

Gutachten

SecuTrial® 2.1 in Compliance mit AMG/GCP und
FDA 21CFR Part 11

Erstellt durch BioMedion GmbH, Göttingen
April 2007

1. Inhalt

1. Inhalt	2
2. Einleitung	3
3. Gegenstand des Gutachtens	3
4. Grundlage der Bewertung	4
5. Architektur	4
6. Übersicht zur Compliance	6
7. Abweichungen	15
8. Zusammenfassung	16
9. Anhang	17

2. Einleitung

Die Nutzung von Computersystemen in Industriezweigen wie Pharma, Biotechnologie und Medizintechnik unterliegt den regulatorischen Anforderungen seitens der Zulassungsbehörden bezüglich elektronischer Aufzeichnungen und elektronischer Signatur.

Das vorliegende Gutachten ist in Auftrag gegeben von der iAS GmbH, Berlin. Gegenstand des Gutachtens ist die von der iAS GmbH vollständig selbst entwickelte Software SecuTrial® 2.1, die der Erfassung von medizinischen Patientendaten im Zusammenhang mit klinischen Studien dient. Das Gutachten ist erstellt durch die BioMedion GmbH, Göttingen. Die BioMedion GmbH ist als Dienstleister und Berater für Pharmaunternehmen seit 2001 tätig. Durch die langjährige Erfahrung auf diesem Gebiet ist die BioMedion GmbH mit den gesetzlichen Anforderungen und deren Auslegungen bestens vertraut.

3. Gegenstand des Gutachtens

Das Gutachten dient der Bewertung der Software SecuTrial® 2.1 in der von der iAS GmbH empfohlenen Konfiguration hinsichtlich der Erfüllung der gesetzlichen Vorgaben und Erfordernisse, die sich aus AMG (12. Novelle) bzw. GCP (EU Richtlinie 2001/20/EG) und FDA 21 CFR Part 11 ergeben. Bei der Begutachtung der einzelnen technischen und Logischen Komponenten haben wir uns an die Systematik der FDA Verordnung 21 CFR Part 11 –Electronic data, electronic signatures gehalten, da diese Anforderungen gleichzeitig alle Anforderungen aus AMG/GCP mit abdeckt. Dazu werden die Anforderungen in tabellarischer Form den Systemfunktionen gegenübergestellt. Als Ergänzung sind im Anhang Abbildungen zur Architektur und zum Sicherheits- bzw. Rollenkonzept von SecuTrial® 2.1 angehängt. Auf diese wird an gegebener Stelle hingewiesen.

Mit diesem Gutachten wird NICHT die generelle Erfüllung der gesetzlichen Anforderungen zertifiziert oder bestätigt, da dies nur durch die zuständigen Behörden selbst und im Rahmen eines offiziellen Audits für eine vom Kunden validierte Studie bzw. Installation möglich ist. Die grundsätzliche Funktionalität ist ebenfalls nicht Gegenstand dieses Gutachtens, da sie durch das Qualitätssystem der iAS GmbH gewährleistet und im Rahmen der Systemvalidierung vom Kunden zu überprüfen ist.

4. Grundlage der Bewertung

Grundlage für dieses Gutachten sind neben den gesetzlichen Grundlagen die nachfolgend aufgeführte Dokumente der iAS GmbH zu SecuTrial® 2.1 und ein zur Bewertung notwendiges Audit am 19. April 2007 bei der iAS GmbH in Berlin.

Dokumentation:

- do PIDDispatcher_sT_2.1_20070215_1.1.pdf
- do_Architektur_secuTrial_2.1_20070212_1.1.pdf
- fk_AT_AuditTrail_20061010_1.0.pdf
- fk_FormBuilder_DB_Versionen_20050224_1.0.pdf
- pb_secuTrial_2.1_I_Begriffe_deu_20070313_1.0.pdf
- pb_secuTrial_2.1_II_FormEngine_deu_20070313_1.0.pdf
- pb_secuTrial_2.1_III_Funktionen_deu_20070411_1.0.pdf
- um_secuTrial_AdminTool_deu_2.1_20070319_1.1.pdf
- um_secuTrial_DataCapture_deu_2.1_20070308_1.0.pdf
- um_secuTrial_ExportSearchTool_deu_2.0_20070313_1.0.pdf
- um_secuTrial_ExportFormats-SRT2.1_eng_20070314_1.0.pdf
- um_secuTrial_FormBuilder_deu_2.1_20070313_1.0.pdf

5. Architektur

Die Software SecuTrial® 2.1 besteht aus mehreren Komponenten, die logisch miteinander verknüpft sind (Abb 1.). Die Kommunikation zwischen den Komponenten erfolgt in unterschiedlichen Sicherheitskontexten, was bei der Bewertung hinsichtlich der Compliance von besonderer Bedeutung ist. Als Webapplikation ist SecuTrial® 2.1 im Regelfall als offenes System einzustufen, daher ist die von der iAS GmbH standardmäßig empfohlene Verschlüsselung für die Authentifizierung und Datenübermittlung vom Client zum Applikationsserver unerlässlich.

