einsatz) ausgibt.

3 Regelwerk zur Verwendung von Schlüsselmaterial in der Vertrauensinfrastruktur der deutschen Stromwirtschaft

3.1 Regeln für Schlüsseleigentümer

Antrag und Korrektheit der Zertifikatsdaten

- Der Antragsteller ist verpflichtet, die im Zertifikatsantrag verlangten Daten vollständig und korrekt anzugeben. Er hat alle Angaben zu unterlassen, die ihn in den ungerechtfertigten Besitz eines Zertifikats bringen.
- Der angebotene und beabsichtigte Verwendungszweck des beantragten Zertifikats müssen übereinstimmen (Beispiel: kein Authentisierungszertifikat beantragen, um es dann zur Signierung zu verwenden).

Schutz des privaten Schlüssels bzw. des Personal Security Environments (PSE)

- Bei der Übergabe des persönlichen Schlüsselmaterials (PSE auf Diskette oder SmartCard) muss sichergestellt werden, dass nur der richtige Empfänger (der ausgewiesene Eigentümer) das Schlüsselmaterial erhält. Dazu bekommt der richtige Empfänger den Datenträger mit dem PSE persönlich ausgehändigt.
- Der Schlüsseleigentümer muss darauf achten, dass der PIN-Brief, über den der Eigentümer die PIN für sein Personal Security Environment (PSE) erhält, niemals in andere Hände gelangt (z. B. PIN-Brief als E-Mail nach dem Ausdrucken löschen und Ausdruck sicher verwahren).
- Wenn die im PIN-Brief zugestellte PIN geändert werden kann, muss die Änderung schnellstmöglich erfolgen. Dabei sind die Regeln im Umgang mit Passwörtern zu beachten (siehe jeweilige Unternehmens-Policy „Passwörter“, nicht Gegenstand dieses Dokuments).

Weitergabe von Schlüsseln, Weitergabe eines Personal Security Environments (PSE)

Das Personal Security Environment (PSE) eines persönlichen privaten Schlüssels, d. h. mit Personenbindung, darf nicht verliehen oder weitergeben werden.

Bei der Übergabe des PSE für einen Schlüssel ohne Personenbindung muss:

- der neue Besitzer den Empfang mit seiner Unterschrift bestätigen,
- der Schlüsseleigentümer dem neuen Besitzer das PSE-Infoblatt aushändigen, das durchgelesen und eingehalten werden muss.

Wird ein Schlüssel ohne Personenbindung an den Eigentümer zurückgegeben, muss die PIN sofort geändert werden.

Verhalten bei Problemen mit dem Personal Security Environment (PSE)

Ein neues Exemplar des PSE mit Datenträger (SmartCard oder Diskette) muss beantragt werden, wenn

- die PIN vergessen worden ist oder
- die PIN nicht mehr rekonstruierbar ist oder
- das PSE unbrauchbar geworden ist (wenn z. B. bei einer SmartCard die PIN nicht mehr über die Administrator-PIN rücksetzbar ist).

Beendigung der Schlüsseleigentümerschaft

Der Eigentümer eines Schlüsselpaares muss unverzüglich den Widerruf des Zertifikats veranlassen, wenn

1. Kenntnis über eine Offenlegung des privaten Schlüssels besteht (Sicherheitsbruch), oder
2. der Datenträger, auf dem sich das PSE eines Schlüssels befindet, nicht nachvollziehbar verlorengegangen ist.

- Mit dem PSE eines widerrufenen Schlüssels darf keine digitale Signatur mehr erzeugt werden.
- Persönliche Schlüssel müssen vom Unternehmen widerrufen werden, wenn der Eigentümer das Unternehmen verlässt. Das zugehörige PSE muss unbrauchbar gemacht werden.

3.2 Regeln für Schlüsselbesitzer

Schutz des privaten Schlüssels bzw. des PSE

Die SmartCard ist jederzeit im unmittelbaren Zugriff zu verwahren. Insbesondere muss die SmartCard aus dem Kartenleser genommen werden, auch wenn sich der Besitzer nur kurzzeitig vom IT-System entfernt.

