Univerzita Komenského v Bratislave
Fakulta matematiky, fyziky a informatiky

Porovnanie API tokenov

Bakalárska práca

2023
Jitka Muravská

Univerzita Komenského v Bratislave
Fakulta matematiky, fyziky a informatiky

Porovnanie API tokenov

Bakalárska práca

Študijný program:	Informatika
Študijný odbor:	Informatika
Školiace pracovisko:	Katedra informatiky
Školiteľ:	RNDr. Richard Ostertág, PhD.

Bratislava, 2023
Jitka Muravská

Univerzita Komenského v Bratislave
Fakulta matematiky, fyziky a informatiky

ZADANIE ZÁVEREČNEJ PRÁCE

Meno a priezvisko študenta: Jitka Muravská
Študijný program: informatika (Jednoodborové štúdium, bakalársky I. st., denná forma)
Študijný odbor: informatika
Typ záverečnej práce: bakalárska
Jazyk záverečnej práce: slovenský
Sekundárny jazyk: anglický

Názov: Porovnanie API tokenov
Comparison of API Tokens

Anotácia: REST aplikačné rozhrania (API) často nebývajú čisto verejné. V takom prípade treba pri implementácii API riešiť aj jeho bezpečnosť. Väčšina schém zabezpečenia API používa token, ktorý je súčasťou jednotlivých požiadaviek. Tieto tokeny sú nejakým spôsobom spojené s identitou a autorizáciou používateľa. Aplikačné rozhranie prevezme požiadavku, extrahuje token, a podľa pravidiel prístupu rozhodne ako pokračovať.

Cieľom práce je porovnanie rôznych API tokenov (napríklad: OAuth 2.0, JWT, PASETO, Protobuf Tokens, Authenticated Requests, Macaroons, Biscuits, …). Prvým krokom bude zozbieranie a popísanie rôznych v praxi používaných API tokenov. Následne sa vykonajú porovnania ich výhod a nevýhod (napríklad rýchlosť, jednoduchosť použitia) na jednoduchej základnej aplikácii.

Vedúci: RNDr. Richard Ostertág, PhD.
Katedra: FMFI.KI - Katedra informatiky
Vedúci katedry: prof. RNDr. Martin Škoviera, PhD.

Spôsob sprístupnenia elektronickej verzie práce:
bez obmedzenia

Dátum zadania: 12.10.2022

Dátum schválenia: 13.10.2022 doc. RNDr. Dana Pardubská, CSc.
garant študijného programu

.....
študent

.....
vedúci práce

Poďakovanie:

Abstrakt

Kľúčové slová:

Abstract

Keywords:

Obsah

Zoznam obrázkov

Zoznam tabuliek

Úvod

Kapitola 1

Schémy zabezpečenia API a využitie tokenov

V tejto kapitole uvedieme viaceré známe prístupy riešenia autentifikácie a autorizácie. Stručne objasníme ako fungujú a aké sú ich výhody a nevýhody. Detailnejšie sa pozrieme na prístup využívajúci API tokeny a samotné tokeny a ich rozdelenie, ktorým sa venuje naša práca.

1.1 Zabezpečenie bez autentifikácie

V prípade, že je aplikačné rozhranie plne verejné, nepotrebuje žiadnu schému zabezpečenia. Ľubovoľný používateľ môže volať rozhranie bez predchádzajúcej autentifikácie a neexistuje spôsob ako obmedziť prístup k volaniam rozhrania.

Jediným identifikátorom autora požiadavky je jeho IP adresa. To je však veľmi slabý identifikátor a nedáva nám veľké možnosti v obmedzení prístupu k rozhraniu.

Hlavnou výhodou tohto riešenia je jednoduchosť implementácie, rozhranie nepotrebuje uchovávať žiadne dáta o používateľoch a všetky požiadavky sú jednoduché, ich rýchlosť závisí len od rýchlosti samotného volania a rýchlosti siete.

Nevýhodou je samozrejme strata kontroly nad prístupom k rozhraniu, ktorá sa obmedzila buď na nejakú kontrolu na základe IP adresy alebo úplne vymizla. A jediným rozumných obmedzením je obmedzenie počtu požiadaviek za nejaký časový interval, či už pre konkrétne IP adresy alebo pre celé rozhranie.

1.2 Zabezpečenie bez schémy

Najjednoduchšie riešenie autentifikácie a autorizácie je posielanie prihlasovacích údajov v každej požiadavke na rozhranie. Klient jednoducho pripojí prihlasovacie údaje ku každej požiadavke a rozhranie si ich overí vo svojej databáze a v prípade úspechu vráti

požadované dáta.

Toto riešenie nie je vhodné ak sa niekde v rámci komunikácie nachádza nezabezpečené spojenie. Útočník, ktorý by takúto komunikáciu zachytil, by mal jednoduchý prístup k prihlasovacím údajom používateľa.

Používanie nezabezpečeného spojenia je všeobecne nebezpečné bez ohľadu na schému zabezpečenia a typ prenášaného údaju používaného na autorizáciu, preto ďalej v práci budeme predpokladať, že spojenia s každým koncovým bodom sú zabezpečené pomocou SSL/TLS.

Aj v prípade zabezpečeného spojenia však existujú zraniteľnosti [40]. Prihlasovacie údaje sú zriedkavo menený identifikátor a teda po ich odchytení sa dajú dlho zneužívať. Okrem samotného úniku citlivých údajov a z toho vyplývajúcich nepríjemností pre používateľa má tento prístup aj ďalšie nevýhody.

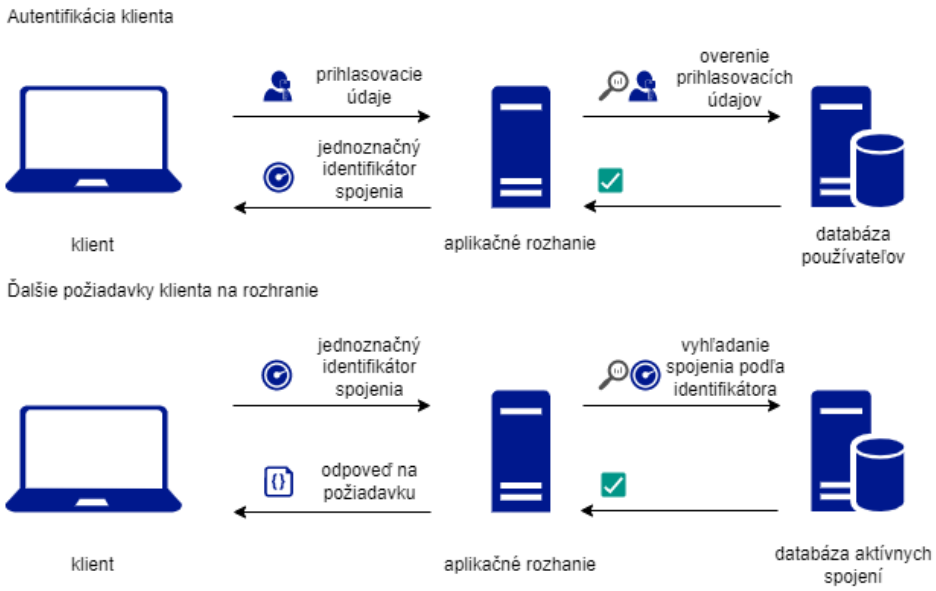
Okrem priameho zneužitia získaných hesiel útočníkom, môže útočník ukladať heslá do databázy odchytených hesiel a následne môžu aj iní útočníci túto databázu použiť pri ďalších útokoch. Tento prístup sa nazýva *slovníkový útok* a môže byť veľmi efektívny. [36]. Ľudia tiež často používajú podobné heslá na všetky svoje účty. Potom sa podľa istých vzorov odhalených v sade hesiel jedného používateľa dajú ľahšie uhádnuť ďalšie heslá. [21].

1.3 Schéma zabezpečenia s využitím identifikátora spojenia

Prvé riešenie, kde môžeme hovoriť o nejakej schéme zabezpečenia, nie len o existencii prihlasovacích údajov a ich overení pri každej požiadavke, je sledovanie každého aktívneho spojenia s rozhraním (angl. session).

Pri prvej požiadavke sa používateľ autentifikuje voči serveru, ten si vytvorí a uloží záznam o spojení. Tento záznam môže obsahovať rôzne základné informácie a o spojení ako čas vytvorenia a informácie o používateľovi, s ktorým je spojenie vytvorené. Dôležitá časť záznamu je jednoznačný identifikátor spojenia v podobe náhodného reťazca. Následne klientovi vráti identifikátor spojenia. Všetky nasledujúce požiadavky klienta budú obsahovať tento identifikátor, podľa ktorého vie server určiť, ktorému používateľovi patria, teda či je autentifikovaný, prípadne či má právo vykonať dané volanie, ak rozhranie implementuje nejakú autorizačnú schému. Popísaná schéma je znázornená na obrázku 1.1.

Oproti predošlému riešeniu pribudla potreba manažovať spojenia, no veľkou výhodou je, že sa už neposielajú citlivé prihlasovacie údaje v každej požiadavke. Rozhranie však stále potrebuje pri každej požiadavke preložiť identifikátor na záznam o používateľovi.



Obr. 1.1: Autentifikačná schéma s použitím identifikátora spojenia.

