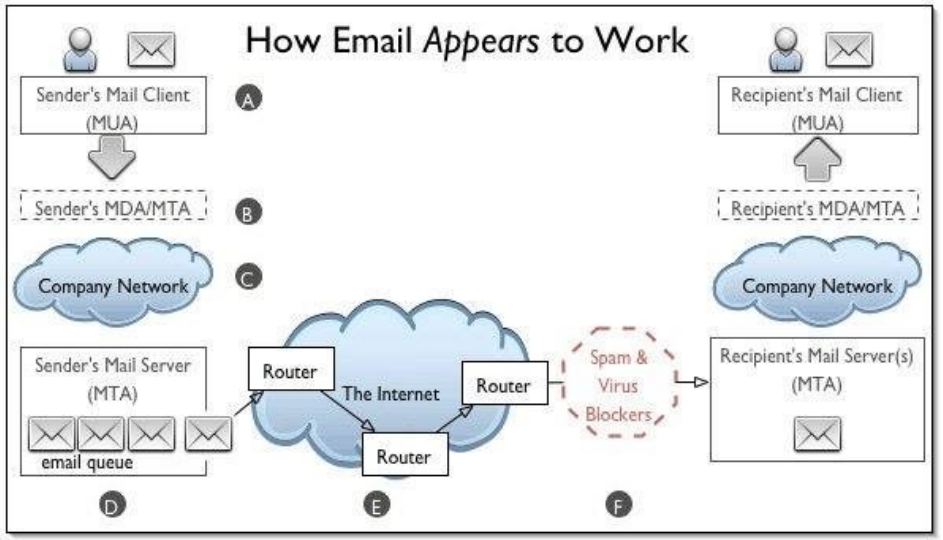
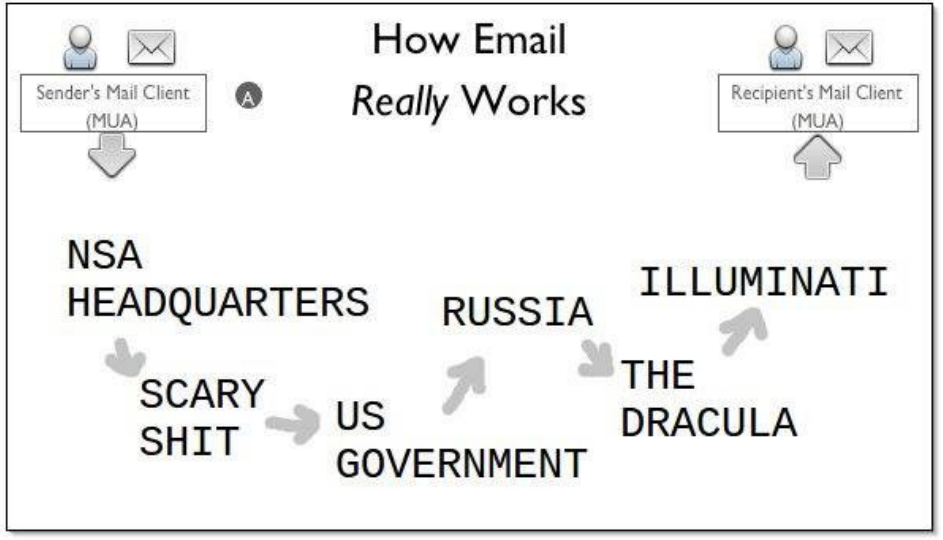




