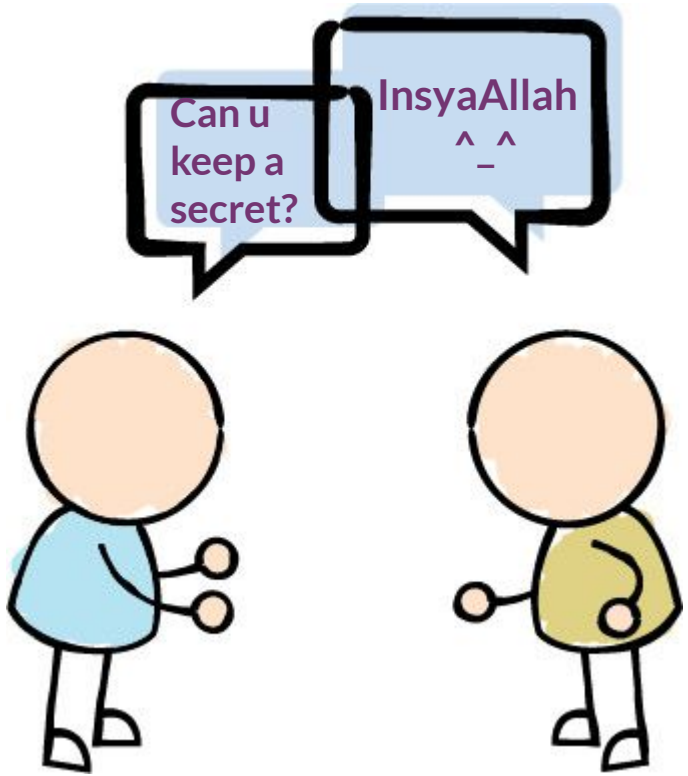
React Native Application Security

Isumi
Batam, Jan 2020

GOALS

1. Intro Application Security
2. Library
3. Using Token

1. Intro



Application Security | Concepts

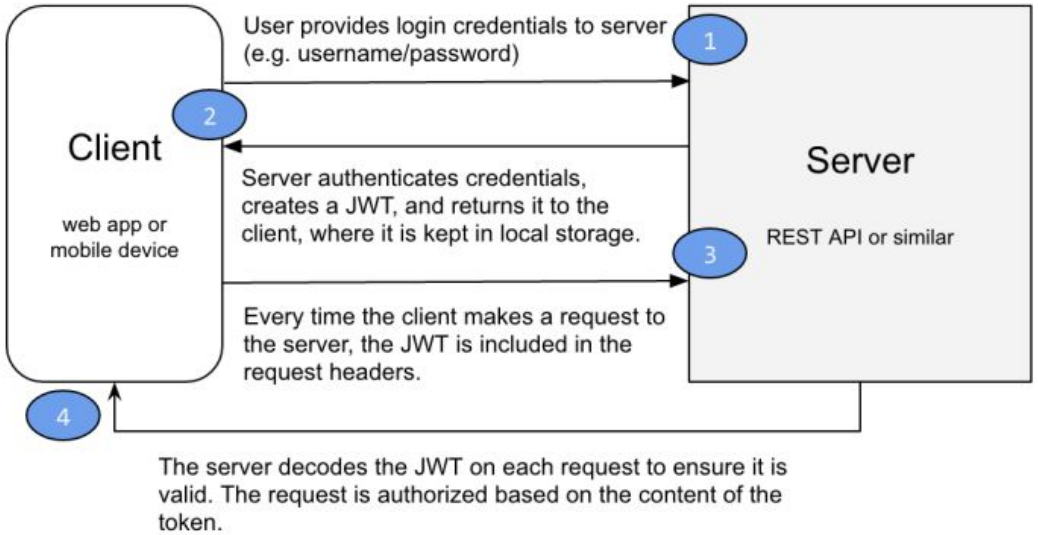
- **Authentication**

  Refers to verify ***who you are***, so you need to use username and password for authentication.
- **Authorization**