1.4 Schéma zabezpečenia využívajúca API kľuče

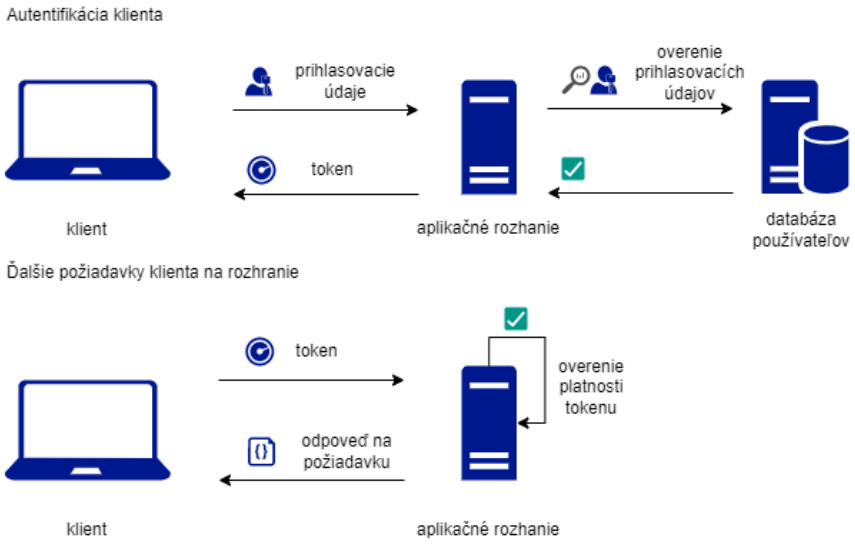
API kľúč je identifikátor používaný na pripojenie k rozhraniu. Identifikuje však aplikáciu alebo službu, nie konkrétneho používateľa. Ak potrebuje aplikácia používať rozhranie, ktoré nie je verejné a na autentifikáciu používa API kľúče, musí si najprv vyžiadať API kľuč a následne ho posielať s každou požiadavkou.

Tento kľúč môže byť zároveň spojený s právami umožňujúcimi vykonávať určité volania, ak dané rozhranie poskytuje rôzne úrovne prístupu.

Použitie API kľúčov nie je veľmi bezpečné, lebo kľúče majú neobmedzenú platnosť a ak príde k ich odchyteniu, jediný spôsob ako zvrátiť ich zneužitie je ich zneplatniť a vygenerovať nové. Ďalšia zraniteľnosť API kľúčov často nastáva pri ich uložení na nesprávne miesto.

Napríklad pri webovej aplikácii nie je bezpečné ukladať kľúč na klientskej strane, ale na serveri a odtiaľ vykonávať API volania. Rovnako pri mobilnej aplikácii nie je bezpečné ukladať kľúč priamo v aplikácii, lebo sa dá získať reverzným inžinierstvom. [14]

Preto sa vo všeobecnosti API kľúče nepoužívajú na ochranu kritických alebo citlivých volaní a zdrojov rozhrania. Naopak vhodné sú na zvýšenie kontroly nad požiadavkami na rozhranie. Je ľahké pomocou nich kontrolovať frekvenciu, či absolútny počet volaní a prípadne monetizovať ich používanie.



Obr. 1.2: Autentifikačná schéma s použitím tokenu.

1.5 Schéma zabezpečenia využívajúca API tokeny

API token (ďalej token) je identifikátor, ktorý slúži na autorizáciu prípadne aj identifikáciu používateľa pri prístupe k rozhraniu. Token môže mať viaceré podoby, jednotlivým typom a formátom sa venujú podkapitoly 1.6 a 1.7.

Tok v rámci schémy zabezpečenia rozhrania funguje podobne ako pri využití identifikátora spojenia, ktorý sme popísali v podkapitole 1.3. Líši sa najmä v tom, že token môže niesť pridanú informáciu a rozhranie vie jeho platnosť overiť bezstavovo. Popísaná schéma s využitím tokenu je zobrazená na obrázku 1.2. Na dosiahnutie tejto výhody je nutné použiť štruktúrovaný formát tokenu. Možné formáty tokenov detailnejšie popíšeme v podkapitole 1.7.

1.6 Typy tokenov

Tokeny využívané v schéme zabezpečenia rozhrania sa dajú rozdeliť podľa ich generického využitia na niekoľko typov. Nie v každom scenári máme explicitne dané aký token využiť, no niektoré sú často vhodnejšie ako iné. V tejto kapitole predstavíme viaceré typy tokenov a to prístupový (angl. access), nositeľský (angl. bearer), obnovovací (angl. refresh) a identifikačný token.

1.6.1 Prístupový token

Prístupový token [37] je najzákladnejší a najčastejšie používaný typ tokenu. Tento token vygeneruje autentifikačný server po autentifikácii používateľa a ďalej slúži na

autorizáciu v rozsahu ako sa určil v rámci autentifikácie konkrétneho používateľa. Prístupový token môže mať rôzne formáty podľa toho ako funguje schéma zabezpečenia rozhrania.

Token je spojený s istými údajmi o používateľovi ako napríklad identifikátor a prístupové práva. Tieto údaje môžu byť uložené priamo v tokene alebo na serveri, v závislosti od toho aký formát tokenu je použitý. Zároveň je s tokenom spojený aj časový limit platnosti tokenu, ktorý býva kvôli bezpečnosti krátky. Po odchytení tokenu totiž môže útočník vystupovať v mene používateľa, ktorého údaje sú uložené v tokene.

1.6.2 Nositeľský token

Nositeľský token reprezentuje najčastejší spôsob použitia prístupového tokenu. Pri jeho použití má nositeľ tokenu prístup k rozhraniu bez ohľadu nato, kto je. Stačí aby v požiadavke poslal platný nositeľský token.

Následne rozhranie nekontroluje identitu používateľa, ale iba platnosť tokenu. Preto pri jeho využití treba prikladať väčší dôraz na bezpečnosť tokenu napríklad tak, že jeho platnosť bude veľmi krátka, napríklad 5 minút.

1.6.3 Obnovovací token

Ako sme už spomínali vyššie má prístupový token často relatívne krátky časový limit platnosti. Ak chce používateľ využívať rozhranie aj po jeho uplynutí, je potrebné aby získal nový prístupový token.

Na riešenie tohto problému existujú dva jednoduché spôsoby. Buď sa používateľ znova autentifikuje a server mu vygeneruje nový prístupový token alebo si klient, cez ktorého používateľ komunikuje s rozhraním bude pamätať prihlasovacie údaje používateľa a využije ich na opätovnú autentifikáciu používateľa. Oba prístupy nie sú ideálne, prvá možnosť je nekomfortná pre používateľa a nie je možná ak je klientom nejaký servis alebo iná aplikácia. Druhá možnosť je nebezpečná, lebo klient musí mať niekde uložené prihlasovacie údaje používateľa a tým sa zvyšuje riziko ich získania útočníkom.

Obnovovací token adresuje problém s krátkou platnosťou prístupových tokenov. Pri prvotnej autentifikácii používateľa server okrem prístupového tokenu vygeneruje aj obnovovací token. Oba tokeny vráti klientovi. Následne keď uplynie platnosť prístupového tokenu, klient pošle požiadavku o nový prístupový token pomocou obnovovacieho tokenu.

Schému s obnovovacími tokenmi využíva napríklad populárny autentifikačný protokol OAuth 2.0 [22].

1.6.4 Identifikačný token

Identifikačný token je špeciálny typ prístupového tokenu. V tomto prípade musí ísť o štruktúrovaný formát tokenu. Token obsahuje identifikátor používateľa a autorizačné údaje. Navyše môže token obsahovať doplnkové údaje ako vydavateľa tokenu, čas platnosti tokenu, čas vydania tokenu a podobne.

Identifikačný token využíva napríklad protokol OpenID Connect (OIDC), čo je nadstavba protokolu OAuth 2.0 o identitu používateľa [43]. OIDC dokonca presne špecifikuje použitie JWT (JSON Web Token), ktorý viac predstavíme v kapitole 2.

1.7 Formáty tokenov

Už sme spomenuli, že existujú rôzne typy tokenov, no iba pri identifikačnom tokene je striktne daný formát tokenu. Pri ostatných typoch sa stretávame s rôznymi formátmi tokenu. Vo všeobecnosti rozoznávame dva formáty tokenov a to nepriehľadné (angl. opaque) a štruktúrované. Existujú aj hybridné formáty, ktoré kombinujú výhody obidvoch spomínaných typov, no pri nich sa dá hovoriť skôr o istých vzoroch ako o formátoch. Najpoužívanejšie sú fantómové a rozdelené (angl. split) tokeny.

1.7.1 Nepriehľadný token

Ide o najjednoduchší formát tokenu. Nepriehľadný token je náhodný reťazec znakov. Jednoduchý je v tom, že nenesie žiadnu pridanú informáciu pre rozhranie. Všetky metadáta o tokene si musí pamätať rozhranie.

Takýto prístup so sebou nesie významné výhody aj nevýhody. Výhodou je, že samotné vytvorenie tokenu je veľmi rýchle, rozhranie jednoducho vygeneruje náhodný reťazec. Navyše vďaka tomu, že nenesie žiadne pridané informácie, nenesie ani citlivé informácie o používateľovi, teda jeho zachytenie útočníkom nie je také nebezpečné. Nevýhodou však je, že rozhranie ho nevie bezstavovo overiť, teda ho musí napríklad vyhľadať v databáze platných tokenov a to je časovo náročné.

1.7.2 Štruktúrovaný token

Na rozdiel od nepriehľadného tokenu štruktúrovaný token obsahuje pridanú informáciu napríklad identifikáciu používateľa, jeho prístupové práva, čas platnosti tokenu, čas vydania tokenu a podobne.

Aby sa predišlo úniku citlivých informácií z tokenu, je token šifrovaný. Využívajú sa rôzne symetrické aj asymetrické algoritmy. Všetky konkrétne protokoly, ktoré rozoberáme v tejto práci, používajú štruktúrované tokeny a v kapitole 2 sa venujeme ich vytváraniu a s ním spojenému šifrovaniu alebo hešovaniu tokenov.

Najväčšou výhodou štruktúrovaného tokenu je, že rozhranie ho môže bezstavovo overiť, lebo pozná kľúč, ktorým bol token zašifrovaný, teda ho vie dešifrovať a získať informácie, ktoré nesie. Zo získaných informácií vie rozhranie overiť platnosť tokenu a autorizovať používateľa.

