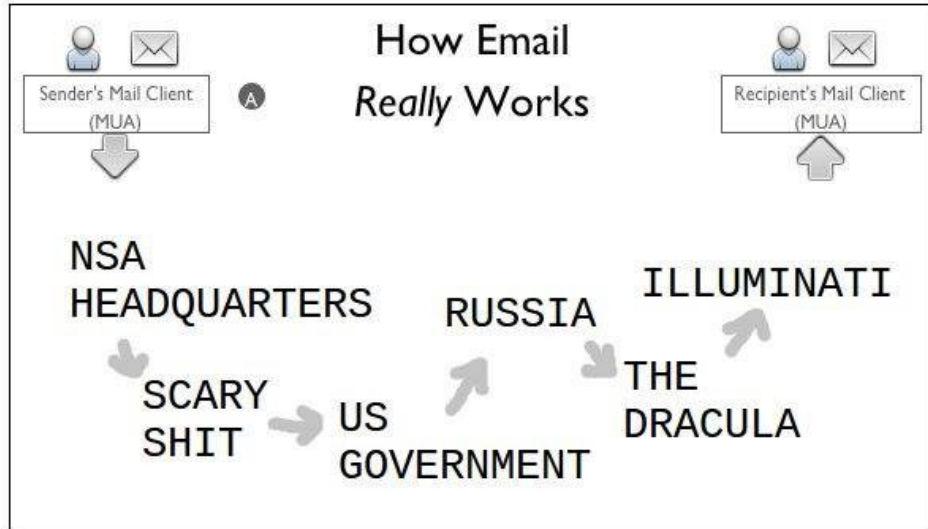
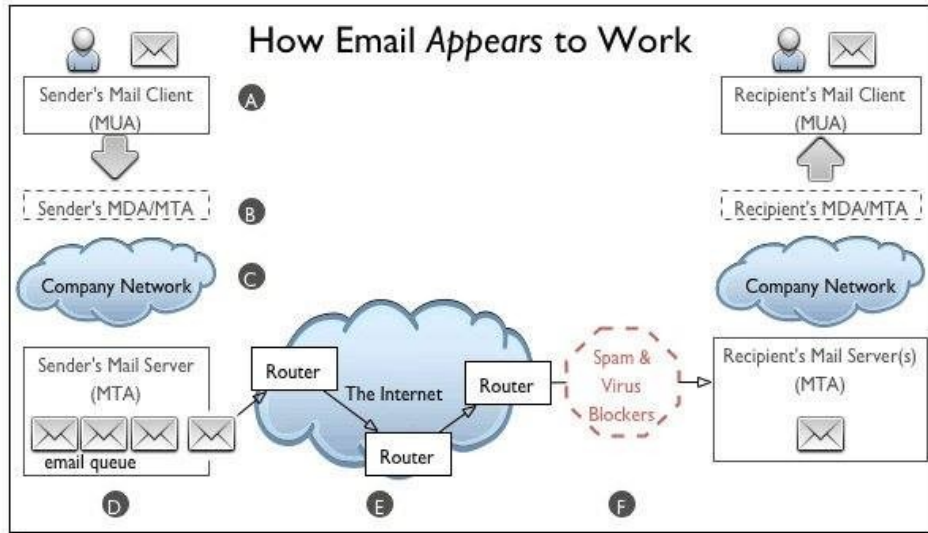


Zero Knowledge



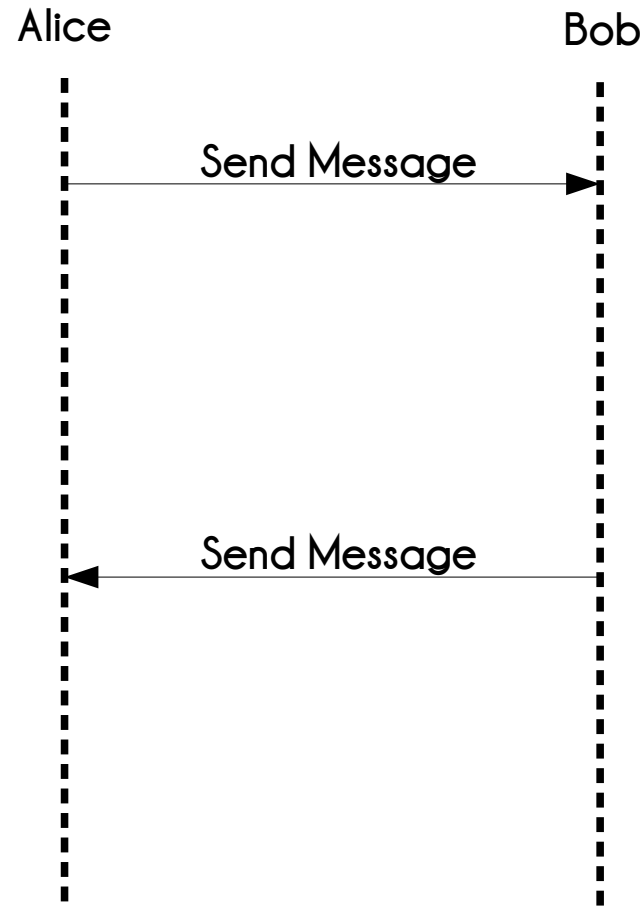
Meeting the Growing
Demand for Security
and Privacy in a
National Security
World