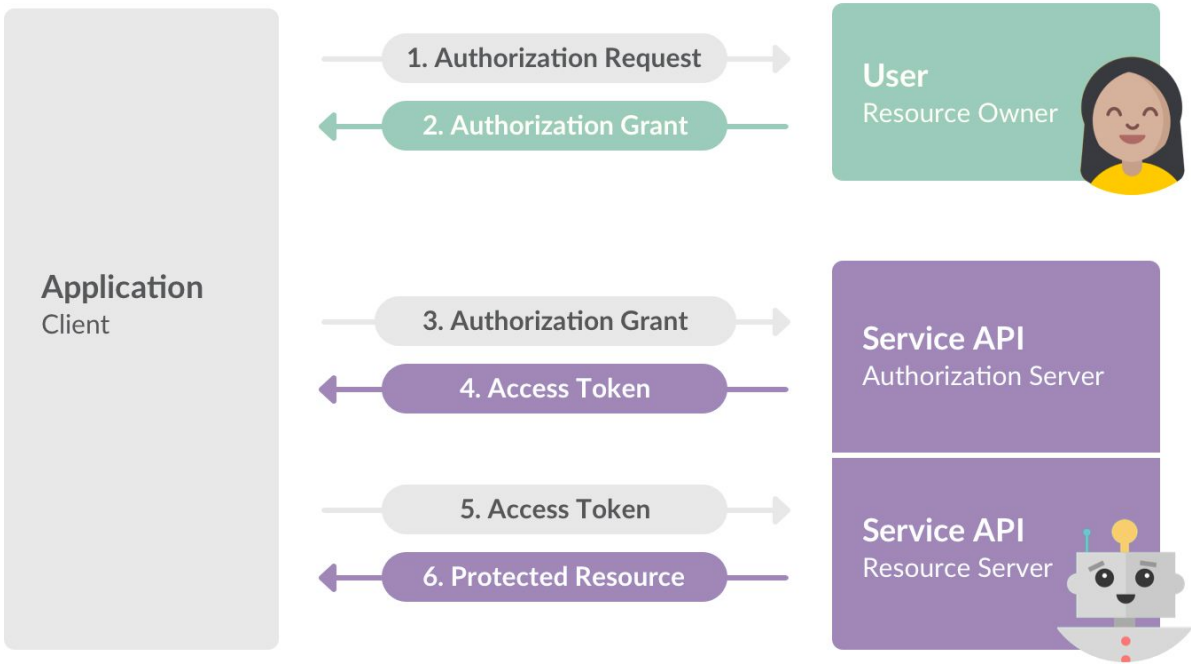
  Refers to ***what you can do***, for example access, edit or delete permissions to some documents, and this happens after verification passes.
- **Encryption**

  Security method where information is encoded and can only be accessed or decrypted by a user with the correct encryption key.

