Bundesamt
für Sicherheit in der
Informationstechnik

Vorstudie Grid Sicherheits-Infrastruktur (GSI)
Ergebnisse des Arbeitspakets 3:
„Sicherheitsmechanismen“

Version: 4.1

Bundesamt für Sicherheit in der Informationstechnik
Postfach 200363
53133 Bonn
Internet: www.bsi.bund.de

Inhaltsverzeichnis

1 Sicherheitsmechanismen: Vorgehensweise

Hier werden die im Teildokument „Ergebnisse des Arbeitspakets 2: Risikoanalyse“ (kurz: „AP2“) für die einzelnen Szenarien identifizierten Risiken zunächst grob in zwei Kategorien eingeteilt: tragbar und nicht tragbar. Die im Folgenden betrachteten Sicherheitsmechanismen orientieren sich ausschließlich an den nicht tragbaren Risiken. Dabei handelt es sich um die im kritischen Bereich der jeweiligen Risikomatrix (Abbildungen 1 bis 5 im Teildokument „Ergebnisse des Arbeitspakets 2: Risikoanalyse“, auf und rechts über der Hauptdiagonalen liegend, im Dokument auch orange bis rot markiert) angesiedelten Risiken.

Die so als nicht tragbar eingestuften Kombinationen von Eintrittwahrscheinlichkeit und Schadenshöhe fasst Tabelle 1 zunächst für alle Szenarien zusammen.

Tabelle 1: Nicht tragbare Risiken gemäß Risikomatrix

Schadenshöhe	Eintrittswahrscheinlichkeit
sehr hoch	niedrig, mittel, hoch oder sehr hoch
hoch	mittel, hoch oder sehr hoch
mittel	hoch oder
niedrig	sehr hoch

2 Ableitung der Mechanismen für die betrachteten Grid Szenarien

Um für die relevanten Szenarien angemessene Sicherheitsmechanismen spezifizieren zu können, werden zunächst – wie in 1 („Sicherheitsmechanismen: Vorgehensweise“) dargelegt – die als nicht tragbar eingestuften Risiken identifiziert. Anschließend werden Maßnahmen beschrieben, die die Eintrittswahrscheinlichkeit einzelner oder auch mehrere der identifizierten Risiken reduzieren. Dabei werden für jede Maßnahme folgende Merkmale betrachtet:

- **Maßnahme**
  identifiziert jede Maßnahme anhand einer eindeutigen ID der Form „M*x*.*y*“, wobei *x* das jeweilige Szenario (1 bis 5) angibt, während *y* die Maßnahmen durchnummeriert
- **Kurzbeschreibung**
  kurze Beschreibung der Maßnahme
- **Ergebnis**
  gibt an, für welche Risiken die Eintrittswahrscheinlichkeit wie stark gesenkt wird
- **Wirkt gegen**
  fasst Risiken und Bedrohungen zusammen, gegen die die Maßnahme wirkt
- **Aktion bei**
  stellt den Bezug zu denjenigen Datenobjekten und Grid-Ressourcen her, auf die die Maßnahme angewendet werden muss
- **Beschreibung**
  erläuternde Beschreibung der Maßnahme

- **Aufwand**
  enthält eine qualitative Abschätzung des für die Umsetzung der Maßnahme erforderlichen Aufwands
- **Grenzen der Wirksamkeit**
  erläutert ggf. die zusätzlich erforderlichen Randbedingungen und von der Maßnahme nicht abgedeckten Wirksamkeitsaspekte

Diese Vorgehensweise wird für jedes der betrachteten Szenarien gesondert durchgeführt. Folgende Szenarien werden dabei betrachtet:

1. Szenario 1: Unternehmensinternes Grid; s. Abschnitt 2.1
2. Szenario 2: Grid für den unternehmensübergreifenden industriellen Einsatz; s. Abschnitt 2.2
3. Szenario 3: Offenes e-Science Grid; s. Abschnitt 2.3
4. Szenario 4: Grids mit personenbezogenen bzw. personenbeziehbaren Daten (z. B. MammoGrid); s. Abschnitt 2.4
5. Szenario 5: Sicherheitskritisches national wichtiges Grid / Katastrophenschutz (K-Grid); s. Abschnitt 2.5

Bei den Maßnahmen wird – sofern das im jeweiligen Szenario Sinn macht – zwischen Grid-spezifischen Maßnahmen und generellen Maßnahmen unterschieden. Für manche Szenarien ist die entsprechende Zuordnung der Risiken nicht eindeutig. Das wird bei der Betrachtung der einzelnen Szenarien erforderlichenfalls näher ausgeführt.

2.1 Szenario 1: Unternehmensinternes Grid

Die Risiken aus Szenario 1, die entsprechend der Risikomatrix aus AP2 als nicht tragbar eingestuft werden (vgl. 1. „Sicherheitsmechanismen: Vorgehensweise“), sind in Tabelle 2 zusammengefasst.

Tabelle 2: Nicht tragbare Risiken gemäß Risikomatrix für Szenario 1

Schadenshöhe	Eintrittswahrscheinlichkeit	Risiko Nr.
sehr hoch	niedrig, mittel, hoch oder sehr hoch	- keine -
hoch	mittel, hoch oder sehr hoch	R1.1, R1.2, R1.3, R1.5, R1.7, R1.11
mittel	hoch oder sehr hoch	- keine -
niedrig	sehr hoch	- keine -

Gegen diese Risiken werden in den folgenden Abschnitten Maßnahmen entwickelt und beschrieben. Dabei wird zwar implizit zwischen Grid-spezifischen Maßnahmen und generellen Maßnahmen unterschieden. Aber bei genauer Betrachtung dieses Szenarios und der Risiken ist die entsprechende Zuordnung der Risiken nicht eindeutig. Vielmehr sind die Risiken auch für vernetze Infrastrukturen, die nicht als Grid zu betrachten sind, typisch. Daher wird auf die explizite Zuordnung der Risiken zu den Kategorien „Grid-spezifischen Maßnahmen“ und „generellen Maßnahmen“ verzichtet.

2.1.1 Sicherheitsmaßnahmen für Szenario 1

Nachfolgend werden die Maßnahmen genauer spezifiziert und bewertet. Dabei wird davon ausgegangen, dass alle Maßnahmen in den Kontext einer geeigneten IT-Sicherheitsleitlinie (*IT Security Policy*) eingebettet sind.

Tabelle 3: Maßnahme M1.1, Organisatorische Variante M1.1.a

Maßnahme	M1.1.a
Kurzbeschreibung	Verpflichtung aller P-lad auf eine geeignete Security-Policy
Ergebnis	Die Eintrittswahrscheinlichkeit von R1.1 sinkt auf niedrig - mittel Die Eintrittswahrscheinlichkeit von R1.5 sinkt auf mittel
Wirkt gegen	R1.1 (B1.1, Vertraulichkeit wird durch Abhören unternehmensinterner Kommunikationsstrecken verletzt) R1.5 (B1.3, Vertraulichkeit oder Integrität der Daten wird durch gezielten Angriff auf Datenbank verletzt)
Aktion bei	Domänenverantwortliche und P-lad DO-SA, DO-SB

Maßnahme	M1.1.a
Beschreibung	Bei Szenario 1 muss die Vertraulichkeit der zugriffsbeschränkten und besonders der geschäftskritischen Daten (DA-z und DA-zz) gewährleistet werden. Nach heutigem Stand der Technik ist das durchgängig nur mittels Kombination technischer und organisatorischer Maßnahmen möglich. Bei einem Grid, das mit solchen Daten arbeitet, sollte daher die Verpflichtung aller Verantwortlichen P-lad auf die Einhaltung der Vertraulichkeitsanforderungen erfolgen. Es liegt dann in der Zuständigkeit des unternehmensintern Verantwortlichen, für eine adäquate Umsetzung zu sorgen.
Aufwand	Mittel
Grenzen der Wirksamkeit	Verpflichtete P-lad könnten sich nicht an die Verpflichtungserklärung halten. Es sollten passende Sanktionierungen vorgesehen werden. Maßnahme M1.1, Technische Variante M1.1.b, beschreibt eine technische Realisierungsvariante dieser Maßnahme mit gleicher Wirkung.

Tabelle 4: Maßnahme M1.1, Technische Variante M1.1.b

Maßnahme	M1.1.b
Kurzbeschreibung	Einsatz von speziellen Mechanismen zum Zugriffschutz, z. B. TCG
Ergebnis	Die Eintrittswahrscheinlichkeit von R1.1 sinkt auf mittel bis niedrig Die Eintrittswahrscheinlichkeit von R1.5 sinkt auf mittel
Wirkt gegen	R1.1 (B1.1, Vertraulichkeit wird durch Abhören unternehmensinterner Kommunikationsstrecken verletzt) R1.5 (B1.3, Vertraulichkeit oder Integrität der Daten wird durch gezielten Angriff auf Datenbank verletzt)
Aktion bei	Domänenverantwortliche und P-lad DO-SA, DO-SB
Beschreibung	Bei einem Grid, das mit Daten dieser Vertraulichkeitsstufe arbeitet, sollte die durchgängige Verpflichtung aller Verantwortlichen P-lad auf den Einsatz hardwarebasierter TCG-Mechanismen erfolgen, etwa in Form geeigneter Vereinbarungen, die den Grad der jeweils sicherzustellenden Vertraulichkeit festschreiben. Mit diesen Mechanismen wäre es möglich, den Zugriff auf vertrauliche Daten auf signierte, d. h. hier authentische und integere, Programme zu beschränken.
Aufwand	Hoch (gesamte Hardware muss ersetzt werden, Umrüstung ist wahrscheinlich nicht möglich)

Maßnahme	M1.1.b
Grenzen der Wirksamkeit	Derzeit sind noch keine Hochleistungsrechnersysteme mit TCG-basierter Hardware verfügbar. Für das vorliegende Szenario ist diese Maßnahme daher eine Möglichkeit für zukünftige Systeme. Die Anwendungen können dann nur noch auf TCG-basierter Hardware ausgeführt werden. D. h. der Einsatz muss im Einzelfall nicht organisatorisch erzwungen werden (setzt natürlich das Einhalten der entsprechenden Vereinbarung voraus). Daneben zeigt sich erfahrungsgemäß auf Dauer auch bei wirksamen und komplexen Mechanismen eine Möglichkeit diese zu umgehen. Für Administratoren, die z. B. als Datenbank-Administratoren mit einem signierten Programm auf der Datenbank arbeiten. Hier muss eine TCG-konforme Implementierung möglichst verhindern, dass über die Admin-Funktionen auch auf vertrauliche Daten zugegriffen werden kann. Wo das nicht möglich ist, muss auf Maßnahme M1.1, Organisatorische Variante M1.1.a, zurückgegriffen werden. (Für weitere Erläuterungen zu TCG und ggf. weiteren Mechanismen s. 3. „Sicherheitsmechanismen: Fazit“.)

Tabelle 5: Maßnahme M1.2

Maßnahme	M1.2
Kurzbeschreibung	Verpflichtung aller Administratoren P-lad auf die vereinbarten Spielregeln und Umsetzung einschlägiger Schutzmaßnahmen
Ergebnis	Die Eintrittswahrscheinlichkeit von R1.2 sinkt auf niedrig Die Eintrittswahrscheinlichkeit von R1.3 sinkt auf niedrig Die Eintrittswahrscheinlichkeit von R1.7 sinkt auf niedrig Die Eintrittswahrscheinlichkeit von R1.11 sinkt auf niedrig
Wirkt gegen	R1.2, R1.3 (B1.1, Vertraulichkeit wird durch Abhören unternehmensinterner Kommunikationsstrecken verletzt) R1.7 (B1.4, Vertraulichkeit oder Integrität der Daten wird durch Angriff auf HW oder SW verletzt) R1.11 (B1.6, Nutzung einer Grid-Ressource (HW, SW, SRV) wird durch gezielten Angriff verhindert)
Aktion bei	P-lad bei DO-SA, DO-SB
Beschreibung	Hier handelt es sich um Umsetzung etablierte Schutzmaßnahmen (Auditing-Mechanismen, Zugangsschutz bei Räumen mit „kritischen“ Ressourcen wie etwa Server, Netzkomponenten etc.).
Aufwand	Niedrig

Maßnahme	M1.2
Grenzen der Wirksamkeit	Gegen Fehlverhalten Einzelner gibt es keinen vollständigen Schutz. Einzelne Administratoren könnten sich evtl. fahrlässig oder vorsätzlich nicht an entsprechende Vorgaben halten. Daher sind Sanktionen für den Fall des Verstoßes vorzusehen. Voraussetzung ist auch hier eine geeignete IT-Sicherheitsleitlinie.

Tabelle 6: Maßnahme M1.3

Maßnahme	M1.3
Kurzbeschreibung	Einrichtung eines P-gad, der über den Teilorganisationen steht, die die Domänen bilden, und das Vertrauen aller genießt
Ergebnis	Die Eintrittswahrscheinlichkeit von R1.1 sinkt auf niedrig Die Eintrittswahrscheinlichkeit von R1.2 sinkt auf niedrig Die Eintrittswahrscheinlichkeit von R1.3 sinkt auf niedrig Die Eintrittswahrscheinlichkeit von R1.5 sinkt auf niedrig Die Eintrittswahrscheinlichkeit von R1.7 sinkt auf niedrig Die Eintrittswahrscheinlichkeit von R1.11 sinkt auf niedrig
Wirkt gegen	R1.1, R1.2, R1.3 (B1.1, Vertraulichkeit wird durch Abhören unternehmensinterner Kommunikationsstrecken verletzt) R1.5 (B1.3, Vertraulichkeit oder Integrität der Daten wird durch gezielten Angriff auf Datenbank verletzt) R1.7 (B1.4, Vertraulichkeit oder Integrität der Daten wird durch Angriff auf HW oder SW verletzt) R1.11 (B1.6, Nutzung einer Grid-Ressource (HW, SW, SRV) wird durch gezielten Angriff verhindert)
Aktion bei	P-lad bei DO-SA, DO-SB sowie Unternehmensleitung
Beschreibung	Ein übergeordneter P-ad wäre in der Lage über Einzelinteressen der Unternehmensteile hinweg ein Security-Policy durchzusetzen.
Aufwand	Mittel
Grenzen der Wirksamkeit	Die Wirksamkeit steht und fällt mit den Mitteln, die dem P-ad zur Durchsetzung der übergeordneten Interessen zur Verfügung stehen. Hier muss auf eine geeignete Positionierung in der Unternehmenshierarchie und geeignete Berichtswege geachtet werden

2.1.2 Übersicht Sicherheitsmechanismen Szenario 1

Die folgende Tabelle 7 liefert eine Kurzübersicht über die Maßnahmen, die zur Verringerung der als nicht tragbar eingestuften Risiken notwendig sind.

