

(((etiCORE: Weiterleiten von Negativnachweisen (Extended Logging für Berechtigungen und Applikationen)

Optionale Erweiterung, um Informationen zu Negativnachweisen (ungültige Applikationen und Berechtigungen vom Service Operator (SO) oder secondary Customer Contract Partner (sCCP) an Product Owner (PO) und primary Customer Contract Partner (pCCP) weiterzuleiten.

Betroffene Komponenten

SO-System, CCP-System, PO-System

Begründung des CRs

Sobald in (((etiCORE einem Terminal ein Nutzermedium präsentiert wird, erfolgen allgemeine Prüfungen. Zusätzlich werden bei der Kontrolle eines elektronischen Fahrscheins (EFS) die tariflichen Informationen geprüft. In beiden Bereichen können die Prüfungen zu einem „Negativnachweis“ (extended Logging bei ungültiger Berechtigung oder Applikation) führen. Diese Negativnachweise werden zurzeit nur vom Terminal an das zugehörige Hintergrundsystem gesendet.

Dieser CR soll ermöglichen, dass zur Betrugsvermeidung und Datenkonsolidierung die Datensätze in Zukunft auch an PO und pCCP gesendet und ausgewertet werden. Dabei kann z.B. das Ausmaß für gefälschte oder kopierte statische Berechtigungen besser erkannt werden, im Rahmen von Motics können ebenfalls Probleme leichter identifiziert werden.

Änderungsfristen seitens Antragsteller

Rechtzeitig vor der allgemeinen Einführung von (((etiCORE, aufgrund des Stichtages 01.05.2028 sollte der CR spätestens 2027 umgesetzt sein

Art der Änderung

Optionale Erweiterung

Umsetzung des CRs

Die Vorprüfungen sind in (((etiCORE spezifiziert, nachfolgend einige Beispiele:

- Aktueller Zeitpunkt ist außerhalb der zeitlichen Gültigkeit von Applikation und/oder Berechtigung
- Status von Applikation und/oder Berechtigung ist <> „OK“
- Hotlist-Prüfung für Motics Applikationen und statischen Berechtigungen inklusive beteiligter SAMs und Organisationen
- Tarifliche Kontrolle:
 - Örtliche und/oder persönliche Gültigkeit nicht gegeben

Schlägt eine dieser Prüfungen fehl, so wird ein spezieller Datensatz vom Terminal zum Hintergrundsystem gesendet (tLogInvalidEntitlement oder tLogInvalidApplication).

In Zukunft sollen diese Nachrichten an PO und pCCP weitergeleitet werden.

Wie bei anderen ION-Nachrichten auch, deren Ursprung vom Terminal kommt, muss die Terminal-Nachricht in eine ION-Nachricht umgewandelt werden. tLogInvalidEntitlement wird zu logInvalidEntitlement und zum PO weitergeleitet. Dieser macht o.g. Monitoring Prüfungen und leitet die Nachricht mit forwardInvalidEntitlementLog an den pCCP weiter. Dieser führt ebenfalls Monitoring Prüfungen durch.

Eine im Hintergrundsystem von Service Operator (SO) oder secondary CCP (Fremd-KVP) eingehende Nachricht „tLogInvalidApplication“ wird per logInvalidApplication an den zuständigen pCCP geleitet.

Der PO prüft aufgrund der in den Negativnachweisen enthaltenen Validierungscode (siehe ValidationEnum in terminal.xsd), wo potenziell gehäuft Betrugsfälle auftreten. Der pCCP wird ebenfalls informiert und kann entsprechend im Rahmen seiner Möglichkeiten Abhilfe schaffen.

- Bei Ablehnung von statischen Berechtigungen aufgrund von Hotlist-Einträgen kann die Menge und die räumliche Verbreitung der Fälschungen/Kopien ermittelt werden
- Die Ablehnung von Motics-Applikationen kann ausgewertet werden
- Falsch ausgestellte statische Berechtigungen mit/ohne Motics werden sichtbar
- Gründe für das Scheitern tariflicher Prüfungen sowie die Menge und ggf. räumliche Häufungen werden sichtbar gemacht

Umsetzung durch AG-S

In den Vorprüfungen und bei der tariflichen Prüfung können Negativnachweise entstehen, die auf die Ungültigkeit von Applikation und/oder Berechtigung schließen lassen. Diese Negativnachweise werden via tLogInvalidEntitlement oder tLogInvalidApplication vom Terminal an das jeweilige Hintergrundsystem geleitet. Mit diesem CR werden dann gezielt Nachrichten mit speziellen Validierungscodes via ION an die zuständigen Hintergrundsysteme von PO und pCCP weitergeleitet.