@bendechrai

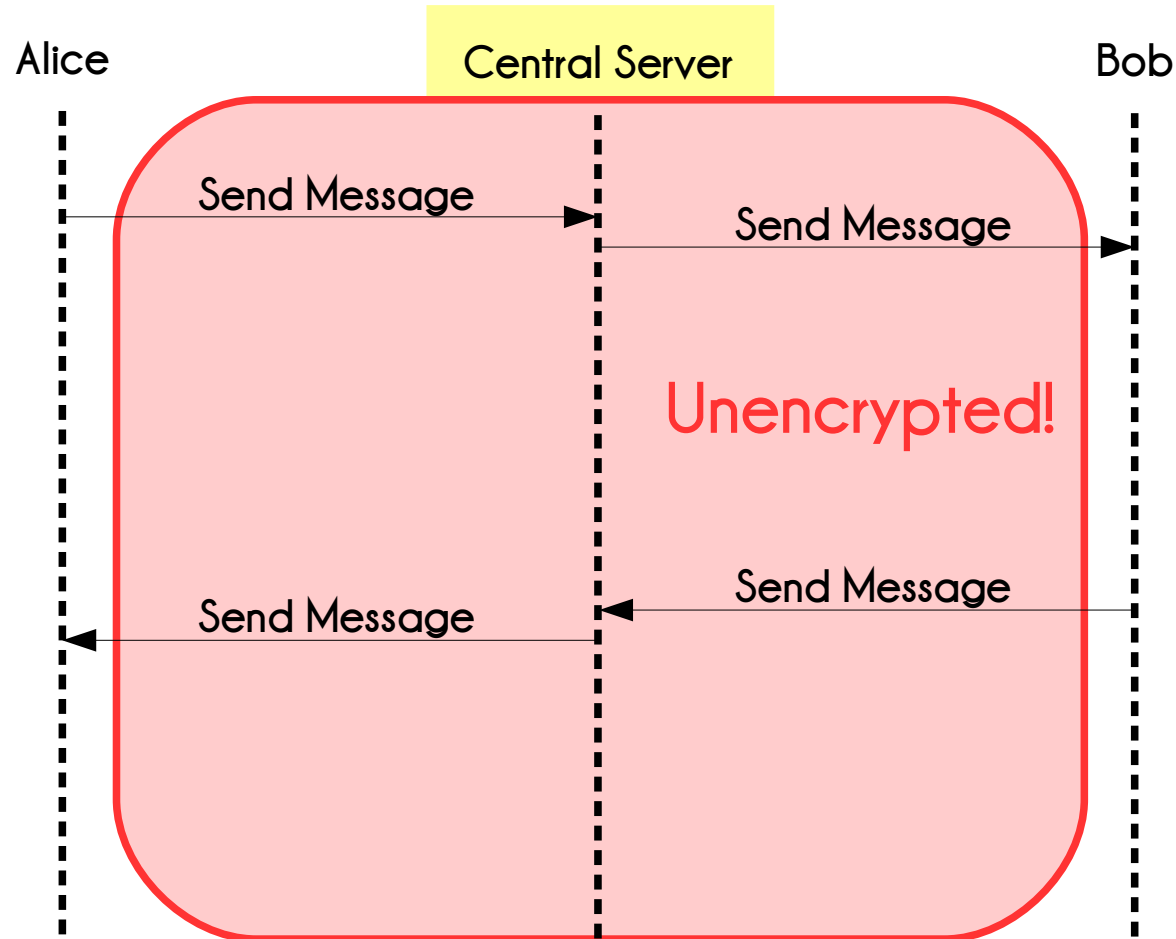
joinind.in/talk/60554

Securing Communications

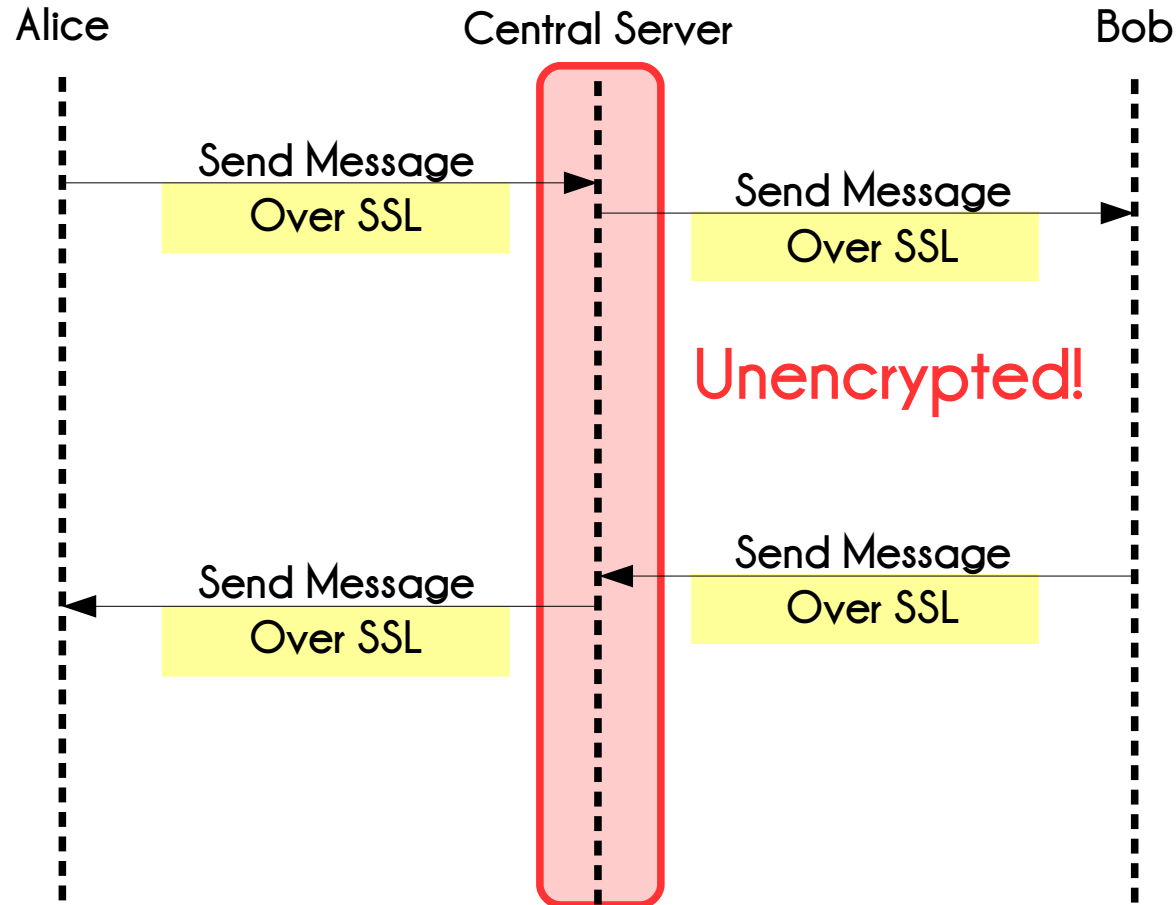
Securing Communications



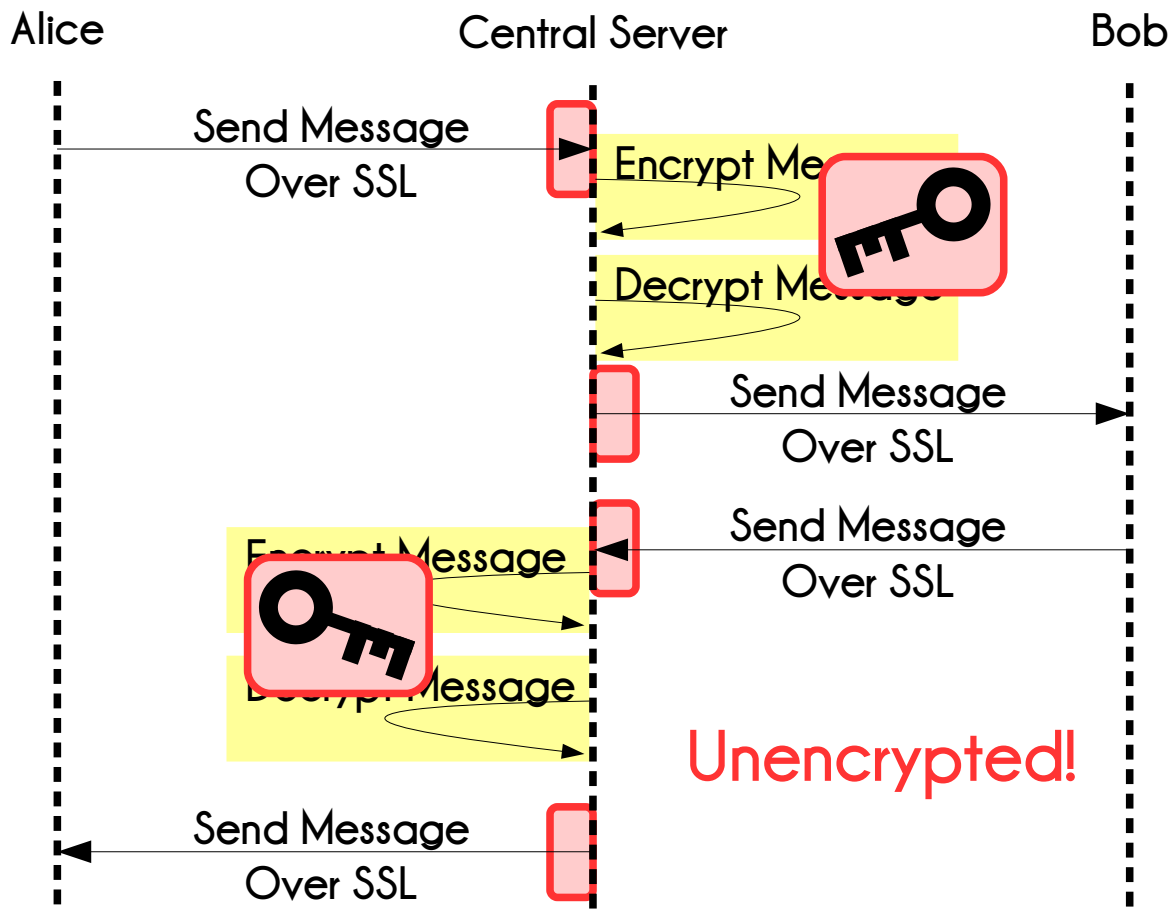
Securing Communications