Tabelle 7 Übersicht über die Sicherheitsmechanismen für Szenario 1

Maß-nahme	Kurzbeschreibung	Wirkt gegen
M1.1.a	Verpflichtung aller P-lad auf eine geeignete Security-Policy	R1.1, R1.5
M1.1.b	Einsatz von speziellen Mechanismen zum Zugriffschutz, z. B. TCG	R1.1, R1.5
M1.2	Verpflichtung aller Administratoren P-lad auf die vereinbarten Spielregeln und Umsetzung einschlägiger Schutzmaßnahmen	R1.2, R1.3, R1.7, R1.11
M1.3	Einrichtung eines P-gad, der über den Teilorganisationen steht, die die Domänen bilden, und das Vertrauen aller genießt	R1.1, R1.2, R1.3, R1.7, R1.11

2.1.3 Fazit für Szenario 1

Die Maßnahmen für Szenario 1 resultieren aus den nicht tragbaren Risiken (s. Tabelle 2; vgl. 1. „Sicherheitsmechanismen: Vorgehensweise“) für dieses Szenario (vgl. auch AP2 - Risikoanalyse). Die Analyse zeigt, dass die nicht tragbaren Risiken hauptsächlich in Bereichen liegen, die nicht Grid-spezifisch sind und denen heute üblicherweise bereits anderweitig (vgl. z. B. GSHB) begegnet wird. Der Schwerpunkt liegt daher auf organisatorischen Maßnahmen (Maßnahme M1.1, Organisatorische Variante M1.1.a; Maßnahme M1.2; Maßnahme M1.3). Speziell zu TCG (Maßnahme M1.1, Technische Variante M1.1.b) sei auf 3. „Sicherheitsmechanismen: Fazit“ verwiesen.

2.2 Szenario 2: Grid für den unternehmensübergreifenden industriellen Einsatz

Die Risiken aus Szenario 2, die entsprechend der Risikomatrix aus AP2 als nicht tragbar eingestuft werden (vgl. 1. „Sicherheitsmechanismen: Vorgehensweise“), sind in Tabelle 8 zusammengefasst.

Tabelle 8: Nicht tragbare Risiken gemäß Risikomatrix für Szenario 2

Schadenshöhe	Eintrittswahrscheinlichkeit	Risiko Nr.
sehr hoch	niedrig, mittel, hoch oder sehr hoch	R2.1, R2.9, R2.10, R2.12, R2.14, R2.15, R2.17
hoch	mittel, hoch oder sehr hoch	R2.3, R2.4, R2.7
mittel	hoch oder sehr hoch	- keine -
niedrig	sehr hoch	- keine -

Gegen diese Risiken werden in den folgenden Abschnitten Maßnahmen entwickelt und beschrieben. Es wird zwischen Grid-spezifischen (vgl. Absatz 2.2.1) Maßnahmen und generellen Maßnahmen (vgl. Absatz 2.2.2) unterschieden. Zusätzlich werden für alle Grid-spezifischen Risiken (RK) Maßnahmen definiert.

2.2.1 Grid-spezifische Sicherheitsmaßnahmen für Szenario 2

Nachfolgend werden die Maßnahmen genauer spezifiziert und bewertet.

Tabelle 9: Maßnahme M2.1, Organisatorische Variante M2.1.a

Maßnahme	M2.1.a
Kurzbeschreibung	Sorgfältige Auswahl und sorgfältige vertragliche Einbindung der Service-Provider für DO-UB
Ergebnis	Die Eintrittswahrscheinlichkeit von R2.1 wird weiter reduziert Die Eintrittswahrscheinlichkeit von R2.4 sinkt auf niedrig Die Eintrittswahrscheinlichkeit von R2.7 sinkt auf hoch bis mittel
Wirkt gegen	R2.1 (B2.1, Auswahl eines nicht vertrauenswürdigen Dienstleisters) R2.4 (B2.3, lokaler Administrator P-lad aus DO-UX erhält unberechtigten Zugriff) R2.7 (B2.5, lokaler Administrator P-lad manipuliert angebotene Grid-Ressourcen)
Aktion bei	Domänen- bzw. Policy-Verantwortliche P-l bei DO-UA

Maßnahme	M2.1.a
Beschreibung	Bei Szenario 2 muss die Vertraulichkeit der zugriffsbeschränkten und besonders der geschäftskritischen Daten (DA-z und DA-zz) gewährleistet werden. Nach heutigem Stand der Technik ist das durchgängig nur mittels Kombination technischer und organisatorischer Maßnahmen möglich. Bei einem Grid, das mit solchen Daten arbeitet, sollte daher die Verpflichtung aller Verantwortlichen P-l auf die Einhaltung der Vertraulichkeitsanforderungen erfolgen. D. h. die P-l gestalten eine Kooperationsvereinbarung, die unter anderem die vorgenannte Vertraulichkeit garantiert und geeigneter Dienstgütevereinbarungen (SLAs) enthält. Es liegt dann in der Verantwortung der P-l unternehmensintern für eine Umsetzung zu sorgen. Dazu gehört auch Maßnahme M2.5, bei der die P-lad verpflichtet werden.
Aufwand	Mittel
Grenzen der Wirksamkeit	Verpflichtete P-l könnten sich nicht an die Verpflichtungsvereinbarung halten. Es sollten passende Sanktionierungen (etwa angemessene Vertragsstrafen bei Verletzung der Vertraulichkeit) vorgesehen werden. Maßnahme M2.1, Technische Variante M2.1.b, beschreibt eine technische Realisierungsvariante dieser Maßnahme mit gleicher Wirkung, die jedoch ebenfalls der vertraglichen Absicherung bedarf, damit die Programme beim Dienstleister ausführbar sind.

Tabelle 10: Maßnahme M2.1, Technische Variante M2.1.b

Maßnahme	M2.1.b
Kurzbeschreibung	Einsatz von speziellen Mechanismen zum Zugriffschutz, z. B. TCG
Ergebnis	Die Eintrittswahrscheinlichkeit von R2.1 wird weiter reduziert Die Eintrittswahrscheinlichkeit von R2.4 sinkt auf niedrig Die Eintrittswahrscheinlichkeit von R2.7 sinkt auf hoch bis mittel
Wirkt gegen	R2.1 (B2.1, Auswahl eines nicht vertrauenswürdigen Dienstleisters) R2.4 (B2.3, lokaler Administrator P-lad aus DO-UX erhält unberechtigten Zugriff) R2.7 (B2.5, lokaler Administrator P-lad manipuliert angebotene Grid-Ressourcen)
Aktion bei	Domänen- bzw. Policy-Verantwortliche P-l bei DO-UA
Beschreibung	Bei einem Grid, das mit Daten dieser Vertraulichkeitsstufe arbeitet, sollte die durchgängige Verpflichtung aller Verantwortlichen P-l und der zugeordneten Administratoren P-lad auf den Einsatz hardwarebasierter TCG-Mechanismen erfolgen, etwa in Form geeigneter Dienstgütevereinbarungen (SLAs), die den Grad der jeweils sicherzustellenden Vertraulichkeit festschreiben. Mit diesen Mechanismen wäre es möglich, den Zugriff auf vertrauliche Daten auf signierte, d. h. hier authentische und integere, Programme zu beschränken.
Aufwand	Hoch (gesamte Hardware muss ersetzt werden, Umrüstung ist wahrscheinlich nicht möglich)

Maßnahme	M2.1.b
Grenzen der Wirksamkeit	Derzeit sind noch keine Hochleistungsrechnersysteme von Sun mit TCG-basierter oder ähnlicher Hardware verfügbar. Für das vorliegende Szenario ist diese Maßnahme daher eine Möglichkeit für zukünftige Systeme. Die Anwendungen können dann nur noch auf TCG-basierter Hardware ausgeführt werden. D. h. der Einsatz muss nicht organisatorisch erzwungen werden. Daneben zeigt sich erfahrungsgemäß auf Dauer auch bei wirksamen und komplexen Mechanismen eine Möglichkeit diese zu umgehen. (Für weitere Erläuterungen zu TCG und ggf. weiteren Mechanismen s. 3. „Sicherheitsmechanismen: Fazit“.)

Tabelle 11: Maßnahme M2.2

Maßnahme	M2.2
Kurzbeschreibung	Vereinbarung einer verbindlichen Rahmen-Policy zwischen allen Ressourcenprovidern eines Grid bzw. Erweiterung der vorhanden Rahmen-Policy zur konkreten Reduktion der hergeleiteten Risiken
Ergebnis	Die Eintrittswahrscheinlichkeit von R2.1 wird weiter reduziert Die Eintrittswahrscheinlichkeit von R2.4 sinkt auf niedrig Die Eintrittswahrscheinlichkeit von R2.7 sinkt auf hoch bis mittel
Wirkt gegen	R2.1 (B2.1, Auswahl eines nicht vertrauenswürdigen Dienstleisters) R2.4 (B2.3, lokaler Administrator P-lad aus DO-UX erhält unberechtigten Zugriff) R2.7 (B2.5, lokaler Administrator P-lad manipuliert angebotene Grid-Ressourcen)
Aktion bei	Domänen- bzw. Policy-Verantwortliche DO-UB und DO-UX, DO-srv, DO-sw, DO-hw
Beschreibung	In der Rahmen-Policy werden domänenübergreifende, einheitliche und den Interessen aller Beteiligten entsprechende Regelungen getroffen. Alle Ressourcenprovider verpflichten sich zur Einhaltung dieser Regeln.
Aufwand	Niedrig (Umsetzung evtl. mittel)
Grenzen der Wirksamkeit	Einzelne Ressourcenprovider könnten sich evtl. nicht an die Regelungen halten. Es sind Sanktionen für den Fall des Verstoßes vorzusehen.

Tabelle 12: Maßnahme M2.3

Maßnahme	M2.3
Kurzbeschreibung	Einsatz vertrauenswürdiger Grid-Middleware

Maßnahme	M2.3
Ergebnis	Die Eintrittswahrscheinlichkeit von R2.3 sinkt auf niedrig
Wirkt gegen	R2.3 (B2.2, Grid-Nutzer P-u aus DO-UX erhält unberechtigten Zugriff)
Aktion bei	P-l bzw. P-lad bei DO-UB und DO-UX, DO-srv, DO-sw, DO-hw
Beschreibung	Fachkundiger Einsatz vertrauenswürdiger Grid-Middleware im Rahmen der „Rahmen-Policy“ bietet zusätzlichen Schutz gegen unbefugte Zugriffe. Alle Ressourcenprovider verpflichten sich zur Einhaltung der entsprechenden Vereinbarung.
Aufwand	Mittel
Grenzen der Wirksamkeit	Nicht sachgerechte Konfiguration der Grid-Middleware kann zu Fehlfunktionen führen und muss daher im Rahmen von QS-Maßnahmen verhindert werden. Einzelne Ressourcenprovider könnten sich evtl. „vorsätzlich“ (z. B. aus Kostengründen) nicht an die Vereinbarungen halten. Es sind Sanktionen für den Fall des Verstoßes vorzusehen. (vgl. Maßnahme M2.2). Speziell die Grid-Engine von Sun sieht nur in begrenztem Umfang technische Maßnahmen zur Sicherheit insbesondere Vertraulichkeit der verarbeiteten Daten vor. Daher ist die Wirksamkeit dieser Maßnahme auf diesen beschränkten Umfang begrenzt und kann nicht alle Sicherheitsanforderungen erfüllen. Hier sollte also eine andere, den Anforderung besser entsprechende Middleware eingesetzt werden.

Tabelle 13: Maßnahme M2.4

Maßnahme	M2.4
Kurzbeschreibung	Konsequenter Einsatz der der Grid-Middleware vorgeschalteten Sicherheitsmechanismen
Ergebnis	Die Eintrittswahrscheinlichkeit von R2.9 sinkt weiter ab
Wirkt gegen	R2.9 (B2.7, Kompromittierung der Verschlüsselungsschlüssel)
Aktion bei	P-l bzw. P-lad bei DO-UB, DO-srv, DO-sw, DO-hw
Beschreibung	Konsequente Nutzung von verfügbaren Mechanismen zur Zugriffsbeschränkung in Verbindung mit verfügbaren Hardware-basierten Sicherheitsmechanismen schützt vor Kompromittierung der Verschlüsselungsschlüssel als Grundlage des Hauptsicherheitsmechanismus.
Aufwand	Mittel
Grenzen der Wirksamkeit	Nicht sachgerechte Auswahl/Konfiguration der Sicherheitsmechanismen kann eine Bedrohung darstellen und muss daher im Rahmen von QS-Maßnahmen verhindert werden. Einzelne Ressourcenprovider könnten sich evtl. „vorsätzlich“ (z. B. aus Kostengründen) nicht an entsprechende Vereinbarungen halten. Es sind Sanktionen für den Fall des Verstoßes vorzusehen (vgl. Maßnahme M2.2).

