Das Berechtigungssystem muss an vielen Stellen überarbeitet werden:

- Fehler geschildert in https://github.com/gematik/api-telematik/pull/2
- Der Resource Match in dieser Policy https://github.com/gematik/api-telematik/blob/4.0.2-Pre1/fd/phr/appc/policy-hcp-perm-cat-other.xml#L10 kann mit der String-equal Funktion auf einen CodedValue (nur mit Codesystem) nicht funktionieren. Beabsichtigt ist ein Vergleich auf practiceSettingCode = 1.3.6.1.4.1.19376.3.276.1.5.4. Offenbar ist die Vergleichsfunktion schlicht falsch (Copy/Paste)
- In einigen Policies befindet sich beim Codesystem noch ein "Todo", u.a. https://github.com/gematik/api-telematik/blob/4.0.2-Pre1/fd/phr/appc/policy-hcp-perm-cat-gynaecology_urology.xml#L12. Muss nachgepflegt werden bei den mittelgranularen Berechtigungskategorien: "ega", "practitioner", "hospital", "laboratory", "physiotherapy", "pychotherapy", "dermatology", "gynaecology_urology", "dentistry_oms", "other_medical", "other_non_medical"
- Einige Permission Policies liefern immer Deny (bspw. aber nicht ausschließlich):
  - https://github.com/gematik/api-telematik/blob/OPB4/fd/phr/appc/policy-hcp-perm-cat-gynaecology_urology.xml
  - https://github.com/gematik/api-telematik/blob/OPB4/fd/phr/appc/policy-hcp-perm-cat-care.xml
- https://github.com/gematik/api-telematik/blob/OPB4/fd/phr/appc/policy-hcp-perm-level-normal.xml

- Alle PolicySetIDs müssen URN-encoded UUIDs sein, was bisher nicht der Fall ist.
- gemSpec_Dokumentenverwaltung#9.2 Policy Document für einen Vertreter und Versicherte: Die Policies enthalten keine Permit oder Deny Rule. Eine Berechtigungsprüfung wird hier zu keinem Ergebnis kommen. Hier ist eine Überarbeitung notwendig.
- Wenn ein Dokument nicht auf der Whitelist steht, aber durch eine Kategorieberechtigung freigegeben ist, ist es trotzdem nicht sichtbar (kein Permit). In der Beispielpolicy (https://github.com/gematik/api-telematik/blob/OPB4/fd/phr/appc/policy-hcp-base-max-example.xml) für einen HCP wird die Whitelist auch zweimal von der Policy-Engine verarbeitet (einmal durch PolicySet von Zeile 66 und einmal durch das PolicySet von Zeile 4) und speziell im "letzten" Fall (Zeile 271, als Teil vom PolicySet Zeile 4), ergibt sich immer ein Deny. Wird noch geprüft, wahrscheinlich Anpassung notwendig
- Unter Kapitel 9.1, Tabelle 46: "Tab_Dokv_500 - XACML 2.0 Policy für einen Versicherten" ist im Knoten "Target" das Element "text() angegeben. Dies ist ein Überbleibsel einer PolicySet-Referenz, die in ePA2 nicht mehr benötigt wird
- Alle Policies (Base, Permission) auslagern per XML, da die Übertragung der Policies in XML ansonsten häufig zu Fehlern führt bei den Herstellern.
  - d.h. keine Policy-Strukturen mehr in der Spezifikation
  - In Spec nur Erläuterungen und Verweis in AFO(s) auf XML (d.h. dann wohl github).
- Filtern nach bestimmten Policies ermöglichen (Metadaten)

