SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA
ZAVOD ZA ELEKTRONIČKE SUSTAVE I OBRADBU INFORMACIJA

# SASL (Simple Authentication and Security Layer)

## Seminarski rad
## Sustavi za praćenje i vođenje procesa

29.svibnja 2005.

JoškoRokov
0036387422

**SADRŽAJ:**

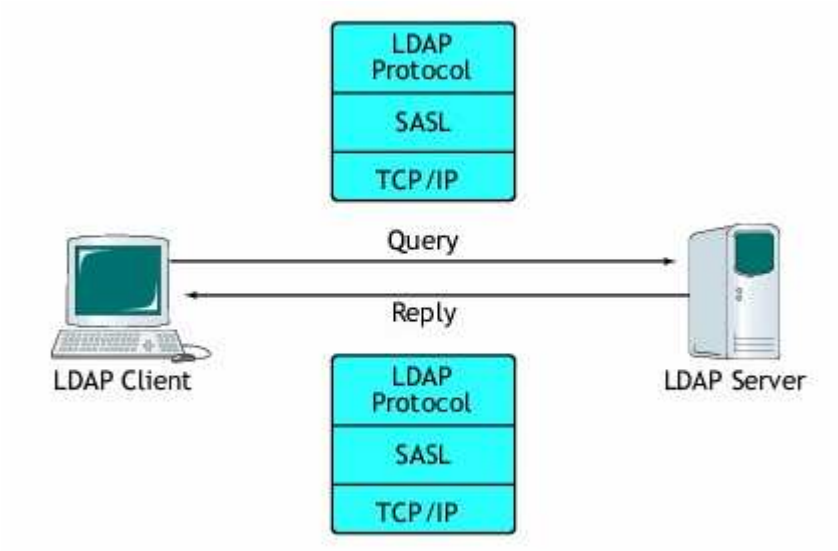
# 1. UVOD

Simple Authentication and Security Layer (SASL) je metoda za dodavanje mogućnosti autentifikacije connection-based protokolima. Za korištenje te specifikacije protokol uključuje naredbu za identificiranje i autentifikaciju korisnika na server te opcionalno i pregovaranje s sigurnosnim slojem za interakcije s nižim protokolima.
Naredba ima zahtijevani argument koji identificira SASL mehanizam. SASL mehanizmi su označeni stringovima, od 1 do 20 znakova u dužini, sastojeći se od velikih slova, znamenki, crtica i/ili podvlaki.
Imena SASL mehanizma moraju biti registrirana u IANA organizaciji.

# 2. SPECIFIKACIJA PROTOKOLA

## 2.1. KLIJENT-SERVER KOMUNIKACIJA

Komunikacija korisnik i servera počinje korisnikovim slanjem početnog upita (naredbe) serveru.
Ako server podržava zatraženi mehanizam, to pokreće razmjenu autentifikacijskog protokola. Taj postupak se sastoji od serije zahtjeva servera i odgovora klijenta koji su specifični za taj mehanizam. Zahtjevi i odgovori su određeni kao binarni okviri proizvoljne duljine. Profil protokola onda specificira kako se ti binarni okviri kodiraju za prijenos preko veze.

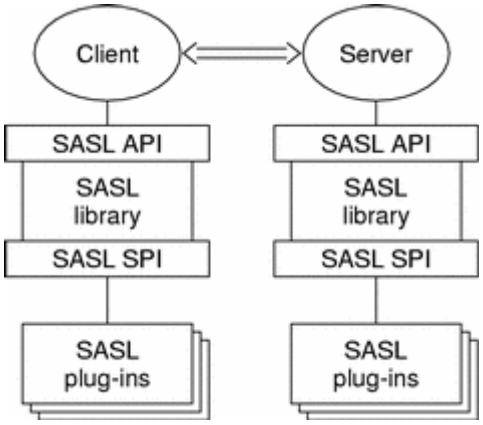



Slika 1.Prikaz primjene SASL-a

Nakon primanja autentifikacijske naredbe ili bilo kojeg odgovora od strane klijenta, server može izdati zahtjev, ukazati na kvar, ili zaključiti dogovor.Profil protokola specificira kako server pokazuje što je od gore navedenoga posrijedi.