Tabelle 14: Maßnahme M2.5

Maßnahme	M2.5
Kurzbeschreibung	Verpflichtung aller Administratoren P-lad auf den vereinbarten Spielregeln entsprechende Arbeitsanweisungen
Ergebnis	Die Eintrittswahrscheinlichkeit von R2.4 sinkt auf niedrig Die Eintrittswahrscheinlichkeit von R2.10 sinkt auf niedrig
Wirkt gegen	R2.4 (B2.3, lokaler Administrator P-lad aus DO-UX erhält unberechtigten Zugriff) R2.10 (B2.8, lokaler Administrator P-lad von DO-UB kompromittiert Verschlüsselung)
Aktion bei	P-l bzw. P-lad bei DO-UB
Beschreibung	Aus der Policy müssen konkrete Handlungs- und Arbeitsanweisungen abgeleitet werden, auf deren Einhaltung die Administratoren verpflichtet werden müssen.
Aufwand	Niedrig
Grenzen der Wirksamkeit	Hier handelt es sicher weniger um eine technische als um eine organisatorische Maßnahme. Gegen Fehlverhalten Einzelner gibt es keinen vollständigen Schutz. Einzelne Administratoren könnten sich evtl. fahrlässig oder vorsätzlich nicht an entsprechende Vorgaben halten. Es sind Sanktionen für den Fall des Verstoßes vorzusehen (vgl. Maßnahme M2.2).

Tabelle 15: Maßnahme M2.6

Maßnahme	M2.6
Kurzbeschreibung	Erweiterung der Grid-Middleware um Sicherheitsmechanismen
Ergebnis	Die Eintrittswahrscheinlichkeit für R2.2 - R2.5, R2.7 - R2.17 sinkt weiter ab

Maßnahme	M2.6
Wirkt gegen	R2.2, R2.3 (B2.2, Grid-Nutzer P-u aus DO-UX erhält unberechtigten Zugriff) R2.4 (B2.3, lokaler Administrator P-lad aus DO-UX erhält unberechtigten Zugriff) R2.5 (B2.4, unberechtigter Zugriff durch P-u aus DO-UX auf DA-zz in DO-UB) R2.7 (B2.5, lokaler Administrator P-lad manipuliert angebotene Grid-Ressourcen) R2.8 (B2.6, fehlerhafte Konfiguration von Sicherheitskunktionen auf Grid-Ressourcen) R2.9 (B2.7, Kompromittierung der Verschlüsselungsschlüssel) R2.10 (B2.8, lokaler Administrator P-lad von DO-UB kompromittiert Verschlüsselung) R2.11, R2.12 (B2.9, Angreifer erlangt unberechtigten Zugriff auf Grid-Ressourcen in DO-UB) R2.13 (B2.10, berechtigter Nutzer P-u nutzt die Grid-Ressourcen in DO-UB unberechtigt) R2.14 (B2.11, P-uzz oder P-u erhält unberechtigten Zugriff die SW in DO-UB) R2.15 (B2.12, Angreifer P-x erhält unberechtigten Zugriff auf die SW in DO-UB) R2.16 (B2.13, P-u erhält unberechtigten Zugriff auf SW in DO-UB und Daten DA-zz) R2.17 (B2.14, Angreifer P-x erhält unberechtigten Zugriff auf SW in DO-UB und DA-zz)
Aktion bei	P-l bzw. DO-srv
Beschreibung	Die Sun-Grid-Engine ist nur in eingeschränktem Maß mit Sicherheitsmechanismen, wie sie im vorliegenden Szenario erforderlich wären ausgestattet. Die Anwender haben dem durch Einbau von Sicherheitsmechanismen aus Applikationsebene Rechnung getragen. Ein Beispiel hierfür ist die Verschlüsselung der Daten auf Anwendungsebene. Kern dieser Maßnahme wäre die Ausstattung der Grid Engine mit Sicherheitsmechanismen ähnlich Globus bzw. der Umstieg auf eine Middleware, die diese Merkmale besitzt.
Aufwand	Sehr hoch
Grenzen der Wirksamkeit	Es ist sehr fraglich, ob diese Maßnahme sinnvoll umgesetzt werden kann. Ein Grund hierfür ist der hohe Aufwand für die Implementierung dieser Mechanismen. Ein weiterer Grund ist die Position des Herstellers, dass diese Grid-Middleware für „Campus-Grids“ entworfen wurde. D. h. für den kooperative Organisationen im Forschungsumfeld, die nur in sehr begrenztem Umfang finanzielle Interessen verfolgen und Vertraulichkeitsanforderungen unterliegen.

2.2.2 Generelle Sicherheitsmaßnahmen für Szenario 2

Tabelle 16: Maßnahme M2.7

Maßnahme	M2.7
Kurzbeschreibung	Verfahren zur Zugriffs- und Zutrittskontrolle für Rechnersysteme in DO-UA, DO-UB
Ergebnis	Die Wahrscheinlichkeit für R2.12 kann weiter abgesenkt werden
Wirkt gegen	R2.12 (B2.9, Angreifer erlangt unberechtigten Zugriff auf Grid-Ressourcen in DO-UB)
Aktion bei	Verantwortliche für Domänen DO-UA, DO-UB
Beschreibung	Für jede der Domänen DO-UA, DO-UB wird ein Verfahren zur Zugriffs- und Zutrittskontrolle für Rechnersysteme nach Grundschutzhandbuch entworfen und implementiert. Die vom Betriebsystem bereitgestellten Zugriffskontrollmechanismen werden aktiviert und genutzt. Zutrittskontrolle wird auf organisatorischer Ebene implementiert.
Aufwand	(nicht allgemein abschätzbar, da stark von den lokalen Randbedingungen abhängig)
Grenzen der Wirksamkeit	Bei nicht regelkonformem oder gar gesetzeswidrigem Benutzerverhalten können die hier beschriebenen Maßnahmen ggf. ausgehebelt werden.

Tabelle 17: Maßnahme M2.8

Maßnahme	M2.8
Kurzbeschreibung	Lokales Sicherheitskonzept für jede Domäne DO-UA, DO-UB
Ergebnis	Eintrittwahrscheinlichkeit für R2.9, R2.12, R2.14, R2.15, R2.17 sinkt weiter ab
Wirkt gegen	R2.9 (B2.7, Kompromittierung der Verschlüsselungsschlüssel) R2.12 (B2.9, Angreifer erlangt unberechtigten Zugriff auf Grid-Ressourcen in DO-UB) R2.14 (B2.11, P-uzz oder P-u erhält unberechtigten Zugriff die SW in DO-UB) R2.15 (B2.12, Angreifer P-x erhält unberechtigten Zugriff auf die SW in DO-UB) R2.17 (B2.14, Angreifer P-x erhält unberechtigten Zugriff auf SW in DO-UB und DA-zz)
Aktion bei	Verantwortliche für DO-UA, DO-UB
Beschreibung	Für jede der Domänen DO-UA und DO-UB wird ein Sicherheitskonzept nach Grundschutzhandbuch entworfen und implementiert. Dieses umfasst insbesondere die Absicherung der lokalen Systeme auf Betriebssystem- und Netzebene, des weiteren Zugriffs- und Zutrittskontrollmechanismen (vgl. Maßnahme M2.9).
Aufwand	Hoch
Grenzen der Wirksamkeit	vgl. GSHB

Tabelle 18: Maßnahme M2.9

Maßnahme	M2.9
Kurzbeschreibung	Verfügbarkeitskonzept für jede Domäne DO-UB
Ergebnis	Schadenshöhe R2.12, R2.14, R2.15, R2.17 sinkt auf mittel
Wirkt gegen	R2.12 (B2.9, Angreifer erlangt unberechtigten Zugriff auf Grid-Ressourcen in DO-UB) R2.14 (B2.11, P-uzz oder P-u erhält unberechtigten Zugriff die SW in DO-UB) R2.15 (B2.12, Angreifer P-x erhält unberechtigten Zugriff auf die SW in DO-UB) R2.17 (B2.14, Angreifer P-x erhält unberechtigten Zugriff auf SW in DO-UB und DA-zz)
Aktion bei	Verantwortlicher DO-UB
Beschreibung	Für jede der Domänen DO-UB wird ein Sicherheitskonzept für den Störungsfall nach Grundschutzhandbuch entworfen und implementiert. Dieses umfasst insbesondere die Redundanzen (zuverlässiges und schnell verfügbares Backup), um Verfügbarkeitsanforderungen zu erfüllen und kompromittierte SW-Ressourcen schnell wieder in Betrieb nehmen zu können. Auch für die HW-Ressourcen müssen ggf. entsprechende Ersatzkomponenten vorgehalten bzw. im Bedarfsfall sofort bereitgestellt werden.
Aufwand	Mittel bis hoch
Grenzen der Wirksamkeit	Besonders die Forderung nach redundanter Hardware ist – wenn überhaupt – nur schwer bzw. mit hohem Aufwand zu erfüllen, sofern es sich um Spezialsysteme handelt.

2.2.3 Übersicht Sicherheitsmechanismen Szenario 2

Die folgende Tabelle 19 liefert eine Kurzübersicht über die Maßnahmen, die zur Verringerung der als nicht tragbar eingestuften Risiken notwendig sind.

Tabelle 19: Übersicht über die Sicherheitsmechanismen für Szenario 2

Maß-nahme	Kurzbeschreibung	Wirkt gegen
M2.1.a	Sorgfältige Auswahl und sorgfältige vertragliche Einbindung der Service-Provider für DO-UB	R2.1, R2.4, R2.7
M2.1.b	Einsatz von speziellen Mechanismen zum Zugriffschutz, z. B. TCG	R2.1, R2.4, R2.7
M2.2	Vereinbarung einer verbindlichen Rahmen-Policy zwischen allen Ressourcenprovidern eines Grid	R2.1, R2.4, R2.7
M2.3	Einsatz vertrauenswürdiger Grid-Middleware	R2.3
M2.4	Konsequenter Einsatz der der Grid-Middleware vorgeschalteten Sicherheitsmechanismen	R2.9
M2.5	Verpflichtung aller Administratoren P-lad auf die vereinbarten Spielregeln	R2.4, R2.10
M2.6	Erweiterung der Grid-Middleware um Sicherheitsmechanismen	R2.2 - R2.5, R2.7 - R2.17
M2.7	Verfahren zur Zugriffs- und Zutrittskontrolle für Rechnersysteme in DO-UA, DO-UB	R2.12
M2.8	Lokales Sicherheitskonzept für jede Domäne DO-UA, DO-UB	R2.9, R2.12, R2.14, R2.15, R2.17
M2.9	Verfügbarkeitskonzept für jede Domäne DO-UB	R2.12, R2.14, R2.15, R2.17

2.2.4 Fazit für Szenario 2

Die Maßnahmen für Szenario 2 resultieren aus den nicht tragbaren Risiken (s. Tabelle 8; vgl. 1. „Sicherheitsmechanismen: Vorgehensweise“) für dieses Szenario (vgl. auch AP2 - Risikoanalyse). Aus der Analyse folgt, dass die nicht tragbaren Risiken hauptsächlich im Bereich der Vertrauenswürdigkeit der Kooperationspartner liegen (Maßnahme M2.1, Organisatorische Variante M2.1.a; Maßnahme M2.2; Maßnahme M2.5; Maßnahme M2.7). Auch sollten die technischen Risiken weitgehend durch in die Grid-Middleware integrierten Sicherheitsmechanismen abgedeckt werden (Maßnahme M2.3; Maßnahme M2.4; Maßnahme M2.6).

Hier zeigt sich erneut ein Grundproblem des Grid-Computing. „Rechenleistung aus der Steckdose“ bedingt den Transport von Eingabedaten zu den Rechenknoten, ebenso die Erzeugung und Speicherung der Ergebnisdaten auf den Rechenknoten. Die Rechenknoten sind entsprechend dem Grid-Paradigma räumlich entfernt und auch unter fremder administrativer Kontrolle. Besitzen diese Daten einen erhöhten Schutzbedarf (etwa geheime Entwicklungsdaten), so sind derzeit keine technischen Lösungen verfügbar, die eine unbefugte Manipulation in der fremden Domäne zuverlässig verhindern. Prinzipbedingt hat der Administrator eines Systems Zugriff auf alle Ressourcen des Systems und zwar auf allen Ebenen.

Maßnahmen zur Erhöhung des Aufwands einer Manipulation sind denkbar, z. B. indem Eingabedaten verschlüsselt zum CE übertragen und dort ebenfalls verschlüsselt gespeichert werden. Erst im Hauptspeicher erfolgt die Entschlüsselung. Damit kann das Risiko für die Manipulation kritischer Daten etwas verringert werden. Eine darüber hinaus gehende wirksame Maßnahme auf technischer Ebene ist derzeit noch nicht verfügbar, wird aber in „Maßnahme M2.1, Technische Variante M2.1.b“ aufgezeigt. Speziell zu TCG sei auf 3. „Sicherheitsmechanismen: Fazit“ verwiesen.

Darüber hinaus gilt auch hier, dass viele der nicht tragbaren Risiken in Bereichen liegen, die nicht Grid-spezifisch bzw. nicht nur im Grid-Umfeld relevant sind und denen heute üblicherweise bereits anderweitig (vgl. z. B. GSHB) begegnet wird. Sorgfältige Vertragsausgestaltung und Sicherheits- und Verfügbarkeitskonzepte (Maßnahme M2.8; Maßnahme M2.9) gehören dazu.

2.3 Szenario 3: Offenes e-Science Grid

Die Risiken aus Szenario 3, die entsprechend der Risikomatrix aus AP2 als nicht tragbar eingestuft werden (vgl. 1. „Sicherheitsmechanismen: Vorgehensweise“), sind in Tabelle 20 zusammengefasst.