Zero Knowledge

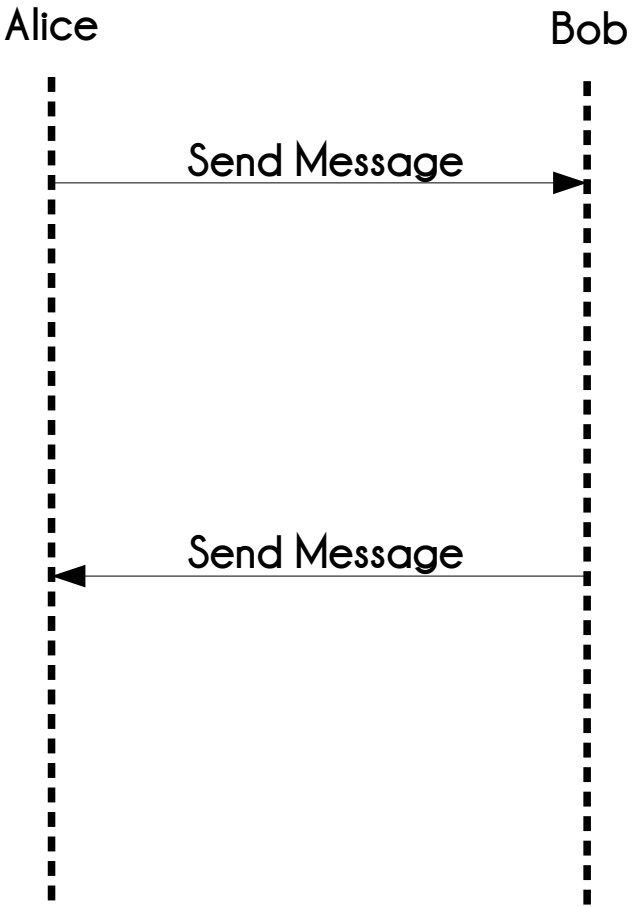
You Can't Leak What You Don't Know