Wenn die PIN eines Schlüssels ohne Personenbindung geändert werden muss, dann ist es erforderlich, dass die neue PIN beim Schlüsseleigentümer verschlossen, d. h. ohne Offenlegung hinterlegt wird (gemäß einer jeweiligen Unternehmens-Policy „Passwörter“, nicht Gegenstand dieses Dokuments).

Nutzungsbeschränkungen des Personal Security Environments (PSE)

- Der private Schlüssel bzw. das Personal Security Environment (PSE) darf nur für die dafür vorgesehenen dienstlichen Zwecke verwendet werden.
- PSE/privater Schlüssel eines Schlüssels ohne Personenbindung darf nicht als persönlicher Schlüssel verwendet werden.
- PSE/privater Schlüssel darf nur auf IT-Systemen eingesetzt werden, die zum Unternehmen gehören bzw. unter dessen Hoheit es betrieben werden, und somit nicht auf privaten Systemen oder Systemen von Dritten.

3.3 Regeln für Zertifikatsnutzer

Nutzungsbeschränkungen für Zertifikate

- Die Anwendung eines öffentlichen Schlüssels zur Verschlüsselung darf nur für den dienstlichen Gebrauch erfolgen.
- Zur Verschlüsselung von eigenen Daten mit Löschung der (unverschlüsselten) Originaldaten (z. B. für eigene Archivierung) darf nur ein dafür vorgesehener Schlüssel verwendet werden, für den eine Kopie des privaten Schlüssels (z. B. in der Zertifizierungsstelle) hinterlegt ist.

Anerkennung externer Zertifikate

- Ein Zertifikat, das nicht im Rahmen der PKI ausgestellt wurde, soll nur nach sorgfältiger Prüfung anerkannt werden.

Prüfung des Widerrufstandes

Bei der manuellen Verwendung eines Zertifikats (Verschlüsselung oder Überprüfung einer digitalen Signatur mit Zertifikat, das nicht im Rahmen der PKI ausgestellt wurde) muss geprüft werden, ob das Zertifikat des Empfängers bzw. des Signierenden noch gültig ist.

3.4 Regeln für Führungskräfte

Grundsätzliches

- Führungskräfte müssen als Anwender von privaten Schlüsseln oder Schlüsselzertifikaten die Regeln für Anwender einhalten.
- Führungskräfte müssen als Betreiber die Regeln für Betreiber einhalten. (Siehe Policy-Dokumente gemäß Anhang „Weiterführende Informationen“)

Kontrollpflichten

- Führungskräfte müssen darauf achten, dass die in ihrem Verantwortungsbereich beschäftigten Anwender und Betreiber die Festlegung dieser Policy einhalten.
- Bei Kenntnisnahme eines Sicherheitsbruchs sollen Führungskräfte eventuelle Risiken und Folgen der Offenlegung des Schlüssels abschätzen und gegebenenfalls minimieren.
- Führungskräfte müssen den erfolgten Widerruf aller persönlichen Schlüssel von Mitarbeitern überprüfen, die das Unternehmen verlassen.

4 Regeln in tabellarischer Übersicht

4.1 Regeln für Schlüsseleigentümer

Thema	Regel
Antrag und Korrektheit der Zertifikatsdaten	• Zertifikatsdaten vollständig und korrekt angeben • Übereinstimmung von angebotenem und beabsichtigten Verwendungszweck des Zertifikats einhalten
Schutz des privaten Schlüssels bzw. des Personal Security Environment (PSE)	• Persönliche Übergabe des Persönlichen Schlüsselmaterials (PSE/privater Schlüssel). • Der PIN-Brief darf niemals in andere Hände gelangen. • Vorgegebene änderbare PIN ist sofort zu ändern unter Beachtung der Passwort-Regeln.