Authentication

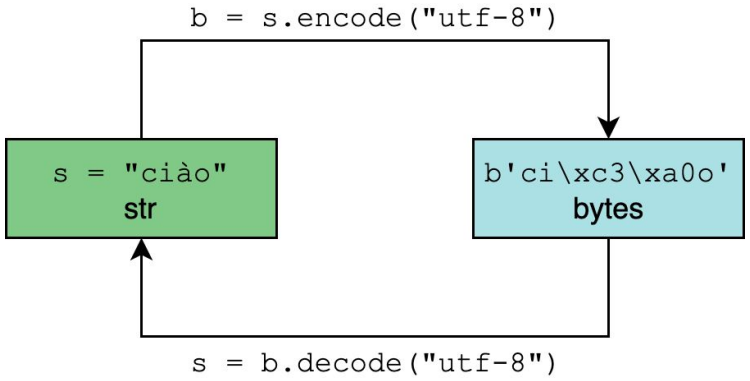


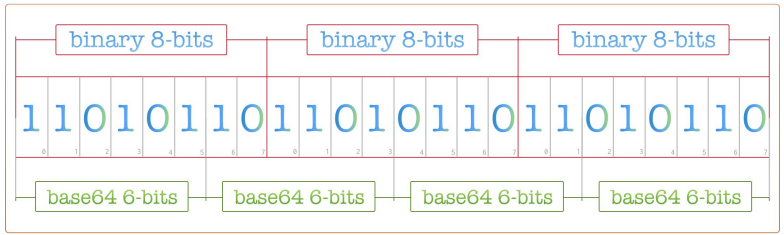
Authorization



Encryption

- **Encode - Decode**

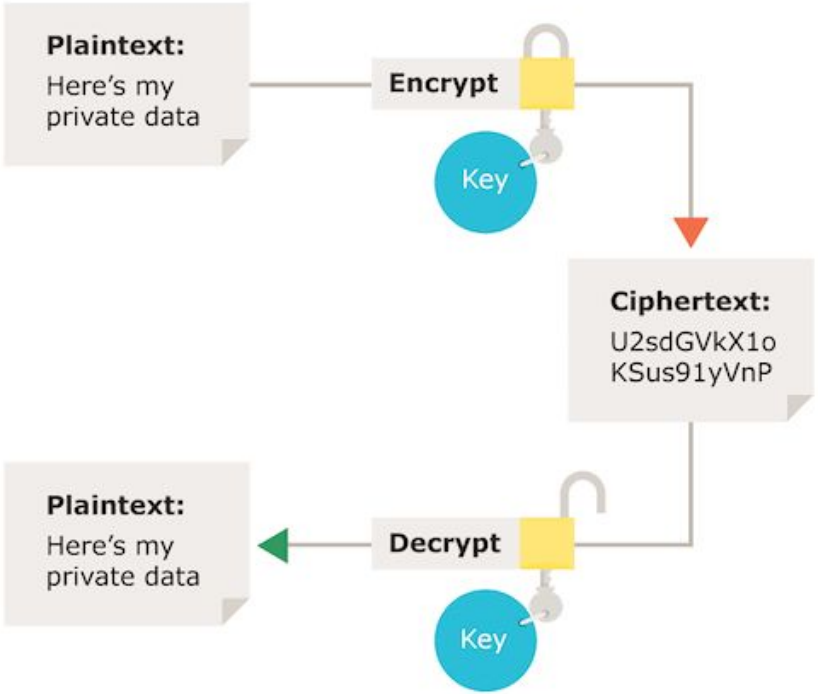




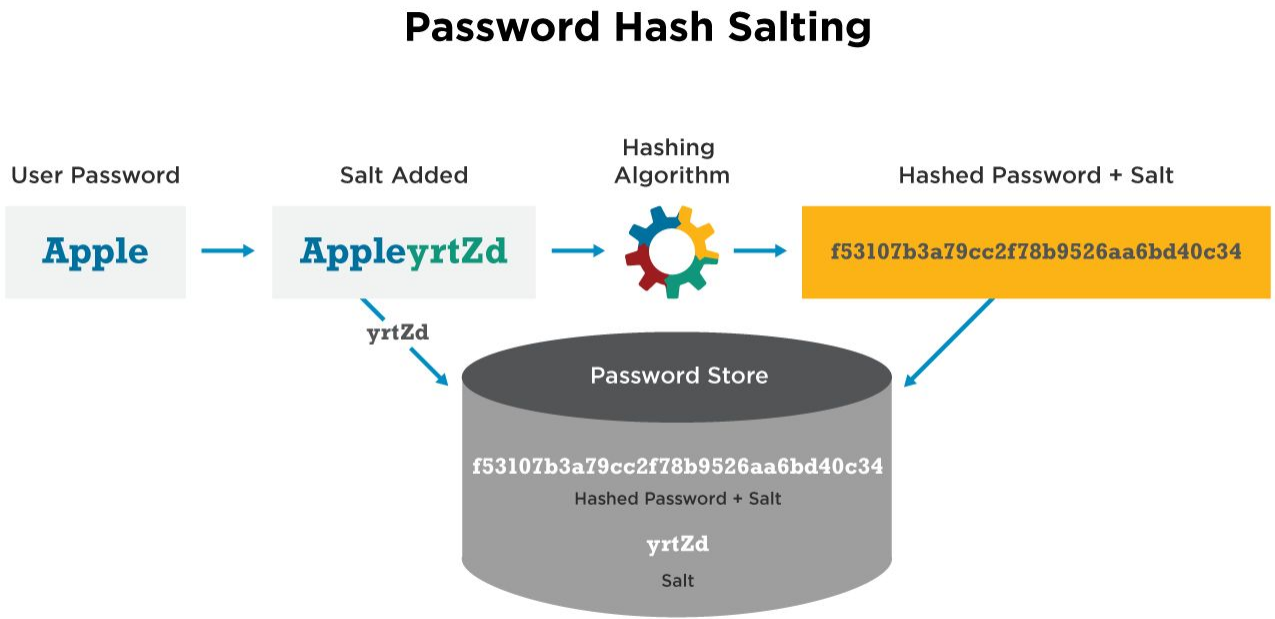
Base64 Character Index Table:

INDEX	CHAR	INDEX	CHAR	INDEX	CHAR	INDEX	CHAR
0	A	16	Q	32	g	48	w
1	B	17	R	33	h	49	x
2	C	18	S	34	i	50	y
3	D	19	T	35	j	51	z
4	E	20	U	36	k	52	0
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8
13	N	29	d	45	t	61	9
14	O	30	e	46	u	62	+
15	P	31	f	47	v	63	/

