

CR 407 (((etiCORE: Applikations-Monitoring und defekte Medien beim PO

Autor? Pflichtfeld
Hoffmann, Wilk

CR Nummer
Dieses Feld ist nicht manuell ausfüllbar und wird automatisch vom System bei der Erstellung eines Workflow-Prozesses beschrieben.
407

Titel der Änderungsanforderung?
Pflichtfeld
(((etiCORE: Applikations-Monitoring und defekte Medien beim PO

Anfordernde Instanz?
Pflichtfeld
VDV ETS

Ansprechpartner (technisch)?
Pflichtfeld
Hoffmann, Wilk

Datum des Änderungsantrags
26.03.2026

Betroffene Komponenten
☐ Personalbedientes KVPT
☐ Kundenbedientes KVPT
☒ KVPS
☐ DLT
☐ DLS
☒ PVS

Begründung des CRs
Problembeschreibung, welche Folgen hätte die Beibehaltung des Problems
Hinweis: Weitere betroffene Komponenten: Hotlist-Service, eTicket Security Hub ESH, siehe auch Umsetzung

PO -Erweitertes Monitoring – notwendige Umsetzung

- Für den PO bleiben Berechtigungen aktiv, obwohl eine Applikation gehotlistet, gesperrt oder terminiert wurde, weil er zurzeit kein Wissen über den Zustand der Applikation hat
- Für den PO besteht keine Möglichkeit, Meldungen von Berechtigungen zu monieren, deren übergeordnete Applikation vom Zustand „OK“ abweicht oder sich auf der Hotlist befindet

Durch die fehlenden Informationen von Applikations-Hotlist und Statusmeldungen zu Applikationen hat der PO kein vollständiges Bild und kann auch damit einige Monitoring Prüfungen nicht durchführen.

Mit diesem CR

- Muss in Zukunft der PO auch die Applikations-Hotlist vom Hotlist-Service abholen können
- Muss der PO in Zukunft an einer zentralen Stelle (ESH) eine Statusliste für Applikationen abrufen
- Muss der primäre CCP in Zukunft an einer zentralen Stelle (ESH) die Applikationsmeldungen für Statusänderungen einreichen

Durch die neuen Informationen zu Applikations-Hotlist und Applikations-Statusmeldungen kann das Monitoring in Zukunft erweitert und zentralisiert werden:

- Beheben des Problems bei gesperrten oder terminierten Applikationen: Der PO kann ein Applikationsregister für die bei ihm gemeldeten Berechtigungen führen, welches alle möglichen Zustände der Applikation berücksichtigt inklusive des virtuellen Zustands „Hotlisted“.
- Beheben des Problems bei gehotlisteten Applikationen: Das Monitoring des PO kann jetzt auf Meldungen von Berechtigungen reagieren, deren übergeordnete Applikation vom Zustand „OK“ abweicht oder sich auf der Hotlist befindet

Hinweis: Dieser CR schließt eine Lücke für ein Melden von gültigen (Deutschland-) Tickets an eine zentrale Stelle für Statistik und eine potenzielle Einnahmenaufteilung und verbessert den gemeldeten Datenbestand.

CCP Erweitertes Monitoring – optionale Umsetzung

Der CCP wird zurzeit nicht darüber informiert, wenn „fremde“ Medien, auf denen sich eine Berechtigung des CCP befindet, gesperrt oder terminiert werden. Durch Abruf der Liste kann das CCP-System diese Lücke schließen und z.B. für den betroffenen Kunden eine Ersatzberechtigung ausstellen.

PO – Defekte und verlorene Medien – optionale Umsetzung

Der PO kann angefragt werden, um aus seiner Sicht gültige Berechtigungen für eine übergebene Applikations-Instanz-ID zu ermitteln. Dabei werden nur zeitlich gültige, nicht gesperrte Berechtigungen gemeldet. Dies kann z.B. zur Unterstützung eines EBE-Prozesses beim SO genutzt werden.