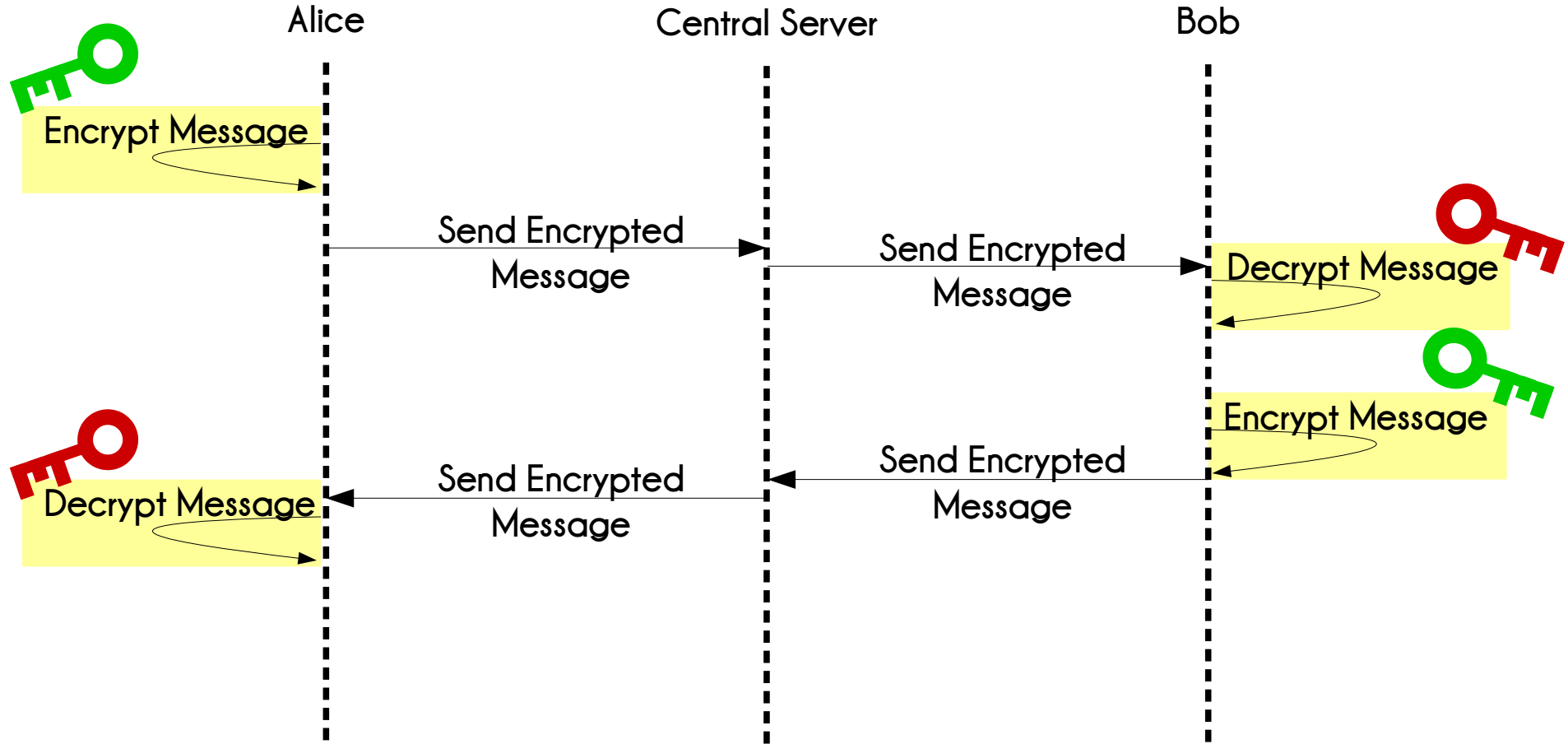
Securing Communications



Securing Communications

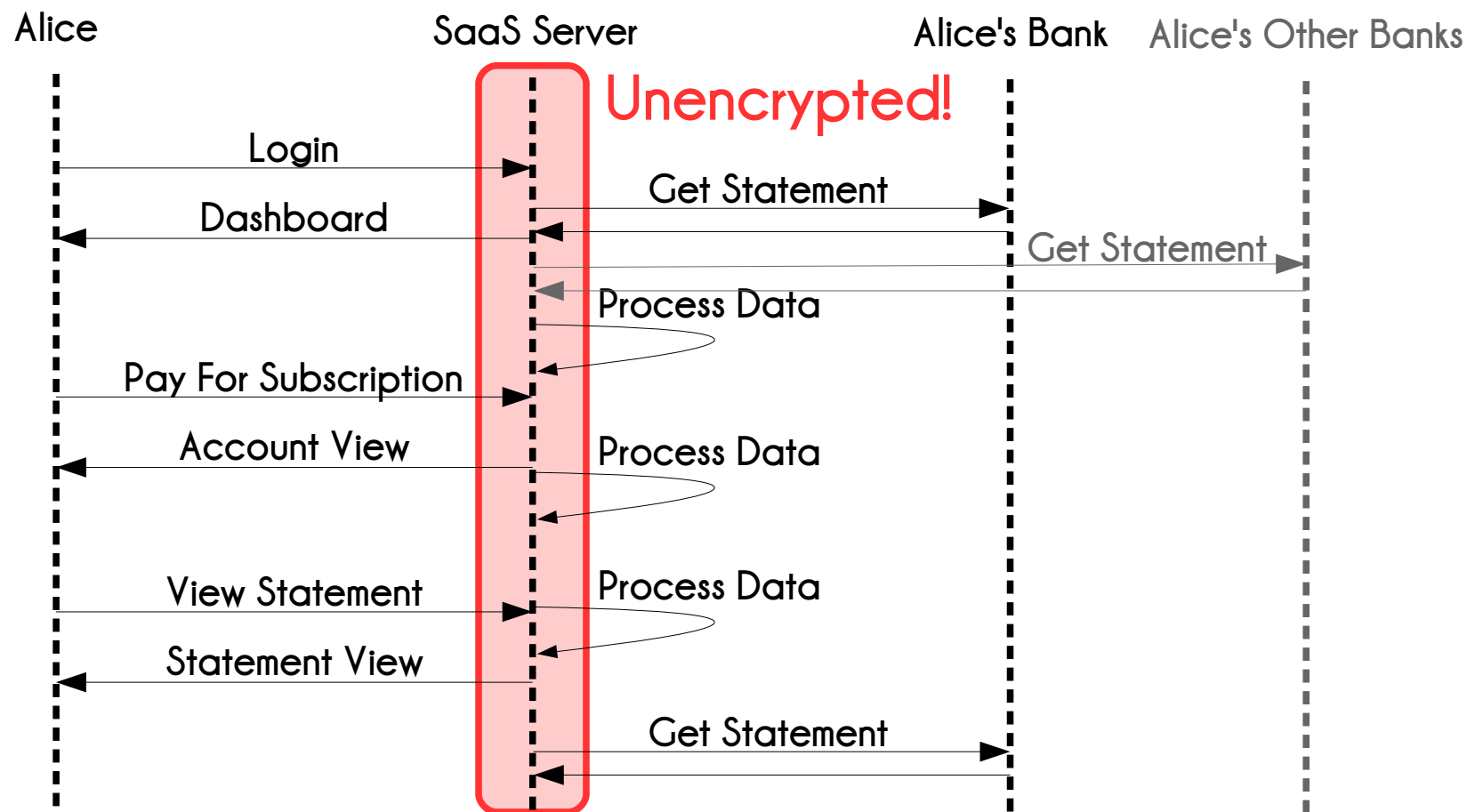


Securing Communications

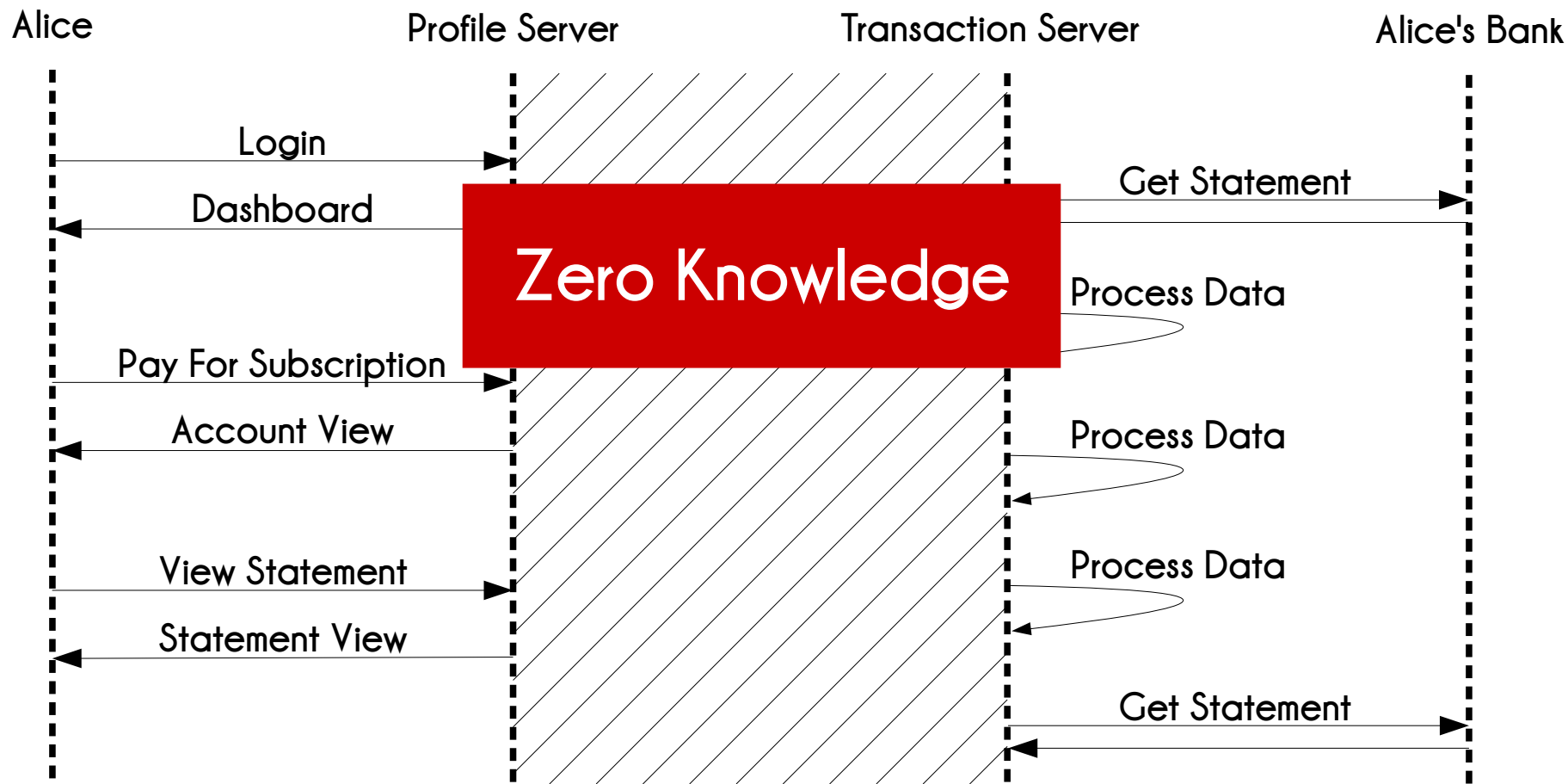


Software as a Service

Software as a Service