Ben Dechrai
Developer Advocate
Auth0

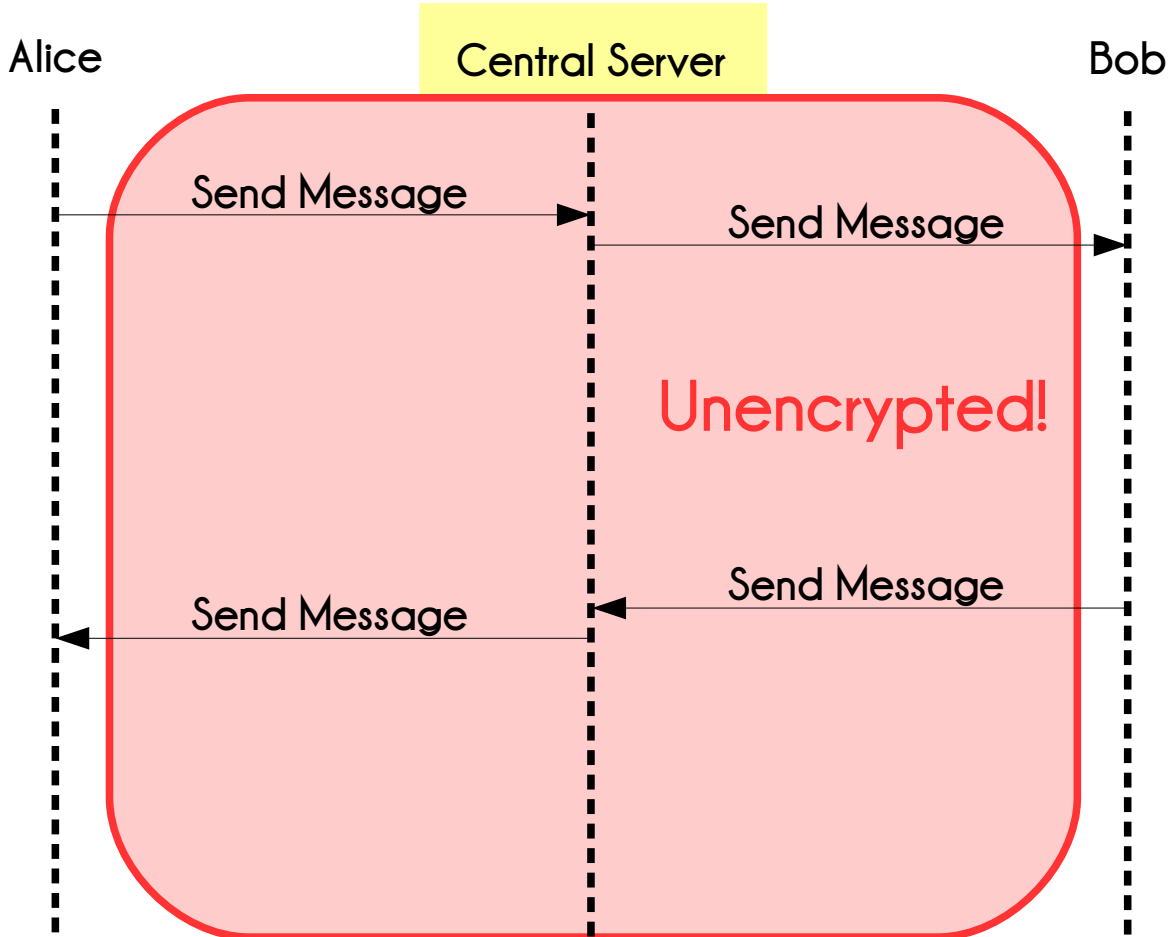
@bendechrai