1.7.3 Fantómový token

Ako sme naznačili v úvode podkapitoly, fantómový token [10] je hybridný formát tokenu. Podľa tohto vzoru autentifikačný server vygeneruje dva tokeny, nepriehľadný token pre klienta a štruktúrovaný token pre rozhranie. Ďalej sa využíva API brána alebo reverzný proxy server (RPS), v ktorom sa uloží dvojica tokenov ako kľúč a hodnota. Kľúčom je nepriehľadný token, hodnotou je štruktúrovaný token.

Následne, keď klient pošle požiadavku na rozhranie, tak pridá nepriehľadný token. API brána alebo RPS ho preloží na štruktúrovaný token a tento štruktúrovaný token poskytne rozhraniu. Rozhranie ho môže bezstavovo overiť a využiť pridané informácie, ktoré nesie.

Brána alebo RPS síce musí vyhľadať záznam s dvojicou tokenov, kde je kľúčom poslaný nepriehľadný token, ale môže si výsledok uložiť do vyrovnávacej pamäte (napríklad služba Redis [42]) pre ďalšie požiadavky. Tým sa zvýši priepustnosť brány alebo RPS a zároveň ubudnú nároky na výkonnosť rozhrania.

Výhodou oproti obyčajnému štruktúrovanému tokenu je, že klient, teda prehliadač alebo iná aplikácia nedržia v pamäti štruktúrovaný token obsahujúci, aj keď zašifrované, citlivé informácie.

1.7.4 Rozdelený token

Rozdelený token [11] má podobnú schému a výhodu ako fantómový token, no navyše ombedzuje štruktúrovaný token vydaný autentifikačným serverom tým, že musí obsahovať podpis chrániaci jeho autenticitu.

V schéme rozdeleného tokenu vydá autentifikačný server len štruktúrovaný token. Podpis z tohto tokenu pošle klientovi a do vyrovnávacej pamäte brány alebo RPS zapíše celý token so zahešovaným podpisom ako kľúčom.

Požiadavky od klienta budú obsahovať ako nepriehľadný token získaný podpis a brána alebo RPS ho zahešuje a preloží na štruktúrovaný token pomocou vyrovnávacej pamäte. Token následne spolu s požiadavkou pošle rozhraniu.

Kapitola 2

Špecifikácia konkrétnych API tokenov

V tejto kapitole predstavíme v praxi využívané API tokeny, ktorými sa zaoberá naša práca. Uvedieme ich formát a základné charakteristiky ako ich vytvorenie, či validácia. Jednotlivé tokeny používajú rôzne kryptografické algoritmy na zabezpečenie integrity a autenticity tokenu. Využíva sa šifrovanie alebo hešovanie s kľúčom [16]. Výsledkom týchto algroritmov je buď elektronický podpis alebo hešovaný autentifikačný kód (HMAC). V oboch prípadoch budeme hovoriť o podpise tokenu. A proces ich vytvárania budeme nazývať podpisovanie.

Ich využitie, výhody či nevýhody rozoberieme v kapitole 3.

2.1 JSON Web Token

Prvý token, ktorým sa budeme zaoberať je JSON web token (JWT) [27]. JWT vznikol ako súčasť JOSE (JSON object signing and encryption) štandardov [6], čo je dokument vypracovaný pracovnou skupinou IETF (Internet Engineering Task Force) na základe aplikácií bezpečnostných mechanizmov v rámci vývoja softvéru. Tieto štandardy popisujú využitie a definujú požiadavky na objekty formátu JSON, ktoré sú bezpečné.

Definujú štandard pre bezpečný prenos JSON objektov medzi službami, ktoré sú schopné ich overiť a dešifrovať. Zavádzajú tri základné formáty JSON objektov a to JWS (JSON Web Signature), JWE (JSON Web Encryption) a JWK (JSON Web Key), ktorým sa detailnejšie venujú ďalšie štandardy [26, 28, 25]. Prvé dva sú formáty zabezpečujúce bezpečnostné vlastnosti JSON objektov. Oba zabezpečujú autentickosť a integritu pomocou elektronických podpisov alebo hešovaného autentifikačného kódu. JWE navyše zabezpečuje aj dôvernosť a to šifrovaním obsahu JSON objektu. Posledný formát JWK je formát pre reprezentáciu kľúčov, ktoré sú použité v kryptografických algoritmoch využitých v JWS a JWE. Kryptografické algoritmy a ich identifikátory sú definované JSON Web Algorithms (JWA) štandardom [24].

2.1.1 Štruktúra JWT

Samotný JWT je v podstate iba serializovaný JSON objekt chránený JWS alebo JWE. Podľa štandardu JWT obsahuje tri samostatné časti oddelené bodkami - hlavičku, telo a podpis. Hlavička a telo sú serializované JSON objekty obsahujúce oprávnenia (angl. claim) vo forme dvojíc kľúč, hodnota. Niektoré kľúče niektorých oprávnení sú definované v štandarde a teda by sa nemali používať pre žiadne iné hodnoty.

A to konkrétne v hlavičke sú najdôležitejšie *typ* a *alg*. Prvý určuje typ tokenu a druhý algoritmus, ktorý bol použitý na vytvorenie podpisu alebo v rámci šifrovania obsahu tokenu. Rôzne možnosti pre algoritmy sú definované v JWA štandardoch.

Telo tvorí logický obsah tokenu, napríklad môže obsahovať oprávnenia týkajúce sa konkrétnej autentifikácie a používateľa, pre ktorého bol token vydaný. Dôležité štandardom popísané kľúče sú napríklad *iss*, *sub*, *exp*, *nbf*, *iat*. Popisujú postupne vydavateľa tokenu, identifikátor používateľa, čas vypršania platnosti tokenu, čas, kedy sa token začne považovať za platný a čas vydania tokenu.

Do tela aj hlavičky sa môžu vkladať ľubovoľné iné oprávnenia, napríklad *admin*, *role*, *permissions*, určujúce oprávnenia používateľa.

2.1.2 Generovanie a validácia JWT

Hlavička a telo sa serializujú pomocou base64url kódovania [29]. V prípade JWE sa telo ešte šifruje. Následne sa obe časti podpíšu algoritmom definovaným v hlavičke a podpis sa zreťazí s hlavičkou a telom. Výsledný reťazec sa používa ako token.

Na overenie platnosti tokenu treba zvalidovať podpis. Podpis je vytvorený pomocou algoritmu definovanom v hlavičke. Teda pri validácii tokenu sa ako prvé dekóduje hlavička tokenu a z nej sa prečíta hodnota v kľúči *alg*.

Na základe hodnoty v kľúči *alg* sa určí algoritmus, ktorý bol použitý na podpis tokenu. Následne sa podpis zvaliduje.

Ak bol token vytvorený pomocou JWE, na prečítanie tela je potrebné ho najprv dešifrovať. V prípade využitia JWS je telo po dekódovaní priamo čitateľné. Následne môžeme overiť informácie o časovej platnosti tokenu, či právach používateľa a pod.

2.2 Platform Agnostic Security Token

Platform Agnostic Security Token (PASETO) je relatívne nový štandard tokenu navrhnutý v roku 2018 a je stále v štádiu RFC draftu [5]. Je inšpirovaný rodinou štandardov JOSE (JWT, JWS, JWE, JWK). Jednoducho povedané snaží sa zjednodušiť implementáciu a použitie kryptografických funkcií.

Rovnako ako JWT, PASETO serializuje JSON objekty a zaručuje rôzne bezpečnostné kvality pri ich prenose cez internet. Pôvodne bol PASETO navrhnutý s dvoma verziami *v1* a *v2* líšiacimi sa v použitých kryptografických algoritmoch. Dnes už existujú štyri verzie *v1*, *v2*, *v3* a *v4* popísané štandardom [3]. Každá verzia tokenu zaručuje autentickosť a integritu obsahu tokenu a to pomocou asymetrického šifrovania v zmysle elektronického podpisu alebo pomocou hešovaného autentifikačného kódu.

2.2.1 Verzie PASETO

Ako sme spomenuli PASETO má štyri verzie. Každá verzia sa delí na dve ďalšie podľa jej využitia na lokálnu a verejnú. Lokálne tokeny majú zašifrované telo a tým zabezpečujú dôvernosť dát uložených v tele tokenu. Na rozdiel od toho sú verejné tokeny nešifrované a dáta v ich tele sú čitateľné pre kohokoľvek s prístupom k danému tokenu.

Každá verzia PASETO používa iný algoritmus na podpisovanie a prípadne šifrovanie tokenu v prípade lokálnych tokenov. Jednotlivé algoritmy pre konkrétne verzie a ich použitie sú popísané v špecifikácii [3].

Novšie verzie *v3* a *v4* prinášajú modernejšie kryptografické algoritmy a pridávajú niektoré funkcionality. Napríklad verzia *v3* prináša nepopierateľnosť autorstva ako novú bezpečnostnú kvalitu. Dosahuje to dokonca bez predĺženia podpisu a to pomocou pridania verejného kľúča do tokenu pred vypočítaním podpisu [39]. Tiež zavádza podporu pre implicitné informácie, teda také informácie, ktoré nie sú uložené priamo v tokene, ale používajú sa pri výpočte podpisu. Teda sú to informácie potrebné pre validáciu tokenu, ale z nejakého dôvodu nie je vhodné ich vkladať priamo do tokenu. Napríklad môže ísť o citlivé interné dáta. Podrobná motivácia za zavedením nových verzií je popísaná v špecifikácii [3].

2.2.2 Štruktúra PASETO

PASETO sa skladá z troch alebo štyroch častí zreťazených bodkou. Časti postupne reprezentujú verziu, využitie, telo a pätu. Prvé tri časti sú povinné a päta je nepovinná, ale dovoľuje nám zapísať akékoľvek ďalšie informácie do tokenu.

- Verzia - reprezentuje verziu PASETO. Môže byť *v1*, *v2*, *v3* alebo *v4*.
- Využitie - určuje využitie tokenu ako lokálne alebo verejné. Možné hodnoty sú *local* alebo *public*.
- Telo - reprezentuje samotné dáta uložené v tokene. Podobne ako pri JWT ide o oprávnenia vo forme dvojíc kľúč hodnota a rovnako sú niektoré dôležité kľúče definované špecifikáciou. [3]
- Päta - môže obsahovať ľubovoľné ďalšie informácie.