Weitergabe von Schlüsseln	• Keine Weitergabe des Personal Security Environments (PSE) eines persönlichen privaten Schlüssels
	• Übergabe von Schlüsseln ohne Personenbindung
	  • schriftlich bestätigen lassen
	  • Kenntnisnahme und Einhaltung des PSE-Infoblattes
	• PIN sofort nach Rückgabe von Schlüssel ohne Personenbindung an den Eigentümer ändern

Verhalten bei Problemen mit dem Personal Security Environment (PSE)	• Ersatzexemplare für unbrauchbar gewordene PSE-Datenträger nur über die zuständige LRA (Local Registration Authority) beziehen.
Beendigung der Schlüsseleigentümerschaft	• Widerruf der Zertifikats bei Offenlegung oder Verlust des Personal Security Environments. • Keine Weiterverwendung des PSE eines widerrufenen Schlüssels. • Widerruf der persönlichen Schlüssel bei Verlassen des Unternehmens muss zweifelsfrei und ohne Ausnahme gewährleistet sein.

4.2 Regeln für Schlüsselbesitzer

Thema	Regel
Schutz des privaten Schlüssels bzw. der PSE	• Die SmartCard jederzeit im unmittelbaren Zugriff verwahren. • PIN-Änderung bei Schlüsseln ohne Personenbindung beim Eigentümer hinterlegen und unter Beachtung der Policy "Passwörter" durchführen.
Nutzungsbeschränkungen des Personal Security Environments	• Benutzung des privaten Schlüssels nur für dienstliche Zwecke. • Benutzung von PSE/privatem Schlüssel nur auf IT-Systemen, die zum Unternehmen gehören bzw. unter dessen Hoheit betrieben werden.

4.3 Regeln für Zertifikatsbenutzer

Thema	Regel
Nutzungsbeschränkungen für Zertifikate	• Zertifikate und die darin enthaltenen öffentlichen Schlüssel nur für den dienstlichen Gebrauch einsetzen. • Verschlüsseln mit Löschung der (unverschlüsselten) Originaldaten nur mit gesicherten Schlüsseln (z. B. Kopie des privaten Schlüssels in der Zertifizierungsstelle hinterlegt).
Anerkennung externer Zertifikate	• Anerkennung fremder Zertifikate nur nach sorgfältiger Prüfung. • Benutzung von PSE/privatem Schlüssel nur auf IT-Systemen, die zum Unternehmen gehören bzw. unter dessen Hoheit betrieben werden.
Prüfung des Widerrufstandes	• Bei manuellem Einsatz eines öffentlichen Schlüssels, der nicht von der PKI stammt, prüfen, ob das Zertifikat gültig ist.

4.4 Regeln für Führungskräfte

Thema	Regel
Grundsätzliches	• Sind Führungskräfte Anwender, gelten für sie die Regeln für Anwender. • Sind Führungskräfte Betreiber, gelten für sie die Regeln für Betreiber im Anhang.
Kontrollpflichten	• Einhaltung der Policy-Regeln im eigenen Verantwortungsbereich. • Risiken und Folgen eines Sicherheitsbruchs im Verantwortungsbereich abschätzen und minimieren. • Kontrolle des Widerrufs aller persönlichen Schlüssel, wenn Mitarbeiter das Unternehmen verlässt.

5 Begriffe in einer Public Key Infrastruktur

Asymmetrische Kryptographie	Ein mathematisches Verfahren zur Datenverschlüsselung, in dem zwei verschiedene mathematisch zusammengehörende Schlüssel zum Verschlüsseln und Entschlüsseln der Daten verwendet werden.
Authentisierung	Benutzer-Authentisierung Benutzer authentisiert sich zertifikatsbasiert gegenüber einer Anwendung mit seinem PSE, anstatt mit Kennung und Passwort.
Besitzer, Schlüsselbesitzer	Der Besitzer eines Schlüssels ist der End-User, der über den privaten Schlüssel (in der Form des Personal Security Environments, PSE) verfügt und für dessen korrekten Einsatz verantwortlich ist. Bei einem persönlichen Schlüsselpaar ist der Eigentümer auch immer der Besitzer, weil es verboten ist, den persönlichen Schlüssel weiterzugeben.
Certification **A**uthority, CA „Trustcenter“	**C**ertification **A**uthority Instanz, die die Bindung eines Public Key’s an einen Benutzer in Form eines Zertifikates herstellt und mit der eigenen digitalen Signatur beglaubigt.
Chipkarte	Karte im Scheckkartenformat gemäß externem Zugriff über ISO 7816-Norm mit eingebettetem Mikrochip. Besitzt dieser Mikrochip einen programmierbaren Controller (CPU), so spricht man von einer SmartCard.
Corporate Directory, Ver-	Das Corporate Directory ist das Verzeichnis, in dem unterneh-