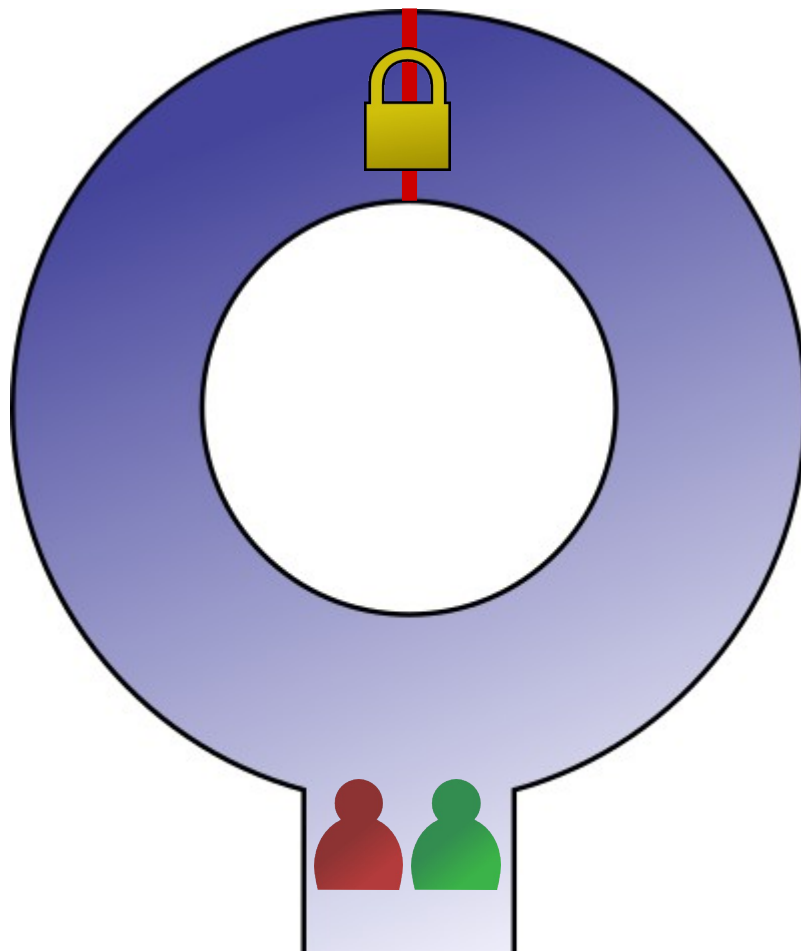


Software as a Service

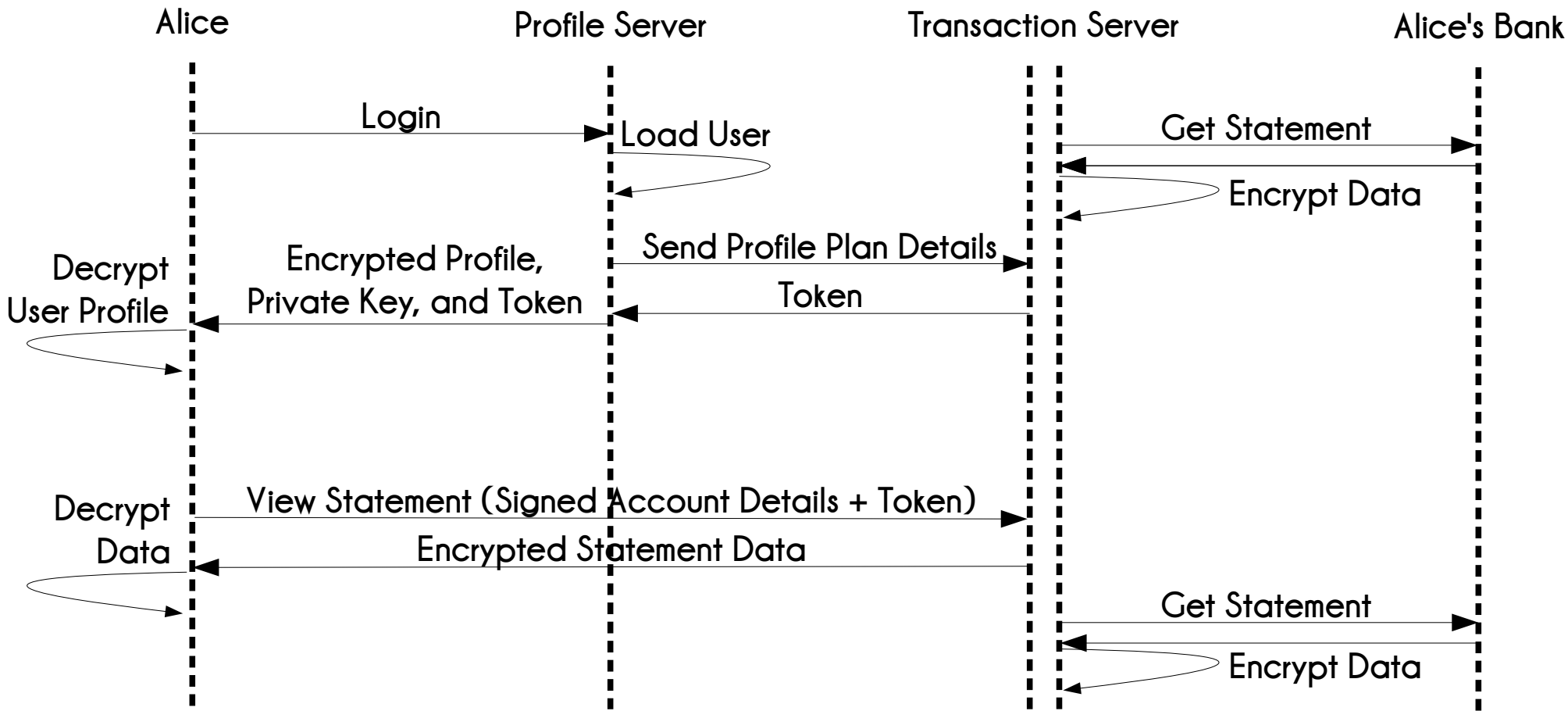


Zero Knowledge

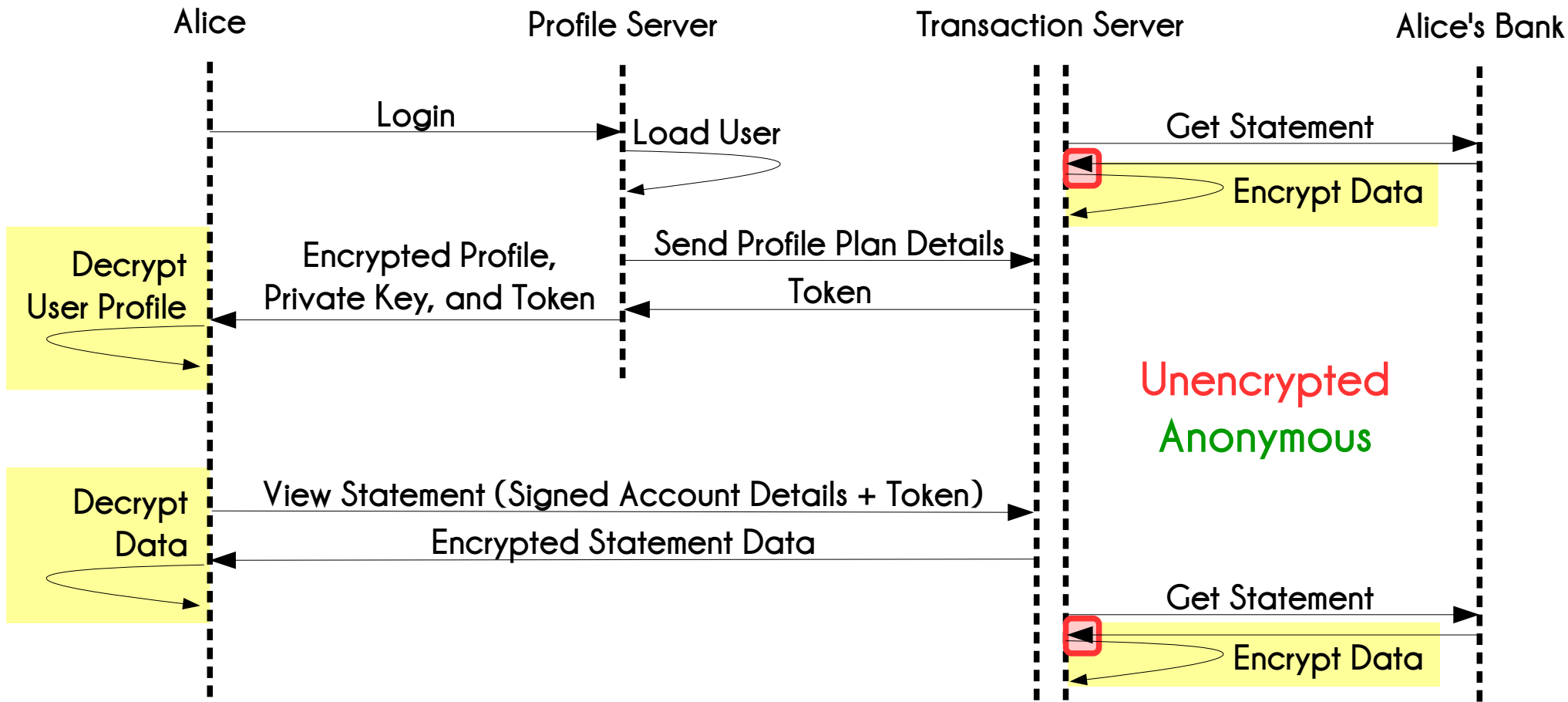
Zero Knowledge



Software as a Service

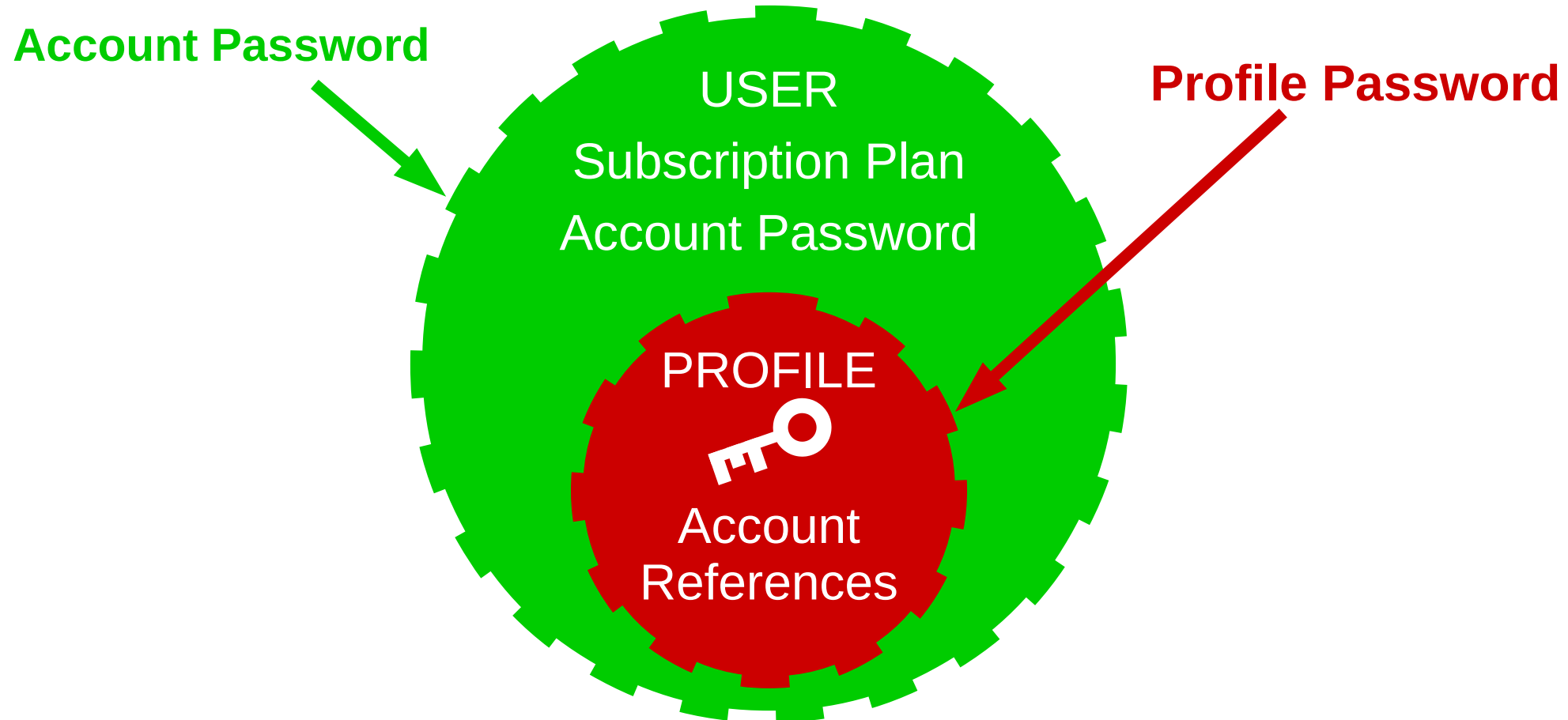


Software as a Service



Profile Encryption

Profile Encryption



Profile Encryption

Account

password

User

```
# username: string
# password: string
# subscription_plan: enum
# profile_data: binary
# profile_private_key: string
# profile_public_key: string
```

