Detyra e dytë nga lënda 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 **studentit** (fakulteti, nota mesatare) / **mësimdhënësit** (titulli, paga) / **punëtorit** (pozita, paga) 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 paraprakisht nga të gjitha palët tjera.

Klienti

1. Të shkruhet një klient i cili ofron dy shërbime: krijimi i shfrytëzuesve dhe qasja në llogarinë e shfrytëzuesve ekzistues.
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 1 (Ass. Edon Gashi)

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

Grupi 2 (Ass. Arbnor Halili)

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