Bisher (etiCORE Release Candidate 6) hat der PO aber keine Informationen über den Status der zugrundeliegenden Applikation („Hotlisted“, „Gesperrt“, „Terminiert“). Der PO weiß zurzeit nicht, ob die angefragte Applikation einen gültigen Status hat.

Damit kann das Beauskunften über vorhandene Berechtigungen nicht alle Ausnahmen abdecken und birgt Betrugspotential.

Durch diesen CR erhält der PO das Wissen und kann in Zukunft zusätzlich die Berechtigungen ausfiltern, für die die Applikation auf der Hotlist, gesperrt oder terminiert ist.

Änderungsfristen seitens Antragsteller

Welche Änderungsfristen werden seitens des Antragstellers benötigt?

Beschluss der Teilnehmer möglichst vor Einführung des endgültigen ersten ((etiCORE Releases (Einführung Ende 2026).

Hinweis zur Art der Änderung: Einige Teile wären verpflichtend, andere sind optional, siehe CR-Text in der Umsetzung.

Art der Änderung

sonstige

Umsetzungsvorschlag

Wie soll die Änderung erfolgen?

* Verpflichtende Umsetzung für ESH, Hotlist-Service und PO für das Monitoring * Zusätzlich verpflichtende Umsetzung für den PO, wenn die Auskunftsfunktion für defekte Medien umgesetzt ist bzw. werden soll. Die Auskunftsfunktion selbst für defekte Medien ist optional * Verpflichtende Umsetzung für den CCP für das Einreichen von Statusmeldungen * Optionale Erweiterung für CCP für das Monitoring von Berechtigungen auf fremden User Medien Hotlist-Service Der Hotlist-Service muss zukünftig das Abholen der Application-Hotlist auch für das PO-System zulassen. ESH Das ESH muss in Zukunft alle Zustände der chipkartenbasierten Applikationen festhalten, die nicht den aktiven Zustand „OK“ beinhalten. Dazu muss es die Attestations zu den Statusänderungen empfangen. * Gesperrt: Der primäre CCP leitet seinen Sperrnachweis für die Applikation an das ESH weiter. Der Eintrag wird auf die Liste gesetzt mit „Gesperrt“ * Entsperrt: Der primäre CCP leitet seinen Entsperrnachweis[1] für die Applikation an das ESH weiter. Dadurch wird im ESH die Applikations-Instanz-ID entfernt, da dann die Applikation wieder den Zustand „OK“ hat. Der Eintrag für die Applikation ist dann nicht mehr auf der Liste * Terminiert: Der primäre CCP leitet seinen Terminierungsnachweis für die Applikation an das ESH weiter. Der Eintrag wird auf die Liste gesetzt mit „Terminiert“ Bereitstellen der Liste: Das ESH stellt eine Liste aller Applikationen bereit, deren Zustand <> „OK“ ist und deren Zertifikate nicht abgelaufen sind. Diese Liste kann von einem PO oder CCP angefordert und synchron an die anfragenden Systeme übermittelt werden. Dabei wird in der Antwort das in ((etiCORE spezifizierte, gepackte Format für Listen verwendet. Die Liste selbst ist nach dem Entpacken im XML-Format. Pro Applikation sind mindestens die Applikations-Instanz-ID und der Zustand der Applikation enthalten. Weitere Felder können noch geklärt werden (z.B. das Datum der Statusänderung). PO Der PO muss die Application-Hotlist vom Hotlist-Service abholen und in seinen Datenbestand integrieren. Der PO muss die Statusliste für chipkartenbasierte Applikationen vom ESH empfangen können und in seinen Bestand integrieren. Dabei muss immer der Bestand durch die neueste Statusliste ersetzt werden. Applikationen beim PO mit dem Zustand „Gesperrt“, deren Applikations-Instanz-ID nicht (mehr) in der ESH-Statusliste und nicht in der Hotlist enthalten ist, muss auf den Zustand „OK“ zurückgesetzt werden. Für den PO ergeben sich damit ein komplettes Bild für den Lifecycle einer Applikation und damit neue Monitoring-Prüfungen: * Bei allen Meldungen von Berechtigungen: 1. ist die zugehörige Applikation auf der Hotlist? -> Hotlist nicht aktuell beim Meldungserzeuger. 