Telo a päta sú vo forme JSON objektu, ktorý je serializovaný pomocou base64url [29].

2.2.3 Generovanie a validácia PASETO

Pri vytváraní tokenu sa musíme najprv rozhodnúť pre verziu a využitie podľa toho aké bezpečnostné požiadavky máme na token. Následne vytvoríme telo tokenu obsahujúce informácie, ktoré chceme pomocou tokenu prenášať, napríklad informácie o vzniku tokenu, jeho platnosti, jeho autorovi, či určenom subjekte. Ďalej môžeme pridať ďalšie informácie do päty tokenu ako napríklad identifikátor kľúča kryptografickej funkcie.

Ak sme zvolili lokálne využitie, tak telo tokenu zašifrujeme. Následne vypočítame podpis z tela a päty tokenu. Šifrovanie aj podpisovanie sa deje pomocou kryptografickej funkcie vybratej podľa verzie a využitia. Nakoniec všetky časti spojíme do jedného reťazca a oddelíme bodkami.

Validácia tokenu je inverzný proces ku generovaniu. Najprv rozdelíme reťazec na časti a zistíme verziu a využitie tokenu a podľa toho vyberieme použitú kryptografickú funkciu. Následne zistíme, či je podpis tokenu platný pomocou adekvátnej kryptografickej funkcie a kľúča. Ak mal token lokálne využitie dešifrujeme jeho telo a skontrolujeme časovú platnosť tokenu, ak to využívaná schéma podporuje a telo obsahuje informácie o platnosti tokenu.

2.3 Fernet

Pôvodne Fernet vznikol ako nástroj na zasielanie bezpečných správ v platforme cloudových služieb Heroku [17]. V súčasnosti už podľa špecifikácie [18] vzniklo veľa implementácií Fernetu v rôznych programovacích jazykoch[13, 35], v rámci Heroku bol implementovaný v Ruby. Fernet bol dokonca vybratý PYCA (Python Cryptographic Authority) [41] ako štandard pre implementáciu symetrického šifrovania v Pythone.

Fernet je štruktúrovaný token, lebo v sebe nesie rôzne informácie, no nijak nešpecifikuje formát týchto informácií. Väčšina implementácií s nimi pracuje ako s obyčajným reťazcom znakov.

Token je navrhnutý s možnosťou pridania viacerých verzií, no v súčasnosti existuje len jediná verzia. V tejto verzií je obsah tokenu zašifrovaný pomocou AES-128-CBC [15] a celý token je podpísaný pomocou HMAC-SHA256 [16]. Z toho vyplýva, že Fernet zaručuje autentickosť, integritu a dôvernosť.

2.3.1 Štruktúra Fernet

Fernet sa skladá z piatich zreťazených častí. Každá časť reprezentuje jednu informáciu o tokene. Jednotlivé časti sú nasledovné:

- Verzia - reprezentuje verziu Fernet tokenu, aktuálne existuje len jedna verzia a je reprezentovaná číslom 0x80. Zaberá vždy 8 bitov.
- Časová pečiatka - reprezentuje čas vytvorenia tokenu. Čas je zachytení ako počet sekúnd od 1.1.1970 v UTC časovej zóne. Zaberá vždy 64 bitov.
- Inicializačný vektor (IV) - reprezentuje náhodný reťazec znakov, ktorý je použitý pri šifrovaní a dešifrovaní tokenu. IV musí byť unikátny a najmä nepredvídateľný pre každý token, preto sa generuje náhodnou funkciou. Zaberá vždy 128 bitov.
- Zašifrované telo - reprezentuje zašifrované dáta uložené v tokene. Môže mať premenlivú dĺžku, no vždy násobok 128 bitov.
- Podpis - reprezentuje výstup HMAC-SHA256 funkcie a zaberá vždy 256 bitov.

Ako vidíme, všetky časti tokenu okrem tela majú pevne danú dĺžku. Vďaka tejto vlastnosti nemusia byť zreťazené časti oddelené žiadnym špeciálnym symbolom, napríklad bodkou, lebo vieme jednoznačne oddeliť verziu, časovú pečiatku, IV aj podpis a tým pádom aj zašifrované telo.

Pre jednoduché prenášanie je celý token zakódovaný pomocou base64url [29].

2.3.2 Generovanie a validácia Fernet

Pri generovaní Fernet tokenu sa využívajú dva kryptografické algoritmy, ktoré vyžadujú kľúč. Fernet definuje 256 bitový kľúč, ktorý je rozdelený na dve 128 bitové časti. Prvá časť reprezentuje podpisový kľúč a druhá šifrovací kľúč.

Existuje iba jedna verzia tokenu s pevne daným algoritmom. Pre vygenerovanie tokenu, potrebujeme zaznamenať aktuálny čas do časovej pečiatky a vygenerovať náhodný reťazec, ktorý bude slúžiť ako IV. Následne zašifrujeme telo tokenu pomocou šifrovacieho kľúča a IV. Ďalej vypočítame podpis z predchádzajúcich častí tokenu pomocou podpisového kľúča. Nakoniec všetky časti spojíme do jedného reťazca a zakódujeme pomocou base64url [29].

Validácia tokenu spočíva v dekódovaní tokenu, rozdelení na časti a overení podpisu. Potom dešifrujeme telo tokenu pomocou šifrovacieho kľúča a IV. Následne prípadne overíme časovú platnosť tokenu, ak telo obsahuje potrebné informácie pre overenie časovej platnosti ako vznik a doba platnosti tokenu.

2.4 Branca

Motiváciou k vzniku Branca tokenu [44] bolo modernizovanie Fernet tokenu. Branca má podobnú štruktúru aj generovanie a validáciu ako Fernet. Branca sa líši najmä v tom, že využíva šifrovaciu a podpisovú funkciu XChaCha20-Poly1305 AEAD [2].

2.4.1 Štruktúra Branca

Branca sa podobne ako Fernet skladá z piatich zreťazených častí. Tieto časti sa však jemne líšia od častí Fernet tokenu a zakódované sú *base62* kódovaním [23].

- Verzia - reprezentuje verziu Branca tokenu, aktuálne existuje len jedna verzia a je reprezentovaná číslom 0xBA. Zaberá vždy 8 bitov.
- Časová pečiatka - reprezentuje čas vytvorenia tokenu. Čas je zachytení ako počet sekúnd od 1.1.1970 v UTC časovej zóne. Zaberá vždy 32 bitov a je zapísaná ako číslo bez znamienka.
- Nonce - reprezentuje náhodný reťazec znakov, ktorý využíva šifrovacia funkcia. Ide v podstate o IV, ale využíva sa naozaj len raz, zatiaľ čo IV sa v blokovej šifre využije viac krát. Zaberá vždy 192 bitov.
- Zašifrované telo - reprezentuje zašifrované dáta uložené v tokene. Môže mať ľubovoľnú dĺžku.
- Podpis - v podobe hešovaného autentifikačného kódu - reprezentuje výstup funkcie Poly1305 a zaberá vždy 128 bitov.

2.4.2 Generovanie a validácia Branca

Vygenerujeme 192 bitový reťazec znakov, ktorý bude slúžiť ako nonce a zachytíme aktuálny čas do časovej pečiatky. Vyrobíme hlavičku zreťazením verzie, časovej pečiatky a nonce. Následne zašifrujeme telo tokenu pomocou šifrovacej funkcie, do ktorej vložíme tajný kľúč, nonce a ako dodatočnú informáciu použijeme hlavičku. Funkcia vráti zašifrované telo a hešovaný autentifikačný kód vypočítaný aj z hlavičky. Nakoniec všetky časti spojíme do jedného reťazca a zakódujeme pomocou *base62* kódovania [23].

Pri validácií tokenu ho ako prvé dekódujeme. Následne overíme, že prvý bajt je 0xBA a token rozdelíme na jednotlivé časti. Dešifrujeme telo a overíme podpis pomocou funkcie XChaCha20-Poly1305 AEAD. Následne môžeme overiť napríklad časovú platnosť tokenu pomocou dodatočných informácií v tele tokenu a časovej pečiatky.

2.5 Macaroons

Macaroons sú tokeny s kontextovými pravidlami. Vznikli v rámci výskumného projektu Belay v spoločnosti Google [19]. Google predstavil Macaroons v práci z roku 2014 [7]. Macaroons sú autorizačné poverenia (angl. credentials) pre cloudové služby s podporou decentralizovanej delegácie medzi službami v rámci cloudu. Ľubovoľná entita vlastniaca token autorizujúci určitý prístup môže tento token *zoslabiť* alebo aj *kontextovo obmedziť* a posunúť ďalšej entite. Zoslabenie aj kontextové obmedzenie sa realizuje pomocou pravidiel. Entitu generujúcu nový Macaroons token budeme označovať ako *cieľová služba*.

Pravidlá sa delia podľa strany, ktorá potvrdí alebo zabezpečí ich naplnenie na pravidlá prvej a tretej strany. Pravidlá prvej strany sú jednoduché predikáty. Na autorizáciu požiadavky sprevádzanej Macaroons tokenom sa musia všetky tieto predikáty vyhodnotiť pravdivo v rámci kontextu danej požiadavky. Pravidlom prvej strany môže byť napríklad obmedzenie typu požiadaviek iba na čítacie. Pravidlá tretích strán vyžadujú dôkaz o nejakej skutočnosti od tretej strany. Pri dôkaze od tretích strán sa využíva princíp dôkazu držiteľa kľúča, kde tretia strana dokáže, že pozná nejaký tajný kľúč napríklad tak, že podpíše zadaný reťazec znakov. Pravidlom tretej strany môže byť požiadavka na doloženie dôkazu od autentifikačného servera, že používateľ je autentifikovaný. Pravidlá tretích strán sa používajú na delegáciu autorizácie medzi službami.