zeichnisdienst	mensweit verfügbare Informationen der Angestellten eingetragen sind. Es dient auch dazu, Zertifikate zu veröffentlichen und unternehmensweit bereitzustellen bzw. durch geeignete Spiegelungsmechanismen ein Teil der Informationen (z. B. Name, Vorname, E-Mail und Zertifikat) auch extern bereit zu stellen.
Digitale Signatur, heute elektronische Signatur	Eine elektronische Signatur stellt eine kryptographische Umformung von Daten dar, um diese vor unbemerkten Verfälschungen zu schützen (Schutz der Integrität). Mit digitaler Signatur wird meistens der Vorgang des digitalen Signierens assoziiert, der regional geltenden Gesetzen unterliegen kann. Die Bedeutung ist weiter gefasst, d. h. entspricht nicht dem Signaturgesetz.
Eigentümer, Schlüsseleigentümer	Der Eigentümer eines Schlüsselpaars ist der End-Benutzer, der für die korrekte Nutzung und Unversehrtheit des privaten Schlüssels verantwortlich ist. Der Eigentümer oder der Aussteller (CA) führt auch den Widerruf des Schlüsselpaars durch.
Hash-Algorithmen	Beim Hashen eines Dokumentes wird zunächst vom Dokument eine z. B. 160 Bit lange Zahl gebildet (Einwegfunktion). Es ist extrem unwahrscheinlich, dass zu verschiedenen Dokumenten ein gemeinsamer Hashwert existiert (kollisionsresistent). Der Hashwert wird anschließend mit dem privaten Signierschlüssel signiert. Die Validierung beim Dokumenten-Empfänger erfolgt dadurch, dass zunächst eigenständig der Hashwert über das Dokument gebildet wird. Anschließend wird dieser mit dem am Dokument mitübermittelten, mit Hilfe des öffentlichen Signierschlüssel des Signierers entschlüsselten, Hashwerts verglichen. Stimmen beide Werte überein, wurde das Dokument nach der Signatur nicht verändert.
Kryptoalgorithmus	Mathematisches Regelwerk, um kryptografische Operationen (z. B. Verschlüsseln, Hashen), ausgehend von elementaren mathematischen Funktionen (z. B. Verschieben, Multiplizieren, Restwert bilden) mit Hilfe von Schlüsseln und Parametern rekursiv zu vollziehen.
LDAP	**L**ightweight **D**irectory **A**ccess **P**rotocol LDAP ist ein TCP/IP-basiertes Directory-Zugangsprotokoll, das sich im Internet und in Intranets als Standardlösung für sichere Verzeichnisdienste etabliert hat.
LRA	**L**ocal **R**egistration **A**uthorities; Autorisierte, anwendernahe Stelle, welche die Identifizierung und Authentifizierung der User sicherstellt, sowie das Schlüsselmaterial an die User übergeben und verwalten soll.
Nutzer, kryptographischer Verfahren in der PKI	• Person (auch: End-Benutzer): Angestellte/-er, Werkstudent/-in, Auszubidende/-er, Consultant (jeweils beim Unternehmen oder einem Geschäftspartner). • Organisation: Projektgruppe (innerhalb oder außerhalb des