2. Gibt es für die zugehörige Applikation einen Sperrnachweis oder eine Terminierung? -> ggf. ist eine Kopie der Applikation im Umlauf * Das Register für Berechtigungen kann jetzt vollständig geführt werden, da auch die Zustände „Hotlisted“ und „Gesperrt“ und „Terminiert“ der übergeordneten Applikation berücksichtigt werden können CCP Verpflichtend: Der primäre CCP muss in Zukunft seine Informationen zu gesperrten, entsperrten oder terminierten Applikationen an das ESH weiterleiten. Hinweis: Das Weiterleiten von Terminierungen ist zurzeit (etiCORE Release Candidate 6) bereits möglich, aber nicht verpflichtend.[2] Auch Terminierungen wären in Zukunft mit diesem CR verpflichtend an das ESH weiterzuleiten. Optional: Der CCP kann mit diesem CR sein eigenes Monitoring erweitern, indem er ebenfalls die Zustandsliste für Applikationen vom ESH abholt. Hintergrund: wurde eine Berechtigung des CCP (Entitlement-Owner) auf einem UM eines anderen CCP (UM-Owner) ausgegeben, so wird der Entitlement-Owner jetzt über Zustandsänderungen der Applikation informiert und kann entsprechend für die seine ausgegebene Berechtigung reagieren. PO – Defekte und verlorene Medien Der PO kann angefragt werden, um gültige Berechtigungen für eine übergebene Applikations-Instanz-ID zu ermitteln. Dabei werden nur zeitlich gültige, nicht gehotlistete (auch nicht per SAM[3] oder Organisation!) und nicht gesperrte Berechtigungen gemeldet, die sich innerhalb einer gültigen Applikation befinden. Dies kann z.B. zur Unterstützung eines EBE-Prozesses beim SO genutzt werden. Vor dem Senden der Antwort überprüft der PO * für die übergebene Applikations-Instanz-ID seinen Bestand für Applikationen und prüft, ob die Applikation den Zustand „Hotlisted“, „Gesperrt“ oder „Terminiert“ hat. * ob es zu der angefragten Applikation Berechtigungen in seinem Bestand gibt * ob die gefundenen Berechtigungen zeitlich gültig sind und nicht auf der Hotlist stehen (auch nicht per SAM- oder Organisations-Hotlist-Eintrag) * ob die gefundenen Berechtigungen nicht gesperrt oder terminiert sind * ob es offene Klärfälle für die relevanten Berechtigungen gibt (z.B. Timeout bei der Ausgabe) Verbleibende Berechtigungen werden als Liste in der Antwort zurückgegeben. **Hinweis**: Der primary CCP erhält vom Teilnehmer, der das defekte Medium erfasst hat, eine Sperranforderung (Hotlisting Demand) für die Applikation mit dem Sperrgrund „22 – Defective Medium“ (bereits in etiCORE spezifiziert). Damit ist der primary CCP über den Sachverhalt informiert. Durch die Nachricht (Sperranforderung) zu dem defekten Medium kann der pCCP automatisch Betrugsversuche

auf Kundenseite erkennen, insbesondere weil er die Informationen zu den Sperrnachweisen für Applikationen hat. [1]: #_msocom_2 [2]: #_msocom_6 [3]: #_msocom_9

— **Umsetzung durch AGS** —

Umsetzungsvorschlag durch
AGS

Zuordnung zu Komponenten

- ☐ Personalbedientes KVPT
- ☐ Kundenbedientes KVPT
- ☐ KVPS
- ☐ DLT
- ☐ DLS
- ☐ PVS

Zuordnung zu Release

— **Antrag verworfen?** —

Nur auszufüllen, wenn der Antrag verworfen wird.

Verworfen durch

— **Kommentar** —

Kommentar