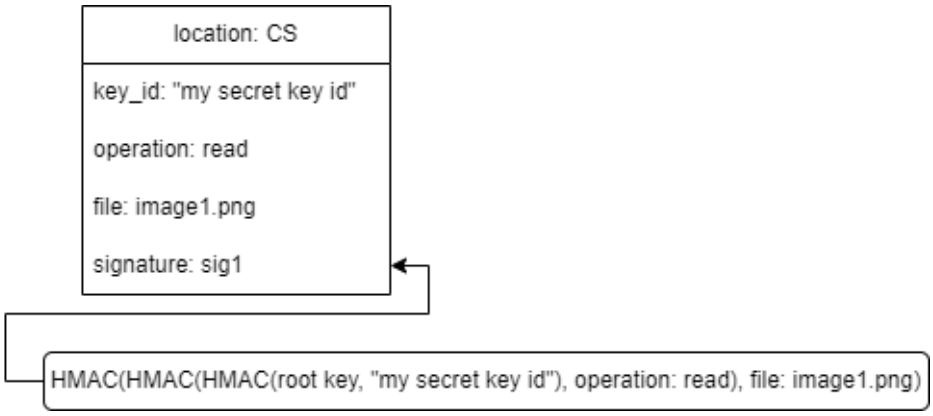
Macaroons zabezpečuje ochranu integrity a autenticity pomocou hešovaného autentifikačného kódu. Pôvodná práca [7] nevyžaduje použitie konkrétnej hešovacej funkcie, no prvá implementácia [12] využíva funkciu HMAC-SHA1 [31].

2.5.1 Štruktúra Macaroons

Macaroons token sa skladá z lokalizácie, identifikátora, pravidiel a podpisu.

- Lokalizácia - reprezentuje nápovedu na lokalitu cieľovej služby. Často reprezentovaná ako URL adresa.
- Identifikátor - slúži na odvodenie koreňového kľúča využitého pri tvorbe tokenu.
- Pravidlá - reprezentujú predikáty, ktoré musia byť splnené pre autorizáciu požiadavky.
- Podpis - reprezentuje postupne generovaný podpis identifikátora a pravidiel tokenu.

Príklad Macaroon tokenu je zobrazený v obrázku 2.1.



Obr. 2.1: Príklad jednoduchého Macaroons tokenu.

2.5.2 Generovanie a delegácia Macaroons

Každá cieľová služba disponuje tajným kľúčom, prípadne spôsobom ako ho vygenerovať. Ku každému tajnému kľúču musí vedieť odvodiť verejný nepriehľadný identifikátor, ktorý dokáže spätne previesť na tajný kľúč. Takého identifikátory môžu byť implementované napríklad ako náhodné noncy reprezentujúce kľúč v databáze alebo pomocou šifrovania s verejným alebo súkromným kľúčom [32].

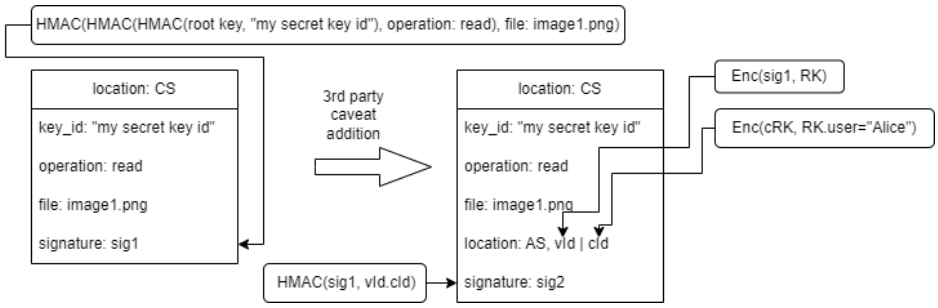
Cieľová služba vytvorí nový token z danej lokácie, identifikátora a tajného kľúča tak, že podpíše identifikátor pomocou tajného kľúča a spojí lokáciu, identifikátor a podpis.

Takto vytvorený token si môžeme predstaviť ako zlatý kľúč, ktorý autorizuje ľubovoľnú požiadavku na cieľovú službu. Cieľová služba môže ďalej token poslať inej službe. Ako sme uviedli v úvode podkapitoly každá služba môže token zoslabiť alebo kontextovo obmedziť pridaním pravidiel.

Pravidlá prvej strany pridá služba tak, že pridá reťazec popisujúci pravidlo do tokenu a podpíše ho pomocou doterajšieho podpisu tokenu ako kľúča. Takto vytvoreným podpisom nahradí predchádzajúci podpis. Tento proces môže zopakovať viac krát a tým pridať ľubovoľný počet pravidiel.

Na pridanie pravidla tretej strany musí mať služba vzťah s danou službou tretej strany a dôverovať jej. Služba pridávajúca pravidlo vygeneruje koreňový kľúč pravidla a potrebuje zabezpečiť, aby ho vedela zderivovať daná služba tretej strany ako aj cieľová služba.

Prvý prípad môže pridávajúca služba zabezpečiť viacerými spôsobmi napríklad tak, že pošle kľúč a pravidlo službe tretej strany cez zabezpečený kanál a tá jej vráti jeho identifikátor cId. Alebo ak zverejňuje služba tretej strany verejný kľúč, prípadne služby zdieľajú tajný kľúč, môže pridávajúca služba vytvoriť cId zašifrovaním koreňového kľúča a pravidla pomocou šifrovacieho kľúča. Druhý prípad zabezpečí pridávajúca služba symetrickým zašifrovaním koreňového kľúča pomocou podpisu tokenu, takto



Obr. 2.2: Príklad pridania pravidla tretej strany, konkrétne pravidla *user="Alice"* na autentifikačný server (AS)

vzniknutý reťazec označme vId.

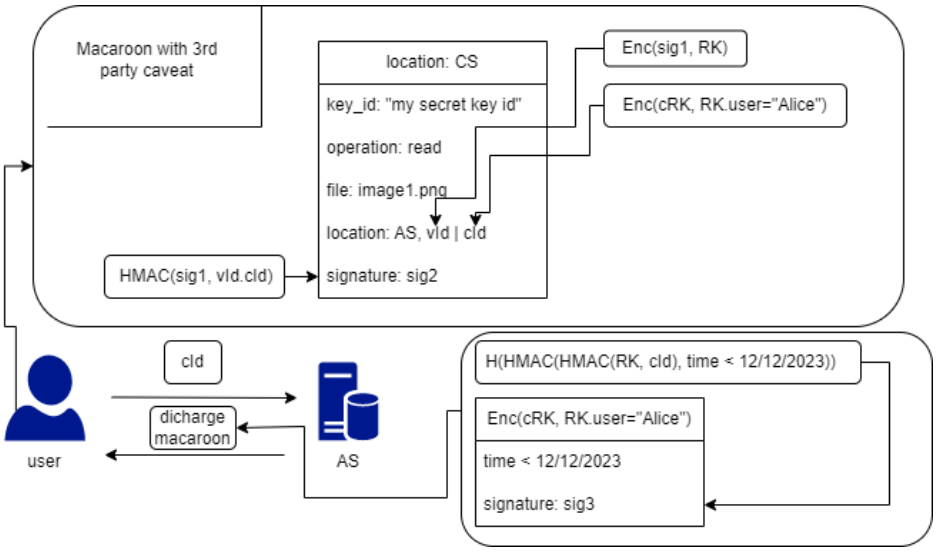
Reťazec reprezentujúci pravidlo tretej stany obsahuje lokáciu služby tretej strany, cId a vId. Pridávajúca služba vloží tento reťazec do zoznamu pravidiel tokenu a vytvorí nový podpis tokenu tým, že podpíše cId a vId pomocou aktuálneho podpisu tokenu. Príklad pridania pravidla tretej strany je na obrázku 2.2. Služba tretej strany vie z cId odvodiť koreňový kľúč pravidla, lebo ho buď sama vytvorila alebo pozná kľúč na dešifrovanie cId. Cieľová služba pozná koreňový kľúč tokenu, teda si vie pomocou postupného podpisovania pravidiel odvodiť kľúč pre dešifrovanie vId.

Tvorba podpisu tokenu teda zodpovedá reťazovej aplikácií funkcie HMAC na identifikátor a pravidlá tokenu. Hešovanie je ireverzibilná operácia, preto nie je možné pravidlá odstraňovať, lebo nato by bolo potrebné vypočítať predchádzajúci podpis tokenu. To je možné iba podpísaním identifikátora koreňovým kľúčom a následným podpisovaním pravidiel vždy pomocou posledného podpisu ako kľúča.

2.5.3 Vytvorenie požiadavky s Macaroons tokenom

Služba komunikujúca s klientom pošle token klientovi. Na vytvorenie požiadavky autorizovanej týmto tokenom, musia byť splnené všetky pravidlá tokenu. Splnenie pravidiel prvej strany závisí od samotného kontextu požiadavky, no pre splnenie pravidiel tretej strany musí klient poskytnúť cieľovej službe dôkazy o ich splnení od daných služieb tretích strán.

Tieto dôkazy sú reprezentované *vybíjacími tokenmi* (angl. discharge Macaroons). Vybíjacie tokeny majú rovnakú štruktúru aj postup generácie ako obyčajné Macaroons tokeny. Potom, čo klient obdrží Macaroons token, ho prehľadá pre všetky pravidlá tretích strán. Pre každé pravidlo tretej strany, pošle požiadavku na službu tretej strany s cId daného pravidla. Služba tretej strany zderivuje koreňový kľúč pravidla a samotné pravidlo z cId. Následne môže vykonať akékoľvek opatrenia na overenie splnenia pravidla klientom, napríklad vyzvať klienta, aby zadal heslo. Ak je pravidlo splnené, vytvorí služba tretej strany vybíjací token z cId pomocou koreňového kľúča pravidla.



Obr. 2.3: Príklad získania vybíjacieho tokenu používateľom.