	Unternehmens), Dienststelle, Geschäftspartner-Firma usw. • Verfahren: Dienst, Client, Server, Zertifizierungsstelle, LRA usw., • Einrichtung: Rechner, Router, Firewall usw. • Ein solcher Nutzer ist entweder Anwender eines Personal Security Environments (PSE) oder eines Zertifikats oder selbst Ziel einer Anwendung von Zertifikaten.
Öffentlicher Schlüssel, public key	Der öffentliche Schlüssel ist der für jedermann zugängliche Teil eines Schlüsselpaars, das in der asymmetrischen Kryptographie verwendet wird.
Personal Security Environment	PSE Summe des Schlüsselmaterials –insbesondere der Privaten Schlüssel-, Zertifikate und weiterer Kontrollinformationen eines Users. Das Personal Security Environment (PSE) besteht hauptsächlich aus dem privaten Schlüssel und anderen Informationen, die dem Nutzer gehören, der allein Zugang zum privaten Schlüssel hat. Das PSE muss deshalb vor dem Zugriff durch Andere geschützt sein. SmartCards, Chipkarten und Disketten sind Datenträger, auf denen das PSE gespeichert wird.
Personalisierung	Zusammenführung von Personendaten zu Kartendaten
Persönlicher Schlüssel	Ein asymmetrisches Schlüsselpaar ist ein persönliches Schlüsselpaar, wenn Besitzer und Eigentümer des dazugehörenden Personal Security Environments nur ein und dieselbe Person sein dürfen und der Name dieser Person im Zertifikat beglaubigt ist.
Persönlicher Schlüssel. privater Schlüssel, private key	Der private Schlüssel ist der geheime Teil des Schlüsselpaars (eines persönlichen Schlüssels, eines Funktionsschlüssels), der in der asymmetrischen Kryptographie verwendet wird.
PIN, Personal Identity Number	Die PIN ist hier ein Passwort, mit dem ein End-Benutzer sich beim Zugriff auf das Personal Security Environment authentifiziert. Die PIN dient zum Vertraulichkeitsschutz des PSE, insbesondere des darin enthaltenen privaten Schlüssels.
Policy, PKI-	Ein Sicherheitskonzept besteht aus organisatorischen und technischen Maßnahmen und ist im Allgemeinen in einer Security-Policy niedergelegt. Die Public Key Infrastruktur wird in einer PKI-Policy niedergelegt und beschreibt das organisatorische Regelwerk, die technischen Komponenten sowie ihr Zusammenspiel. Die PKI-Policy ist das zentrale Dokument einer PKI schlechthin und definiert das Sicherheitslevel der PKI. Dieses Dokument beschreibt den Umgang mit Schlüsselmaterial unabhängig, wie es generiert oder zertifiziert/beglaubigt wurde und gilt für alle Teilnehmer am Verfahren.