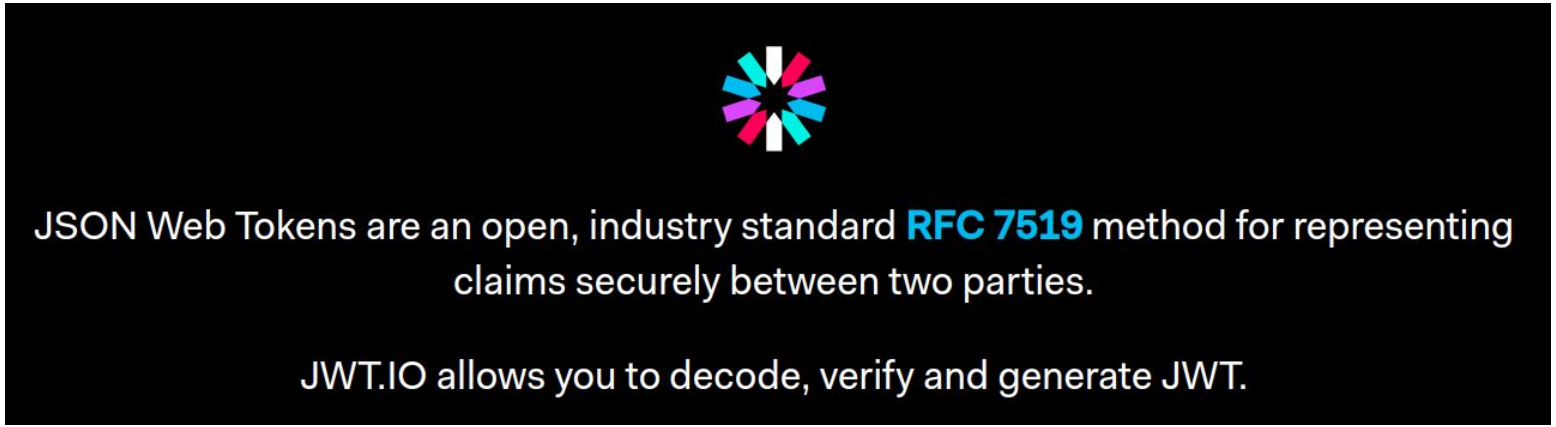
- **Encrypt - Decrypt**

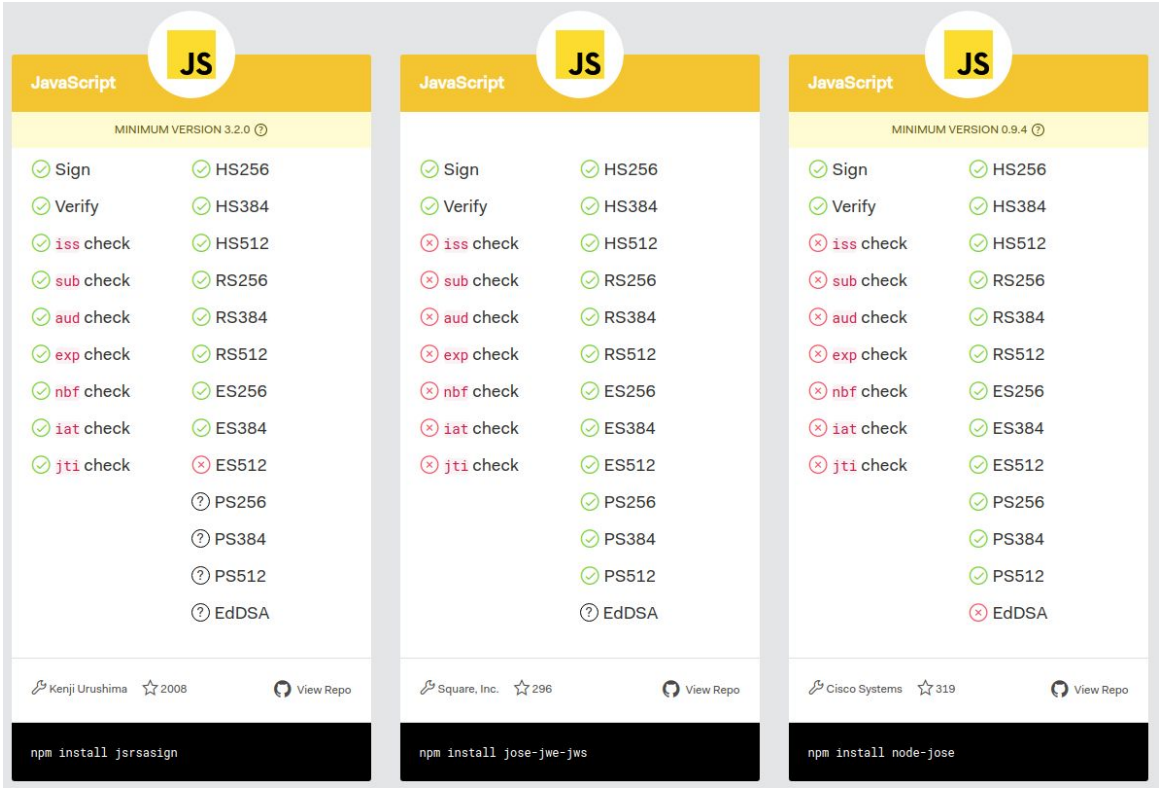


- **Hashing**


Password Hash Salting
User Password
Apple
Salt Added
AppleyrtZd
Hashing Algorithm
Hashed Password + Salt
f53107b3a79cc2f78b9526aa6bd40c34
yrtZd
Password Store
f53107b3a79cc2f78b9526aa6bd40c34
Hashed Password + Salt
yrtZd
Salt

2. Library


JSON Web Tokens are an open, industry standard RFC 7519 method for representing claims securely between two parties.
JWT.IO allows you to decode, verify and generate JWT.


JavaScript
JS
MINIMUM VERSION 3.2.0
Sign
Verify
iss check
sub check
aud check
exp check
nbf check
iat check
jti check
HS256
HS384
HS512
RS256
RS384
RS512
ES256
ES384
ES512
PS256
PS384
PS512
EdDSA
Kenji Urushima
2008
View Repo
npm install jsrsasign
JavaScript
JS
Sign
Verify
iss check
sub check
