Bundesamt
für Sicherheit in der
Informationstechnik

BSI – Technische Richtlinie

Bezeichnung:	Accountmanagement IT-Sicherheit
Anwendungsbereich:	De-Mail
Kürzel:	BSI TR 01201 Teil 2.3
Version:	1.3

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-0
E-Mail: de-mail@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhaltsverzeichnis

1 Einleitung

Dieses Modul beinhaltet die IT-Sicherheitsanforderungen, die sich speziell auf das Accountmanagement beziehen und über die generellen Anforderungen an die Sicherheit aus dem Modul [TR DM Si M] hinausgehen, und ist Bestandteil von [TR DM ACM M].

2 IT-Strukturanalyse

Die Grundlage für die Erarbeitung dieses Moduls bildet die in [TR DM Si ÜK] angenommene Netzinfrastruktur eines DMDA.

Bei der Erstellung des realen IT-Sicherheitskonzeptes sind die hier enthaltenen Bedrohungen, Sicherheitsziele, zwingenden Anforderungen und Empfehlungen zu berücksichtigen. Näheres regelt [TR DM Si M].

2.1 Erfassung des IT-Verbundes

In diesem Modul wird auf den IT-Verbund verwiesen, der bereits in [TR DM Si ÜK] skizziert ist.

3 Bedrohungen

Folgende generische Bedrohungen werden für das Account Management angenommen:

3.1 Falsche Zuordnung eines De-Mail-Kontos zu einer natürlichen Person bzw. Institution

Bei einer falschen Zuordnung eines De-Mail-Kontos zu einer natürlichen Person bzw. Institution kann das Ziel, eine authentische Kommunikation, die insbesondere auf einer gesicherten Identifizierung, die gesicherte Erfassung der Identitätsdaten und der gesicherten und eindeutigen Zuordnung zum Konto basiert, nicht mehr erreicht werden. Eine falsche Zuordnung oder eine nicht nachvollziehbare Zuordnung kann etwa durch folgende Umstände erfolgen:

- Technisches Versagen
- Menschliches Versagen
- Fehlerhafte Identifizierung
- Manipulation der Zuordnung des De-Mail-Kontos
- Manipulation/Fälschung der De-Konto-Daten inkl. Dokumentation
- Löschung/Verlust von Konto-Daten inkl. Dokumentation

3.2 Missbräuchliche Nutzung eines Accounts

Gelingt es einem Angreifer, in den Besitz der Authentisierungsdaten zu gelangen oder eine Schwachstelle in den verwendeten IT-Verfahren und IT-Systemen auszunutzen, kann er mit der Identität des Kontoinhabers agieren und sich im Rechts- und Geschäftsverkehr als diesen ausgeben.

4 Sicherheitsziele

Dieses Modul enthält die Sicherheitsziele in Bezug auf das Account Management und ergänzt insoweit das [TR DM Si ÜK].

4.1 Zuverlässige Identifizierung und Erfassung der Teilnehmer

Die Erfassung der Identitätsdaten und die Identifizierung des Kontoinhabers muss zuverlässig erfolgen. Die Identitätsattribute der natürlichen Personen und Institutionen müssen eindeutig festgestellt und in die Systeme unverfälscht übernommen werden.

4.2 Nachvollziehbarkeit der Identitätsdaten und der Zuordnung zum De-Mail-Konto

Die Dokumentation der Identitätsdaten und der Zuordnung zwischen Identität und De-Mail-Konto muss zu jeder Zeit vollständig, authentisch und unverfälscht nachvollziehbar sein.

4.3 Verhinderung des unbefugten Zugriffs auf die Authentisierungsinformationen

Der unbefugte Zugriff auf die geheimen und nicht kopierbaren Teile der Authentisierungsinformationen muss ausgeschlossen sein.

4.4 Verhinderung der unbefugten Veränderung von Authentisierungs- und Identifizierungsinformationen

Die unbefugte Veränderung von Authentisierungs- und Identifizierungsinformationen muss ausgeschlossen sein.

5 Anforderungen

5.1 Verifikation von Identitätsattributen

Im Sicherheitskonzept muss mindestens festgehalten werden:

- wie die Identitätsattribute erfasst werden,
- wie die Verifikation durchgeführt wird und
- wie die Übermittlung der Identitätsattribute sowie der Verifikationergebnisse erfolgt.

Bei der Übermittlung muss sichergestellt sein, dass:

- die Identitätsattribute korrekt sind und
- vertraulich übermittelt werden.

Sofern sich der DMDA zur Identifizierung der Nutzer vertrauenswürdiger Dritter bedient, hat er sicherzustellen, dass die Qualität des Gesamtprozesses einschließlich dessen Zuverlässigkeit und Fachkunde auch in diesem Fall gewährleistet wird.

5.2 Erfassung

Die Daten zur Identität sind zuverlässig im System zu hinterlegen und dem De-Mail-Konto zuzuordnen. Die Anbindung des Kontoadministrators an das Accountmanagement muss verschlüsselt, integer und authentisiert erfolgen. Für die Authentisierung sind Mechanismen wie bei dem Authentisierungsniveau „hoch“ einzusetzen.

5.3 Authentisierungsniveaus

Für die Authentisierung des Nutzers sind folgende Authentisierungsmethoden für die beiden zugelassenen Authentisierungsniveaus vorzusehen:

- Normal
  - Die Authentisierung erfolgt mittels Konto-Name und Passwort. Es ist insbesondere die Maßnahme „2.11 Regelung des Passwortgebrauchs“ aus dem IT-Grundschutz zu beachten. Des Weiteren ist die maximale Gültigkeitsdauer für ein Passwort ein Jahr.
- Hoch
  - Die Authentisierung muss mit zwei von einander unabhängigen Sicherungsmitteln z. B. mit Besitz und Wissen erfolgen. Das Authentisierungstoken muss sicherstellen, dass das Geheimnis nicht kopiert und ausgelesen werden kann. Des Weiteren muss die Einmaligkeit der Authentisierungsinformationen, die innerhalb eines Anmeldeprozesses übertragen werden, gewährleistet sein. Die Authentisierung muss gleichen Anforderungen bei falscher Authentisierung und den Freischaltprozess erfüllen, wie das Authentisierungsniveau „normal“. Es sind die Anforderungen an die kryptographischen Verfahren und Schlüssellängen aus [TR 02102] zu beachten.

5.4 Authentisierung des Nutzers

Es ist sicherzustellen, dass der Nutzer keinen Zugriff auf sein De-Mail-Konto hat, bevor er sich ordnungsgemäß authentisiert hat. Der Nutzer hat sich jeweils vor Zugriff auf sein Konto gegenüber dem Dienst des DMDA mit Authentisierungsniveau „normal“ oder „hoch“ zu authentisieren.

Die Authentisierungsinformationen des Nutzers werden auf ihre Gültigkeit hin geprüft. Im Erfolgsfall wird der Nutzer zur Nutzung der gestatteten Funktionen autorisiert. Im Fehlerfall wird eine Fehlermeldung ausgegeben.

Der DMDA hat sich davon zu überzeugen, dass die bei der Erzeugung des Tokens für das Authentisierungsniveau „hoch“ eingesetzten Prozesse eine hinreichende Qualität und Vertrauenswürdigkeit in Bezug auf das angestrebte Authentisierungsniveau aufweisen. Wenn als Authentisierungstoken für das Authentisierungsniveau „hoch“ der nPA zum Einsatz kommt, darf der DMDA ohne weiteres von der Eignung des Tokens und der Ordnungsmäßigkeit der diesbezüglichen Prozesse ausgehen.