Následne môže pridať do vybíjacieho tokenu ľubovoľné ďalšie pravidlá vrátane pravidiel tretích strán. Nakoniec pošle vybíjací token klientovi. Príklad získania vybíjacieho tokenu je na obrázku 2.3.

Keď klient získa vybíjací token pre každé pravidlo tretej strany, vytvorí požiadavku na cieľovú službu, ku ktorej priloží Macaroons token a všetky vybíjacie tokeny.

2.5.4 Spracovanie požiadavky cieľovou službou

Predtým ako cieľová služba autorizuje požiadavku od klienta zvaliduje priložený Macaroons token. Pre úspešnú validáciu tokenu musia byť všetky pravidlá splnené a podpis tokenu korektný.

Splnenie pravidiel prvej strany overí cieľová služba overením splnenia predikátu každého pravidla v rámci kontextu požiadavky. Pravidlá tretej strany overí služba rekurzívne. Pre každé pravidlo nájde vybíjací token a z vId pravidla zderivuje koreňový kľúč pravidla. Rekurzívne overí všetky pravidlá vo vybíjacom tokene a pomocou koreňového kľúča pravidla overí korektnosť podpisu vybíjacieho tokenu. Ak sú všetky pravidlá splnené a podpisy všetkých tokenov korektné autorizuje služba požiadavku klienta.

2.6 Bisquits

Ako posledný predstavíme najmladší token rozoberaný v tejto práci. Bisquits token bol predstavený v roku 2021 v blogu od spoluautora z firmy Clever Cloud [9]. Vo voľne dostupnom repozitári [8] nájdeme detailne popísanú motiváciu a vývoj tokenu. Pôvodne bol Bisquits implementovaný v jazyku Rust, no v súčasnosti je k dispozícii aj

implementácia v ďalších jazykoch, všetky nájdeme v repozitári [8].

Bisquits bol inšpirovaný Macaroons, implementuje podobnú schému zabezpečenia aj funkcionality. Rovnako dovoľuje delegovať autorizáciu medzi službami a ľubovoľná entita vlastniaca token ho môže *zoslabiť* alebo aj *kontextovo obmedziť*. Hlavným rozdielom oproti Macaroons je, že Bisquits tokeny používajú na postupné vytváranie podpisu asymetrické šifrovanie, konkrétne podpisovú funkciu Ed25519 [30]. Ďalším veľkým rozdielom je, že Bisquits používa na modelovanie práv, kontrol a dát v rámci tokenu špeciálny variant Datalogu bez negácie a na konkrétnych dátových typoch [33].

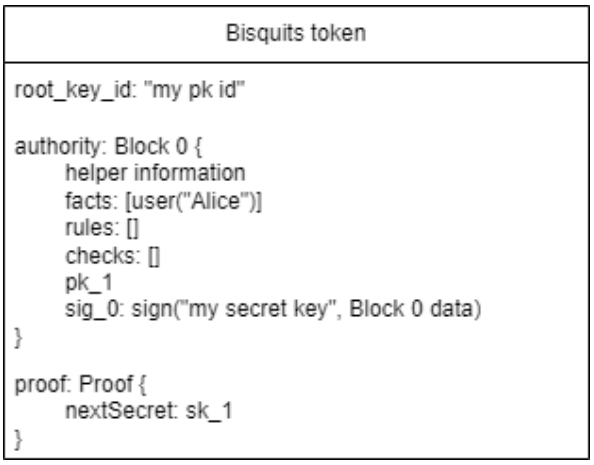
Zoslabenie a kontextové obmedzenie tokenu sa realizuje pomocou pridania nového bloku. Blok môže pridať aj služba tretej strany, v takom prípadne budeme hovoriť o externom bloku.

2.6.1 Štruktúra Bisquits

Samotný token sa skladá z blokov a niektorých globálnych informácií pre celý token. Globálne informácie sú identifikátor koreňového verejného kľúča a dôkaz, ktorý slúži na pridávanie ďalšieho bloku. Každý token obsahuje autoritatívny blok, ktorý pridala služba vytvárajúca token.

Každý blok obsahuje serializovaný datalogový program, podpis bloku a verejný kľúč, v prípade, že ide o externý blok, aj podpis bloku službou tretej strany a príslušný verejný kľúč služby tretej strany. Príklad základného Bisquits tokenu je na obrázku 2.4.

Datalogový program sa skladá z faktov, pravidiel, kontrol a pomocných informácií, detailnú schému formátu nájdeme v súbore schema.proto repozitára [8]. Fakty a pravidlá sú bežné datalogové fakty a pravidlá. Kontroly sú množiny datalogových dotazov. Dotaz je splnený práve vtedy, keď je jeho výsledok aspoň jeden fakt. Kontrola je splnená práve vtedy, keď je splnený aspoň jeden dotaz z množiny dotazov danej kontroly. Okrem toho definuje Bisquits aj politiky, ktoré vytvára entita validujúca token. Viac o politikách rozoberieme v nasledujúcej podkapitole. Bloky a politiky môžu mať anotáciu definujúcu, ktorým blokom dôverujú a teda s faktami a pravidlami, ktorých blokov pracujú. Vždy platí, že blok verí autoritatívnemu bloku, sebe a informáciám v službe validujúcej token. Anotáciou môže blok definovať, že dôveruje aj všetkým predchádzajúcim blokom alebo všetkým blokom podpísaným konkrétnym verejným kľúčom. Posledná možnosť sa využíva pre integráciu služieb tretích strán do autorizačnej schémy. Datalogový program je serializovaný ako Protocol Buffer [20] podľa konkrétnej schémy definovanej v súbore schema.proto alebo v novšej verzii pomocou base64url kódovania [29].



Obr. 2.4: Príklad Bisquits tokena s jediným blokom.

2.6.2 Generovanie a delegácia autorizácie

Na vygenerovanie nového Bisquits tokenu potrebuje služba dvojicu súkromného a verejného kľúča. Do tokenu vloží verejný kľúč alebo jeho identifikátor ako koreňový verejný kľúč daného tokenu. Vytvorí autoritatívny blok, do ktorého vloží základné fakty a pravidlá platné pre tento token. Následne vygeneruje novú dvojicu kľúčov pk_1 a sk_1. Kľúč pk_1 vloží do autoritatívneho bloku a sk_1 do dôkazu tokenu. Kľúč sk_1 bude slúžiť na podpísanie ďalšieho bloku tokenu a pk_1 na overenie tohto podpisu. Nakoniec celý autoritatívny blok podpíše súkromným koreňovým kľúčom a podpis vloží do bloku.

Takto vytvorený token môže služba poslať iným službám a tieto môžu pridávať ďalšie bloky a tým obmedzovať autorizačné práva tokenu. Na vytvorenie i-teho bloku potrebuje služba vygenerovať dvojicu kľúčov pk_{i+1}, sk_{i+1}, kde pk_{i+1} vloží do bloku a sk_{i+1} do dôkazu tokenu. Blok môže pridať aj služba tretej strany, v takom prípade musí vložiť aj podpis bloku služby tretej strany a verejný kľúč služby tretej strany. Celý blok následne podpíše kľúčom sk_i, ktorý vybrala z dôkazu tokenu pred jeho nahradením.

Ľubovoľná služba môže token zapečatiť a znemožniť tak pridávanie nových blokov. Zapečatenie tokenu pozostáva z podpísania posledného bloku kľúčom sk_{last} z dôkazu tokenu. Tento podpis sa vloží do dôkazu tokenu.

2.6.3 Validácia Bisquits

Služba validujúca Bisquits token musí vedieť odvodiť koreňový verejný kľúč tokenu z jeho identifikátora. Služba token deserializuje a postupne zvaliduje všetky podpisy tokenov. Podpis $i+1$-vého bloku validuje pomocou kľúča pk_{i+1} vloženého vnútri i-teho bloku. Podpis autoritatívneho bloku validuje pomocou koreňového verejného kľúča a podpis služby tretej strany pomocou verejného kľúča danej služby uloženého vnútri daného bloku. Ak je token zapečatený validuje podpis v dôkaze tokenu pomocou verej-

ného kľúča v poslednom bloku, ak token nie je zapečatený skontroluje, či verejný kľúč v poslednom bloku tvorí dvojicu so súkromným v dôkaze tokenu.

Ak je token validný, prebehnú postupne všetky kontroly v blokoch a to tak, že sa spustí daný datalogový program nad faktami a pravidlami podľa anotácie bloku a následne sa vykonajú dotazy v kontrolách. Fakty definuje aj samotná služba, napríklad vytvorí fakty na základe kontextu požiadavky. Príkladom takýchto faktov je typ operácie a IP adresa volajúceho. Token je validný iba ak sú splnené všetky kontroly.

Okrem kontrol v rámci blokov tokenu môže validujúca služba definovať ďalšie kontroly a politiky a pravidlá. Pravidlá odvádzajú nové fakty len z faktov odvodených autoritatívnym blokom prípadne samotnou službou. Kontroly a politiky pracujú len nad faktami odvodenými autoritatívnym blokom a službou samotnou. Tieto kontroly musia byť tiež všetky splnené, aby bol token validný.

Politiky definujú väčšie kontroly, taktiež pozostávajú zo zoznamu dotazov. Delia sa na dva typy - povoľovacie a zamietacie politiky. Politika je splnená ak je splnený aspoň jeden dotaz danej politiky. Pri validácii tokenu sa vyhodnocujú politiky postupne po jednej. Ak je splnená povoľovacia politika, token je validný. Ak je splnená zamietacia politika alebo nie je splnená žiadna politika, token je nevalidný. Vyhodnocovanie končí s prvou splnenou politikou.

2.6.4 Delegácia časti autorizácie na tretiu stranu

Každá služba môže využiť inú službu na nejakú časť autorizácie. Na tento účel slúžia externé bloky. Ak chce služba A delegovať autorizáciu na službu B, vytvorí blok s anotáciou obsahujúcou verejný kľúč služby B a vytvorí kontrolu, ktorá používa fakty, ktoré vie zabezpečiť len služba B. Následne pošle službe B informácie potrebné pre autorizáciu danej požiadavky službou B, ktorá vykoná ľubovoľné operácia nutné pre autorizáciu danej požiadavky a ak je úspešná vráti službe A nový externý blok obsahujúci potrebné fakty a kontroly.