Tabelle 20: Nicht tragbare Risiken gemäß Risikomatrix für Szenario 3

Schadenshöhe	Eintrittswahrscheinlichkeit	Risiko Nr.
sehr hoch	niedrig, mittel, hoch oder sehr hoch	R3.1
hoch	mittel, hoch oder sehr hoch	R3.2, R3.4, R3.17, R3.19
mittel	hoch oder sehr hoch	- keine -
niedrig	sehr hoch	- keine -

Gegen diese Risiken werden in den folgenden Abschnitten Maßnahmen entwickelt und beschrieben. Es wird zwischen Grid-spezifischen (vgl. Absatz 2.3.1) Maßnahmen und generellen Maßnahmen (vgl. Absatz 2.3.2) unterschieden.

2.3.1 Grid-spezifische Sicherheitsmaßnahmen für Szenario 3

Nachfolgend werden die Maßnahmen genauer spezifiziert und bewertet.

Tabelle 21: Maßnahme M3.1, Organisatorische Variante M3.1.a

Maßnahme	M3.1.a
Kurzbeschreibung	Sorgfältige Auswahl und sorgfältige vertragliche Einbindung der Kooperationspartner untereinander.
Ergebnis	Die Eintrittswahrscheinlichkeit von R3.1 wird weiter reduziert Die Eintrittswahrscheinlichkeit von R3.2 sinkt auf hoch bis mittel Die Eintrittswahrscheinlichkeit von R3.4 sinkt auf hoch bis mittel
Wirkt gegen	R3.1 (B3.1, Auswahl eines nicht vertrauenswürdigen Kooperationspartners) R3.2 (B3.2, lokaler Administrator P-lad manipuliert DA-z) R3.4 (B3.3, lokaler Administrator P-lad manipuliert DA-nz)
Aktion bei	Domänen- bzw. Policy-Verantwortliche in den DO-Px

Maßnahme	M3.1.a
Beschreibung	Bei Szenario 3 bestehen hohe Integritätsanforderungen an die Daten (DA-z und DA-nz). Nach heutigem Stand der Technik ist dies auch in diesem Szenario durchgängig nur mittels Kombination technischer und organisatorischer Maßnahmen möglich. Grundlage dieser Maßnahmen ist üblicherweise eine Vereinbarung zwischen den Kooperationspartnern. Dies ist auch bereits in der Beschreibung der organisatorischen Grundlagen der Grid-Bildung vorgesehen. Die Vereinbarungen sind dort als Policies, denen die Kooperationspartner zustimmen, beschrieben. Im vorliegenden Szenario sollten daher die Anforderungen an die Integrität von DA-z und DA-nz explizit festgelegt werden. Es liegt dann in der Verantwortung der Domänenverantwortlichen, organisationsintern für eine Umsetzung zu sorgen. Dazu gehört auch Maßnahme M3.3, bei der die P-lad entsprechend verpflichtet werden.
Aufwand	Mittel
Grenzen der Wirksamkeit	Verpflichtete P-l könnten sich nicht an die Verpflichtungsvereinbarung halten. Es sollten passende Sanktionierungen (etwa angemessene Vertragsstrafen bei Verletzung der Vertraulichkeit) vorgesehen werden. Maßnahme M3.1, Technische Variante M3.1.b, beschreibt eine technische Realisierungsvariante dieser Maßnahme mit gleicher Wirkung, die jedoch ebenfalls der vertraglichen Absicherung bedarf, damit die Programme beim Dienstleister ausführbar sind.

Tabelle 22: Maßnahme M3.1, Technische Variante M3.1.b

Maßnahme	M3.1.b
Kurzbeschreibung	Einsatz von speziellen Mechanismen zum Zugriffschutz, z. B. TCG
Ergebnis	Die Eintrittswahrscheinlichkeit von R3.1 wird weiter reduziert Die Eintrittswahrscheinlichkeit von R3.2 sinkt auf hoch bis mittel Die Eintrittswahrscheinlichkeit von R3.4 sinkt auf hoch bis mittel
Wirkt gegen	R3.1 (B3.1, Auswahl eines nicht vertrauenswürdigen Kooperationspartners) R3.2 (B3.2, lokaler Administrator P-lad manipuliert DA-z) R3.4 (B3.3, lokaler Administrator P-lad manipuliert DA-nz)
Aktion bei	Domänen- bzw. Policy-Verantwortliche in den DO-Px
Beschreibung	Bei einem Grid, das mit Daten dieser Vertraulichkeitsstufe arbeitet, sollte die durchgängige Verpflichtung aller Verantwortlichen P-l und der zugeordneten Administratoren P-lad auf den Einsatz hardwarebasierter TCG-Mechanismen erfolgen, etwa in Form geeigneter Dienstgütevereinbarungen (SLAs), die den Grad der jeweils sicherzustellenden Vertraulichkeit festschreiben. Mit diesen Mechanismen wäre es möglich, den Zugriff auf vertrauliche Daten auf signierte, d. h. hier authentische und integere, Programme zu beschränken.
Aufwand	Hoch (gesamte Hardware muss ersetzt werden, Umrüstung ist wahrscheinlich nicht möglich)

Maßnahme	M3.1.b
Grenzen der Wirksamkeit	Derzeit sind noch keine Hochleistungsrechnersysteme von mit TCG-basierter Hardware oder ähnlichen Hardwarezusätzen verfügbar. Für das vorliegende Szenario ist diese Maßnahme daher eine Möglichkeit für zukünftige Systeme. Die Anwendungen können dann nur noch auf TCG-basierter Hardware ausgeführt werden. D. h. der Einsatz muss nicht organisatorisch erzwungen werden. Daneben zeigt sich erfahrungsgemäß auf Dauer auch bei wirksamen und komplexen Mechanismen eine Möglichkeit diese zu umgehen. (Für weitere Erläuterungen zu TCG und ggf. weiteren Mechanismen s. 3. „Sicherheitsmechanismen: Fazit“.)

Tabelle 23: Maßnahme M3.2

Maßnahme	M3.2
Kurzbeschreibung	Vereinbarung einer verbindlichen Rahmen-Policy zwischen allen Ressourcenprovidern eines Grid
Ergebnis	Die Eintrittswahrscheinlichkeit von R3.1 wird weiter reduziert Die Eintrittswahrscheinlichkeit von R3.2 sinkt auf hoch bis mittel Die Eintrittswahrscheinlichkeit von R3.4 sinkt auf hoch bis mittel
Wirkt gegen	R3.1 (B3.1, Auswahl eines nicht vertrauenswürdigen Kooperationspartners) R3.2 (B3.2, lokaler Administrator P-lad manipuliert DA-z) R3.4 (B3.3, lokaler Administrator P-lad manipuliert DA-nz)
Aktion bei	Domänen- bzw. Policy-Verantwortliche in den DO-Px
Beschreibung	In der Rahmen-Policy werden domänenübergreifende, einheitliche und den Interessen aller Beteiligten entsprechende Regelungen getroffen. Alle Ressourcenprovider verpflichten sich zur Einhaltung dieser Regeln.
Aufwand	Niedrig (Umsetzung evtl. mittel)
Grenzen der Wirksamkeit	Einzelne Ressourcenprovider könnten sich evtl. nicht an die Regelungen halten. Es sind Sanktionen für den Fall des Verstoßes vorzusehen.

Tabelle 24: Maßnahme M3.3

Maßnahme	M3.3
Kurzbeschreibung	Verpflichtung aller Administratoren P-lad auf die vereinbarten Spielregeln

Maßnahme	M3.3
Ergebnis	Die Eintrittswahrscheinlichkeit von R3.2 sinkt auf hoch bis mittel Die Eintrittswahrscheinlichkeit von R3.4 sinkt auf hoch bis mittel
Wirkt gegen	R3.2 (B3.2, lokaler Administrator P-lad manipuliert DA-z) R3.4 (B3.3, lokaler Administrator P-lad manipuliert DA-nz)
Aktion bei	P-lad bei DO-x
Beschreibung	Hier handelt es sicher weniger um eine technische als um eine organisatorische Maßnahme.
Aufwand	Niedrig
Grenzen der Wirksamkeit	Gegen Fehlverhalten Einzelner gibt es keinen vollständigen Schutz. Einzelne Administratoren könnten sich evtl. fahrlässig oder vorsätzlich nicht an entsprechende Vorgaben halten. Es sind Sanktionen für den Fall des Verstoßes vorzusehen (vgl. Maßnahme M3.2).

Tabelle 25: Maßnahme M3.4

Maßnahme	M3.4
Kurzbeschreibung	Programmgesteuerter Integritätsschutz im Hauptspeicher
Ergebnis	Die Eintrittswahrscheinlichkeit von R3.2 sinkt auf mittel Die Eintrittswahrscheinlichkeit von R3.4 sinkt auf mittel
Wirkt gegen	R3.2 (B3.2, lokaler Administrator P-lad manipuliert DA-z) R3.4 (B3.3, lokaler Administrator P-lad manipuliert DA-nz)
Aktion bei	P-swp bei DO-x
Beschreibung	Analog zu der in Szenario 2 eingesetzten Verschlüsselung der Anwendungsdaten bei der Übertragung und bei der Speicherung sollen in diesem Szenario kryptographische Methoden zum Integritätsschutz auf Anwendungsebene erfolgen. Konkret wird unmittelbar vor Start der eigentlichen Berechnung ein programminterner Integritätscheck der Eingabedaten durchgeführt. Ebenso werden die Ergebnisdaten mit einem Integritätsmerkmal versehen bevor sie abgespeichert werden. Beispiel für einen solchen Mechanismus wäre die digitale Signatur.
Aufwand	Mittel
Grenzen der Wirksamkeit	Die P-lad haben auch Zugriff auf den Datenbereich jeden Prozesses (auch hier besteht das Problem, dass der lokale Administrator alle Programme, die zur Berechnung der Checksumme oder zur Signatur benötigt werden, „in der Hand hat“ und sowohl Eingabeparameter als auch die Berechnung selbst und sogar die Ergebnisse manipulieren kann). Es besteht also weiterhin die Möglichkeit, eine Manipulation vorzunehmen. Es ist jedoch mehr Aufwand und mehr technisches Know-How erforderlich, so dass die Eintrittswahrscheinlichkeit sinkt.

Tabelle 26: Maßnahme M3.5

Maßnahme	M3.5
Kurzbeschreibung	Verbindliche Einführung des CAS für VOs
Ergebnis	Die Eintrittswahrscheinlichkeit von R3.17 sinkt um ein bis zwei Stufen
Wirkt gegen	R3.17 (B3.15, Fehlerhafte Gestaltung des Grid Map File)
Aktion bei	Ressourcen-Provider, P-srv, P-hw, P-sw
Beschreibung	Die Autorisierung für jede Domäne, die über das Mapping-File erfolgt, wird – wie in Absatz 1.3.1.4.4.1 in [1] beschrieben – an den *Community Authorization Service* (CAS) delegiert. Der Aufwand liegt dann beim Betreiber des CAS und skaliert linear mit der Zahl der CE's.
Aufwand	Mittel
Grenzen der Wirksamkeit	Bis heute ist die Bereitschaft der Ressourcen-Provider gering, die Administrator-Rechte der Systeme, für die sie die Verantwortung tragen, an die VO abzugeben. CAS ist abwärtskompatibel, d. h. es wird auch hier ein lokales Mapping durchgeführt (CAS erhält sozusagen die Obermenge aller Rechte und vergibt diese dann feingranular an die Nutzer). Hier entsteht eine neue Gefahr durch die Kompromittierung des CAS.

Tabelle 27: Maßnahme M3.6

Maßnahme	M3.6
Kurzbeschreibung	Pflicht zur Signierung von im Grid eingesetzter Software
Ergebnis	Die Eintrittswahrscheinlichkeit von R3.17 sinkt um ein bis zwei Stufen
Wirkt gegen	R3.19 (B3.16, P-u setzt maliziöse Software ein)
Aktion bei	Forscher P-u, d.h. hier Nutzer von Software, die nicht zu SRV oder SW gehört
Beschreibung	Alle Programme, die nicht unter der Kontrolle von P-srv oder P-sw stehen müssen von Seiten des Erstellers signiert werden. Dies stellt sicher, dass auch der Ersteller maliziöser Software identifiziert werden kann. Daraus resultieren Sanktionsmöglichkeiten gegenüber dem Ersteller. Die Signierung der Software beinhaltet dann gleichzeitig die Verantwortung für die Freiheit von Schadfunktionen. Damit kann auch nicht signierte Software in der Verantwortung eines Nutzer signiert und eingesetzt werden. Die Ausführung unsignierter Software wird technisch verhindert.
Aufwand	Hoch

Maßnahme	M3.6
Grenzen der Wirksamkeit	Diese Maßnahme wirkt nicht unmittelbar gegen vorsätzliche Handlungen. D.h. ein böswilliger Nutzer P-u würde nicht ummittelbar daran gehindert eine maliziöse Software zur Ausführung zu bringen. Allerdings müsste er befürchten, dass das Einbringen der Software in das Grid bis zu ihm persönlich zurückverfolgt werden kann. Dies bedingt, dass die Nutzer auch über diese Möglichkeit und die ggf. folgenden Sanktionen informiert werden.

2.3.2 Generelle Sicherheitsmaßnahmen für Szenario 3

Es wird von Schutzmaßnahmen auf Ebene des Grundschutzhandbuchs ausgegangen. Diese Voraussetzung wurde in der Risikoanalyse bei der Risikoeinschätzung berücksichtigt. Für über diesen Grundschutz hinaus gehende generelle, d. h. nicht Grid-spezifische Maßnahmen wurde in Szenario 3 kein Bedarf identifiziert.

2.3.3 Übersicht Sicherheitsmechanismen Szenario 3

Die folgende Tabelle 28 liefert eine Kurzübersicht über die Maßnahmen, die zur Verringerung der als nicht tragbar eingestuften Risiken notwendig sind.