Securing Communications

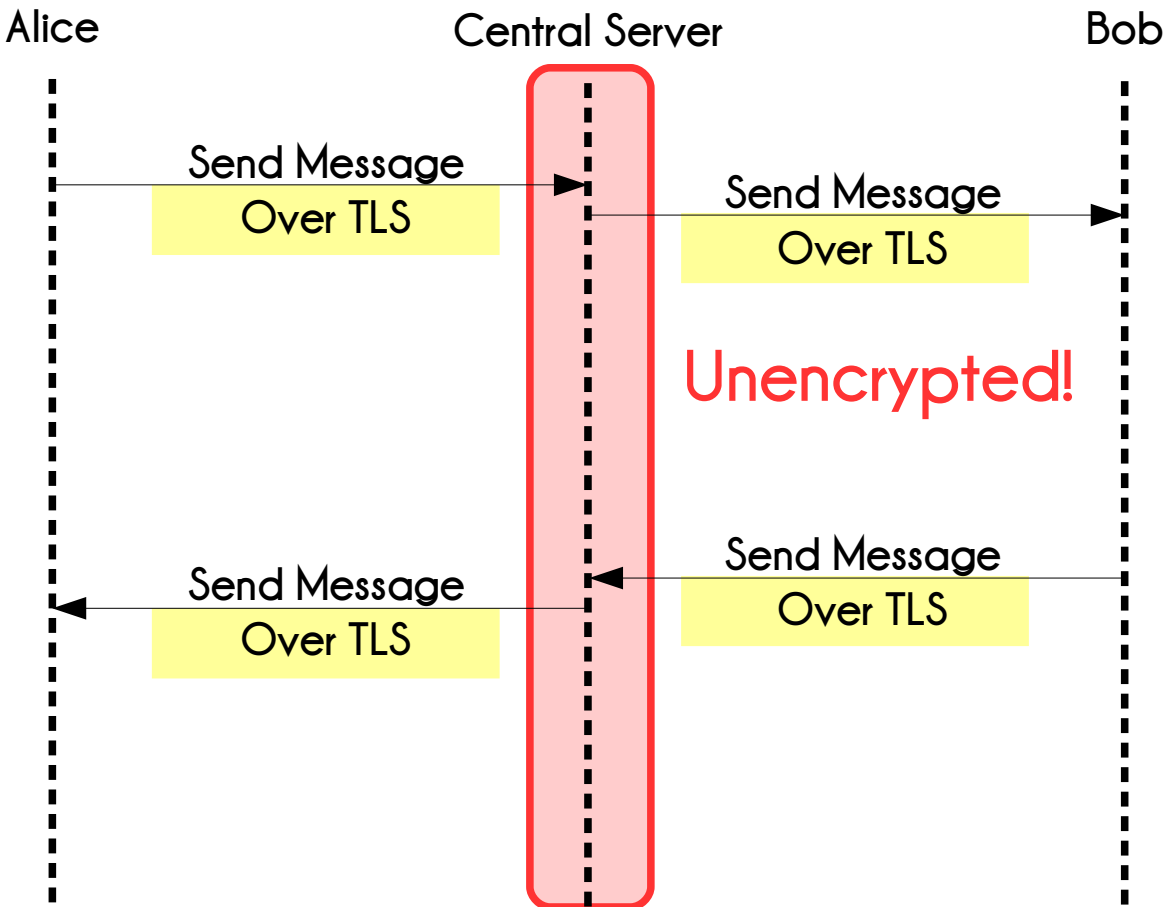
Securing Communications



