Përshkrimi i projektit të dytë – Siguria e të Dhënave

Vlerat në bold i merrni për projektin tuaj nga lista e faqës tjetër.

Serveri

1. Të shkruhet një **TCP**/**UDP** server i autorizimit i cili ruan shfrytezuesit në mënyrë të sigurt në bazë të shënimeve **MYSQL**/**JSON**/**XML** duke shfrytëzuar teknikat e salted hashing për ruajtje të fjalëkalimeve.
2. Përveç informatave të shfrytëzuesit, serveri i autorizimit ruan të dhënat e **shpenzimeve** (lloji fatures, viti, muaji, vlera ne euro) për shfrytëzuesin. Shfrytëzuesi duhet ta ketë së paku edhe një atribut shtesë sipas dëshirës.
3. Serveri i autorizimit ka një çelës publik **XML**/**X.509** i cili dihet paraprak- isht nga të gjitha palët tjera.

Klienti

1. Të shkruhet një klient i cili ofron dy shërbime: krijimi i shfrytëzuesve, qasja në llogarinë e shfrytëzuesve ekzistues dhe regjistrimi i shpenzimeve.
2. Procesi i regjistrimit shkon duke ia dërguar të dhënat e shfrytëzuesit serverit të autorizimit i cili kthen përgjigjen përkatëse (OK ose ERROR).
3. Procesi i qasjes (login) shkon duke ia dërguar llogarinë dhe fjalëkalimin serverit të autorizimit i cili kthen përgjigjen përkatëse (OK ose ERROR).
4. Në rast të qasjes (login) me sukses serveri i autorizimit duhet ta kthejë një **JWT**/**XML** të nënshkruar me çelësin e vet privat në të cilin gjenden faktet rreth shfrytëzuesit (id, të dhënat e shfrytëzuesit).
5. Klienti duhet ta vërtetojë nënshkrimin e serverit dhe në rast suksesi duhet ta shfaqë një pamje ku gjenden faktet rreth shfrytëzuesit. Në rast të dështimit të validimit të nënshkrimit të shfaqet mesazhi përkatës i gabimit.

Komunikimi klient-server
Të gjitha kërkesat që klienti i dërgon te serveri i autorizimit duhet të jenë të enkriptuara me CBC DES. Skema e mesazheve duhet të jetë:

base64(<IV>+rsa(<KEY>)+des(<MSG>))

ku <IV> dhe <KEY> gjenerohen rastësisht (duke thirrur crypto API për gjenerim të sigurt të vlerave random). Çelësi simetrik <KEY> duhet të enkriptohet me çelësin publik të serverit të autorizimit. Të gjitha përgjigjet e kthyera nga serveri duhet të jenë të enkriptuara me çelësin e njejtë (<KEY>) të formës base64(<IV'>+des(<MSG>)) ku <IV'> është vlerë tjetër e rastit. Simboli + paraqet vargëzimin e bajtave.

Grupi	Protokoli	Baza e shënimeve	Çelësi publik	Nënshkrimi
1	UDP	XML	X.509	JWT
2	UDP	XML	XML	JWT
3	TCP	JSON	XML	JWT
4	UDP	JSON	XML	XML
5	UDP	XML	X.509	JWT
6	UDP	XML	X.509	XML
7	UDP	MYSQL	XML	JWT
8	TCP	JSON	XML	XML
9	UDP	JSON	X.509	JWT
10	UDP	JSON	X.509	XML
11	TCP	MYSQL	X.509	XML
12	UDP	MYSQL	X.509	XML
13	TCP	XML	X.509	XML
14	UDP	XML	X.509	XML
15	TCP	XML	X.509	XML
16	TCP	JSON	XML	XML
17	TCP	XML	XML	XML
18	UDP	XML	XML	XML
19	UDP	MYSQL	X.509	JWT
20	TCP	JSON	X.509	XML
21	TCP	JSON	XML	XML
22	TCP	MYSQL	X.509	JWT
23	UDP	MYSQL	X.509	XML
24	UDP	JSON	XML	JWT
25	TCP	XML	XML	JWT
26	UDP	MYSQL	XML	XML
27	TCP	MYSQL	X.509	JWT
28	UDP	XML	XML	XML
29	TCP	XML	XML	JWT
30	UDP	JSON	X.509	JWT
31	UDP	MYSQL	X.509	JWT
32	UDP	JSON	X.509	XML
33	TCP	XML	X.509	XML
34	UDP	XML	X.509	XML
35	TCP	JSON	XML	XML

36	TCP	MYSQL	X.509	JWT
37	TCP	JSON	XML	JWT
38	UDP	JSON	XML	XML
39	UDP	XML	X.509	JWT
40	UDP	XML	X.509	XML
41	UDP	MYSQL	XML	JWT
42	TCP	JSON	XML	XML
43	UDP	JSON	X.509	JWT