Nakon zaprimanja zahtjeva, klijent može izdati odgovor ili prekinuti dogovor. Profil protokola specificira kako klijent ukazuje što je od prije navedenoga posrijedi.

Tijekom razmjene autentifikacijskog protokola, mehanizam izvodi autentifikaciju, odašilje autorizirani identitet (poznat i kao *userid*) od klijenta do servera, i pregovara o uporabi sigurnosnog sloja specifičnog za mehanizam. Ako je upotreba sigurnosnog sloja ugovorena tada mehanizam mora također definirati ili pregovarati o maksimalnoj veličini buffera šifre koji je svaka strana u stanju primiti.




Slika 2. Klijent i server s implementiranim SASL-om

Odaslani autorizirani identitet može biti različit od identiteta u klijentovom akreditivu. To dopušta agentima kao što je proxy server autentifikaciju koristeći vlastite akreditacije. S bilo kojim mehanizmom, odašiljanje i autorizacija identiteta praznog stringa upućuje server na izvlačenje autorizacijskog identiteta iz klijentovog akreditiva.

Ako je upotreba sigurnosnog sloja dogovorena, to se primjenjuje na sve podatke naknadno poslane tom vezom. Sigurnosni sloj počne djelovati odmah nakon posljednjeg odgovora autentifikacijske razmjene za podatke poslane od strane klijenta i potvrdne indikacije za podatke poslane od strane servera. Kad se aktivira sigurnosni sloj, tok protokola se procesira od strane sigurnosnog sloja u buffer šifre.

Svaki buffer se pretvara preko veze u slijed okteta kojima prethode 4 okteta polja koji predstavljaju dužinu navedenog buffera. Dužina šifre ne smije biti veća od maksimalne veličine koja je definirana ili određena pregovorom s drugom stranom.

## 2.2. ZAHTJEVI PROTOKOLA

Za korištenje prijenavedene specifikacije protokol mora sadržavati slijedeće informacije:

1. Naziv usluge koji se izabire iz registra udruge IANA.

2. Definicija naredbe za inicijalizaciju razmjene autentifikacijskog protokola.

   Naredba bi trebala imati opcionalni parametar dajući inicijalni odgovor. Taj opcionalni parametar dozvoljava klijentu izbjegavanje zaobilaznog puta kad koristi mehanizam koji definira da se prvo šalju klijentovi podaci.

3. Definicija metode kojom se izvršava razmjena autentifikacijskog protokola,uključujući način na koji su zahtjevi i odgovori kodirani, kako server ukazuje na završetak ili grešku razmjene, kako klijent prekida razmjenu, i kako metoda razmjene djeluje s ograničenjima dužine linija u protokolu.