Private Key	Beim symmetrischen Verfahren spricht man von einem geheimen Schlüssel, den beide Kommunikationspartner besitzen. Beim asymmetrischen Verfahren hat jeder Teilnehmer einen öffentlichen Schlüssel (Public Key) und einen privaten Schlüssel. Mit dem privaten Schlüssel wird signiert und mit dem öffentlichen Schlüssel die Unterschrift geprüft (validiert). Mit dem privaten Schlüssel kann der Empfänger die mit dem öffentlichen Schlüssel des Empfängers verschlüsselte Nachricht wieder entschlüsseln siehe auch Public Key Kryptographie
Public Key Infrastructure	PKI PKI ist die Summe aller Instanzen und Verfahren, die zum Einsatz der Public Key Kryptographie notwendig sind. Sie werden im Allgemeinen in einer Policy beschrieben.
Public Key Kryptographie	Verschlüsselungsverfahren, bei dem 2 verschiedene Schlüssel zum Ver- und zum Entschlüsseln einer Nachricht verwendet werden (daher auch die Bezeichnung asymmetrische Kryptographie). In der praktischen Anwendung wird einer dieser Schlüssel mit den Identifikationsdaten des Inhabers veröffentlicht (= public key) und der andere dem Inhaber auf einem sicheren Weg (häufig auf einer SmartCard) übergeben oder gleich in der SmartCard generiert. Eine wichtige Anwendung der Public Key Kryptographie ist die elektronische Signatur, bei der ein Dokument mit dem private key signiert wird und bei der dann der Empfänger mit Hilfe des public key die Signatur überprüft.
Registration Authority	Registration Authority, auch Local Registration Authority (LRA) Stelle, an der die zweifelsfreie Identitätsfeststellung des Endanwenders und die Ausgabe von Schlüsselmaterial stattfindet.
Registrierung	Feststellung der Identität im Personalisierungsprozess in einer (L)RA und signierte Weitergabe der Daten über einen sicheren Kanal an das Trustcenter. Voraussetzung ist die Antragstellung. Dem Teilnehmer im Verfahren für digitale Signaturen wird dabei ein geeigneter, möglichst eindeutiger Name zugewiesen.
S/MIME	**S**ecure **M**ultipurpose **I**nternet **M**ail **E**xtensions Ermöglicht das sichere Versenden und den sicheren Empfang von E-Mails.
Schlüssel, Schlüsselpaar	Ein zusammengehörendes Paar, bestehend aus einem privaten und einem öffentlichen Schlüssel, das zur Durchführung der asymmetrischen Kryptographie benötigt wird, wird hier als

	„Schlüsselpaar“ oder abkürzend als „Schlüssel“ bezeichnet.
Schlüsselmaterial	Die Zusammenfassung von persönlichem Schlüsselmaterial (Personal Security Environment) und dazugehörendem (öffentlichem) Schlüsselzertifikat.
Schlüsselsicherung (Key Backup)	„Schlüsselsicherung“ ist als Instanz in der Unternehmens-PKI-Organisation zuständig für die Sicherung privater Schlüssel, mit denen Entschlüsselungen vorgenommen werden sollen von Daten, deren unverschlüsseltes Original nicht verfügbar ist. Diese Komponente der PKI übernimmt, speichert und gibt Zugriff auf private Schlüssel bzw. ermöglicht die Anforderung auf die Wiederbeschaffung von Originaldaten (Data Recovery). Sie liegt nur im Einflussbereich des Unternehmens.
Schlüsselzertifikat	Ein Zertifikat ist eine Beglaubigung, die bestätigt, dass ein öffentlicher Schlüssel an Informationen, die Person, Organisation, Verfahren oder Einrichtung als Nutzer des zugehörigen privaten Schlüssels identifizieren, gebunden ist. Bei einem Zertifikat für einen persönlichen Schlüssel bestehen diese Informationen im wesentlichen aus den Identitätsdaten des Schlüsseleigentümers. Bei einem Zertifikat für einen Schlüssel ohne Personenbindung identifizieren die Informationen z. B. eine Dienststelle, eine Funktion, einen Server, ein IT-System, ein Verfahren, die berechtigt sind, den dazugehörigen Schlüssel einzusetzen. Kein Gegenstand der Ausarbeitung.
Security Policy	Verbindliches Dokument zur Beschreibung der Sicherheitspolitik eines Unternehmens. Mögliche Geschäftsrisiken werden bewertet und ggf. Maßnahmen festgelegt. Risiken sind sowohl unerwartete negative Ereignisse als auch unrealisierte geschäftliche Chancen. IT-Security ist Teil der Sicherheitspolitik; PKI-Policy ist Teil der Security Policy. Somit ergänzt dieses Dokument die Security Policy des Einzelunternehmens.
SmartCard	Kleinrechner im Scheckkartenformat. Sie besitzt einen Chip (auf einem Modul aufgebracht), der einen Prozessor, Datenspeicher (File System) und ein Betriebssystem enthält. Ein wesentlicher Aspekt des Betriebssystems ist der integrierte Zugriffsschutz auf Daten im File System. Erst nach Eingabe einer korrekten PIN oder durch eine Authentisierung kann z. B. der entsprechende Zugriffsstatus erreicht werden, so dass die in der jeweiligen Datei enthaltenen Daten an die Außenwelt abgegeben werden. Der Prozessor führt auch selbstständig kryptographische Rechenoperationen durch.
Sperrung (des Signatur-Zertifikats)	Vorgang, der dazu dient, bei der Überprüfung/Validierung der Signatur bei der CA oder replizierten Auskunftsdiensten das Zertifikat als ungültig zu erkennen (online). Die Sperrung kann der Teilnehmer oder sein Vertreter vornehmen lassen. Die kartenausgebende Instanz bzw. die CA als Zertifikatsausstellende Instanz muss hier eine Vertreterfunktion haben. Die Sperrung muss den Zeitpunkt enthalten und darf nicht rückwirkend erfolgen. Es besteht Unterrichtungspflicht.