Nachfolgend wird kurz die grundlegende Architektur des Systems beschrieben in Hinblick auf verwendete Sicherheitskontexte und Verwaltungsfunktionen. Die Begrifflichkeiten sind wie folgt definiert:

- Anbieter bezeichnet die Organisation, die das System serverseitig hostet und Kunden einrichtet/verwaltet.
- Kunde bezeichnet die Organisation, die eine Studie durchführt.
- Anwender bezeichnet die teilnehmenden Ärzte, die die Patientendaten/Medizindaten erfassen.

Die drei Hauptkomponenten von SecuTrial® 2.1, Datenbank, Applikationsserver und Webclient bilden zwei unterschiedliche Sicherheitsbereiche, deren Zugangsrechte klar getrennt sind.

Die Datenbank und der Applikationsserver werden ausschließlich vom Anbieter verwaltet und unterliegen den beim Anbieter geltenden Sicherheitsrichtlinien. In der Regel unterliegt die Verwaltung der Kunden und die Datenbankverwaltung getrennten Geschäftsbereichen beim Anbieter. Datenbank Administratoren haben dabei keinen Zugriff auf die Applikation und Applikationsverantwortliche dagegen keinen direkten Zugriff auf die Datenbank. Die Kommunikation zwischen den beiden

Komponenten Datenbank und Applikationsserver findet mittels eines technischen Datenbankbenutzers statt.

Der Webclient ist frei verfügbar und bildet den einzigen Zugang für den Kunden und den Anwender. Dieser Zugang wird für die Verwaltung von Studien, Anwenderverwaltung (Ärzte) und zur Erfassung der Patientendaten (Medizindaten) durch die Anwender verwendet. Es gibt für den Kunden und den Anwender keine direkte Zugriffsmöglichkeit auf den Applikationsserver oder die Datenbank.

Neben den drei Hauptkomponenten existiert als notwendige Erweiterung aus datenschutzrechtlichen Gründen der PIDDispatcher. Dieses Modul kommuniziert beim Anlegen eines neuen Patienten zwischen Webclient und Applikationsserver mit der Patientenliste. Hier wird für jeden namentlichen Patienten ein eindeutiges Pseudonym erzeugt, unter dessen Kennung die medizinischen Daten in der Datenbank abgelegt werden. (Abb. 2) Dadurch ist gewährleistet, dass Rückwärtsaufschlüsselung von medizinischen Daten auf einen namentlichen Benutzer nicht direkt möglich ist. Nur in der Patientenliste ist eine Zuordnung möglich. Die Patientenliste ist jedoch nicht Bestandteil von SecuTrial® 2.1 . Da hier keine studienrelevanten Daten verwaltet bzw. übermittelt werden, ist der PIDDispatcher nicht Gegenstand dieses Gutachtens.

6. Übersicht zur Compliance

Diese Liste der Anforderungen aus FDA 21 CFR Part 11 dient der Klärung, ob die gesetzlichen Anforderungen vom begutachteten System erfüllt werden und wo ggfs. Abweichungen auftreten.

Absatz Nr.	Fragen / Anforderungen	Ja / Nein	Kommentar
Elektronische Aufzeichnungen (electronic records)			
Absatz 11.10: Closed Systems			
§ 11.10 (a)	Ist das System validiert?	Ja	<p>SecuTrial® 2.1 unterliegt im Qualitätssystem der iAS GmbH einer ordentlichen Versionsfreigabe. Diese erfolgt nur nach erfolgreichen Test sowohl im Whitebox als auch im Blackbox Verfahren. Die von der iAS GmbH gehosteten Kundendatenbanken sind im Rahmen der jeweiligen Projektumsetzung getestet und freigegeben. Die Freigabe wird im System dokumentiert (siehe § 11.10 (e) und Abb. 1)</p> <p>Für Anbieter, die SecuTrial® 2.1 unabhängig von der iAS GmbH hosten und verwalten ist es erforderlich über geeignete Systeme, Sicherheitskonzepte, Verwaltungszuständigkeiten und die entsprechende Dokumentation darüber zu verfügen.</p>
§ 11.10 (a)	Nimmt das System ungültige und veränderte Aufzeichnungen wahr?	Ja	<p>SecuTrial® 2.1 verfügt über eine integrierte Möglichkeit der elektronischen Signatur, die entsprechend den Kundenanforderungen an jedem relevanten Eingabepunkt bei der Erfassung der Daten mit jeweils beiden Komponenten (ID und PIN) abgefragt werden kann. Eine Veränderung der Daten macht die Signatur ungültig. Dies wird im Formularfenster angezeigt.</p>
§ 11.10	Archivieren, Wiederauffindung	Ja	Es stehen geeignete Mittel zur