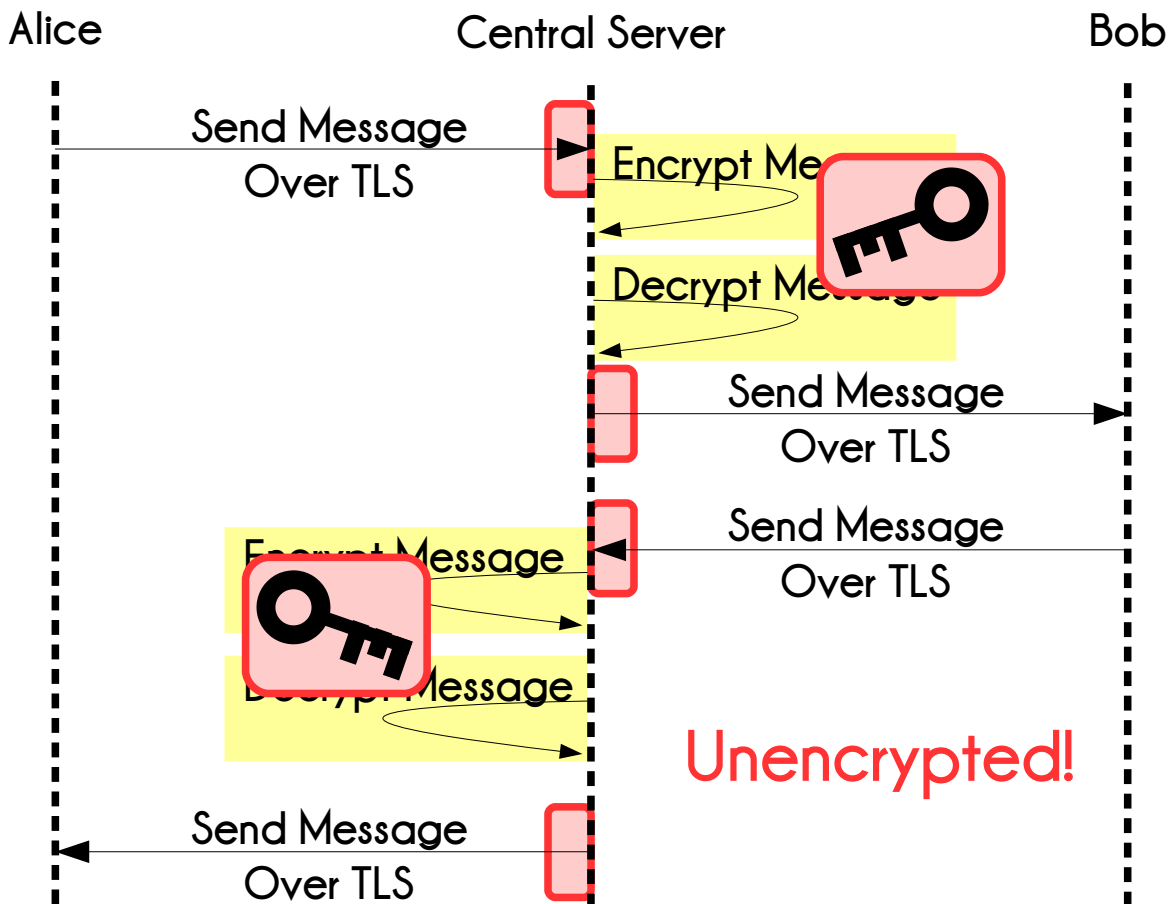
Securing Communications



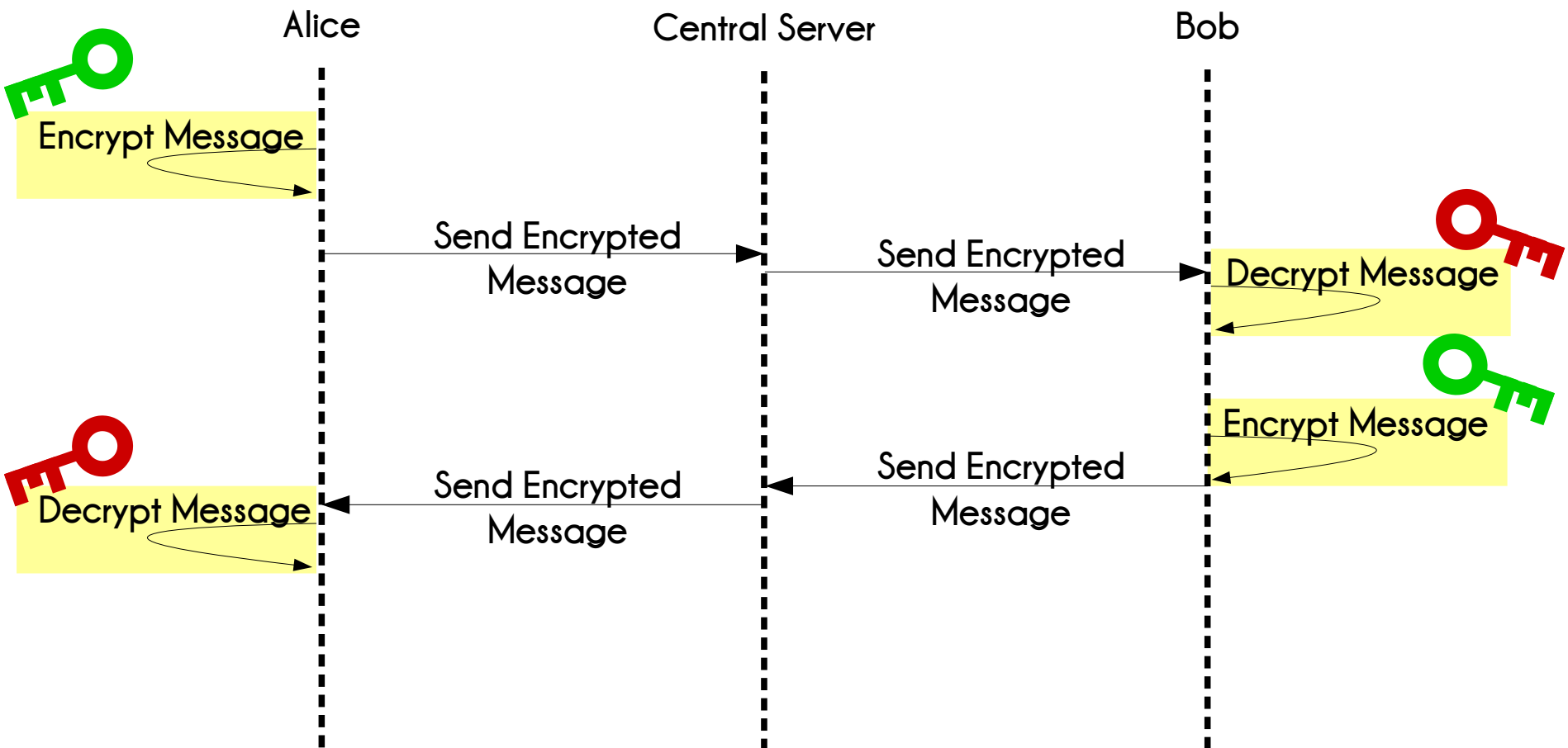