Kapitola 3

Teoretické porovnanie API tokenov

V tejto kapitole porovnáme rôzne parametre konkrétnych tokenov podľa informácií získaných z ich dokumentácií a iným zdrojov. Tieto informácie sme zhrnuli v kapitole 2. Pri jednotlivých parametroch vysvetlíme ich význam a teda aj dôležitosť pri porovnávaní tokenov. Porovnávať budeme všetky tokeny popísané v kapitole 2 a nepriehľadný token popísaný v podkapitole 1.7.1. Nepriehľadný token je formát tokenu, nie konkrétny token. Pre jednoduchosť budeme v tejto kapitole pod pojmom nepriehľadný token myslieť náhodný reťazec s podpisom, ktorý vznikol pomocou asymetrického šifrovania.

Kapitola je štruktúrovaná podľa porovnávaných vlastností a jej výsledkom je tabuľka **??** zhrňujúca závery porovnania.

3.1 Bezpečnosť

V rámci porovnávania bezpečnosti tokenov nebudeme detailne rozoberať bezpečnosť jednotlivých kryptografických funkcií. Detaily ohľadom týchto funkcií je možné nájsť v ich citovaných dokumentáciach. Všetky tokeny ponúkajú možnosť použiť kryptografické funkcie, ktoré sú všeobecne považované za bezpečné.

Zameriame sa na porovnanie kryptografických primitív a z nich vyplývajúcich bezpečnostných kvalít a na náchylnosti na zraniteľnosti vyplývajúce zo špecifikácie tokenu.

3.1.1 Kryptografické primitíva

Pri tokenoch rozoznávame tri kryptografické primitíva a to asymetrické šifrovanie vo forme elektronického podpisu, symetrické šifrovanie a hešovanie s kľúčom. Výstupom hešovania s kľúčom je hešovaný autentifikačný kód.

Symetrické šiforvanie sa vrámci nami porovnávaných tokenov využíva na šifrovanie obsahu tokenu a teda na ochranu dôvernosti informácií uložených v tokene. Elektronický podpis a hešovanie zaručujú ochranu autenticity a integrity tokenu. Rozdiel v

použití elektronického podpisu a hešovania je v tom, že v prípade elektronického podpisu ide o asymetrické šifrovanie, teda podpis vie overiť ľubovoľná entita, ktorá pozná verejný kľúč tvoriaci dvojicu so súkromných kľúčom, ktorým bol token podpísaný. Takýto verejný kľúč je zväčša verejne dostupný a vie ho získať ľubovoľná entita. V prípade hešovania ide o symetrickú kryptografiu, pravosť hešovaného autentifikačného tokenu vie overiť len entita, ktorá pozná tajný kľúč, ktorým bol token zahešovaný, čo je často len entita, ktorá token vytvorila.

Výhodou elektronického podpisu teda je, že autenticitu a integritu tokenu môže overiť ľubovoľná entita. Výhodou hešovania je, že je rýchlejšie pri generovní kľúča a generovaní aj overovaní podpisu ako algoritmy pre digitálne podpisy, aj keď v prípade niektorých algoritmov nad eliptickými krivkami je rýchlosť porovnateľná [34]. Pri porovnaní iba algoritmov definovaných v JWA [1] vystupuje hešovanie s kľúčom vždy rýchlejšie.

V prípade JWT si môžeme vybrať, či budeme používať elektronický podpis alebo hešovanie s kľúčom a pomocou nastavenia oprávnenia *alg* v hlavičke na požadovanú hodnotu. Všetky možnosti hodnôt oprávanenia *alg* definuje JWA [24]. Štandard ponúka aj možnosť *alg=none*, v tomto prípade nezaručuje JWT žiadne bezpečnostné kvality a je to jedna zo známych zraniteľností [38] JWT. Ak služba akceptuje aj JWT s *alg=none* ako platné tokeny, útočník jednoducho zamení hodnotu *alg='čokoľvek'* na *alg=none*, odstráni podpis z tokenu a môže ľubovoľne zmeniť token, napríklad si zvýši autorizačné práva. Bezpečné implementácie JWT, by nikdy nemali tokeny s *alg=none* považovať za platné.

PASETO využíva v prípade lokálneho využitia hešovanie a v prípade verejného využitia elektronický podpis. Fernet, Branca a Macaroon využívajú hešovanie s kľúčom a Biscuits využíva elektronický podpis. Nepriehľadný token sme pre potreby tejto kapitoly definovali s použitím elektronického podpisu.

Symetrické šifrovanie a z neho vyplývajúcu ochranu dôvernosti umožňujú tokeny JWT, konkrétne vo forme JWE, PASETO s lokálnym využitím, Fernet a Branca. Biscuits a Macaroons neposkytujú žiadnu ochranu dôvernosti. Nepriehľadný token tiež neposkytuje ochranu dôvernosti, no z definície nenesie žiadnu informáciu, teda v jeho prípade nie je dôvernosť čoho chrániť.

3.1.2 Zraniteľnosti

Pozrieme sa na tri časté zraniteľnosti tokenov a akými prostriedkami im konkrétne tokeny predchádzajú. Rozoberieme zratiteľnosti:

- Útok pomýlením algoritmu (angl. algorithm confusion attack) – útočník donúti overovaciu službu použiť nesprávny algoritmus na overenie podpisu tokenu.

- Útok opakovaním (angl. replay attack) – útočník odchytí token a následne ho opakovane používa na autorizáciu vlastných požiadaviek. Tento útok je priamo spojený s hlavnou nevýhodou používania tokenov v autentifikačnej a autorizačnej schéme a to problémom odvolania (angl. revocation).

- Problém odvolania – problém odvolania je spočíva v schopnosti služby zneplatniť vydané tokeny. Napríklad po odhlásení používateľa alebo po zitení, že token bol zneužitý.

V prípade podpisov tokeny používajú asymetrické šifrovanie a teda dvojicu súkromného a verejného kľúča alebo hešovanie s kľúčom, ktorý je súkromný. Jediný kľúč, ku ktorému má útočník ľahký prístup je verejný kľúč z dvojice kľúčov použitých pri asymetrickom šifrovaní. Útok pomýlením algoritmu potom prebehne tak, že útočník podpíše token funkciou hešovania s kľučom, kde ako kľúč použije získaný verejný kľúč. Následne oklame overovaciu službu, aby token overila pomocou funkcie hešovania s kľúčom, kde ako kľúč použije tento verejný kľúč. Takýmto spôsobom overovacia služba potrvdí platnosť ľubovoľného tokenu, ktorý jej útočník podvrhne. Aby bol tento útok úspešný, musí overovacia služba používať asymetrické šifrovanie na podpis tokenu a zároveň podporovať aj vyvtváranie podpisu tokenu pomocou hešovania s kľúčom.

Existuje viacero spôsobov ako predchádzať útokom pomýlením algoritmu. Najspoľahlivejším spôsobom je podpora jediného kryptografického primitíva na podpis tokenu, napríklad jedine elektronický podpis alebo jedine hešovanie s kľúčom. Takto útočník jednoducho nemá ako oklamať overovaciu službu, ktorý algorimus má použiť pri overovaní, lebo pozná len jeden a ten má implicitne daný.

V prípade použitia viacerých kryptografických primitív sa dá predchádzať týmto útokom pomocou vloženia identifikátora kľúča, ktorým sa overí podpis do tokenu. Následne pri overovaní služba zistí, ktorým algoritmom bol token podpísaný. Taktiež z pridaného identifikátora odvodí, ktorý kľúč má použiť na overenie, ak je to verejný kľúč z dvojice kľúčov pre asymetrické šifrovanie, ale zistený podpisový algoritmus z tokenu je hešovanie s kľúčom, vyhodnotí token za neplatný. Útočník už nedokáže oklamať službu aby použila zlý algoritmus na overienie pospisu, lebo ak by sa o to pokúsil nebude sedieť identifikátor kľúča s podpisovým algoritmom. Úspešnosť tejto métody ochrany nezávisí len od špecifikácie tokenu, ale najmä od jeho konkrétnej implementácie, pretože záleží na implementácií ako bude pracovať s identifikátorom kľúča a či vôbec vyžaduje jeho použitie.

Tokeny využívajúce jediné ktyptografické primitívum sú Fernet, Branca, Biscuits a Macaroons. Sú teda bezpečné proti útokom pomýlením algoritmu, no všetky nejakým spôsobom podporujú budúce verzionovanie tokenu, ktoré môže teoreticky priniesť aj nové kryptografické primitíva. Preto do budúcnosti môžu byť zraniteľné útokom pomýlením algoritmu ak nebudú implementovať inú ochranu voči tomuto útoku. V sú-

časnosti už Macaroons aj Biscuits vyžadujú vloženie identifikátora kľúča do tokenu v rámci ich formátov, teda aj v prípade podpory ďalších kryptografických primitív budú bezpečné proti útokom pomýlením algoritmu.

Jediné kryptografické primitívum využíva aj nepriehľadný token, ale v tomto prípade to nie je veľmi dôležité, lebo nenesie žiadnu informáciu a všetky autorizačné údaje sú uložené v stave overovacej služby. Teda aj v prípade úspešného útoku pomýlením algoritmu, služba síce vyhodnotí podpis tokenu za platný, no ak nezodpovedá žiadnym dátam uloženým v stave služby, tak neprinesie útočníkovi žiadne autorizačné práva.