(b)	(Retrieval), Ausdrucken und Anzeigen von Daten		Verfügung.
§ 11.10 (c)	Langfristige Sicherung der archivierten Aufzeichnungen	Ja	Die Daten befinden sich über die gesamte Laufzeit einer Studie im Serversystem. Nach Abschluss einer Studie werden ALLE Daten der Studie in lesbaren Formaten auf langzeitstabilen optischen Medien an den Kunden übergeben. Die iAS GmbH hält darüber hinaus alle Softwareversionen von SecuTrial® vor, so dass jederzeit gewährleistet ist, dass die Daten durch Re-Import wieder im Originalsystem einzusehen sind.
§ 11.10 (c)	Ist die Haltezeit für die Aufzeichnungen vorgegeben?	NA	Die Verwaltung der archivierten Daten nach Abschluss einer Studie obliegt dem jeweiligen Kunden.
§ 11.10 (c)	Können die Aufzeichnungen während ihrer Haltezeit sofort wiedergewonnen werden?	Ja	Alle Daten sind entsprechend Zugriffsrechten jederzeit für den Kunden abrufbar (z.B. für Auswertungszwecke).
§ 11.10 (c)	Gibt es Utilities / Tools, die sicherstellen, dass ein Aufzeichnung, für dessen Erfassung eine bestimmte Softwareversion benutzt wurde, auch dann noch lesbar sein wird, wenn diese Software nicht mehr erhältlich ist?	Ja	Die Studien werden nach Abschluss in lesbaren Formaten an den Kunden übergeben. Die iAS GmbH hält darüber hinaus alle Softwareversionen von SecuTrial® vor, so dass jederzeit gewährleistet ist, dass die Daten durch Re-Import wieder im Originalsystem einzusehen sind. Zudem ist der Quellcode für SecuTrial® 2.1 hinterlegt.
§ 11.10 (c)	Gibt es ein vorgegebenes Verfahren zur Aufbewahrung der Aufzeichnungen während der Haltezeit?	NA	Die Verwaltung der archivierten Daten nach Abschluss einer Studie obliegt dem jeweiligen Kunden.
§ 11.10(d)	Beschränkt sich der System-Zugang nur auf die befugten Personen?	Ja	SecuTrial® 2.1 verfügt über ein eigenes Rechte- und Rollenkonzept. Die Verwaltung

			der Anwender liegt beim Kunden. Jeder Anwender verfügt über eine eindeutige ID und ein nur ihm selbst bekanntes Passwort.
§ 11.10 (d)	Wird der Systemzugang durch ein Verfahren geregelt und kontrolliert?	Ja	Der Systemzugang bietet entsprechend der Systemarchitektur und dem Rechte- und Rollenkonzept separat verwaltete Zugänge zu den Modulen. Prozeduren, die den Zugang regeln, werden für die anbieterseitigen Systembereiche von der iAS GmbH verwaltet und angewandt. Die Verwaltung und Umsetzung der entsprechenden Prozeduren auf Kundenseite unterliegt dem Kunden.
§11.10(e)	Gibt es einen sicheren, vom Rechner erzeugten, mit einem Zeitstempel versehenen Audit Trail, der Datum und Zeit der Eingaben und Handlungen aufzeichnet, die elektronische Aufzeichnungen erstellen, ändern oder löschen?	Ja	SecuTrial® 2.1 bietet drei verschiedene Arten des Audit Trail: Die erfassten Patientendaten (Medizindaten) werden mit Zeitstempel und Grund der Eingabe in der Datenbank erfasst. Bei Änderungen wird immer ein neuer Datenbankeintrag erzeugt, das heißt, dass bestehende Einträge nicht gelöscht oder verändert werden können. Änderungen an der Konfiguration und am Design von Studien werden über freigegebene Versionen nachvollziehbar gespeichert. Vorherige Versionen werden archiviert. Alle Änderungen, die in der Administration gemacht werden, werden als inkrementelle Einträge in eine separate Logtabelle geschrieben. So ist auch die Systemverwaltung jederzeit