Securing Communications



Securing Communications

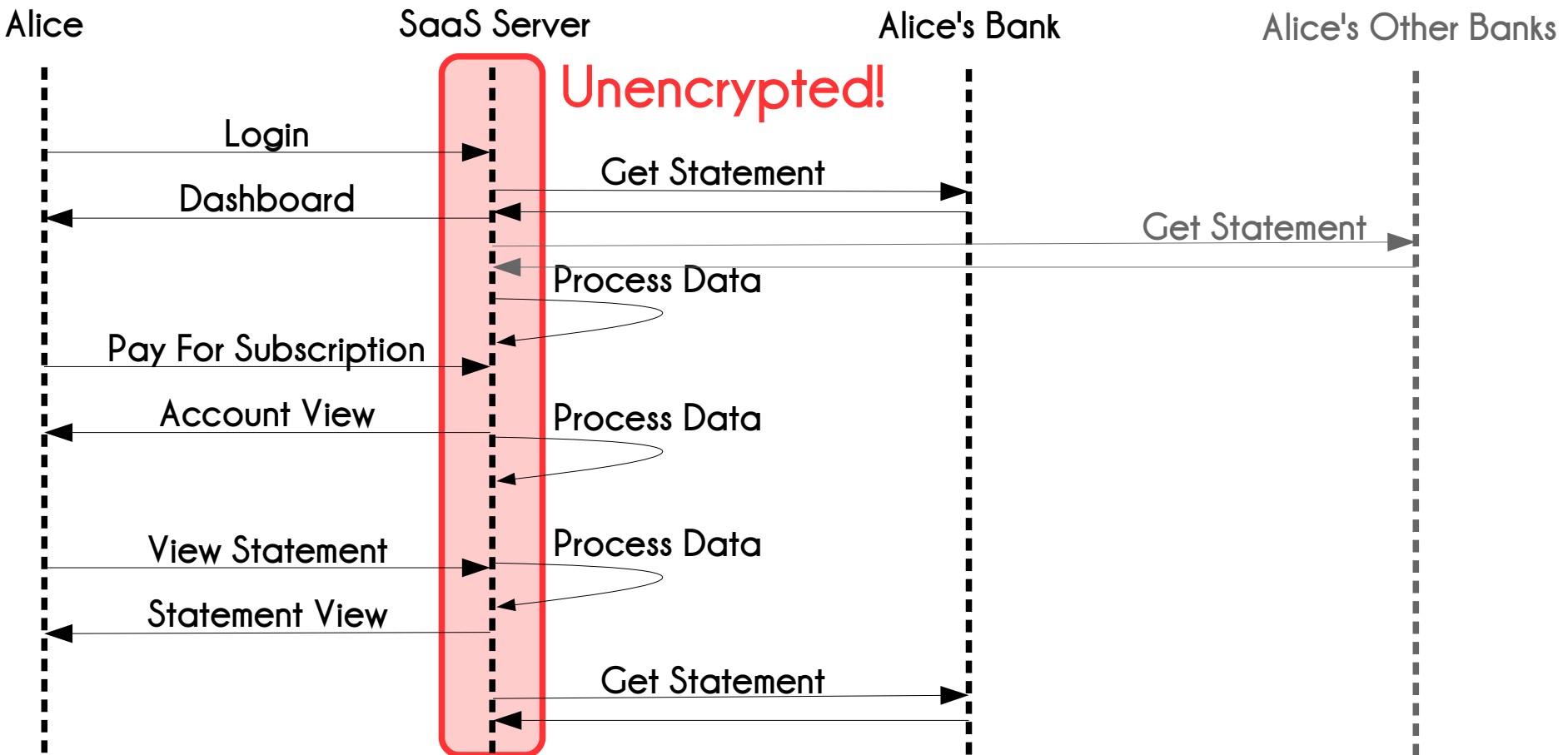