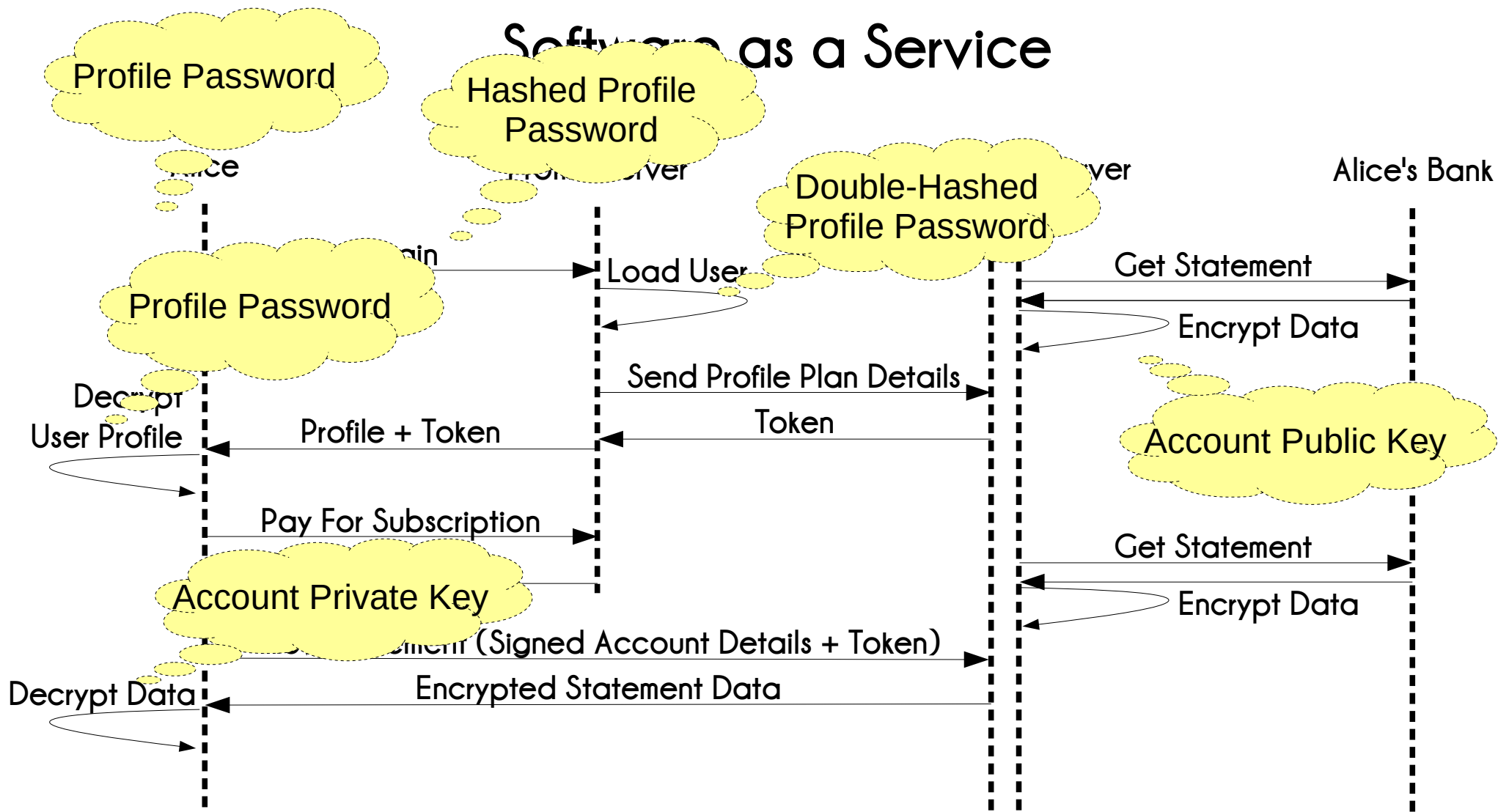
Profile

```
# account_references: array [
  id => private_key
]
```

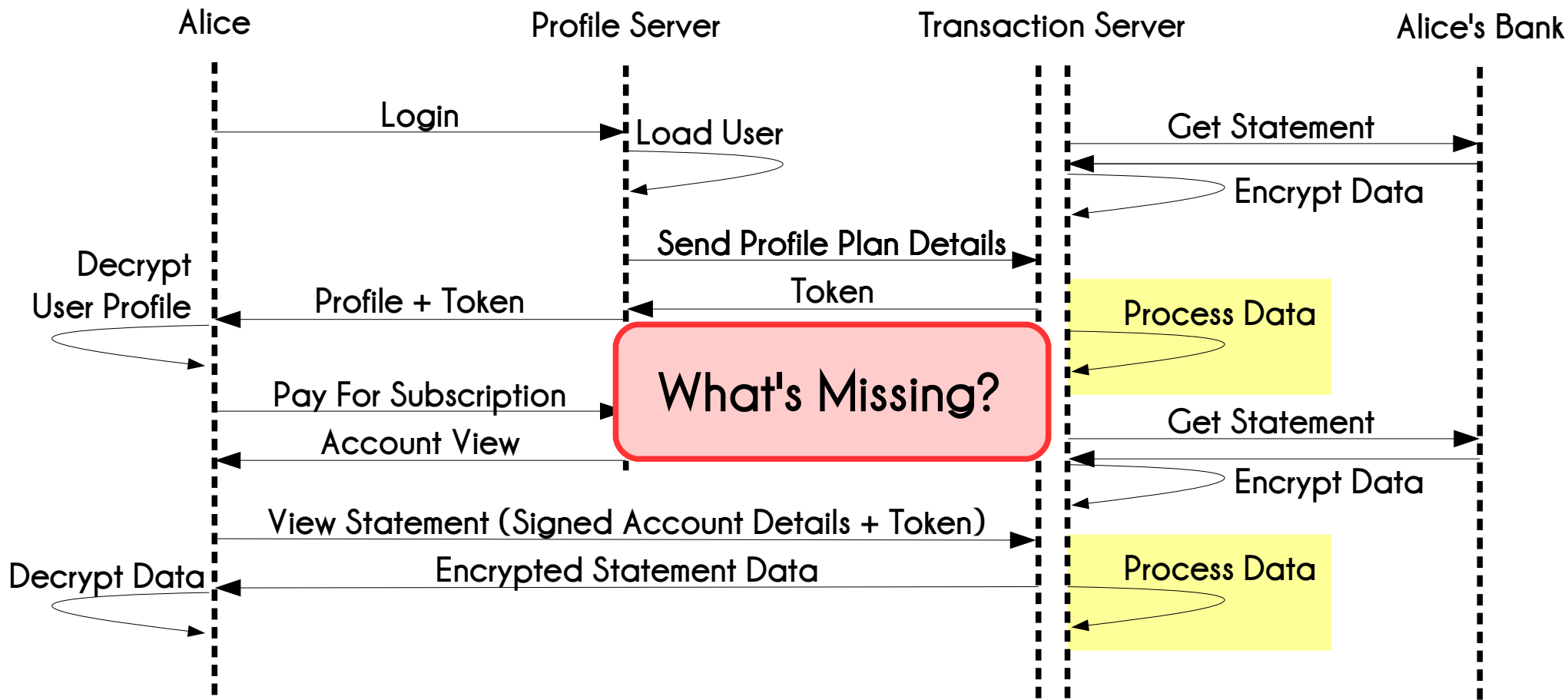
Account

```
# id: integer
# public_key: string
```

Software as a Service



Software as a Service



Processing Encrypted Data

Processing Encrypted Data



FIRST BANK OF WIKI

1425 JAMES ST, PO BOX 4000
VICTORIA BC V8X 3X4 1-800-555-5555

CHEQUING ACCOUNT STATEMENT

Page : 1 of 1

JOHN JONES
1643 DUNDAS ST W APT 27
TORONTO ON M6K 1V2

Statement period	Account No.
2003-10-09 to 2003-11-08	00005-123-456-7

Date	Description	Ref.	Withdrawals	Deposits	Balance
2003-10-08	Previous balance				0.55
2003-10-14	Payroll Deposit - HOTEL			694.81	695.36
2003-10-14	Web Bill Payment - MASTERCARD	9685	200.00		495.36
2003-10-16	ATM Withdrawal - INTERAC	3990	21.25		474.11
2003-10-16	Fees - Interac		1.50		472.61
2003-10-20	Interac Purchase - ELECTRONICS	1975	2.99		469.62
2003-10-21	Web Bill Payment - AMEX	3314	300.00		169.62
2003-10-22	ATM Withdrawal - FIRST BANK	0064	100.00		69.62
2003-10-23	Interac Purchase - SUPERMARKET	1559	29.08		40.54
2003-10-24	Interac Refund - ELECTRONICS	1975		2.99	43.53
2003-10-27	Telephone Bill Payment - VISA	2475	6.77		36.76
2003-10-28	Payroll Deposit - HOTEL			694.81	731.57
2003-10-30	Web Funds Transfer - From SAVINGS	2620		50.00	781.57
2003-11-03	Pre-Auth. Payment - INSURANCE		33.55		748.02
2003-11-03	Cheque No. - 409		100.00		648.02
2003-11-06	Mortgage Payment		710.49		-62.47
2003-11-07	Fees - Overdraft		5.00		-67.47
2003-11-08	Fees - Monthly		5.00		-72.47

Bills

Cash

Fees

Groceries

Hobbies

Transfer

Travel

???