	SigG macht weitere Anforderungen an das Sperrmanagement.
Trust Center, Trustcenter	Instanz mit den möglichen Aufgaben Erzeugung von Schlüsselpaaren, sichere Aufbewahrung von Schlüsselmaterial, Ausstellen, Veröffentlichung und Rücknahme von Public Key-Zertifikaten, siehe auch Certification Authority, CA
Verifizieren, Verifikation, Validierung	Beim Verifizieren einer digitalen Signatur wird festgestellt, ob die signierten Daten unverfälscht sind und von der Person, Organisation, dem Verfahren oder der Einrichtung stammen, welche die digitale Signatur erstellt hat, siehe auch Hashwert.
Verschlüsselung	Die Verschlüsselung verhindert, dass unberechtigte Personen oder Dritte die elektronische Kommunikation verwerten können. Dabei werden mathematische Verfahren verwandt, welche die Daten in eine zwar lesbare, aber unverwertbare Form umwandeln (verschlüsseln). Die Rückumwandlung in die ursprüngliche Form (Entschlüsselung) ist nur autorisierten Personen, Organisationen, Verfahren oder Einrichtungen vorbehalten.
Widerruf, Revocation	Zertifikate können oder müssen in bestimmten Fällen durch die Eigentümer oder Besitzer oder Dritte, die nicht dem Unternehmen angehören, widerrufen werden, bevor ihre Gültigkeit abläuft. Mögliche Gründe, die einen Widerruf erzwingen, sind Offenlegung des Personal Security Environments (PSE), Diebstahl oder Verlust des PSE bzw. alle Fälle, in denen der Missbrauch eines PSE vermutet werden muss. Durch einen Widerruf wird der Gebrauch dieses Zertifikats und des zugehörigen PSE dauerhaft unterbunden; denn eine nachfolgende Aufhebung des Widerrufs ist nicht möglich.
Zertifikatsnutzer, Relying Party, Empfänger, Verifizierer, Validierer	Dies sind Personen, Organisationen, Verfahren oder Einrichtungen, die das Zertifikat bzw. den darin enthaltenen öffentlichen Schlüssel benutzen zum Verschlüsseln (vor dem Senden von Daten) oder Verifizieren (nach Empfang von signierten Daten).

6 Anhang 1: Weiterführende Informationen

§ Einsatz von Verschlüsselung und Elektronischer Signatur im elektronischen Geschäftsverkehr der deutschen Elektrizitätswirtschaft

Studie, Status veröffentlicht, 28 Seiten

§ Sicherheitsrahmenbedingungen für den elektronischen Geschäftsverkehr im deutschen Strommarkt

Gemeinsame Erklärung der Verbände

§ Sicherheitspolitik (PKI-Policy), Version 1.0
VDEW-Empfehlungen

§ Umgang mit Schlüsselmaterial, Version 1.0
VDEW-Empfehlungen

§ Technische PKI-Interoperabilität, Version 1.0
VDEW-Empfehlungen

§ Umsetzungsempfehlungen, Version 1.0
VDEW-Empfehlungen

§ Zertifizierungsrichtlinie (Certification Practice Statement), Version 1.0
VDEW-Empfehlungen