4. Identifikacija okteta pri kojem se dogovara djelovanje u sigurnosnom sloju u oba smjera.

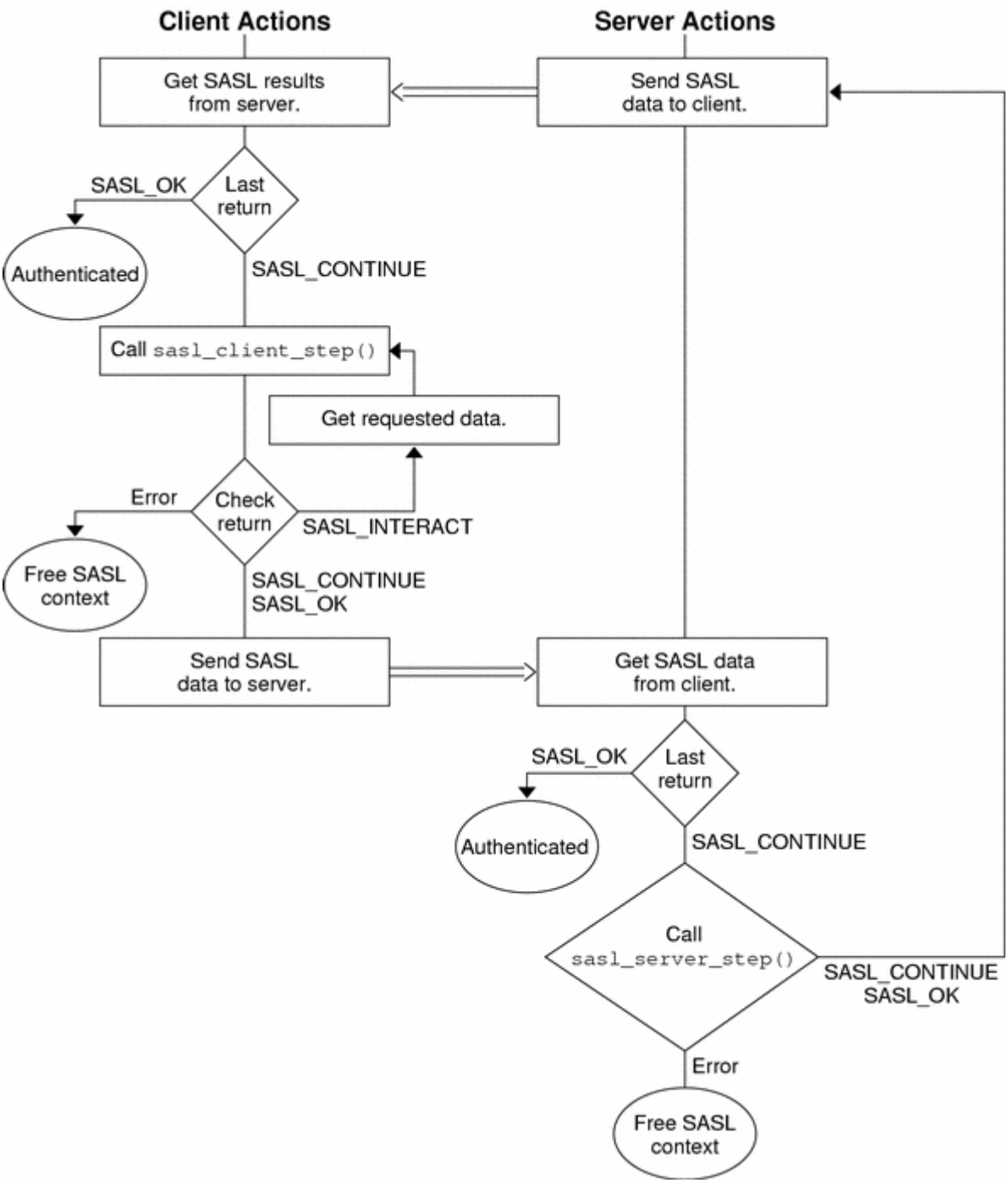
5. Specifikacija koja kaže kako će autentifikacijski identitet poslan od klijenta do servera biti predstavljen.

## 2.3. SPECIFIČNI SLUČAJEVI KOMUNIKACIJE

***Klijent prvi šalje podatke:***

Neki mehanizmi specificiraju da je prvi poslani podatak u autentifikacijskom protokolu odaslan od klijenta prema serveru.
Ako profil protokola dozvoljava da naredba koja započinje razmjenu autentifikacijskog protokola sadrži inicijalni odgovor klijenta, taj parametar bi trebao biti korišten s takvim mehanizmima.

Ako nije zadan inicijalni klijentov odgovor ili ako profil protokola ne dopušta naredbu koja sadrži inicijalni odgovor klijenta, tada server izdaje zahtjev bez ikakvih podataka. Klijentov odgovor na taj zahtjev se tada koristi kao inicijalni odgovor klijenta. (Server tada nastavlja sa slanjem ostalih zahtjeva i nastavlja s normalnim radom.)