Processing Encrypted Data

 **FIRST BANK OF WIKI**
1425 JAMES ST, PO BOX 4000
VICTORIA BC V8X 3X4 1-800-555-5555

CHEQUING ACCOUNT STATEMENT
Page : 1 of 1

		Statement period	Account No.
		2003-10-09 to 2003-11-08	

Date	Description	Ref.	Withdrawals	Deposits	Balance
2003-10-08					0.55
2003-10-14				694.81	695.36
2003-10-14		9685	200.00		495.36
2003-10-16		3990	21.25		474.11
2003-10-16			1.50		472.61
2003-10-20		1975	2.99		469.62
2003-10-21		3314	300.00		169.62
2003-10-22		0064	100.00		69.62
2003-10-23		1559	29.08		40.54
2003-10-24		1975		2.99	43.53
2003-10-27		2475	6.77		36.76
2003-10-28				694.81	731.57
2003-10-30		2620		50.00	781.57
2003-11-03			33.55		748.02
2003-11-03			100.00		648.02
2003-11-06			710.49		-62.47
2003-11-07			5.00		-67.47
2003-11-08			5.00		-72.47

Bills

Cash

Fees

Groceries

Hobbies

Transfer

Travel

???

Processing Encrypted Data



Bills

Cash

Fees

Groceries

Hobbies

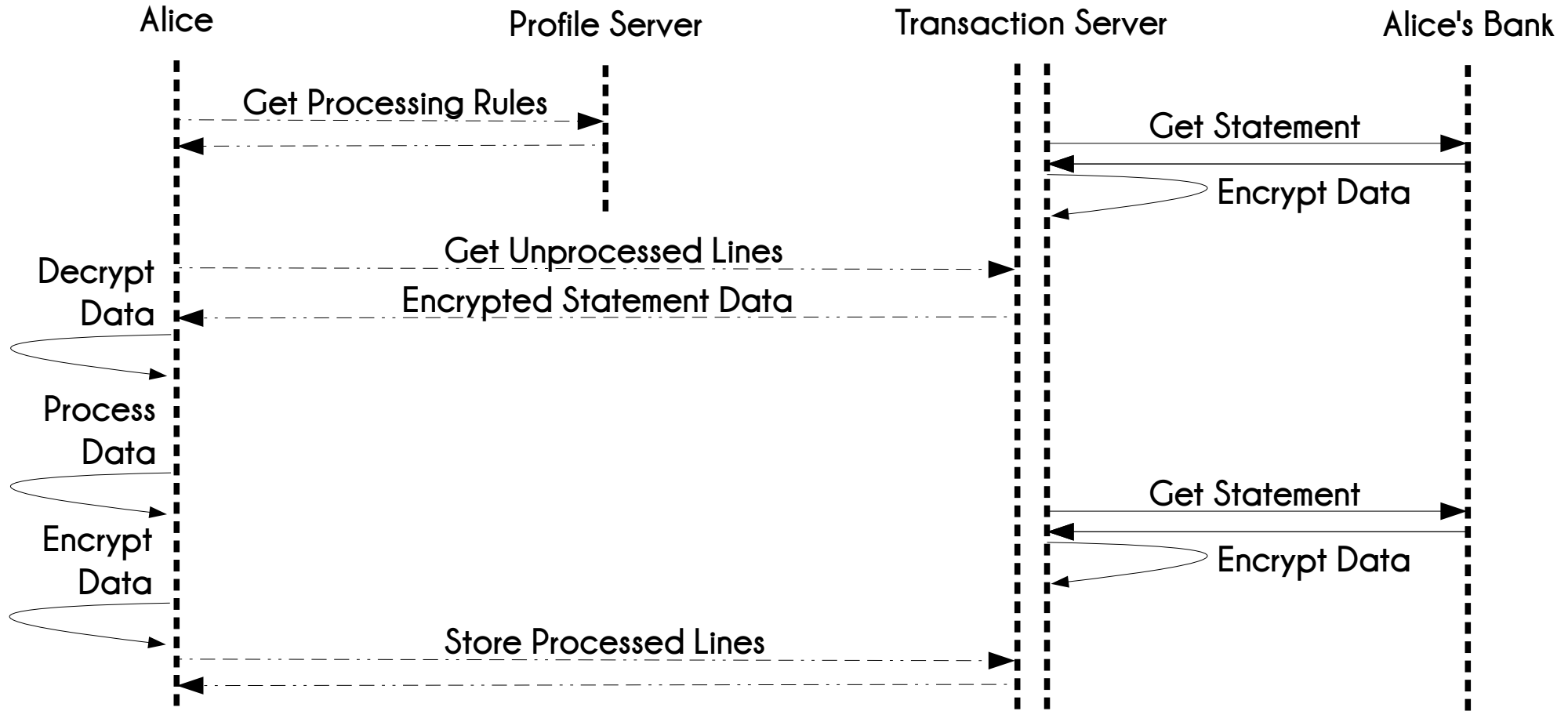
Transfer

Travel

???