			nachvollziehbar.
§ 11.10 (e)	Steht im Falle einer Änderung an einem elektronischen Aufzeichnung die zuvor aufgezeichnete Information weiter zur Verfügung (wird sie z.B. durch die Änderung nicht überlagert?)	Ja	Bestehende Einträge in SecuTrial® 2.1 werden nie überschrieben, bei Änderungen wird der original Datensatz in die Archivtabelle verschoben.
§ 11.10 (e)	Ist der Grund für die Änderung enthalten.	Ja	Da Änderungen wie neuerfasste Daten behandelt werden (s.o.) stehen auch hier alle relevanten Informationen im Audit Trail.
§ 11.10 (e)	Ist der Audit Trail einer elektronischen Aufzeichnung während deren Haltezeit wieder auffindbar?	Ja	Der Audit Trail wird über den gesamten Studienzeitraum geführt. Nach Abschluss einer Studie wird der Audit Trail mit exportiert.
§ 11.10 (e)	Steht der Audit Trail für Prüf- und Kopierzwecke der FDA zur Verfügung?	Ja	Der Zugang wird kundenseitig über geeignete Exportfunktionen geregelt.
§ 11.10 (e)	Die Zeit des Audit Trail soll sich auf eine vorgegebene Standard-Zeit beziehen.	Ja	Datenbankeinträge werden mit der Serverzeit gestempelt. Die Serverzeit wird mit offiziellen Zeitservern synchronisiert.
§ 11.10 (f)	Wenn die Folge der Systemschritte oder Ereignisse wichtig ist, wird dies vom System auch berücksichtigt (wie z.B. bei einem Prozessleitsystem)?	NA	Entfällt.
§ 11.10 (g)	Stellt das System sicher, dass nur befugte Personen das System benutzen und elektronisch signieren können, Zugriff zu der Operation oder den Eingabe- oder Ausgabegeräten des Rechnersystems haben, ein Aufzeichnung ändern oder sonstige Operationen durchführen können?	Ja	Der Systemzugang bietet entsprechend der Systemarchitektur und dem Rechte- und Rollenkonzept separat verwaltete Zugänge zu den Modulen. Prozeduren, die den Zugang regeln, werden für die anbieterseitigen Systembereiche von der iAS GmbH verwaltet und angewandt. Die Verwaltung und Umsetzung der entsprechenden

			Prozeduren auf Kundenseite unterliegt dem Kunden. Zugang zum System ist nur mit gültigem Account (ID) und Passwort möglich.
§ 11.10 (h)	Kann das System, die Identität des Eingabegerätes prüfen oder die Herkunft von (Mess-) Daten und Steuerbefehlen?	NA	Nicht Zutreffend.
§ 11.10(i)	Gibt es Trainingskurse, einschließlich training on the job für Systemanwender, Entwickler, IT-Support Personal?	Ja	Die iAS GmbH bietet entsprechende Schulungen an.
§ 11.10(i)	Es müssen Unterlagen mit Angaben darüber vorhanden sein, welche Ausbildung, Schulung, Training und Erfahrung die Personen haben sollen, die ER/ES Systeme entwickeln, warten oder benutzen.	JA	Nachweise werden seitens der iAS GmbH in den Personalakten geführt. Die Verantwortlichkeit für Nachweise der Anwender liegt beim Kunden. Für Anbieter, die SecuTrial® 2.1 unabhängig von der iAS GmbH hosten und verwalten ist es erforderlich diese Nachweise selber zu erbringen.
§ 11.10(j)	Gibt es eine schriftliche Bescheinigung, die eine Person für die Handlungen haftbar und verantwortlich macht, die unter ihrer elektronischer Signatur gestartet wurden?	NA	In Kundenverantwortung.
§ 11.10(k)	Wird die Verteilung, der Zugang zu und die Benutzung der Betriebs- und Wartungsdokumentation für das System kontrolliert?	Ja	Das Qualitätssystem der iAS GmbH regelt den Zugang zu der Dokumentation. Für Anbieter, die SecuTrial® 2.1 unabhängig von der iAS GmbH hosten und verwalten ist es erforderlich diesen Zugang selber zu regeln.
§ 11.10 (k)	Gibt es ein formales Verfahren zur Kontrolle über Verteilung, Zugang zur, Nutzung und Änderungen der Systemdokumentation.	Ja	Das Qualitätssystem der iAS GmbH regelt den Zugang zu der Dokumentation. Für Anbieter, die SecuTrial® 2.1 unabhängig von der iAS