Tabelle 28: Übersicht über die Sicherheitsmechanismen für Szenario 3

Maßnahme	Kurzbeschreibung	Wirkt gegen
M3.1.a	Sorgfältige Auswahl und sorgfältige vertragliche Einbindung der Kooperationspartner untereinander.	R3.1, R3.2, R3.4
M3.1.b	Einsatz von speziellen Mechanismen zum Zugriffschutz, z. B. TCG	R3.1, R3.2, R3.4
M3.2	Vereinbarung einer verbindlichen Rahmen-Policy zwischen allen Ressourcenprovidern eines Grid	R3.1, R3.2, R3.4
M3.3	Verpflichtung aller Administratoren P-lad auf die vereinbarten Spielregeln	R3.2, R3.4
M3.4	Programmgesteuerter Integritätsschutz im Hauptspeicher	R3.2, R3.4
M3.5	Verbindliche Einführung des CAS für VOs	R3.17
M3.6	Pflicht zur Signierung von im Grid eingesetzter Software	R3.19

2.3.4 Fazit für Szenario 3

Die Maßnahmen für Szenario 3 resultieren aus den nicht tragbaren Risiken (s. Tabelle 20; vgl. 1. „Sicherheitsmechanismen: Vorgehensweise“) für dieses Szenario (vgl. auch AP2 - Risikoanalyse). Nicht tragbare Risiken liegen demnach hauptsächlich im Bereich der Vertrauenswürdigkeit der Kooperationspartner (Maßnahme M3.1, Organisatorische Variante M3.1.a; Maßnahme M3.2; Maßnahme M3.3). Die technischen Risiken sind sehr weit gehend durch die in Globus integrierten Sicherheitsmechanismen abgedeckt (Maßnahme M3.5). Speziell zu TCG sei auf 3. „Sicherheitsmechanismen: Fazit“ verwiesen.

Hier zeigt sich erneut ein Grundproblem des Grid-Computing. „Rechenleistung aus der Steckdose“ bedingt den Transport von Eingabedaten zu den Rechenknoten, ebenso die Erzeugung und Speicherung der Ergebnisdaten auf den Rechenknoten. Die Rechenknoten sind entsprechend dem Grid-Paradigma räumlich entfernt und auch unter fremder administrativer Kontrolle. Besitzen diese Daten eine erhöhten Schutzbedarf, oder wie in diesem Szenario einen hohen Bedarf an Integrität, so sind derzeit keine technischen Lösungen verfügbar, die eine unbefugte Manipulation in der fremden Domäne zuverlässig verhindern. Prinzipbedingt hat der Administrator eines Systems Zugriff auf alle Ressourcen des Systems, und zwar auf allen Ebenen.

Allerdings sind Maßnahmen zur Erhöhung des Aufwands für eine Manipulation möglich. Einen Ansatz hierfür zeigt Szenario 2 auf. Hier werden die Eingabedaten verschlüsselt zum CE übertragen dort gespeichert. Erst im Hauptspeicher erfolgt die Entschlüsselung. Analog sind im vorliegenden Szenario kryptographische Maßnahmen zum Integritätsschutz sowie die Signierung der eingesetzten Software ratsam (Maßnahme M3.4; Maßnahme M3.6). Damit kann das Risiko für die Manipulation kritischer Daten und zur Beeinträchtigung durch maliziöse Software etwas verringert werden. Eine darüber hinaus gehende wirksame Maßnahme auf technischer Ebene ist derzeit noch nicht verfügbar, wird aber in „Maßnahme M3.1, Technische Variante M3.1.b“ aufgezeigt. Daneben kann – wie in jedem Globus-Szenario – das Risiko einer falschen Konfiguration des Grid Map File durch Einsatz von CAS verringert werden (Maßnahme M3.5).

2.4 Szenario 4: Grids mit personenbezogenen bzw. personenbeziehbaren Daten (z. B. Mammo-Grid)

Die Risiken aus Szenario 4, die entsprechend der Risikomatrix aus AP2 als nicht tragbar eingestuft werden (vgl. 1. „Sicherheitsmechanismen: Vorgehensweise“), sind in Tabelle 29 zusammengefasst.

Tabelle 29: Nicht tragbare Risiken gemäß Risikomatrix für Szenario 4

Schadenshöhe	Eintrittswahrscheinlichkeit	Risiko Nr.
sehr hoch	niedrig, mittel, hoch oder sehr hoch	R4.3, R4.4, R4.14, R4.15, R4.26, R4.27
hoch	mittel, hoch oder sehr hoch	R4.2, R4.7, RK4.5
mittel	hoch oder sehr hoch	R4.24
niedrig	sehr hoch	R4.11, R4.12

Gegen diese Risiken werden in den folgenden Abschnitten Maßnahmen entwickelt und beschrieben. Es wird zwischen Grid-spezifischen (vgl. Absatz 2.4.1) Maßnahmen und generellen Maßnahmen (vgl. Absatz 2.4.2) unterschieden. Zusätzlich werden für alle Grid-spezifischen Risiken (RK) Maßnahmen definiert.

2.4.1 Grid-spezifische Sicherheitsmechanismen für Szenario 4

Nachfolgend werden die Maßnahmen genauer spezifiziert und bewertet.

Tabelle 30: Maßnahme M4.1, Organisatorische Variante M4.1.a

Maßnahme	M4.1.a
Kurzbeschreibung	Verpflichtung aller P-lad auf das Datenschutzgeheimnis

Maßnahme	M4.1.a
Ergebnis	Die Eintrittswahrscheinlichkeit von R4.7 sinkt auf niedrig Die Eintrittswahrscheinlichkeit von R4.11 sinkt auf niedrig. Die Eintrittswahrscheinlichkeit von R4.12 sinkt auf niedrig.
Wirkt gegen	R4.7 (B4.6, P-lad manipulieren die Pseudonymisierungssoftware) R4.11 (B4.10, P-lad greifen unberechtigt auf DA-zp oder DA-z zu) R4.12 (B4.11, P-lad manipuliert Patientendaten)
Aktion bei	Domänenverantwortliche DO-srv, DO-sw, DO-hw
Beschreibung	An der Administration komplexer verteilter Infrastrukturen sind in der Regel zahlreiche Personen P-lad beteiligt. Speziell für Szenario 4 muss die Vertraulichkeit der personenbeziehbaren Daten (DA-zp und DA-z) gewährleistet werden. Nach heutigem Stand der Technik ist das durchgängig nur mittels organisatorischer Maßnahmen möglicht. Bei einem Grid,, das mit personenbeziehbaren Daten arbeitet, sollte daher die durchgängige Verpflichtung aller Administratoren P-lad auf das Datenschutzgeheimnis erfolgen. Diese Verpflichtung sollte eine Komponente der in Maßnahme M4.2 beschriebenen Datenschutz-Policy sein.
Aufwand	Mittel
Grenzen der Wirksamkeit	Verpflichtete P-lad könnten sich nicht an die Verpflichtungserklärung halten. Es sollten passende Sanktionierungen vorgesehen werden (teilweise ohnehin gegeben, z. B. ist Verrat von Patientengeheimnissen ein Straftatbestand). Maßnahme M4.1, Technische Variante M4.1.b, beschreibt eine technische Realisierungsvariante dieser Maßnahme mit gleicher Wirkung.

Tabelle 31: Maßnahme M4.1, Technische Variante M4.1.b

Maßnahme	M4.1.b
Kurzbeschreibung	Einsatz von speziellen Mechanismen zum Zugriffschutz, z. B. TCG
Ergebnis	Die Eintrittswahrscheinlichkeit von R4.7 sinkt auf niedrig. Die Eintrittswahrscheinlichkeit von R4.11 sinkt auf niedrig. Die Eintrittswahrscheinlichkeit von R4.12 sinkt auf niedrig
Wirkt gegen	R4.7 (B4.6, P-lad manipulieren die Pseudonymisierungssoftware) R4.11 (B4.10, P-lad greifen unberechtigt auf DA-zp oder DA-z zu) R4.12 (B4.11, P-lad manipuliert Patientendaten)
Aktion bei	Domänenverantwortliche DO-srv, DO-sw, DO-hw

Maßnahme	M4.1.b
Beschreibung	In Zukunft werden Technologien verfügbar sein, die den Zugriff lokaler Administratoren auf Daten des von Ihnen administrierten Rechners über Mechanismen auf Hardwareebene einschränken. Diese Mechanismen werden allgemein als TCG-Mechanismen bezeichnet.
Aufwand	Hoch (gesamte Hardware muss ersetzt werden, Umrüstung ist wahrscheinlich nicht möglich)
Grenzen der Wirksamkeit	Erfahrungsgemäß zeigt sich auf Dauer auch bei wirksamen und komplexen Mechanismen eine Möglichkeit diese zu umgehen. (Für weitere Erläuterungen zu TCG und ggf. weiteren Mechanismen s. 3. „Sicherheitsmechanismen: Fazit“.)

Tabelle 32: Maßnahme M4.2

Maßnahme	M4.2
Kurzbeschreibung	Vereinbarung einer verbindlichen Datenschutz-Policy zwischen allen Ressourcenprovidern eines Grid
Ergebnis	Die Eintrittswahrscheinlichkeit von R4.12 sinkt auf mittel
Wirkt gegen	R4.12 (B4.11, Ressourcenprovider greifen unberechtigt auf DA-zp oder DA-z zu)
Aktion bei	Domänenverantwortliche DO-srv, DO-sw, DO-hw
Beschreibung	In der Datenschutz-Policy werden domänenübergreifende, einheitliche und dem Datenschutzgesetz (BDSG) entsprechende Regelungen getroffen. Alle Ressourcenprovider verpflichten sich zur Einhaltung dieser Regeln.
Aufwand	Niedrig (Umsetzung evtl. mittel)
Grenzen der Wirksamkeit	Einzelne Ressourcenprovider könnten sich evtl. nicht an die Regelungen halten. Es sind Sanktionen für den Fall des Verstoßes vorzusehen.

Tabelle 33: Maßnahme M4.3

Maßnahme	M4.3
Kurzbeschreibung	Erweiterung der Grid-Middleware um Auditing-Funktionen
Ergebnis	Die Eintrittswahrscheinlichkeit für R4.24 sinkt auf mittel
Wirkt gegen	R4.24 (B 4.23, keine ausreichende Auditing-Funktionalität)
Aktion bei	Entwickler der Grid-Middleware, P-srv

Maßnahme	M4.3
Beschreibung	Die Grid-Middleware-Komponenten, die für den Transport von Daten zuständig sind, d. h. GridFTP und RFTP werden um eine Auditing-Funktionalität erweitert. Dies ermöglicht das für ein Grid zentrale Erfassen und Nachverfolgen aller Datentransporte mit diesen beiden Werkzeugen. Die Auditdaten stehen dann an zentraler Stelle für ggf erforderliche datenschutzrechtliche Auswertungen zur Verfügung.
Aufwand	Mittel bis hoch
Grenzen der Wirksamkeit	Datentransporte auf Applikationsebene, bspw. mittels der Kommunikations-API der verwendeten Bibliothek zur parallelen Programmierung, können so nicht nachvollzogen werden (vgl. dazu die folgende Maßnahme M4.4). Um diese Maßnahme umzusetzen, müssen auch die Replikationsdienste entsprechend erweitert werden. Die Ortstransparenz, die manche Replikationsdienste bieten ist hier allerdings kontraproduktiv (um z. B. beweisen können, dass man alle Daten gelöscht hat, muss man alle Replikate kennen).

Tabelle 34: Maßnahme M4.4

Maßnahme	M4.4
Kurzbeschreibung	Erweiterung der der Programmier-API um Auditing-Funktionen
Ergebnis	Die Eintrittswahrscheinlichkeit für R4.24 sinkt auf niedrig
Wirkt gegen	R4.24 (B4.23, keine ausreichende Auditing-Funktionalität)
Aktion bei	Entwickler der API, P-sw
Beschreibung	Die Kommunikations-Bibliotheken der API zur parallelen Programmierung wird mit Funktionen zum Nachvollziehen von Kommunikationsvorgängen ausgestattet. Dies ermöglicht das für ein Grid zentrale Erfassen aller Datentransporte der eingesetzten Software. Die Audit-Daten stehen dann an zentraler Stelle für ggf. erforderliche datenschutzrechtliche Auswertungen zur Verfügung.
Aufwand	Sehr hoch (alle API müssen erweitert und alle Sofwarekomponenten neu kompiliert oder zumindest neu gebunden (gelinkt) werden)
Grenzen der Wirksamkeit	Die ohnehin zeitkritische Kommunikation in Grid-Systemen würde noch langsamer, die Zahl der sinnvoll parallelisierbaren Applikationen geringer (vgl. „*Amdahls Law*“, nach dem der mögliche Geschwindigkeitszuwachs bei Parallelisierung vor allem durch den nicht parallelisierbaren Anteil eines Problems beschränkt ist). Es ist zu erwarten, dass eine solche Modifikation auf keine positive Resonanz in der „Grid-Community“ stoßen würde. Die Autoren schätzen daher die Wahrscheinlichkeit der Umsetzung dieser Maßnahme als ausgesprochen gering ein.