Slika 3. Dijagram toka SASL mehanizma

***Server paralelno šalje indikaciju završetka i novi zahtjev:***

Neki mehanizmi mogu specificirati zajedno slanje podataka zahtjeva servera i indikaciju uspješnog završetka razmjene. Ti podaci bi mogli primjerice biti autentifikacija servera za određenog klijenta.
Ako profil protokola ne dopušta takvo slanje tada server izdaje zahtjev bez indikacije uspješnog završetka. Klijent tada odgovara bez podataka. Nakon primitka praznog odgovora server indicira uspješan završetak.

***Višestruka autentifikacija:***

Može postojati samo jedno uspješno SASL pregovaranje u jednom razdoblju razmjene podataka ako nije drukčije određeno u profilu protokola. U tom slučaju kad se jednom završi razmjena autentifikacijskog protokola, daljnji pokušaji iniciranja razmjene autentifikacijskog protokola se neće izvršiti.

U slučaju da profil eksplicitno dopušta višestruke SASL razmjene, tada ni u kojem slučaju ne smiju višestruki sigurnosni slojevi biti istovremeno aktivni.

Ako je neki sigurnosni sloj aktivan a slijedeća SASL razmjena ne zahtijeva sigurnosni sloj, originalni sigurnosni sloj ostaje aktivan.

Ako je sigurnosni sloj aktivan a slijedeća SASL razmjena izabire drugi sigurnosni sloj, tada drugi sloj zamijeni prvoga.

## 3. RAZLIKA SASL-a i OSTALIH SIGURNOSNIH PROTOKOLA

Postavlja se pitanje o vezi između SASL i raznih servisa poput Ipsec-a i TLS-a koji omogućavaju sigurnu vezu.
Dvije su ključne karakteristike SASL mehanizma:

1. Razdvajanje autorizacijskog identiteta i identiteta u klijentovom akreditivu. To dopušta agentima poput proxy servera autentifikaciju koristeći vlastiti akreditiv ali svejedno zahtijevajući pristup za korisnika kojega oni zastupaju.

2 .Nakon uspješnog završetka autentifikacijske razmjene server zna autorizirani identitet koji klijent želi koristiti. To dopušta serverima pomak u stanje «*korisnik je autoriziran*» sadržano u protokolu.

Ove karakteristike su veoma važne u nekim aplikacijskim protokolima, iako ih Transport Security servisi uvijek ne podržavaju.

Ponekad je poželjno omogućiti unutar postojeće veze upotrebu sigurnosnog servisa koji ne odgovara SASL modelu. (npr.TLS)
To se može srediti dodavanjem naredbe protokolu, primjerice «*STARTTLS*». Takva naredba bi trebala biti različita od one koja pokreće razmjenu SASL autentifikacijskog protokola.

U određenim situacijama, razumno je koristiti SASL ispod jednog od Transport Security servisa.
Transportni servis omogućio bi sigurnost veze, autentifikacijom klijenta i SASL bi pregovarao o autorizaciji identiteta.
SASL je upravo ono što pomiče takav protokol iz «*unauthenticated*» u «*authenticated*» stanje.
Navedimo primjer: Eksplicitna namjena EXTERNAL SASL mehanizma je rukovanje u slučaju gdje transportni servis osigurava sigurnost veze i autentificira korisnika, a SASL pregovara o autorizaciji identiteta.

Kada se SASL koristi ispod dovoljno «*jakog*» Transport Security servisa, SASL sigurnosni sloj je najčešće suvišan.
Korisnik i server bi tada vjerojatno pregovarali bez SASL sigurnosnog sloja.