aud check
exp check
nbf check
iat check
jti check
HS256
HS384
HS512
RS256
RS384
RS512
ES256
ES384
ES512
PS256
PS384
PS512
EdDSA
Square, Inc.
296
View Repo
npm install jose-jwe-jws
JavaScript
JS
MINIMUM VERSION 0.9.4
Sign
Verify
iss check
sub check
aud check
exp check
nbf check
iat check
jti check
HS256
HS384
HS512
RS256
RS384
RS512
ES256
ES384
ES512
PS256
PS384
PS512
EdDSA
Cisco Systems
319
View Repo
npm install node-jose

3. Using Token

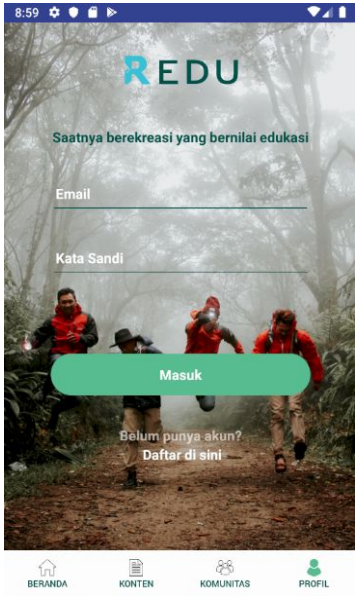
AsyncStorage

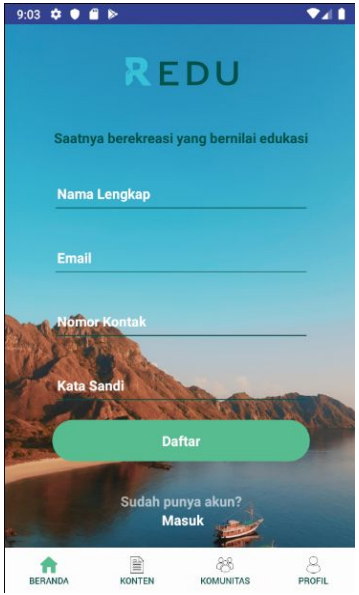
Simple, unencrypted, asynchronous, persistent, key-value storage system that is global to the app.

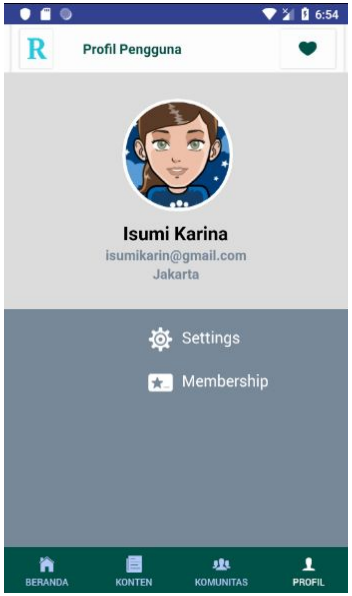
For more details:
https://www.npmjs.com/package/@react-native-community/async-storage

Exercise

Implementation AsyncStorage in your app. ;)







BINAR ACADEMY