Tabelle 35: Maßnahme M4.5

Maßnahme	M4.5
Kurzbeschreibung	Erweiterung von GridFTP um Komponentenauthentisierung
Ergebnis	Die Eintrittswahrscheinlichkeit der durch RK4.3 induzierten Risiken sinkt um eine Stufe
Wirkt gegen	RK4.3 (BK4.1, Authentizität der kommunizierenden Instanzen)
Aktion bei	Entwickler der Grid-Middleware, P-srv
Beschreibung	Die an GridFTP beteiligten Instanzen werden mit einem Authentisierungs- und Autorisierungsmechanismus ähnlich dem „MyProxy"-Mechanismus auf Absatz 1.3.1.4.4 ausgestattet. Damit wird sichergestellt, dass nur vom Benutzer authentisierte und autorisierte Instanzen miteinander kommunizieren.
Aufwand	Hoch
Grenzen der Wirksamkeit	Hängt von der Handhabung des Proxy Certification File ab (vgl. Maßnahme M4.10 und Maßnahme M4.11)

Tabelle 36: Maßnahme M4.6

Maßnahme	M4.6
Kurzbeschreibung	GRAM Job Control Authentisierung
Ergebnis	Die Eintrittswahrscheinlichkeit der durch RK4.4 induzierten Risiken sinkt um eine Stufe
Wirkt gegen	RK4.4 (BK4.2, Authentizität von GRAM und GRAM-Adapter)
Aktion bei	Entwickler der Grid-Middleware, P-srv
Beschreibung	GRAM und GRAM-Adapter werden mit einem Authentisierungs- und Autorisierungsmechanismus ähnlich dem „MyProxy"-Mechanismus auf Absatz 1.3.1.4.4 in [1] ausgestattet. Damit wird sichergestellt, dass nur vom Benutzer authentisierte und autorisierte Instanzen miteinander kommunizieren .
Aufwand	Hoch
Grenzen der Wirksamkeit	Hängt von der Handhabung des Proxy Certification File ab (vgl. Maßnahme M4.9 und Maßnahme M4.10)

Tabelle 37: Maßnahme M4.7

Maßnahme	M4.7
Kurzbeschreibung	Verbindliche Einführung des CAS für VOs

Maßnahme	M4.7
Ergebnis	Die Eintrittswahrscheinlichkeit der durch RK4.5 induzierten Risiken sinkt auf niedrig bis mittel
Wirkt gegen	RK4.5 (BK4.3, Hohe Komplexität und hoher Aufwand bei der Handhabung des Mapping File)
Aktion bei	Ressourcen-Provider, P-srv, P-hw, P-sw
Beschreibung	Die Autorisierung, die wie in Risiko RK4.5 für jede Domäne über das Mapping-File erfolgt, wird – wie in Absatz 1.3.1.4.4.1 in [1] beschrieben – an den *Community Authorization Service* (CAS) delegiert. Der Aufwand liegt dann beim Betreiber des CAS und skaliert linear mit der Zahl der CE's.
Aufwand	Mittel
Grenzen der Wirksamkeit	Bis heute ist die Bereitschaft der Ressourcen-Provider gering, die Administrator-Rechte der Systeme, für die sie die Verantwortung tragen n die VO abzugeben.

Tabelle 38: Maßnahme M4.8

Maßnahme	M4.8
Kurzbeschreibung	Starke Authentisierung der Client-Nutzer/Client-Systeme gegenüber der Middleware
Ergebnis	Die Eintrittswahrscheinlichkeit der durch RK4.2 induzierten Risiken sinkt um eine bis zwei Stufen
Wirkt gegen	RK4.2 (BK4.5, Nur einfache Authentisierung der Client-Nutzer/Client-Systeme)
Aktion bei	Datenerheber P-e, Grid Nutzer P-u
Beschreibung	Die Client-Systeme werden um Mechanismen zu starken Authentisierung erweitert (bspw. Zwei-Wege-Authentisierung). Ebenso wird sichergestellt, dass nur autorisierte Client-Systeme Zugriff auf das Grid erhalten.
Aufwand	Hoch
Grenzen der Wirksamkeit	Begrenzt durch das Nutzerverhalten beim Einsatz der Authentisierungsmechanismen

Tabelle 39: Maßnahme M4.9

Maßnahme	M4.9
Kurzbeschreibung	Sichere Speicherung des Proxy Certification File
Ergebnis	Die Eintrittswahrscheinlichkeit der durch RK4.6 induzierten Risiken sinkt um eine Stufe

Maßnahme	M4.9
Wirkt gegen	RK4.6 (BK4.6: Zugriff auf „Proxy Certification Files“)
Aktion bei	P-srv, P-hw
Beschreibung	Die Vertraulichkeit des Proxy Certification File wird durch auf Betriebssystemebene verfügbare Zugriffskontrollmechanismen sichergestellt.
Aufwand	Niedrig
Grenzen der Wirksamkeit	Der Administrator eines Rechners kann weiterhin das Proxy Certification File und damit den temporären privaten Schlüssel eines Grid Nutzers einsehen und damit in dessen Namen handeln.

Tabelle 40: Maßnahme M4.10

Maßnahme	M4.10
Kurzbeschreibung	Zugriff auf das Proxy Certification File nur durch Grid-Middleware-Komponenten
Ergebnis	Die Eintrittswahrscheinlichkeit der durch RK4.6 induzierten Risiken sinkt um eine bis zwei Stufen
Wirkt gegen	RK4.6 (BK4.6, Zugriff auf „Proxy Certification Files“)
Aktion bei	P-srv, P-hw
Beschreibung	Das Proxy Certification File wird zusätzlich verschlüsselt und kann dann nur durch einen in die Grid-Middleware eingebrachten Schlüssel gelesen werden.
Aufwand	Niedrig
Grenzen der Wirksamkeit	Der Aufwand für einen Zugriff des Administrators eines Rechners wird wesentlich erhöht, jedoch prinzipbedingt nicht gänzlich verhindert werden können.

2.4.2 Generelle Sicherheitsmaßnahmen für Szenario 4

Tabelle 41: Maßnahme M4.11

Maßnahme	M4.11
Kurzbeschreibung	Verfahren zur Zugriffs- und Zutrittskontrolle für Rechnersysteme in DO-e
Ergebnis	Die Wahrscheinlichkeit für R4.2 sinkt auf niedrig Die Wahrscheinlichkeit für R4.15 kann weiter abgesenkt werden

Maßnahme	M4.11
Wirkt gegen	R4.2 (B4.2, P-p greift unberechtigt auf DA-zpp eines anderen zu) R4.15 (B4.14, DA-zpp werden durch P-p manipuliert)
Aktion bei	Verantwortlicher für Domäne DO-e
Beschreibung	Für jede der Domänen DO-e wird ein Verfahren zur Zugriffs- und Zutrittskontrolle für Rechnersysteme nach Grundschutzhandbuch entworfen und implementiert. Die vom Betriebsystem bereitgestellten Zugriffskontrollmechanismen werden aktiviert und genutzt. Zutrittskontrolle wird auf organisatorischer Ebene implementiert.
Aufwand	(nicht allgemein abschätzbar, da stark von den lokalen Randbedingungen abhängig)
Grenzen der Wirksamkeit	Benutzerverhalten

Tabelle 42: Maßnahme M4.12

Maßnahme	M4.12
Kurzbeschreibung	Lokales Sicherheitskonzept für jede Domäne DO-e
Ergebnis	Eintrittwahrscheinlichkeit für R4.2 sinkt auf niedrig Eintrittwahrscheinlichkeit für R4.3 sinkt auf mittel Eintrittwahrscheinlichkeit für R4.4 wird weiter abgeschwächt Eintrittwahrscheinlichkeit für R4.14 wird weiter abgeschwächt Eintrittwahrscheinlichkeit für R4.15 wird weiter abgeschwächt
Wirkt gegen	R4.2 (B4.2, P-p greift unberechtigt auf DA-zpp eines anderen zu) R4.3, R4.4 (B4.3, Angreifer P-x erlangt gezielt Zugriff auf die DA-zpp (Personendaten)) R4.14 (B4.13, DA-zpp werden innerhalb DO-e durch P-lad manipuliert) R4.15 (B4.14, DA-zpp werden innerhalb DO-e durch P-p manipuliert)
Aktion bei	Verantwortlicher für DO-e
Beschreibung	Für jede der Domänen DO-e wird ein Sicherheitskonzept nach Grundschutzhandbuch entworfen und implementiert. Dieses umfasst insbesondere die Absicherung der lokalen Systeme auf Betriebssystem- und Netzebene, des weiteren Zugriffs- und Zutrittskontrollmechanismen (vgl. Maßnahme M4.13).
Aufwand	Hoch
Grenzen der Wirksamkeit	-

Tabelle 43: Maßnahme M4.13

Maßnahme	M4.13
Kurzbeschreibung	Verfügbarkeitskonzept für jede Domäne DO-e
Ergebnis	Schadenshöhe R4.26 sinkt auf mittel
Wirkt gegen	R4.26 (B4.25, Störungsszenario, Löschung von Patientendaten durch Fehlhandlung)
Aktion bei	Verantwortlicher DO-e
Beschreibung	Für jede der Domänen DO-e wird ein Sicherheitskonzept für den Störungsfall nach Grundschutzhandbuch entworfen und implementiert. Dieses umfasst insbesondere die Redundanzen (zuverlässiges und schnell verfügbares Backup), um Verfügbarkeitsanforderungen zu erfüllen.
Aufwand	Hoch
Grenzen der Wirksamkeit	-

Tabelle 44: Maßnahme M4.14

Maßnahme	M4.14
Kurzbeschreibung	Katastrophenkonzept für jede Domäne DO-e
Ergebnis	Schadenshöhe R4.27 sinkt auf mittel
Wirkt gegen	R4.27 (B4.25, Katastrophenszenario, Löschung der Patientendaten durch höhere Gewalt)
Aktion bei	Verantwortlicher DO-e
Beschreibung	Für jede der Domänen DO-e wird ein Sicherheitskonzept für den Katastrophenfall nach Grundschutzhandbuch entworfen und implementiert. Dieses umfasst insbesondere die Redundanzen (Reservesysteme, Backup), um Verfügbarkeitsanforderungen gegen den Katastrophenfall zu erfüllen.
Aufwand	Hoch
Grenzen der Wirksamkeit	-

Tabelle 45: Maßnahme M4.15

Maßnahme	M4.15
Kurzbeschreibung	Lokales Sicherheitskonzept für jede Domäne DO-zpp

Maßnahme	M4.15
Ergebnis	Eintrittwahrscheinlichkeit für R4.2 sinkt auf niedrig Eintrittwahrscheinlichkeit für R4.14 wird weiter abgesenkt
Wirkt gegen	R4.2 (B4.2, P-p greift unberechtigt auf DA-zpp eines anderen zu) R4.14 (B4.13, DA-zpp werden innerhalb DO-e durch P-lad manipuliert)
Aktion bei	Verantwortlicher für DO-zpp
Beschreibung	Für jede der Domänen DO-zpp wird ein Sicherheitskonzept nach Grundschutzhandbuch entworfen und implementiert. Dieses umfasst insbesondere die Absicherung der lokalen Systeme auf Betriebssystem- und Netzebene, des weiteren Zugriffs- und Zutrittskontroll-mechanismen (vgl. Maßnahme M4.11).
Aufwand	Hoch
Grenzen der Wirk-samkeit	-

2.4.3 Übersicht Sicherheitsmechanismen Szenario 4

Die folgende Tabelle 46 liefert eine Kurzübersicht über die Maßnahmen, die zur Verringerung der als nicht tragbar eingestuften Risiken notwendig sind.

Tabelle 46: Übersicht über die Sicherheitsmechanismen für Szenario 4

Maß-nahme	Kurzbeschreibung	Wirkt gegen
M4.1.a	Verpflichtung aller P-lad auf das Datenschutzgeheimnis	R4.7, R4.11, R4.12
M4.1.b	Einsatz von speziellen Mechanismen zum Zugriffschutz, z. B. TCG	R4.7, R4.11, R4.12
M4.2	Vereinbarung einer verbindlichen Datenschutz-Policy zwischen allen Ressourcen-providern eines Grid	R4.12
M4.3	Erweiterung der Grid-Middleware um Auditing-Funktionen	R4.24
M4.4	Erweiterung der der Programmier-API um Auditing-Funktionen	R4.24
M4.5	Erweiterung von GridFTP um Komponentenauthentisierung	RK4.3
M4.6	GRAM Job Control Authentisierung	RK4.4
M4.7	Verbindliche Einführung des CAS für VOs	RK4.5
M4.8	Starke Authentisierung der Client-Nutzer/Client-Systeme gegenüber der Middleware	RK4.2
M4.9	Sichere Speicherung des Proxy Certification File	RK4.6
M4.10	Zugriff auf das Proxy Certification File nur durch Grid-Middleware-Komponenten	RK4.6
M4.11	Verfahren zur Zugriffs- und Zutrittskontrolle für Rechnersysteme in DO-e	R4.2, R4.15
M4.12	Lokales Sicherheitskonzept für jede Domäne DO-e	R4.2, R4.3, R4.4, R4.14, R4.15
M4.13	Verfügbarkeitskonzept für jede Domäne DO-e	R4.26
M4.14	Katastrophenkonzept für jede Domäne DO-e	R4.27
M4.15	Lokales Sicherheitskonzept für jede Domäne DO-zpp	R4.2, R4.14

2.4.4 Fazit für Szenario 4

Die Maßnahmen für Szenario 4 resultieren aus den nicht tragbaren Risiken (s. Tabelle 29; vgl. 1. „Sicherheits-mechanismen: Vorgehensweise“) für dieses Szenario (vgl. auch AP2 - Risikoanalyse). Aus der Analyse folgt, dass die nicht tragbaren Risiken nicht nur im Bereich der Vertrauenswürdigkeit der Kooperationspartner liegen, sondern dass hier dem Datenschutz besondere Aufmerksamkeit gewidmet werden muss. Daher wird hier besonderer Wert auf entsprechende Verpflichtungen der Administratoren (Maßnahme M4.1, Organisatorische Variante M4.1.a; Maßnahme M4.2), auf wirksame Authentisierungsmechanismen (Maßnahme M4.5; Maßnahme M4.6; Maßnahme M4.8; Maßnahme M4.9; Maßnahme M4.10; Maßnahme M4.11) und auf entsprechende Auditing-Funktionen

(Maßnahme M4.3; Maßnahme M4.4) gelegt. Daneben kann – wie in jedem Globus-Szenario – das Risiko einer Kompromittierung des Grid Map File durch Einsatz von CAS verringert werden (Maßnahme M4.7).

Daneben sind Maßnahmen zur Sicherstellung ausreichender Verfügbarkeit und zum Schutz vor Katastrophen erforderlich (Maßnahme M4.12; Maßnahme M4.13; Maßnahme M4.14; Maßnahme M4.15). Eine wirksame Maßnahme, um auf technischer Ebene Schutz gegen unbefugten Zugriff durch Administratoren zu gewährleisten, ist derzeit noch nicht verfügbar, wird aber in „Maßnahme M3.1, Technische Variante M3.1.b“ aufgezeigt. Speziell zu TCG sei auf 3. „Sicherheitsmechanismen: Fazit“ verwiesen.

