1. (1) 4 osnovna elementa SOA Governance.
Pravila postupanja, procesi, metrika i organizacija.

2. (2) Uloga registra, repozitorija i po čemu se razlikuju.
Registar pohranjuje informacije o uslugama: definicije, sučelja, operacije, parametri.
Repozitorij je mjesto pohrane podataka, omogućuje korištenje usluga na razne načine.
Pohrana pravila o korištenju usluga i drugih metapodataka koji određuju upravljanje uslugom (verzija, status, odnosi).
Za razliku od registra, repozitorij je uvijek namjenjen internoj primjeni.

3. (2) Ti broja bankovnog računa na HUB1 i HUB3? Koji je cilj e-HUBa?
BBAN konstrukcija transakcijskog računa u Republici Hrvatskoj sastoji se od 17 brojčanih znakova i izgleda ovako: AAAAAAA-BBBBBBBBBB
slova A – sedmeroznamenkasti vodeći broj kreditne institucije koji određuje Hrvatska narodna banka
slova B – deseteroznamenkasti broj transakcijskog računa koji određuje kreditna institucija koja vodi transakcijski račun

IBAN konstrukcija transakcijskog računa u RH sastoji se od 21 alfanumeričkog znaka i izgleda ovako: HR kk AAAAAAA BBBBBBBBBB
HR – dvoslovna oznaka za Republiku Hrvatsku,
kk – dvoznamenkasti kontrolni broj koji se računa prema međunarodnoj normi ISO 7064, MOD 97-10
slova A – sedmeroznamenkasti vodeći broj kreditne institucije koji određuje Hrvatska narodna banka (kao u BBAN-u),
slova B – deseteroznamenkasti broj transakcijskog računa koji određuje kreditna institucija koja vodi transakcijski račun (kao u BBAN-u)

Cilj e-HUBa je imati HUB3 obrazac u elektroničkom obliku, potpisan i pravovaljan.

4. (1) Razlika identifikacije, autentikacije i autorizacije.
identifikacija – utvrđuje o kojoj se osobi radi
autentikacija – potvrđuje se identitet korisnika
autorizacija – korisniku se dodjeljuju odgovarajuća prava pristupa

5. (1) Razlika između simetrične i asimetrične kriptografije? Može li se simetrična koristiti za digitalni potpis? A asimetrična? Objasni.
Simetričnom kriptografijom se poruka šifrira i dešifrira istim unaprijed dogovorenim ključem.
Kod asimetrične kriptografije se šifriranje i dešifriranje obavlja javnim i privatnim ključevima koji rade isključivo u paru. Nešto šifrirano javnim ključem može se dešifrirati samo odgovarajućim privatnim ključem i obrnuto.

Simetrična se ne može koristiti ia potpis jer je potrebno imati nešto što ima samo potpisnik. Zato se koristi asimetrična jer tada obje strane imaju po jedan ključ.

6. (2) Objasni postupak digitalnog potpisivanja. Što se tim postupkom može dokazati?
Pošiljatelj izračuna hash poruke i potpiše ga vlastitim privatnim ključem. Taj šifrirani hash se dodaje na poruku i šalje kao tekst. Primatelj iz poruke vadi šifrirani hash i dešifrira ga javnim ključem pošiljatelja. Iz poruke izračuna novi hash i ukoliko su ta dva hasha ista dokazuje se identitet pošiljatelja i integritet poruke.

7. (1) Vrste digitalnog potpisa u RH? Koja vrsta zamjenjuje vlastoručni potpis ili vlastoručni potpis i pečat?
U RH postoji elektronički potpis i napredni elektronički potpis. Napredni elektronički potpis zamjenjuje vlastoručni potpis ili vlastoručni potpis i pečat.

8. (3) Čemu služi vremenska oznaka? Objasni postupak vremenskog označavanja i provjere.
Vremenska oznaka osigurava pouzdanost digitalnog potpisa i posliej isteka valjanosti ili opoziva certifikata potpisnika. Pomoću vremenske oznake se može dokazati da je potpis napravljen prije isteka valjanosti certifikata.

Prvo, podnosilac zahtjeva za vremenskom oznakom izračuna sažetak dokumenta na kojega želi staviti vremensku oznaku. Zatim se taj sažetak šalje centru za vremensko označavanje. TSA prima poslani sažetak, kreira vremensku oznaku te na temelju ta dva objekta stvara novi sažetak. Novi sažetak TSA potpisuje svojim privatnim ključem i šalje nazad podnositelju zahtjeva za vremenskom oznakom. Podnositelj zahtjeva dokument posprema zajedno s vremenskom oznakom i sažetkom.

Podnositelj zahtjeva prvo izračunava sažetak originalnih podataka, nakon toga tom sažetku nadodaje vremensku oznaku koju je dobio od TSA i ponovo izračunava sažetak. Nakon toga, pošiljatelj dohvaća certifikat TSA koji sadrži javni ključ i njime dešifrira poruku dobivenu od TSA. Time postupkom dokazuje se da je TSA zaista šifrirao (potpisao) tu poruku svojim privatnim ključem. Nakon toga dešifriranu poruku od TSA usporedimo sa sažetkom koji smo prije izračunali. Ako su te dvije poruke iste, to znači da su dokument i vremenska oznaka ostali nepromijenjeni.