## 4. SASL MEHANIZMI

Neki primjeri SASL mehanizama registrirani u IANA-i su dani u nastavku:

| MECHANISMS | USAGE | REFERENCE | OWNER |
|---|---|---|---|
| KERBEROS_V4 | LIMITED | [RFC2222] | IESG <iesg@ietf.org> |
| GSSAPI | COMMON | [RFC2222] | IESG <iesg@ietf.org> |
| SKEY | OBSOLETE | [RFC2444] | IESG <iesg@ietf.org> |
| EXTERNAL | COMMON | [RFC2222] | IESG <iesg@ietf.org> |
| CRAM-MD5 | LIMITED | [RFC2195] | IESG <iesg@ietf.org> |
| ANONYMOUS | COMMON | [RFC-ietf-sasl-anon-05.txt] | IESG <iesg@ietf.org> |
| OTP | COMMON | [RFC2444] | IESG <iesg@ietf.org> |
| GSS-SPNEGO | LIMITED | [Leach] | Paul Leach <paulle@microsoft.com> |
| PLAIN | COMMON | [RFC2595] | IESG <iesg@ietf.org> |
| SECURID | COMMON | [RFC2808] | Magnus Nystrom <magnus@rsasecurity.com> |

| | | | |
|---|---|---|---|
| NTLM | LIMITED | [Leach] | Paul Leach <paulle@microsoft.com> |
| NMAS_LOGIN | LIMITED | [Gayman] | Mark G. Gayman <mgayman@novell.com> |
| NMAS_AUTHEN | LIMITED | [Gayman] | Mark G. Gayman <mgayman@novell.com> |
| DIGEST-MD5 | COMMON | [RFC2831] | IESG <iesg@ietf.org> |
| 9798-U-RSA-SHA1-ENC | COMMON | [RFC3163] | robert.zuccherato@entrust.com |
| 9798-M-RSA-SHA1-ENC | COMMON | [RFC3163] | robert.zuccherato@entrust.com |
| 9798-U-DSA-SHA1 | COMMON | [RFC3163] | robert.zuccherato@entrust.com |
| 9798-M-DSA-SHA1 | COMMON | [RFC3163] | robert.zuccherato@entrust.com |
| 9798-U-ECDSA-SHA1 | COMMON | [RFC3163] | robert.zuccherato@entrust.com |
| 9798-M-ECDSA-SHA1 | COMMON | [RFC3163] | robert.zuccherato@entrust.com |
| KERBEROS_V5 | COMMON | [Josefsson] | Simon Josefsson <simon@josefsson.org> |
| NMAS-SAMBA-AUTH | LIMITED | [Brimhall] | Vince Brimhall <vbrimhall@novell.com> |

Tablica 1. SASL mehanizmi registrirani u IANA-i

### 4.1. KERBEROS VERSION4

Kod ovog mehanizma prvi upit se sastoji od nasumično izabranog 32-bitnog broja u mrežnom rasporedu bajtova.
Klijent odgovara s Kerberos kartom i autentikatorom za prvi «*service.hostname@realm*», gdje je «*service*» ime servisa sadržano u profilu protokola, «*hostname*» prva komponenta imena glavnog računala (sve s malim slovima), a «*realm*» Kerberos područje servera.
Kriptirano polje s ispitnom šifrom uključeno u Kerberos autentifikatora sadrži upit servera u mrežnom rasporedu bajtova.
Nakon dekripcije i provjere karte i autentifikatora server provjerava dali je ispitni broj ekvivalentan onom poslanom 32-bitnom broju.

Ako je verifikacija usješna, server dodaje jedinicu tom broju te konstruira 8 okteta od kojih su prva četiri uvećani ispitni broj, peti je maska koja specificira podržane sigurnosne slojeve, a zadnja tri sadrže maksimalnu vrijednost buffera šifre koju je server u stanju primiti.
Server kriptirani skup okteta šalje klijentu koji iz prva četiri može razlučiti da li je prihvaćen ili ne.

Klijent konstruira podatke tako da u prva četiri okteta stavlja prijenavedeni ispitni broj, peti specificira sigurnosni sloj, slijedeća tri sadrže maksimalnu vrijednost buffera šifre koju je u stanju primiti,a ostali okteti sadrže autorizacijski identitet. Dužina podataka mora biti višekratnik od 8 okteta.Klijent također šifrira podatke i šalje ih nazad serveru.