			GmbH hosten und verwalten ist es erforderlich diesen Zugang selber zu regeln.
Absatz 11.30: Open Systems			
§ 11.30	Ist der Zugang zum System zusätzlich zu den in § 11.10 geforderten Bedingungen verschlüsselt?	Ja	Die von der iAS GmbH gehosteten Systeme lassen nur verschlüsselte Kommunikation zwischen Webclient und Applikationsserver zu. Da die Verschlüsselung serverseitig konfiguriert wird, ist es für Anbieter, die SecuTrial® 2.1 unabhängig von der iAS GmbH hosten und verwalten erforderlich, die Verschlüsselung für ihre Applikationsserver selber zu konfigurieren.
§ 11.30	Besteht die Möglichkeit, die Authentizität, Integrität und Vertraulichkeit der Daten durch geeignete Signaturen zu gewährleisten?	Ja	SecuTrial® 2.1 verfügt über eine integrierte Möglichkeit der elektronischen Signatur, die entsprechend den Kundenanforderungen an jedem relevanten Eingabepunkt bei der Erfassung der Daten mit jeweils beiden Komponenten (ID und PIN) abgefragt werden kann. Eine Veränderung der Daten macht die Signatur ungültig. Dies wird im Formularfenster angezeigt.
Elektronische Signaturen			
Absatz 11.50: Signature Manifestation			
§ 11.50 (a)	Enthalten die unterschriebenen elektronischen Dokumente folgende Informationen? Gedruckter Name des Unterzeichners Datum und Uhrzeit der Signatur Bedeutung der Signatur (wie Genehmigung, Überprüfung, Verantwortung)	Ja	Die Informationen werden für jede erzeugte Signatur erzeugt und unveränderbar gespeichert.
§ 11.50 (b)	Werden die oben genannten Informationen auf dem Bildschirm angezeigt und	Ja	Die Signaturen werden an der jeweiligen Position im Formular (Dokument) angezeigt. Die

	erscheinen auf gedruckten Kopien des elektronischen Dokuments?		Gültigkeit der Signatur wird ebenfalls angezeigt.
Absatz 11.70: Signature/record linking.			
§ 11.70	Werden Unterschriften mit den jeweils zugehörigen elektronischen Dokumenten verknüpft um sicherzustellen, dass sie nicht getrennt, kopiert oder auf sonstige Weise durch normale Medien für Fälschungszwecke übertragen werden?	JA	Die Signaturen werden Datenbank basiert gespeichert und gelten für einen Datensatz bzw. für einen Bereich eines Datensatzes. (Die Konfiguration dazu ist Studienabhängig und wird durch die Anforderungen des Kunden beschrieben.) ein Übertragen von Signaturen ist technisch nicht möglich.
Elektronische Signaturen (allgemein)			
Absatz 11.100: Allgemeine Anforderungen			
§ 11.100 (a)	Sind elektronische Signaturen eindeutig einer Person zuzuordnen?	Ja	Die elektronischen Signaturen werden durch Eingabe der ID und des Passworts eindeutig einem Benutzer zugeordnet. Da Benutzer IDs eineindeutig sind, ist die eindeutige Zuordnung gewährleistet.
§ 11.100 (a)	Gibt es Verfahren um sicherzustellen, dass die elektronischen Signaturen niemals wiederverwendet oder einer anderen Person zugewiesen werden?	Ja	IDs sind eineindeutig und können nicht einem weiteren Benutzer zugeordnet werden.
§ 11.100 (b)	Wird vor einer elektronischen Signatur die Identität einer Person verifiziert?	NA	In Kundenverantwortung.
§ 11.100 (c)	Bestätigung gegenüber der Behörde, dass die elektronischen Signaturen rechtsverbindlich und den gleichen Stellenwert haben sollen, wie die herkömmlichen eigenhändigen Unterschriften.	NA	In Kundenverantwortung.
Absatz 11.200: Elektronische Signaturen (nicht-biometrisch)			
§ 11.200 (a)(1)(i)	Bestehen nicht-biometrische Signaturen aus mindestens zwei Komponenten, wie Identifikationscode und Passwort, oder Identifikationskarte und Passwort?	Ja	Signaturen benötigen immer die Eingabe von beiden Komponenten: ID und Passwort.
§ 11.200 (a)(1)(ii)	Wenn mehrere nicht-biometrische Signaturen	Ja	Signaturen benötigen immer die Eingabe von beiden