9. (1) Opiši XSS i SQL upad. U čemu je razlika?
XSS-napadi (engl. Cross-Site Scripting) jesu napadi u kojima zlonamjerni korisnici, umjesto regularnih podataka, unose programski kod.

SQL-upadi (engl. SQL injection) jesu način napada u kojem zlonamjerni korisnik unošenjem odgovarajućih podataka (bilo kroz HTML obrasce ili kroz upitni dio URI-ja ili tijelo HTTP-zahtjeva) mijenja početni SQL-upit na način da dobiva upit koji on želi.

10. (2) Što znate o WS-Security?

WSS (WS-Security, Web Services Security) je komunikacijski protokol koji osigurava sigurnost primjene Web servisa.
Cilj je postizanje sigurnosti s kraja na kraj komunikacije, a ne samo na razini prijenosa.
WS-Security ne definira format potpisa ili šifriranja. Umjesto toga, specificira način kako će se format, definiran drugom specifikacijom, ugraditi u SOAP poruku.
Protokol WSS sadrži i detalje o korištenju: jezika SAML (Security Assertion Markup Language), Kerberosa (autentifikacijski protokol) te digitalnih certifikata kao što su certifikati X.509 koji se koriste u primjeni PKI infrastrukture.
Prikazuje kako pripojiti sigurnosne tokene na poruke u izvršavanju Web servisa.

11. (2) Što znate o PCI DSS?

PCI DSS - Payment Card Industry Data Security Standard
Sigurnosni standard za kartično poslovanje, definira minimalne sigurnosne mjere i procese.
PCI DSS regulira zahtjeve koji se odnose na upravljanje sigurnošću podataka, sigurnosne procedure, mrežnu arhitekturu,oblikovanje programske potpore za obradu podataka te ostale kritične zaštitne mjere u kartičnom poslovanju.

12. (2) Što znate o SSL/TLS? Kada korisnik može imati povjerenje u HTTPS?

SSL/TLS je protokol koji se koristi za ostvarivanje sigurne razmjene povjerljivih podataka, poput korisničkog imena i zaporke, broja kreditne kartice i sl. temelji se na upotrebi kriptografije te infrastrukture javnih ključeva (engl. Public key infrastructure - PKI).
Privatni i javni ključevi, adresa počinje oznakom https://, sva komunikacija između preglednika i web poslužitelja se šifrira.
Korisnik može imati povjerenje u HTTPS Kad je uspostavljena sigurna veza (sjedište weba ima valjani certifikat potpisan od strane pouzdanog CA u kojeg korisnik ima povjerenja) i kada se pojavi ikona lokota u pregledniku i adresa počinje oznakom https://

13. (2) Zahtjevi za pametne kartice (tokene)? Što je potrebno osigurati kod izdavanja tokena?

14. Što je to kanonikalizacija i zašto je ona bitna pri digitalnom potpisivanju XML-ovskih dokumenata?

Kanonikalizacija je postupak svođenja XML dokumenata na isti oblik. Ona je bitna jer pošto XML nema strogo normiran oblik, može doći do sitnih razlika poput jednog razmaka više, što onda u hash-u dovodi do potpuno različitog sažetka, što bi značilo da dva logički jednaka

dokumenta mogu dovesti do toga da provjera digitalnog potpisa padne, iako dokument logički nije promijenjen.

15. Što znači da funkcija šifriranja treba biti jednosmjerna osobna funkcija?
To znači da mora biti jednosmjerna zato jer iz šifrata nebi smjelo biti moguće rekonstruirati originalni ulaz. A osobna je zato jer treba jamčiti da je vrlo mala šansa da dva različita ulaza daju isti izlaz.

16. Čemu služi norma XML encryption, a čemu služi norma XML signature?
XML encryption – on objašnjava kako šifrirati XML dokument, odnosno kako ugraditi šifrirani sadržaj u XML dokument. On nije algoritam šifriranja.
XML signature – on objašnjava kako ubaciti digitalni potpis u XML dokument. On nije algoritam digitalnog potpisa.

17. Navedite barem 6 zahtjeva norme PCI DSS.
1. Tijekom prijenosa putem otvorenih, javnih mreža, svi podatci o vlasniku kartice moraju se štiti šifriranjem
2. Razvijati i održavati sigurne sustave i aplikacije
3. Svi pohranjeni podatci o vlasniku kartice moraju se uvijek i bezuvjetno štiti
4. Nužno je koristiti i redovito ažurirati antivirusni softver
5. Redovito provjeravati sigurnost sustava i procesa
6. Maksimalno ograničiti fizički pristup podatcima o vlasniku kartice

18. Što znate o normi EMV?
To je norma koju su napravili Europay, mastercard i Visa, ona definira interakciju između pametne kartice i uređaja za obradu kartica te ima donesene specifikacije i za beskontaktna plaćanja. Cilj te norme je prihvaćanje pametnih kartica diljem svijeta i osigurati sigurnost i konzistentnost platnih transakcija na prodajnim mjestima.

19. Objasnite slijedeće provjere pri kartičnoj naplati: AVS I CVC.
AVS – provjera koja prilikom kartičnog plaćanja provjerava adresu stanovanja kupca koja je navedena na kartici. Sustav će tu adresu usporediti s onom koju posjeduje kartična kuća.
CVC – provjera kod koje se prilikom online plaćanja gdje nije moguće upisati pin kartice, upisuju 3 ili 4 znamenke koje se nalaze na poleđini kartice.