Viac kryptografických primitív a využívú JWT a PASETO. Obe podporujú asymetrické šifrovanie aj hešovanie s kľúčom na podpisovanie tokenu. V prípade JWT bol útok pomýlením algoritmu jednou zo známych zraniteľností v niektorých implementáciach [38]. Konkrétne útok prebiehal tak, že útočník si vybral službu používajúcu elektronický podpis. Získal jej verejný kľúč *pub_key*, vytvoril podvodný token *mal_token* a do jeho hlavičky zapísal *alg=HS256* (HS256 označuje funkciu HMAC-SHA256), následne funkciou HMAC-SHA256 podpísal token s využitím verejného kľúča služby ako tajného kľúča pre funkciu. Služba, ktorá využívala zraniteľnú knižnicu a na podpisovanie iba elektronický podpis overila token zavolaním funkcie knižnice, napríklad *verify(mal_token, pub_key)*, lebo si myslela, že overuje token podpíaný elektronickým podpis a jeho overenie teda treba verejný kľúč *pub_key*. Knižnica následne prečítala z tokenu, že má overiť podpis pomocou HMAC-SHA256 a využiť pri tom *pub_key* ako kľúč. Toto overenie bolo samozrejme úspešné, lebo token bol naozaj podpísaný funkciou HMAC-SHA256 s kľúčom *pub_key*. V súčastnosti už tieto konkrétne implementácie zaviedli ochranu voči útoku pomýlením algoritmu (pomocou identifikátora kľúča), no nič nezaručuje, že neexistujú iné implementácie s touto zraniteľnosťou. Popísaný útok dáva útočníkovi možnosť získať ľubovoľné práva, lebo celý *mal_token* môže vytvoriť presne tak ako potrebuje. Išlo teda o veľmi nebezpečný útok.

PASETO využíva verzionovanie tokenu ako prevenciu voči útoku pomýlením algortimu. Ide o podobnú techniku ako pri vložení identifikátora kľúča do tokenu, no navyše vyžaduje kontrolu formátu kľúča. Špecifikácia PASETO [3] prikazuje každej knižnici, ktorá chce implementovať PASETO, logicky rozlišovať medzi kľúčami určenými pre rôzne podpisové funkcie. V rámci špecifikácie sa ochrane voči útoku pomýlením algoritmu venuje dedikovaný dokument [4]. Kľúč k ľubovoľnému algortimu musí byť vždy uložený tak, aby sa dalo jasne určiť, pre ktorý algoritmus sa má použiť. Tento cieľ sa dá dosiahnuť napríklad tak, že sa kľúč uloží v nejakej štruktúre spolu s verziou a využitím tokenu. Následne pri validácií podpisu tokenu musí prebehnúť kontrola rovnosti verzie a využitia v kľuči s verziou a využitím v tokene. Podobne ako pri JWT popísaná ochrana bude úspešná len v prípade, že ju knižnice implementujúce PASETO budú využívať. Výhodou PASETO je, že sa ochrana vyžaduje v špecifikácii, teda každá knižnica, ktorá chce úspešne implementovať špecifikáciu PASETO ju musí implementovať.

V prípade JWT štandard [27] nevyžaduje využitie identifikátora kľúča.

Kapitola 4

Návrh a implementácia jednoduchého rozhrania

V tejto kapitole navrhneme a implementujeme jednoduché rozhranie s použitím viecerých API tokenov pre autentifikáciu a autorizáciu.

Kapitola 5

Porovnanie na jednoduchom rozhraní

V tejto kapitole porovnáme jednotlivé API tokeny na nami implementovanom rozhraní. Výsledkom budú naše pozorovania pri implementacii a použití rozhrania s jednotlivými typmi API tokenov.

Záver

Literatúra

[1] R. Gunawan A. Rahmatulloh and F. M. S. Nursuwars. Performance comparison of signed algorithms on json web token. https://iopscience.iop.org/article/10.1088/1757-899X/550/1/012023/pdf.

[2] S. Arciszewski. Aead xchacha20 poly1305. https://datatracker.ietf.org/doc/html/draft-irtf-cfrg-xchacha-03.

[3] S. Arciszewski. Paseto specification. https://github.com/paseto-standard/paseto-spec.

[4] S. Arciszewski. Paseto specification. https://github.com/paseto-standard/paseto-spec/blob/master/docs/02-Implementation-Guide/03-Algorithm-Lucidity.md.

[5] S. Arciszewski. Paseto: Platform-agnostic security tokens, Apríl 2018. https://paseto.io/rfc/.

[6] Richard Barnes. Use Cases and Requirements for JSON Object Signing and Encryption (JOSE). RFC 7165, Apríl 2014.

[7] Arnar Birgisson, Joe Gibbs Politz, Úlfar Erlingsson, Ankur Taly, Michael Vrable, and Mark Lentczner. Macaroons: Cookies with contextual caveats for decentralized authorization in the cloud. In *Network and Distributed System Security Symposium*, 2014.

[8] Clever Cloud. Bisquits repository. https://github.com/biscuit-auth/biscuit.

[9] Geoffroy Couprie. Biscuit, the foundation for your authorization systems. https://www.clever-cloud.com/blog/engineering/2021/04/12/introduction-to-biscuit/.

[10] Curity. The phantom token approach. https://curity.io/resources/learn/phantom-token-pattern/.

[11] Curity. The split token approach. https://curity.io/resources/learn/split-token-pattern/.

[12] Robert Escriva. libmacaroons. https://github.com/rescrv/libmacaroons.

[13] Amit Eyal. C++ fernet implementation. https://github.com/IamAmitE/FernetCpp/.

[14] Fallible. We reverse engineered 16k apps, here's what we found, Január 2017. https://hackernoon.com/we-reverse-engineered-16k-apps-heres-what-we-found-51bdf3b456bb#.io6e11q6n.

[15] Sheila Frankel, K. Robert Glenn, and Scott G. Kelly. The AES-CBC Cipher Algorithm and Its Use with IPsec. RFC 3602, September 2003.

[16] Sheila Frankel and Scott G. Kelly. Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec. RFC 4868, May 2007.

[17] Harold Giménez. Fernet legacy specification. https://github.com/heroku/legacy-fernet.

[18] Harold Giménez. Fernet specification. https://github.com/fernet/spec/blob/f16a35d3cfd8cdb2d8c7f7d10ce6c4d6058b19d2/Spec.md.

[19] Google. Belay research project. https://sites.google.com/site/belayresearchproject/home.

[20] Google. Protocol buffers documentation. https://protobuf.dev/overview/.

[21] Weili Han, Zhigong Li, Minyue Ni, Guofei Gu, and Wenyuan Xu. Shadow attacks based on password reuses: A quantitative empirical analysis. *IEEE Transactions on Dependable and Secure Computing*, 15(2):309–320, 2018.

[22] Dick Hardt. The OAuth 2.0 Authorization Framework. RFC 6749, 2012.

[23] Kejing He, Xiancheng Xu, and Qiang Yue. A secure, lossless, and compressed base62 encoding. In *2008 11th IEEE Singapore International Conference on Communication Systems*, pages 761–765, 2008.

[24] Michael Jones. JSON Web Algorithms (JWA). RFC 7518, Máj 2015.

[25] Michael Jones. JSON Web Key (JWK). RFC 7517, Máj 2015.

[26] Michael Jones, John Bradley, and Nat Sakimura. JSON Web Signature (JWS). RFC 7515, Máj 2015.

[27] Michael Jones, John Bradley, and Nat Sakimura. JSON Web Token (JWT). RFC 7519, Máj 2015.

[28] Michael Jones and Joe Hildebrand. JSON Web Encryption (JWE). RFC 7516, Máj 2015.

[29] Simon Josefsson. The Base16, Base32, and Base64 Data Encodings. RFC 4648, Október 2006.

[30] Simon Josefsson and Ilari Liusvaara. Edwards-Curve Digital Signature Algorithm (EdDSA). RFC 8032, Január 2017.

[31] Dr. Hugo Krawczyk, Mihir Bellare, and Ran Canetti. HMAC: Keyed-Hashing for Message Authentication. RFC 2104, Február 1997.

[32] Butler Lampson, Martín Abadi, Michael Burrows, and Ted Wobber. Authentication in distributed systems: Theory and practice. volume 10, pages 165–182, Október 1991.

[33] Ninghui Li and John C. Mitchell. Datalog with constraints: A foundation for trust management languages. In *Proceedings of the Fifth International Symposium on Practical Aspects of Declarative Languages*, Január 2003.

[34] Luis Lizama, Leonardo Arrieta, Flor Mendoza, Luis Servín, and Eric Simancas-Acevedo. Public hash signature for mobile network devices. *Ingeniería Investigación y Tecnología*, 20:1–10, Apríl 2019.

[35] Rodney Lorrimar. Haskell fernet implementation. `https://github.com/IamAmitE/FernetCpp/`.

[36] Arvind Narayanan and Vitaly Shmatikov. Fast dictionary attacks on passwords using time-space tradeoff. In *Proceedings of the 12th ACM Conference on Computer and Communications Security*, CCS '05, page 364–372, New York, NY, USA, 2005. Association for Computing Machinery.

[37] Okta. Access token: Definition, architecture, usage and more. `https://www.okta.com/identity-101/access-token/`.

[38] Okta. Critical vulnerabilities in json web token libraries. `https://auth0.com/blog/critical-vulnerabilities-in-json-web-token-libraries/#Meet-the--None--Algorithm`.

[39] Thomas Pornin and Julien P. Stern. Digital signatures do not guarantee exclusive ownership, 2005. `http://www.bolet.org/~pornin/2005-acns-pornin+stern.pdf`.

[40] Agathoklis Prodromou. Tls security 6: Examples of tls vulnerabilities and attacks, Marec 2019. https://www.acunetix.com/blog/articles/tls-vulnerabilities-attacks-final-part/.

[41] PYCA. Python cryptography library. https://github.com/pyca/cryptography.

[42] Redis. Redis. https://redis.io/.

[43] N. Sakimura, NRI, J. Bradley, Ping Identity, Microsoft, M. Jones, B. de Medeiros, Google, and C. Mortimore. Openid connect core 1.0 incorporating errata set 1, November 2014. https://openid.net/specs/openid-connect-core-1_0.html#IDToken.

[44] Mika Tuupola. Branca specification. https://github.com/tuupola/branca-spec.