2.5 Szenario 5: Sicherheitskritisches national wichtiges Grid / Katastrophenschutz (K-Grid)

Die Risiken aus Szenario 5, die entsprechend der Risikomatrix aus AP2 als nicht tragbar eingestuft werden (vgl. 1. „Sicherheitsmechanismen: Vorgehensweise“), sind in Tabelle 47 zusammengefasst.

Tabelle 47 Nicht tragbare Risiken gemäß Risikomatrix für Szenario 5

Schadenshöhe	Eintrittswahrscheinlichkeit	Risiko Nr.
sehr hoch	niedrig, mittel, hoch oder sehr hoch	R5.1, R5.2, R5.3, R5.10- R5.15, R5.18, R5.19
hoch	mittel, hoch oder sehr hoch	R5.4, R5.7, R5.9, R5.17
mittel	hoch oder sehr hoch	- keine -
niedrig	sehr hoch	- keine -

Gegen diese Risiken werden in den folgenden Abschnitten Maßnahmen entwickelt und beschrieben.

2.5.1 Sicherheitsmaßnahmen für Szenario 5

Nachfolgend werden die Maßnahmen genauer spezifiziert und bewertet. Dabei werden vor allem organisatorische Maßnahmen berücksichtigt. Als technische Maßnahmen kommen zusätzlich zwar solche infrage, die in den vorhergehenden Szenarien bereits dargestellt wurden. Aber wegen des hohen Abstraktionsgrades einerseits und der Ausrichtung auf die konkreten Gegebenheiten in den beteiligten Organisationen andererseits, deren detaillierte Berücksichtigung den Rahmen dieser Studie sprengen würde, werden hier konkrete technische Maßnahmen nur in geringem Umfang vorgeschlagen.

Tabelle 48 Maßnahme M5.1

Maßnahme	M5.1
Kurzbeschreibung	Erarbeitung spezifischer Vorschriften, Gesetze und Verordnungen, die alle wesentlichen für das Bilden und Betreiben eines K-Grid erforderlichen Randbedingungen, Voraussetzungen, Verantwortlichkeiten und Anforderungen festschreiben.
Ergebnis	Die Eintrittswahrscheinlichkeit der Risiken wird überhaupt erst beherrschbar
Wirkt gegen	alle Risiken, speziell R5.1 (B5.1, Auswahl nicht geeigneter Partner in der Phase der Bildung des Grid) R5.2 (B5.2, Erforderliche Grid-Ressourcen fallen während der Nutzung aus)
Aktion bei	Gesetzgeber
Beschreibung	Die Rahmenbedingungen für den Betrieb eines dem jeweiligen Anforderungsfall entsprechenden K-Grid müssen wegen der besonderen Betriebssituation und der sehr unterschiedlichen Ressourcenprovider – verbindlich vorgegeben werden.
Aufwand	Mittel bis hoch

Maßnahme	M5.1
Grenzen der Wirksamkeit	Die Einhaltung der gesetzlichen Vorschriften kann nicht als uneingeschränkt vorausgesetzt werden. Es sind angemessene Sanktionen gegen Verstöße vorzusehen. Es können in einem Katastrophenfall Situationen auftreten, die so nicht vorhergesehen wurden. Hier müssen den Verantwortlichen ausreichende Spielräume gewährt werden.

Tabelle 49 Maßnahme M5.2

Maßnahme	M5.2
Kurzbeschreibung	Sorgfältige Auswahl und sorgfältige vertragliche/gesetzliche Einbindung der beteiligten Provider von Grid-Ressourcen
Ergebnis	Die Eintrittswahrscheinlichkeit von R5.1 wird weiter reduziert
Wirkt gegen	R5.1 (B5.1, Auswahl nicht geeigneter Partner in der Phase der Bildung des Grid)
Aktion bei	Domänen- bzw. Policy-Verantwortliche P-dap/P-lad bei allen beteiligten Domänen, besonders bei DO-FW
Beschreibung	Bei Szenario 5 muss die Funktionsfähigkeit des Grid „bei Bedarf“ schnellstens gewährleistet werden. Hier müssen daher spezifische, an die jeweils relevanten (hier nicht allgemein betrachteten) Katastrophenszenarien, Anforderungen definiert und deren Einhaltung gewährleistet werden. Hier sind vor allem gesetzliche Vorschriften und ergänzende Verordnungen erforderlich, deren Einhaltung auch praktisch gesichert sein muss (vgl. Maßnahme M5.1).
Aufwand	Hoch
Grenzen der Wirksamkeit	Bei der Auswahl der Grid-Ressourcen und ihrer Betreiber muss Wert auf persönliche, institutionelle und technische Zuverlässigkeit und Einhaltung der betreffenden Gesetze und Vorschriften gelegt werden.

Tabelle 50 Maßnahme M5.3

Maßnahme	M5.3
Kurzbeschreibung	Regelmäßige Überprüfung von Aufbaufähigkeit und anschließender Funktionsfähigkeit des Grid in Form von Katastrophenübungen.
Ergebnis	Die Eintrittswahrscheinlichkeit von R5.1 wird weiter reduziert

Maßnahme	M5.3
Wirkt gegen	R5.1 (B5.1, Auswahl nicht geeigneter Partner in der Phase der Bildung des Grid) R5.2 (B5.2, Erforderliche Grid-Ressourcen fallen während der Nutzung aus) R5.4 (B5.3, Einsatzkräfte liefern falsche Eingabedaten) R5.5 (B5.4, Datenprovider liefern falsche Basisdaten)
Aktion bei	Domänen- bzw. Policy-Verantwortliche P-dap/P-lad bei allen beteiligten Domänen, besonders bei DO-FW
Beschreibung	Da ein K-Grid erst im Bedarfsfall (=Katastrophenfall) in Betrieb genommen wird, ist die regelmäßige Überprüfung von Aufbaufähigkeit und anschließender Funktionsfähigkeit des Grid (einschl. der Eingabe- und Basisdaten) im Rahmen von Katastrophenübungen ständig neu zu verifizieren.
Aufwand	Hoch
Grenzen der Wirksamkeit	Während der Ausfall von Grid-Ressourcen im Rahmen einer Übung simuliert und dann ggf. aufgefangen werden kann, sind die Risiken R5.3 und R5.4 besonders durch menschliches Versagen als wesentlichster Faktor gekennzeichnet, der sich auch durch intensives Training nie vollständig ausschließen lässt.

Tabelle 51 Maßnahme M5.4

Maßnahme	M5.4
Kurzbeschreibung	Verfügbarkeitskonzept für jede Domäne DO-FW, DO-AWA, DO-BBK, DO-BAM, DO-GRZ1, DO-GRZ2
Ergebnis	Die Eintrittswahrscheinlichkeiten von R5.2 und R5.3 werden weiter reduziert
Wirkt gegen	R5.2 (B5.2, Erforderliche Grid-Ressourcen fallen während der Nutzung aus) R5.3 (B5.2, Erforderliche Grid-Ressourcen fallen während der Nutzung aus)
Aktion bei	Domänen- bzw. Policy-Verantwortliche P-dap/P-lad bei allen beteiligten Domänen, besonders bei DO-FW. Zusätzlich bei den Betreibern der Kommunikationsstrecken.
Beschreibung	Hier muss bereits während der Konzeptphase auf ausreichende Redundanz der einzelnen Komponenten geachtet werden. Hierzu zählen aufgrund der verteilten Standorte auch die Redundanz der Kommunikationsstrecken zwischen den einzelnen Domänen bzw. deren Ressourcen.
Aufwand	Mittel bis hoch
Grenzen der Wirksamkeit	Insbesondere die Wirksamkeit gegen DDoS Angriffe ist maßgeblich abhängig von der Mitwirkung der Betreiber der Kommunikationsstrecken.

Tabelle 52 Maßnahme M5.5

Maßnahme	M5.5
Kurzbeschreibung	Absicherung der Korrektheit der Eingabedaten (z. B. 4-Augenprinzip)
Ergebnis	Die Eintrittswahrscheinlichkeit von R5.4 wird weiter reduziert
Wirkt gegen	R5.4 (B5.3, Einsatzkräfte liefern falsche Eingabedaten)
Aktion bei	Personen, die Eingabedaten liefern (P-u)
Beschreibung	Um die versehentliche oder absichtliche Eingabe fehlerhafter Daten durch P-u zu verhindern, kann z. B. das 4-Augenprinzip angewendet werden.
Aufwand	Niedrig bis mittel
Grenzen der Wirksamkeit	Nicht jeder Einsatzort erlaubt und nicht jede Aufgabenstellung erfordert diese Maßnahme.

Tabelle 53 Maßnahme M5.6

Maßnahme	M5.6
Kurzbeschreibung	Verpflichtung aller P-dap/P-lad auf die nötige Vertraulichkeit und Überprüfung von deren Integrität
Ergebnis	Die Eintrittswahrscheinlichkeit von R5.7, R5.9, R5.10 - R5.15, R5.17 - R5.19 sinkt auf niedrig bis mittel bzw. wird weiter abgesenkt.
Wirkt gegen	R5.7 (B5.5, Basisdaten durch Datenprovider (P-dap) unberechtigt verändert) R5.9 (B5.6, Basisdaten durch die lokalen Administratoren (P-lad) verändert) R5.10, R5.11 (B5.7, Ergebnisdaten durch lokalen Admin in HW-Domänen manipuliert) R5.12, R5.13 (B5.8, Ergebnisdaten durch lokalen Admin in DO-BBK manipuliert) R5.14, R5.15 (B5.9, Ergebnisdaten durch Datenprovider (P-dap) in DO-BBK manipuliert) R5.17 (B5.10/B5.11, lokaler Administrator (P-dap/P-lad) gibt Daten an Außenstehende) R5.18, R5.19 (B5.12, P-uz aus DO-BBK/DO-FW gibt die Ergebnisdaten unberechtigt weiter)
Aktion bei	Domänenverantwortliche für jede der Domänen DO-FW, DO-AWA, DO-BBK, DO-BAM, DO-GRZ1, DO-GRZ2
Beschreibung	Es muss möglichst ausgeschlossen werden, dass ein P-dap/P-lad bewusst Änderungen bzw. Manipulationen an Datenbeständen vornimmt, also vorsätzlich handelt.
Aufwand	Niedrig bis mittel

Maßnahme	M5.6
Grenzen der Wirksamkeit	Gegen Fehlverhalten Einzelner gibt es keinen vollständigen Schutz. Einzelne Administratoren könnten sich evtl. fahrlässig oder vorsätzlich nicht an entsprechende Vorgaben halten. Daher sind Sanktionen für den Fall des Verstoßes vorzusehen.

Tabelle 54 Maßnahme M5.7

Maßnahme	M5.7
Kurzbeschreibung	Gewährleistung der Authentizität aller P-dap/P-lad bei der Eingabe von bzw. dem Zugriff auf Daten
Ergebnis	Die Eintrittswahrscheinlichkeit von R5.15 – R5.20 wird jeweils weiter abgesenkt.
Wirkt gegen	R5.15 (B5.9, lokaler Administrator P-dap greift unberechtigt zu) R5.16, R5.17 (B5.10/B5.11, lokaler Administrator (P-dap/P-lad) gibt Daten an Außenstehende) R5.18, R5.19 (B5.12, P-uz aus DO-BBK/DO-FW gibt die Ergebnisdaten unberechtigt weiter) R5.20 (B5.13, Außenstehender erlangt Zugriff auf Ergebnisdaten und gibt diese weiter)
Aktion bei	Domänenverantwortliche für jede der Domänen DO-FW, DO-AWA, DO-BBK, DO-BAM, DO-GRZ1, DO-GRZ2
Beschreibung	Um sicherzustellen, dass generell nur Berechtigte Daten in das Grid einbringen bzw. auf die Daten im Grid zugreifen können, sind geeignete Maßnahmen zu starken Authentisierung unabdingbar (etwa auf Basis von Chip-Karten, Token o. ä.). Eine spezielle Ausprägung für P-dap beschreibt auch Maßnahme M5.8 bzw. Maßnahme M5.9.
Aufwand	Niedrig bis mittel
Grenzen der Wirksamkeit	Diese technische Maßnahme kann nicht gegen jedes Fehlverhalten Einzelner schützen, s. dazu auch Maßnahme M5.6.

Tabelle 55 Maßnahme M5.8

Maßnahme	M5.8
Kurzbeschreibung	Besondere Gewährleistung der Authentizität aller P-dap bei der Eingabe von bzw. dem Zugriff auf Daten durch auf biometrischen Verfahren beruhenden starken Authentikationsmechanismen
Ergebnis	Die Eintrittswahrscheinlichkeit von R5.15 und R5.20 sinkt auf mittel bzw. niedrig.