© gematik – öffentlich_Entwurf

    - Alle von Base-Policy referenzierten Policy(Set)s in die Metadaten der Base Policy (DocumentEntry.referenceIdList) aufführen
    - Suchen (Queries) prüfen und anpassen, sofern notwendig
- Behandlung von Elternnotiz in U-Heft
    - Versicherter kann bisher Elternnotiz nur lesen; muss sie auch einstellen können (C,U,R,D, M noch nicht geklärt)
    - Umsetzung:
        - Rechtematrix (=Zugriffsunterbindungsregeln DokV) wird nicht angepasst
        - Stattdessen stellt Rechtematrix maximale Rechte der Zugriffsgruppen dar
        - Maximale Rechte können ggf. weiter über Vorgaben in JSON-Dateien zu den einzelnen MIOs/strukturierten Dokumenten eingeschränkt werden
        - Entsprechend Formulierung muss unter die Rechtematrix ergänzt werden, etwa:
          Die DokV MUSS die angegebenen Zugriffsrechte als maximale Zugriffsrechte für die abgebildeten Nutzergruppen durchsetzen und ggf. weitere spezifischere Zugriffsrechte gemäß JSON-Dateien […] durchsetzen.
        - Die JSON-Datei für das U-Heft muss entsprechend (ggf.) überarbeitet werden, um die Rechte entsprechend widerzuspiegeln
    - Blacklisting/Whitelisting auf MIO-Teildokumente nicht erlaubt
- Aufnahme eines Hinweistextes im FdV, dass Versionen über Blacklists/Whitelists bei Document Replace nicht aktualisiert werden
- Dokumentenverwaltung: Prüfung KTR=oid_epa_ktr sicherstellen, ggf. auch in Policy aufnehmen
- LEI-Dokumente (z. B. MIOs) nur als ganzes berechtigen (analog zum Löschen
- FdV: Löschen von Ordnerzuordnungen explizit verbieten. Setzen neuer Ordnerzuordnungen explizit verbieten. (d.h. beim Einstellen eines Dokuments kann natürlich schon der Ordner eGA angegeben werden).
    - Informellen "Folder Management" Text im FdV mit überarbeiten
    - Ausnahme: 1a*-Kategoriezuordnung (und damit Folder) sollen vom Versicherten geändert werden können -> separater Änderungseintrag
- Gelöschten Dokumente müssen von der Whitelist entfernt werden
- Gelöschte Dokumente dürfen NICHT von der Blacklist gelöscht werden
- Verstecken von einzelnen Sammlungsdokumenten (mixed, uniform) durch den Versicherten verbieten
    - Mindestens zu prüfen: Blacklisting, Änderung confidentialityCode auf vertraulichere Stufe, weitere?
- Freigaben/Sperren von Ordnerinstanzen ermöglichen
    - Auf Black/Whitelist setzen
        - Suchen nach Ordnern, für die LEI nicht berechtigt ist, müssen dann aus Ergebnisliste entfernt werden
        - FdV#A_20774 auch entsprechend anpassen (Freigabe von MIOs über Whitelisting einzelner Dokumente)

© gematik – öffentlich_Entwurf

- Einige MIOs (Typ uniform) werden ebenfalls auf Ordner umgestellt, um verschiedene Versionen dazugehöriger Dokumente verwenden zu können
  - In dem Rahmen muss noch die Berechtigungsverwaltung und die DM-Kategorien angepasst werden (+ mglw Leitfaden, FdV?)
- Berechtigungen auf die Elternnotiz für Versicherten sollen separat behandelt werden
  - d.h. Rechte gehen über die üblichen Kategorierechte, die dem Versicherten eingeräumt werden (z. B. childrecord) an der Stelle hinaus
  - Umsetzung möglicherweise über "Zwitterstatus" der Elternnotizdokumente, d.h. ein solches Dokument gehört zu Kategorien patientdoc und childrecord gleichzeitig
  - Ermöglicht Erstellen, Löschen und Aktualisieren und auch Blacklisten sowie auch einzelnes Whitelisten dieses Dokuments durch den Versicherten
  - Denke "Versicherter darf Operation auf Dokument als Kategorie patientdoc oder Kategorie U-Heft ausführen"
  - Exakte Umsetzungsdetails sind noch auszuarbeiten
- Policy für eMP-Kategorie prüft derzeit nur auf den Medikationsplan selbst, nicht auf die Einwilligung. Es ist sinnvoll, dass die Policy beide Arten von Dokumenten in der Kategorieprüfung für eMP zulässt
- Die APPC-Erweiterung "urn:ihe:iti:appc:2016:document-entry:related-folder:code" muss in der Dokumentenverwaltung spezifiziert werden. Es handelt sich um eine XACML-Prüfung, die prüfen soll, ob ein Dokument in einem Ordner liegt, der einen bestimmten Code in seiner codeList verwendet.
- Dokumente, die noch nicht hochgeladen wurden, können auf die Blacklist gesetzt werden, d.h. die Dokumentenverwaltung darf Policies annehmen, auf denen Dokumente auf der Blacklist stehen, die zu diesem Zeitpunkt nicht in der Dokumentenverwaltung vorliegen.

© gematik – öffentlich_Entwurf