	während einer ununterbrochenen Sitzung geleistet werden, wird dann das Passwort bei jeder Signaturenhandlung gefordert?		Komponenten: ID und Passwort.
§11.200 (a)(1)(ii)	Wenn die Signaturen nicht in einer ununterbrochenen Sitzung geleistet werden, werden dann beide Komponenten der nicht-biometrischen elektronischen Signatur bei jedem Signieren ausgeführt?	Ja	Signaturen benötigen immer die Eingabe von beiden Komponenten: ID und Passwort.
§11.200 (a)(2)	Werden die nicht-biometrischen Signaturen nur von ihren echten Inhabern benutzt?	Ja	IDs sind eindeutig und können nicht einem weiteren Benutzer zugeordnet werden. Die Weitergabe von IDs und Passwörtern ist seitens der iAS GmbH nicht zulässig. Kundenseitig sind entsprechende Vorschriften nötig, die die Weitergabe von Benutzerinformationen untersagen.
§11.200 (a)(3)	Müssten bei dem Versuch der Fälschung einer nicht-biometrischen elektronischen Signatur mindestens zwei Personen kooperieren?	Ja	Die Anwenderverwaltung liegt beim Kunden, entsprechende Verfahren sind vorzugeben.
Absatz 11.300: Kontrollen der Identifikationscodes und Passwörter			
§ 11.300(a)	Gibt es Kontrollen, um die Einmaligkeit von jedem kombinierten Identifikationscode und Passwort zu wahren, so dass keine andere Person die gleiche Kombination von Identifikationscode und Passwort haben kann?	Ja	IDs sind eindeutig und können nicht einem weiteren Benutzer zugeordnet werden.
§ 11.300(b)	Gibt es Verfahren um sicherzustellen, dass die Gültigkeit der Identifikationscodes regelmäßig überprüft / revidiert wird?	NA	In Kundenverantwortung.
§	Erlöschen die Passwörter	Ja	Das System verfügt über eine

11.300(b)	regelmäßig und werden sie revidiert?		eigene Passwortverwaltung. Passwörter müssen eine bestimmte Mindestlänge aufweisen und mindestens einen numerischen Wert enthalten. Passwörter müssen nach vorgegebenen Regeln geändert werden (Standardgültigkeit=6 Monate).
§ 11.300(b)	Gibt es ein Verfahren, um Identifikationscodes und Passwörter wieder aufzurufen, wenn jemand aus der Firma ausscheidet oder versetzt wird?	Ja	Die erfassten Daten stehen unabhängig vom eingebenden Anwender zur Verfügung. Anwender können nicht gelöscht werden.
§ 11.300(b)	Ist das System so konfiguriert, dass es unbefugte Zugriffsversuche feststellen kann?	Ja	Ein Anwenderaccount wird nach drei fehlgeschlagenen Anmeldeversuchen gesperrt und kann nur vom Administrator wieder freigegeben werden.
§ 11.300(c)	Gibt es ein Verfahren zur Änderung eines Passwortes, wenn es potentiell offen gelegt wurde oder abhanden gekommen ist?	Ja	Passwörter können administrativ neu generiert werden.
11.300(c)	Gibt es ein Verfahren zur Verlustverwaltung (loss management), wenn ein Gerät abhanden gekommen ist oder gestohlen wurde?	NA	Nicht zutreffend, da elektronische Signatur.
§ 11.300(d)	Gibt es ein Verfahren, um den Versuch der unbefugten Nutzung festzustellen und das Sicherheitssystem zu informieren?	NA	Nicht zutreffend.
§ 11.300(e)	Gibt es einen Eingangs- und regelmäßigen Test der Token und Karten?	NA	Nicht zutreffend.
§ 11.300(e)	Wird in diesem Test überprüft, ob auch keine unbefugten Veränderungen vorgenommen worden sind?	NA	Nicht zutreffend.

7. Abweichungen

Abweichungen von den gesetzlichen Anforderungen aus AMG/GCP und FDA 21 CFR Part 11 wurden bei der Untersuchung der Software SecuTrial® 2.1 nicht festgestellt. Die Systemarchitektur und besonders die Verfahrensweisen, die zur Nachvollziehbarkeit von Änderungen hinsichtlich der gespeicherten Daten aber auch der Studienkonfiguration bzw. der Änderungen in der Systemverwaltung implementiert sind, stellen in den Kernbereichen weit über die geforderten Minimalanforderungen sicher, dass die behördlichen Anforderungen erfüllt sind.

Allerdings gibt es einen kritischen Punkt in der Erfassung der Patientendaten (Medizindaten). Aus datenschutzrechtlichen Gründen ist es erforderlich, dass alle Datensätze, die für einen Patienten erfasst wurden, dann vollständig gelöscht werden, wenn der Patient sein Einverständnis zur Teilnahme an der entsprechenden Studie zurückzieht und darüber hinaus die Löschung der Daten fordert.

SecuTrial® 2.1 bietet die Möglichkeit für einen Anwender, einen Patienten zum Löschen zu markieren. Dabei stehen zwei Zustände für das Löschen eines Patienten zur Auswahl:

- Nur Löschen des Patienten – Erfasste Daten bleiben zu Auswertungszwecken erhalten, Löschen des Patienten wird geloggt.
- Vollständiges Löschen – Alle Daten, die unter dem Pseudonym dieses Patienten erfasst wurden werden unwiderruflich gelöscht. Löschen des Patienten wird geloggt.

Funktional kann ein Anwender für beide Zustände ausschließlich von einem administrationsberechtigten Benutzer gelöscht werden. Der Vorgang wird in jedem Fall geloggt.

