## *1. Set de metode de acces*

IBM Cloud oferă securitate funcțională, de infrastructură și operațională pentru platforma de bază. Cu toate acestea, IBM Cloud Local este unic prin faptul că fiecare client furnizează propria infrastructură și centru de date, deținând securitatea fizică.

Mediul de cloud de pe IBM Cloud este compatibil cu cele mai restrictive standarde de securitate ale tehnologiei informației IBM (IT), care respectă sau depășesc standardele din industrie. Aceste standarde includ următoarele: rețeaua, criptarea datelor și controlul accesului:

- Testarea ACL (Access Control Lists), permisiunilor și posibilităților de penetrare.
- Identificarea, autentificarea și autorizarea.
- Protecția informațiilor și a datelor
- Serviciul de integritate și disponibilitate a datelor
- Managementul vulnerabilităților și erorilor
- Detectarea atacurilor de tip Denial of service, dar și a celor sistematice
- Răspuns la incidentele de securitate

Aplicația Android va fi accesată folosind o autentificare particularizată pentru a utiliza Mobile Client Access client SDK pentru accesul clienților, realizându-se totodată și conectarea la IBM Cloud. Mobile Client Access client SDK pentru clientul mobil oferă interfața AuthenticationListener, astfel încât să se poată implementa un flux de autentificare personalizat. Interfața AuthenticationListener expune trei metode care sunt apelate în diferite faze în timpul procesului de autentificare: metoda onAuthenticationChallengeReceived care este folosită atunci când apare o cerere de autentificare personalizată de la serviciul Mobile Client Access, metoda onAuthenticationSuccess care este apelată după o autentificare reușită și metoda care se apelează în caz de eșec al autentificării. După crearea interfeței personalizate AuthenticationListener, aceasta va trebui înregistrată înainte de a începe utilizarea folosind BMSClient. După ce se inițializează clientul SDK și se înregistrează interfața AuthenticationListener personalizată, se poate începe să se facă cereri pentru aplicația back-end mobilă. Pentru a obține un jeton de autentificare ce poate fi utilizat pentru a gestiona jurnalele stocate într-un anumit spațiu de lucru se va utiliza metoda UAA (User Account and Authentication). Jetonul de autentificare se poate obține fie utilizând cloud-ul IBM Cloud CLI (Command Line Interface), fie utilizând Login REST API. Pentru a putea gestiona jurnalele utilizând un jeton de autentificare UAA, va fi nevoie să se obțină următoarele informații: un jeton UAA pentru a accesa serviciul Log Analysis folosind API-urile RESTful și GUID-ul (Globally Unique IDentifier) spațiului de lucru.

Managementul accesului se face prin intermediul listelor de control al accesului (ACL), prin URL-uri semnate în prealabil, sau prin autentificare. În cazul folosirii listelor de control al accesului autentificările sunt generate pentru fiecare instanță de stocare, nu pentru utilizatori individuali. Ca atare, ACL-urile nu au capacitatea de a restricționa sau de a acorda acces la un anumit utilizator, ci doar la o instanță de stocare. Cu toate acestea, se poate permite oricărei alte instanțe de stocare COS (Cloud Object Storage), precum și publicului larg, să acceseze resursa. În cazul URL-urilor semnate în prealabil este posibil să se creeze URL-uri care pot fi setate să expire atât pentru cererile PUT, cât și pentru cele GET, utilizând un CLI, un SDK sau o bibliotecă. În cazul autentificării fiecare solicitare făcută IBM COS utilizând API-ul S3 trebuie autentificată utilizând o implementare a header-ului de autorizare AWS (Amazon Web Services). IBM COS acceptă metode de autentificare Signature Version 2 și Signature Version 4. Signature

Version 4 este considerată mai sigură, deoarece folosește mai degrabă o cheie derivată decât cheia de acces secret ca parte a semnăturii. Utilizarea unei semnături oferă posibilitatea verificării identității și integrității datelor în tranzit și, deoarece fiecare semnătură este legată de marcajul de timp al cererii, nu este posibilă reutilizarea antetelor de autorizare. Header-ul este compus din patru componente: o declarație a algoritmului, informații despre acreditare, anteturi semnate și semnătura calculată.