Server dekriptira podatke i provjerava ispitni broj te ispituje dali je prvi identificirani u Kerberos karti autoriziran za spajanje na autorizacijski identitet. Nakon ove verifikacije proces autentifikacije je gotov.

### 4.2. S/KEY MEHANIZAM

U ovom mehanizmu za razliku od prethodnog klijent šalje prvi odgovor s autorizacijskim identitetom.
Server tada izdaje upit koji sadrži decimalni sekvencni broj iza kojeg slijedi razmak i seed string za zadani autorizacijski identitet.

Klijent tada odgovara s «one-time» šifrom kao 64-bitnom vrijednosti u mrežnom rasporedu bajtova ili kodirano u tzv. «*six English words*» format. Server mora potvrditi primljenu šifru, te je nakon verifikacije proces autentifikacije završen.

### 4.3. EKSTERNI MEHANIZAM

Kao i u prethodnom mehanizmu klijent šalje početni odgovor s autorizacijskim identitetom.
Server koristi tu informaciju izvan SASL-a u svrhu određivanja autoriziranosti klijenta da se autentificira kao autorizacijski identitet.

Ako je klijent autoriziran server indicira završetak autentifikacijske razmjene, dok u suprotnom slučaju server indicira kvar.
Sustav koji dostavlja tu eksternu informaciju može biti npr. Ipsec ili TLS.

Ako klijent pošalje prazni string kao autorizacijski identitet, tada se autorizacijski identitet izvodi iz autentifikacijskog akreditiva koji postoji u sustavu koji dostavlja eksternu autentifikaciju.

## 5. SIGURNOST SASL-a

Mehanizmi koji podržavaju potpunu zaštitu su projektirani tako da su pregovor sigurnosnim slojem i autorizacija identiteta potpuno zaštićeni. Klijent se izabirom sigurnosnog sloja s potpunom zaštitom automatski zaštićuje od aktivnog napada preuzimanja veze i promjene autentifikacijske razmjene.

Kada server ili klijent podržavaju višestruki mehanizam autentifikacije od kojih svaki ima različitu sigurnosnu snagu, moguće je da napadač uspije postići da se koristi samo najslabiji sloj po sigurnosti.

Da bi se zaštitilo od takvih napada potrebno je da klijent ili server (ovisno tko podržava više mehanizama) ima podesivu minimalnu snagu koju će koristiti. Nije suvišno da provjera minimalne snage bude na serveru, pošto aktivni napadač može promijeniti mehanizam koji će klijent vidjeti kao podržan od strane servera, što može dovesti do problema autentifikacije korisnikovog akreditiva na najslabijem podržanom mehanizmu.

Klijentov odabir SASL mehanizma je tada otvoren i može biti promijenjen od strane aktivnog napadača. Bitno je da svaki novi SASL mehanizam bude dizajniran tako da aktivni napadač ne može pristupiti autentifikaciji sa slabijim sigurnosnim osobinama samom promjenom imena i/ili upita i odgovora.

Bilo koja interakcija protokola prije autentifikacije događa se javno i može biti promijenjena od strane aktivnog napadača. U slučaju da klijent izabere potpunu zaštitu, bitno je da svaki sigurnosno osjetljivi protokol izvrši pregovaranje tek nakon završetka procesa autentifikacije. Protokoli bi trebali biti dizajnirani tako da svako pregovaranje prrije autentifikacije bude ili zanemareno ili potvrđeno tek nakon završetka procesa autentifikacije.

## 6. ZAKLJUČAK

Simple Authentication and Security Layer (SASL) je metoda za dodavanje mogućnosti autentifikacije connection-based protokolima.

Uz pomoć te metode otvaraju nam se vrata brojnim primjenama autorizacije korisnika uz relativno veliku sigurnost pri povezivanju dvaju strane mreže tj. sučelja korisnik – server.

## 7. LITERATURA

[1] http://www.ietf.org/rfc/rfc2222.txt

[2] http://qwww.iana.org/assignments/sasl-mechanisms

[3] http://docs.sun.com