Im ersten Fall gibt es keinerlei Beanstandungen, da die erfassten Daten erhalten bleiben.

Im zweiten Fall empfehlen wir dem Anbieter eine schriftliche Erklärung des Patienten vor dem endgültigen Löschen zu fordern und vorzuhalten, damit einwandfrei nachgewiesen werden kann, warum der entsprechende Patient inklusive der erfassten Daten gelöscht wurde.

8. Zusammenfassung

Die Software SecuTrial® 2.1 der iAS GMBH erfüllt nach unserer Begutachtung alle zutreffenden Punkte der gesetzlich vorgeschriebenen Anforderungen aus AMG und 21CFR Part 11. Die Dokumentation der Software bietet dem Anbieter und Kunden ausreichend Grundlage, die genannten Kriterien nachzuvollziehen.

Die Software SecuTrial® 2.1 in der von der iAS GmbH empfohlenen Konfiguration bietet ausreichend Grundlage um zusammen mit den kundenseitig notwendigen Arbeits- und Verfahrensanweisungen so wie der ordentlichen Systemdokumentation ein validiertes System zu etablieren.

Dieses Gutachten kann als Basis für die Validierung des Systems dienen, sie ersetzt sie allerdings nicht. Des weiteren ist jeder Anbieter und Kunde, der unter den gesetzlichen Anforderungen arbeitet, in der Pflicht, die iAS GmbH hinsichtlich Ihres Qualitätsstandards zu auditieren.