Maßnahme	M5.8
Wirkt gegen	R5.15 (B5.9, lokaler Administrator P-dap greift unberechtigt zu) R5.20 (B5.13, Außenstehender erlangt Zugriff auf Ergebnisdaten und gibt diese weiter)
Aktion bei	Domänenverantwortliche für die Domäne DO-FW
Beschreibung	Um sicherzustellen, dass nur Berechtigte Daten in das Grid einbringen bzw. auf die Daten im Grid zugreifen können, sind bei den „vor Ort“ eingesetzten Personen (Domäne DO-FW, also im Bereich Lagezentrum, Feuerwehr, Einsatzkräfte etc.) ggf. spezielle Maßnahmen zur zuverlässigen Authentisierung erforderlich, die für den „Feldeinsatz“ geeignet sind. Die hier benötigten starken Authentikationsmechanismen müssen auch unter schwierigen Einsatzbedingungen zuverlässig funktionieren. Dazu können u. U. Verfahren, die auf Biometrie basieren, angewendet werden (z. B. Erkennen von Fingerabdrücken, Stimmidentifikation etc.).
Aufwand	hoch
Grenzen der Wirksamkeit	Auch biometrische Verfahren weisen Schwachstellen auf, die den konkreten Einsatzszenarien gegenüber gestellt werden müssen. Speziell können hier Randbedingungen eintreten, die die Anwendung solcher Verfahren erschweren oder ausschließen. So kann etwa die Erkennung von Fingerabdrücken problematisch werden, wenn die Einsatzkräfte vor Ort einsatzbedingt stark verschmutzte Hände haben. Entsprechend können auf akustischer oder optischer Identifikation beruhende Maßnahmen durch starke Lärm- bzw. Rauchentwicklung behindert werden. Die derzeit verfügbaren Verfahren sind für den Einsatz in „ungünstiger“ Umgebung (Wald, Matsch, Regen, Rauch, …) weniger gut bis gar nicht geeignet. Evtl. ist alternativ oder in Kombination Maßnahme M5.9 vorzusehen.

Tabelle 56 Maßnahme M5.9

Maßnahme	M5.9
Kurzbeschreibung	Besondere Gewährleistung der Authentizität aller P-dap bei der Eingabe von bzw. dem Zugriff auf Daten durch auf Verwendung von ID-Token beruhenden starken Authentikationsmechanismen
Ergebnis	Die Eintrittswahrscheinlichkeit von R5.15 und R5.20 sinkt auf mittel bzw. niedrig.
Wirkt gegen	R5.15 (B5.9, lokaler Administrator P-dap greift unberechtigt zu) R5.20 (B5.13, Außenstehender erlangt Zugriff auf Ergebnisdaten und gibt diese weiter)
Aktion bei	Domänenverantwortliche für die Domäne DO-FW

Maßnahme	M5.9
Beschreibung	Um sicherzustellen, dass nur Berechtigte Daten in das Grid einbringen bzw. auf die Daten im Grid zugreifen können, sind bei den „vor Ort“ eingesetzten Personen (Domäne DO-FW, also im Bereich Lagezentrum, Feuerwehr, Einsatzkräfte etc.) ggf. spezielle Maßnahmen zur zuverlässigen Authentisierung (Zwei-Faktoren-Authentisierung) erforderlich, die für den „Feldeinsatz“ geeignet sind. Die hier benötigten starken Authentikationsmechanismen müssen auch unter Einsatzbedingungen zuverlässig funktionieren. Dazu können u. U. Verfahren, die auf ID-Token basieren, angewendet werden (z. B. SecureID-Token, RFID etc.). Evtl. ist alternativ oder in Kombination Maßnahme M5.8 vorzusehen.
Aufwand	hoch
Grenzen der Wirksamkeit	Auch die auf ID-Token beruhenden Verfahren weisen Schwachstellen auf, die den konkreten Einsatzszenarien gegenüber gestellt werden müssen. Speziell können hier Randbedingungen eintreten, die die Anwendung solcher Verfahren erschweren oder ausschließen. So kann etwa die zuverlässige Verwendung eines durch Hitzeeinwirkung beschädigten RFID-Tags problematisch werden. Entsprechend können auch andere Formen von ID-Token (spezielle Chipkarten, USB-Sticks, PDA-Software etc.) unter bestimmten Einsatzbedingungen unbrauchbar werden. Die derzeit verfügbaren Produkte sind für den Einsatz in „ungünstiger“ Umgebung (Wald, Matsch, Regen, Rauch, …) weniger gut bis gar nicht geeignet. Evtl. ist alternativ oder in Kombination Maßnahme M5.8 vorzusehen.

Tabelle 57 Maßnahme M5.10

Maßnahme	M5.10
Kurzbeschreibung	Schneller und effizienter Abbau der VO mit Entzug aller Rechte
Ergebnis	Die Eintrittswahrscheinlichkeit von R5.17 - R5.19 sinkt auf niedrig bis mittel bzw. wird weiter abgesenkt.
Wirkt gegen	R5.17 (B5.10/B5.11, lokaler Administrator (P-dap/P-lad) gibt Daten an Außenstehende) R5.18, R5.19 (B5.12, P-uz aus DO-BBK/DO-FW gibt die Ergebnisdaten unberechtigt weiter)
Aktion bei	Domänenverantwortliche für jede der Domänen DO-FW, DO-AWA, DO-BBK, DO-BAM, DO-GRZ1, DO-GRZ2
Beschreibung	Der schnelle und effizienten Abbau der VO nach Beendigung des K-Falles mit Entzug aller beim Aufbau des Grid erteilten K-Fall-spezifischen (Sonder-)Zugriffsrechte ist ebenso wichtig wie der schnelle Aufbau des Grid. Es soll ja nach dem K-Fall z. B. kein Umweltschützer mehr auf Datenbanken der Polizei zugreifen können.
Aufwand	Niedrig bis mittel
Grenzen der Wirksamkeit	Gegen Fehlverhalten Einzelner gibt es keinen vollständigen Schutz. Einzelne Administratoren könnten sich evtl. fahrlässig oder vorsätzlich nicht an entsprechende Vorgaben halten. Daher sind Sanktionen für den Fall des Verstoßes vorzusehen.

2.5.2 Übersicht Sicherheitsmechanismen Szenario 5

Die folgende Tabelle 58 liefert eine Kurzübersicht über die Maßnahmen, die zur Verringerung der als nicht tragbar eingestuften Risiken notwendig sind.

Tabelle 58 Übersicht über die Sicherheitsmechanismen für Szenario 5

Maß-nahme	Kurzbeschreibung	Wirkt gegen
M5.1	Erarbeitung spezifischer Vorschriften, Gesetze und Verordnungen, die alle wesentlichen für das Bilden und Betreiben eines K-Grid erforderlichen Randbedingungen, Voraussetzungen, Verantwortlichkeiten und Anforderungen festschreiben	R5.1, R5.2
M5.2	Sorgfältige Auswahl und sorgfältige vertragliche/gesetzliche Einbindung der beteiligten Provider von Grid-Ressourcen	R5.1
M5.3	Regelmäßige Überprüfung von Aufbaufähigkeit und anschließender Funktionsfähigkeit des Grid in Form von Katastrophenübungen	R5.1, R5.2, R5.4, R5.5
M5.4	Verfügbarkeitskonzept für jede Domäne DO-FW, DO-AWA, DO-BBK, DO-BAM, DO-GRZ1, DO-GRZ2	R5.2, R5.3
M5.5	Absicherung der Korrektheit der Eingabedaten (z. B. 4-Augenprinzip)	R5.4
M5.6	Verpflichtung aller P-dap/P-lad auf die nötige Vertraulichkeit und Überprüfung von deren Integrität	R5.7, R5.9, R5.10 - R5.15, R5.17 - R5.19
M5.7	Gewährleistung der Authentizität aller P-dap/P-lad bei der Eingabe von bzw. dem Zugriff auf Daten	R5.15 - R5.20
M5.8	Besondere Gewährleistung der Authentizität aller P-dap bei der Eingabe von bzw. dem Zugriff auf Daten durch auf biometrischen Verfahren beruhenden starken Authentikationsmechanismen	R5.15, R5.20
M5.9	Besondere Gewährleistung der Authentizität aller P-dap bei der Eingabe von bzw. dem Zugriff auf Daten durch auf Verwendung von ID-Token beruhenden starken Authentikationsmechanismen	R5.15, R5.20
M5.10	Schneller und effizienter Abbau der VO mit Entzug aller Rechte	R5.17 - R5.19

2.5.3 Fazit für Szenario 5

Die Maßnahmen für Szenario 5 resultieren aus den nicht tragbaren Risiken (s. Tabelle 47; vgl. 1. „Sicherheitsmechanismen: Vorgehensweise“) für dieses Szenario (vgl. auch AP2 - Risikoanalyse). Ergebnis der Analyse war, dass die nicht tragbaren Risiken hauptsächlich im Bereich der Verfügbarkeit der Grid-Ressourcen im Bedarfsfall und der dann zu gewährleistenden Integrität der Eingangsdaten liegen. Die Maßnahmen bewegen sich hier also stark im Bereich von Gesetzen/Verordnungen/Verträgen (Maßnahme M5.1; Maßnahme M5.2), im regelmäßigen Üben des Herstellens der Grid-Funktionalität auf Basis von sonst eher eigenständig eingesetzten Ressourcen einschl. entsprechender Sicherstellung der Verfügbarkeit und des „sicheren“ Grid-Abbaus (Maßnahme M5.3; Maßnahme M5.4; Maßnahme M5.10) und im Sicherstellen der Datenintegrität, u. a. durch Gewährleistung der Authentizität der zugreifenden Personen (Maßnahme M5.5; Maßnahme M5.7; Maßnahme M5.8; Maßnahme M5.9).

Daneben ist es unabdingbar sicherzustellen, dass die als Administratoren eingesetzten Personen die nötige Eignung und Verlässlichkeit besitzen (Maßnahme M5.6).

3 Sicherheitsmechanismen: Fazit

Die für die einzelnen Szenarien

1. Szenario 1: Unternehmensinternes Grid; s. Abschnitt 2.1
2. Szenario 2: Grid für den unternehmensübergreifenden industriellen Einsatz; s. Abschnitt 2.2
3. Szenario 3: Offenes e-Science Grid; s. Abschnitt 2.3
4. Szenario 4: Grids mit personenbezogenen bzw. personenbeziehbaren Daten (z. B. MammoGrid); s. Abschnitt 2.4
5. Szenario 5: Sicherheitskritisches national wichtiges Grid / Katastrophenschutz (K-Grid); s. Abschnitt 2.5

erarbeiteten und aufgeführten Sicherheitsmechanismen und Maßnahmen lassen eine Reihe von Gemeinsamkeiten, ebenso aber auch spezifische Anforderungen für einzelne oder auch Kombinationen der betrachteten Szenarien erkennen.

Die Maßnahmen wurden jeweils aus den nicht tragbaren Risiken für die einzelnen Szenarien (vgl. AP2 - Risikoanalyse) abgeleitet. Ein – je nach Szenario – mehr oder weniger großer Anteil der nicht tragbaren Risiken liegt dabei in Bereichen, die nicht Grid-spezifisch sind und denen heute üblicherweise bereits anderweitig (z. B. durch Maßnahmen nach GSHB) begegnet wird.

Während sich in einigen Szenarien Sicherheitsmechanismen der Grid-Middleware nutzen lassen (wenn auch teilweise erst nach deren noch nicht abgeschlossener vollständiger Implementierung), hängt in vielen Fällen sehr viel von der Vertrauenswürdigkeit der handelnden Personen, hier vor allem der Administratoren, und Organisationen ab. Da helfen nur verbindliche Regelungen (Gesetze, Verträge mit Sanktionsandrohungen etc.) und die strikte Überwachung ihrer Einhaltung. Aber auch mit solchen Regelungen lassen sich Risiken natürlich nie vollständig beherrschen.

Viele Risiken ergeben sich aus dem Problem, dass sowohl Software als auch Daten (Eingabedaten, Zwischenergebnisse, Ausgabedaten) aller Art von Administratoren mit entsprechenden technischen Zugriffsmöglichkeiten potenziell unberechtigt eingesehen (und damit auch kopiert und weitergegeben) werden können. Zwar gibt es am Markt einige Betriebsplattformen, die ein – im Vergleich bspw. zu „Standard-Unix“ – erweitertes Berechtigungskonzept technisch unterstützen. Aber Zugriffsschutz im hier geforderten Sinne wird möglicherweise erst mit flächendeckender Einführung von „Trusted-Computing“-Plattformen, wie sie derzeit von der TCG (*Trusted Computing Group*) in Fortführung der Aktivitäten der TCPA (*Trusted Computing Platform Alliance*) voran getrieben werden, möglich sein. Allerdings müssen existierende Anwendungen und Middleware-Komponenten erst aufwändig an TCG bzw. die dabei verwendeten TPM (*Trusted Platform Module*) angepasst werden, so dass allein aus diesem Grund die Nutzung dieser Technik frühestens mittelfristig zu erwarten ist.

Hinzu kommt, dass derzeit noch keine Hochleistungsrechnersysteme mit TCG-basierter Hardware verfügbar sind. Auf TCG basierende Maßnahmen sind daher als eine Möglichkeit für zukünftige Systeme anzusehen. Dann kann damit allerdings „technisch“ erzwungen werden, dass Anwendungen nur noch auf TCG-basierter Hardware ausgeführt werden, die Nutzung von TCG muss also nicht rein organisatorisch durchgesetzt werden.

Bei aller berechtigter Erwartung an TCG-basierte technische Mechanismen: auch diese sind kein Allheilmittel. Erfahrungsgemäß findet sich auf Dauer bei allen wirksamen komplexen Mechanismen eine Möglichkeit, diese zu umgehen. In diesem Sinne sind die hier zusammengefassten Maßnahmen nicht als statische Sammlung, sondern als stetig weiterzuentwickelndes und zu ergänzendes Grundgerüst zu verstehen.

TCG wird hier als ein Beispiel für hardwarenah realisierte Schutzmechanismen dargestellt. Exemplarisch sind bei TCG vor allem die Randbedingungen für eine erfolgreiche Nutzung. Denn auch bei anderen Ansätzen, die ähnliche oder technisch vergleichbare bzw. verwandte Ziele verfolgen, wie etwa DRM (*Digital Rights Management*), gilt das zuletzt Gesagte bzgl. Anpassung von Anwendungen und Middleware sowie bzgl. geeigneter Hochleistungsrechnersysteme mit angepassten Betriebssystemen entsprechend.

Referenzen

[1] Vorstudie Grid Sicherheits-Infrastruktur (GSI) Ergebnisse des Arbeitspakets 1: „Relevante Grid-Szenarien und ihr Schutzbedarf“, Version 8.4 - 19.06.2006