Client Side Processing

Client Side Processing



Transactions

Id	description	category_Id
1	ba8763c245f4365g1==	543
2	afc760edc1983acc4==	264

Transaction Categories

Id	name
264	856a59c75e7895f8g==
543	d8e5f0ab51c97fa5d==

's Bank

Decryp
Dat

Proce
Dat

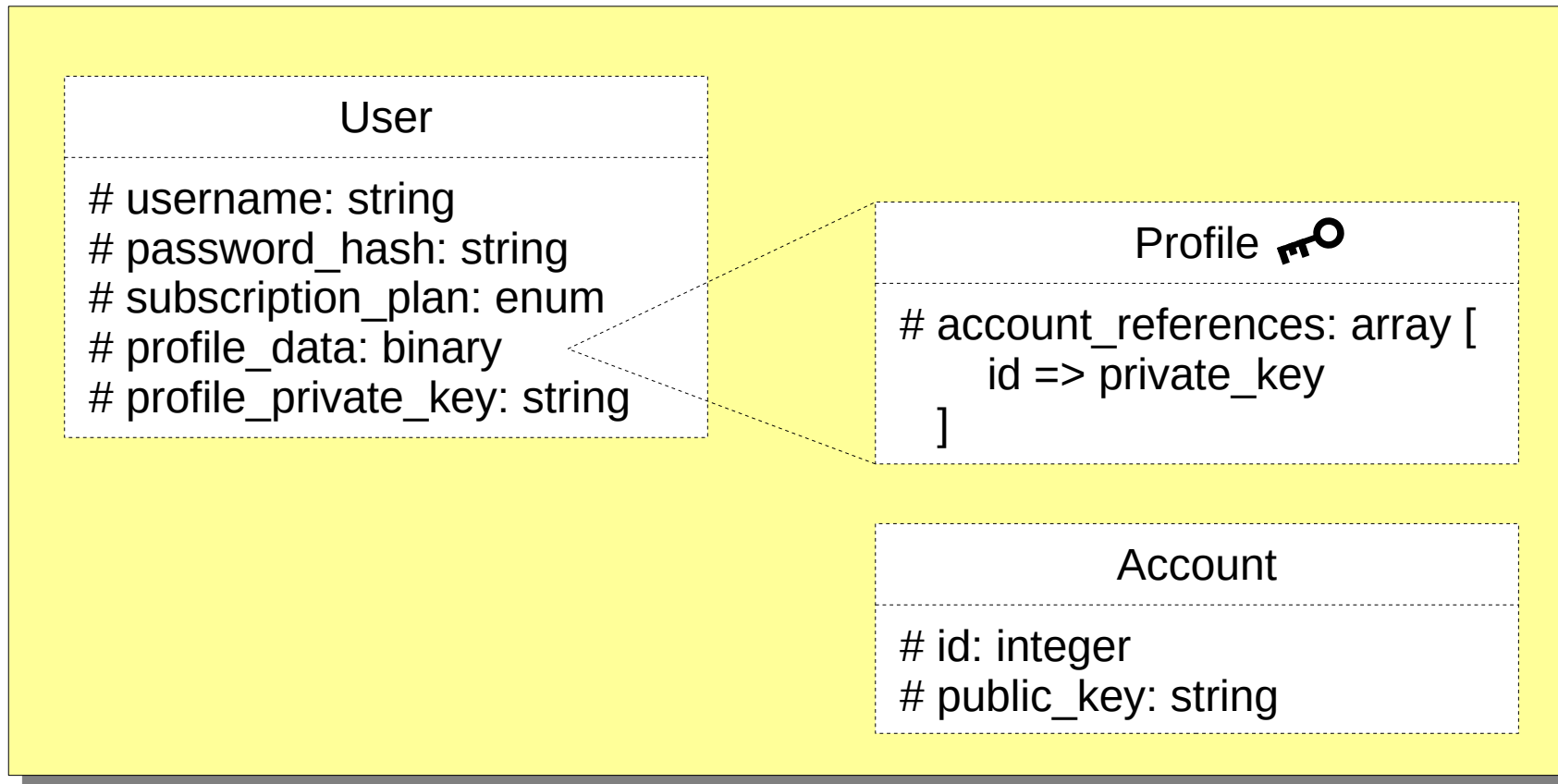
Encryp
Dat

store received data

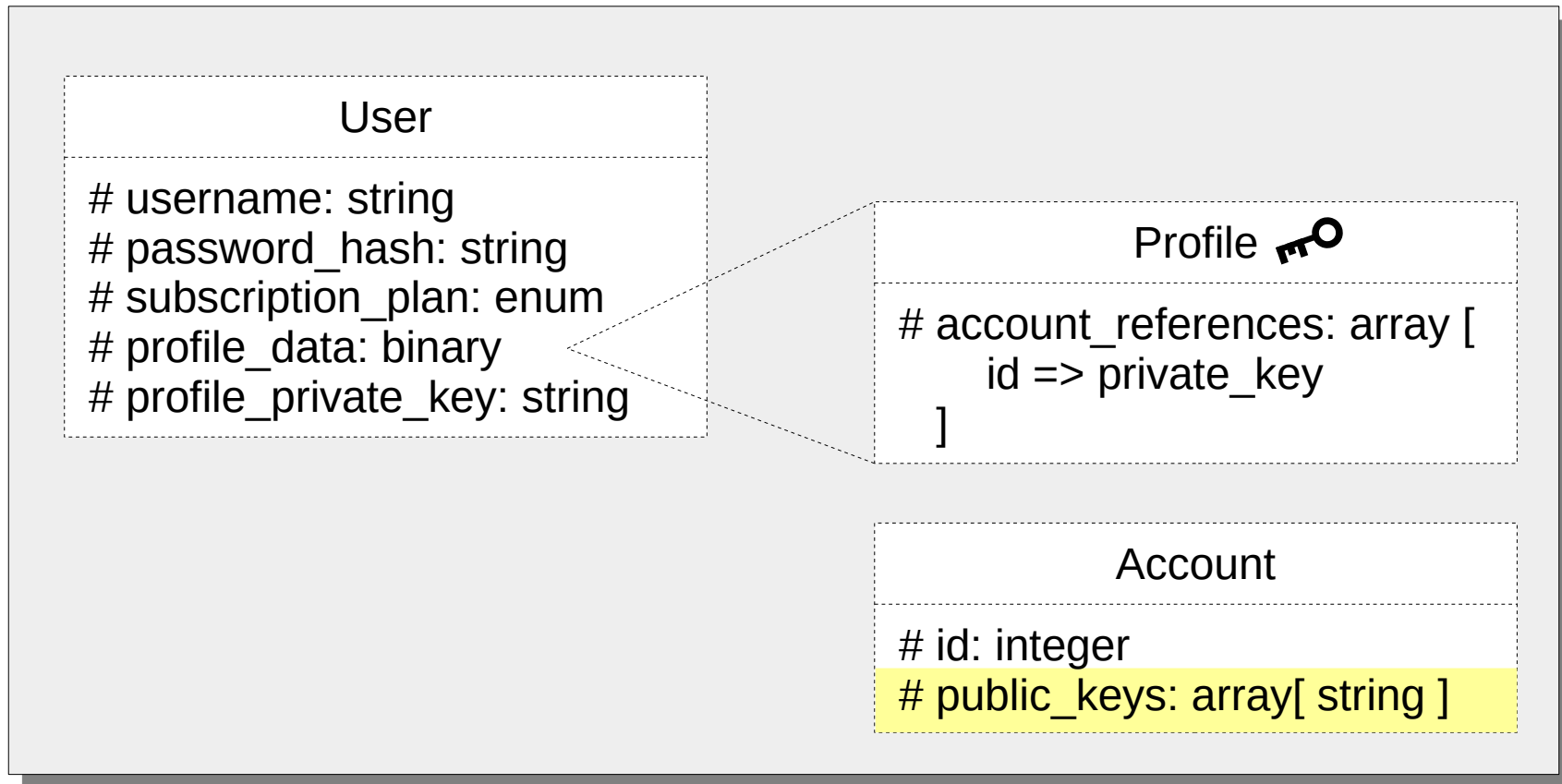
Demo

Sharing Data Anonymously Between Users

Sharing Data Anonymously Between Users

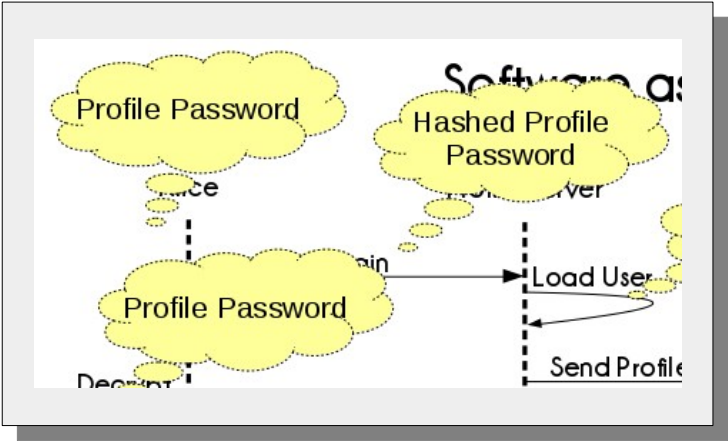


Sharing Data Anonymously Between Users

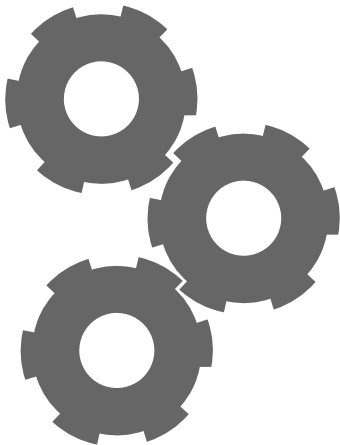


The Issues

The Issues



Private Keys on
Profile Server



Processing Done
Client Side

Transactions

Id	description	category_Id
1	ba8763c245f4365g1==	543
2	afc760edc1983acc4==	264

Transaction Categories

Id	name
264	856a59c75e7895f8g==
543	d8e5f0ab51c97fa5d==

Account

id: integer

public_keys: array[string]

Graphing

What Next?

What Next?

Build a stand-alone data processor platform

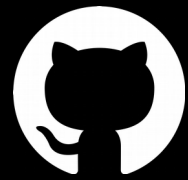
Define processing rules

Work towards a generic standard so that other projects can use the same data processor platform

Release as a RaspberryPi image and off-the-shelf appliance

...

P R O F I T ?



privacybastion/zeroknowledge-demo

Zero Knowledge

Competition!



Meeting the Growing
Demand for Security
and Privacy in a
National Security
World

@bendechrai

joinind.in/talk/60554

Competition!



Ben Dechrai

@bendechrai

I'm working on my #DPC17 talk, and just came up with a competition to give one of my #elehpants away!



3:28 PM - 14 Apr 2017



Zero Knowledge



Meeting the Growing
Demand for Security
and Privacy in a
National Security
World

@bendechrai

join.in/talk/60554

Competition!



Zero Knowledge



Meeting the Growing
Demand for Security
and Privacy in a
National Security
World

@bendeckrai

joind.in/talk/60554

Competition!



Signal Private Messenger



<https://ben.sc/signal>

+61 415 127 120



Zero Knowledge



Meeting the Growing
Demand for Security
and Privacy in a
National Security
World

@bendeckrai

joinind.in/talk/60554