Göttingen, 25. April 2007

Christian Offermann
BioMedion GmbH

9. Anhang

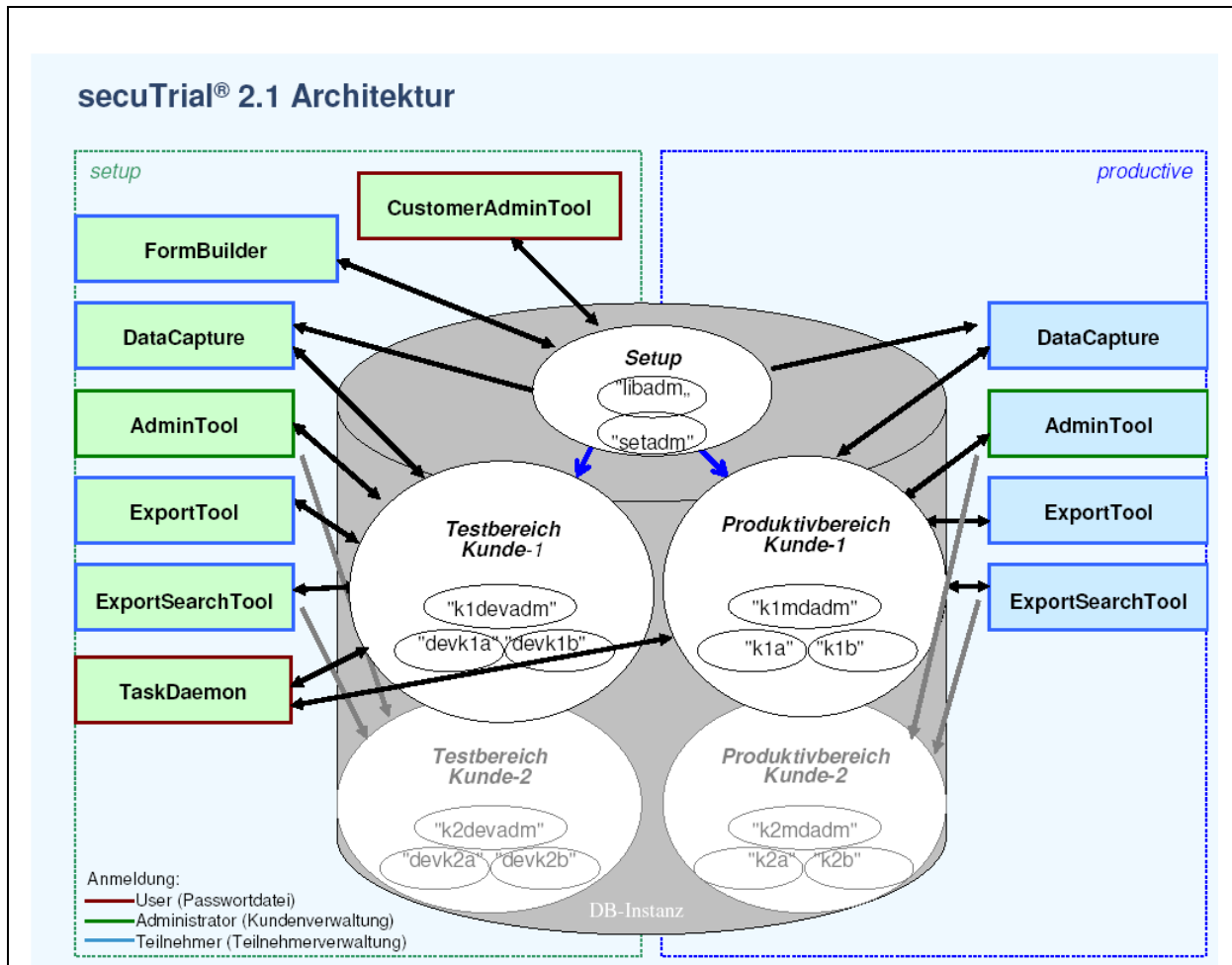


Abb1 Systemarchitektur

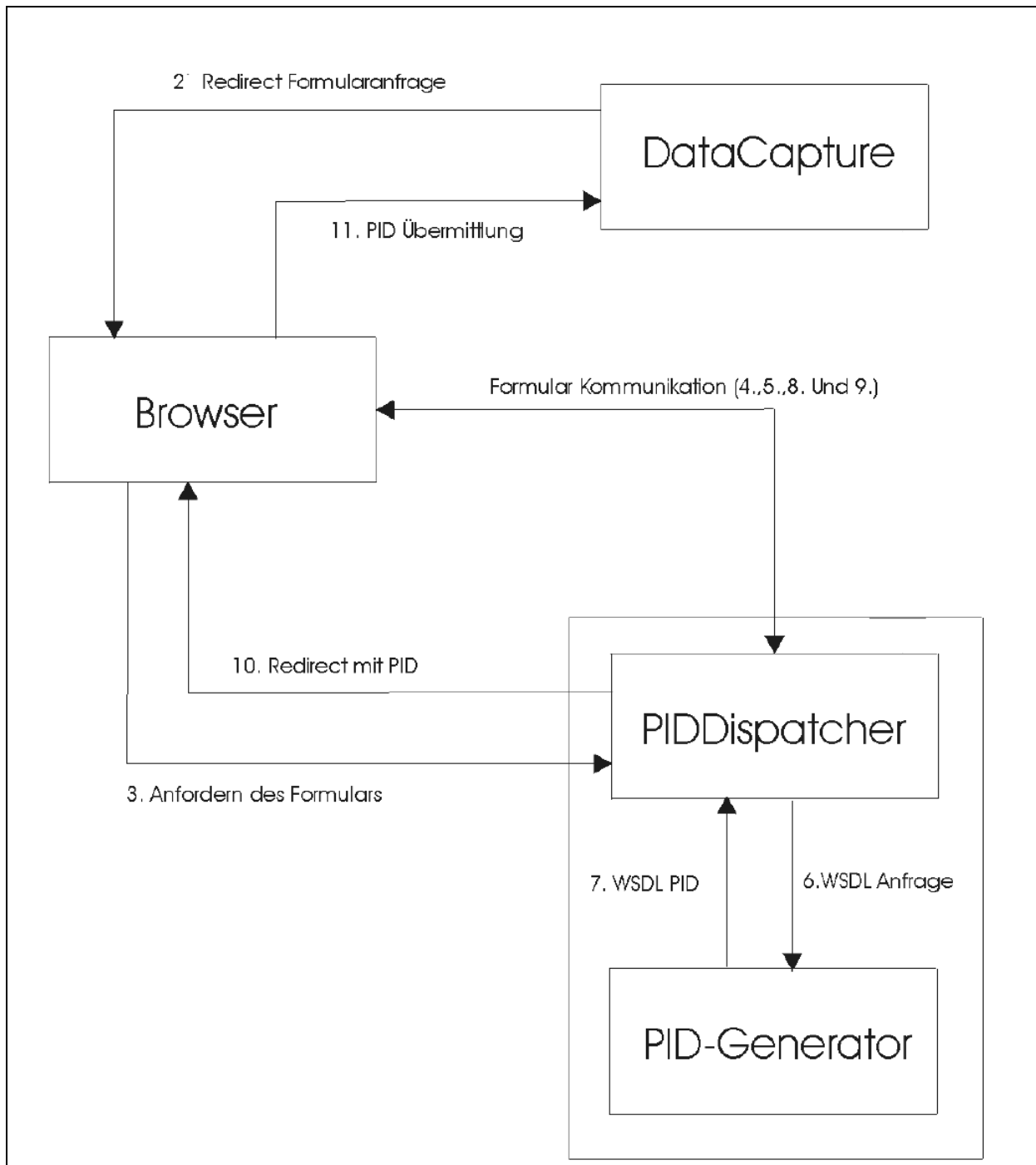


Abb 2 Kommunikation PIDDispatcher