Dieser CR ist optional. Für eine funktionierende Nachrichtenkette muss jede betroffene Systemkomponente diesen CR umsetzen:

- Terminal: erzeugen der Nachricht und weiterleiten an das operative Hintergrundsystem
- Operatives Hintergrundsystem von SO und CCP: weiterleiten als ION-Nachricht an das PO-System oder pCCP-System
- PO-System: Empfang und ggf. Weiterleitung an pCCP
- pCCP-System: Empfang von ION-Nachrichten von PO oder sCCP und SO

Im Sinne der Datensparsamkeit werden nur die für das Monitoring relevante Nachrichten weitergeleitet. Das erste Hintergrundsystem muss also die Nachrichten im Hinblick auf den Validierungscode auswerten. Dabei werden nur Nachrichten weitergeleitet, deren Code in nachfolgender Tabelle aufgeführt ist:

Wert	Kurzbeschreibung	Typ
1	Inauthentic Data	Berechtigung oder Applikation
3	Spatially Invalid	Berechtigung
4	Invalid Personal Entitlement	Berechtigung
5	Hotlisted SAM for static Entitlement	Berechtigung
6	Hotlisted Organisation for static Entitlement	Berechtigung
12	Hotlisted static Entitlement	Berechtigung

Wert	Kurzbeschreibung	Typ
13	Hotlisted Motics Application	Applikation
14	SCE-ID found in static entitlement without Motics	Berechtigung
16	SCE-ID in static entitlement with Motics does not match SCE-ID in certificate	Berechtigung

Wie bei anderen ION-Nachrichten auch, deren Ursprung vom Terminal kommt, muss die Terminal-Nachricht in eine ION-Nachricht umgewandelt werden. tLogInvalidEntitlement wird zu logInvalidEntitlement und zum PO weitergeleitet. Dieser macht Monitoring Prüfungen und leitet die Nachricht mit forwardInvalidEntitlementLog an den pCCP weiter. Dieser führt ebenfalls Monitoring Prüfungen durch. Wird die ungültige Berechtigung beim pCCP erfasst, so leitet dieser sie an den PO weiter, der sie ohne Weiterleitung verarbeitet.

Eine im Hintergrundsystem von Service Operator (SO) oder secondary CCP (Fremd-KVP) eingehende Nachricht „tLogInvalidApplication“ wird per logInvalidApplication an den zuständigen pCCP geleitet. Wird die ungültige Applikation direkt beim pCCP erfasst, so wird sie dort ohne Weiterleitung direkt verarbeitet. Einziger verbleibender Validierungscode für ungültige Applikationen ist die „13“ (s.o.).

Der PO prüft aufgrund der in den Negativnachweisen enthaltenen Validierungscodes (siehe ValidationEnum in terminal.xsd), wo potenziell gehäuft Betrugsfälle auftreten. Der pCCP wird ebenfalls informiert und kann entsprechend im Rahmen seiner Möglichkeiten Abhilfe schaffen.

Folgende Prüfungen bzw. Auswertungen sind aufgrund der Negativnachweise möglich.

PO (primär) /pCCP (nach Weiterleitung):

- Bei Ablehnung von statischen Berechtigungen aufgrund von Hotlist-Einträgen kann die Menge und die räumliche Verbreitung der Fälschungen/Kopien ermittelt werden
- Falsch ausgestellte statische Berechtigungen mit/ohne Motics werden räumlich und quantitativ sichtbar
- Gründe für das Scheitern tariflicher Prüfungen sowie die Menge und ggf. räumliche Häufungen werden sichtbar gemacht

Nur pCCP:

- Die Ablehnung von Motics-Applikationen kann örtlich und quantitativ ausgewertet werden