Securing Communications

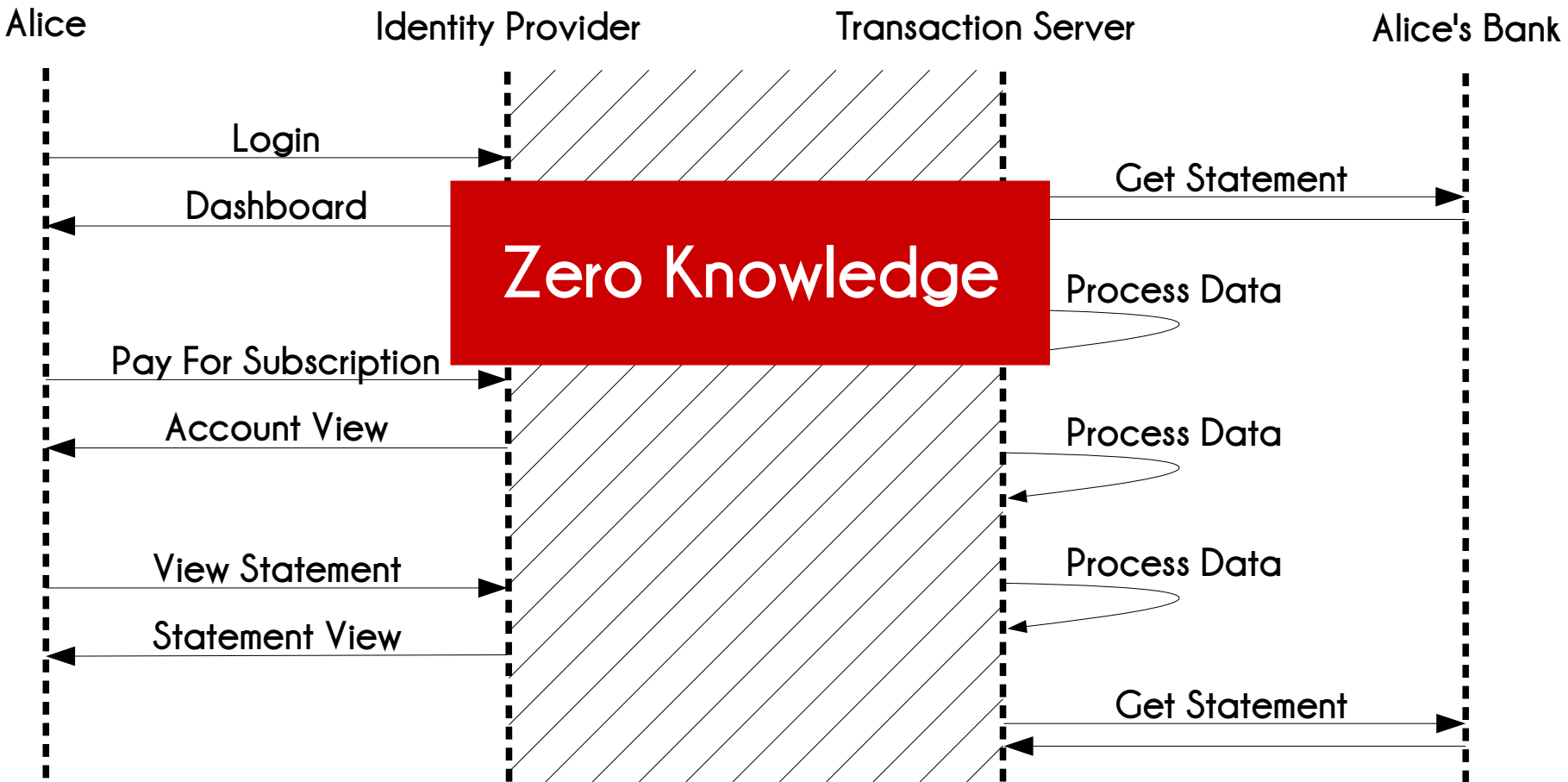


Software as a Service

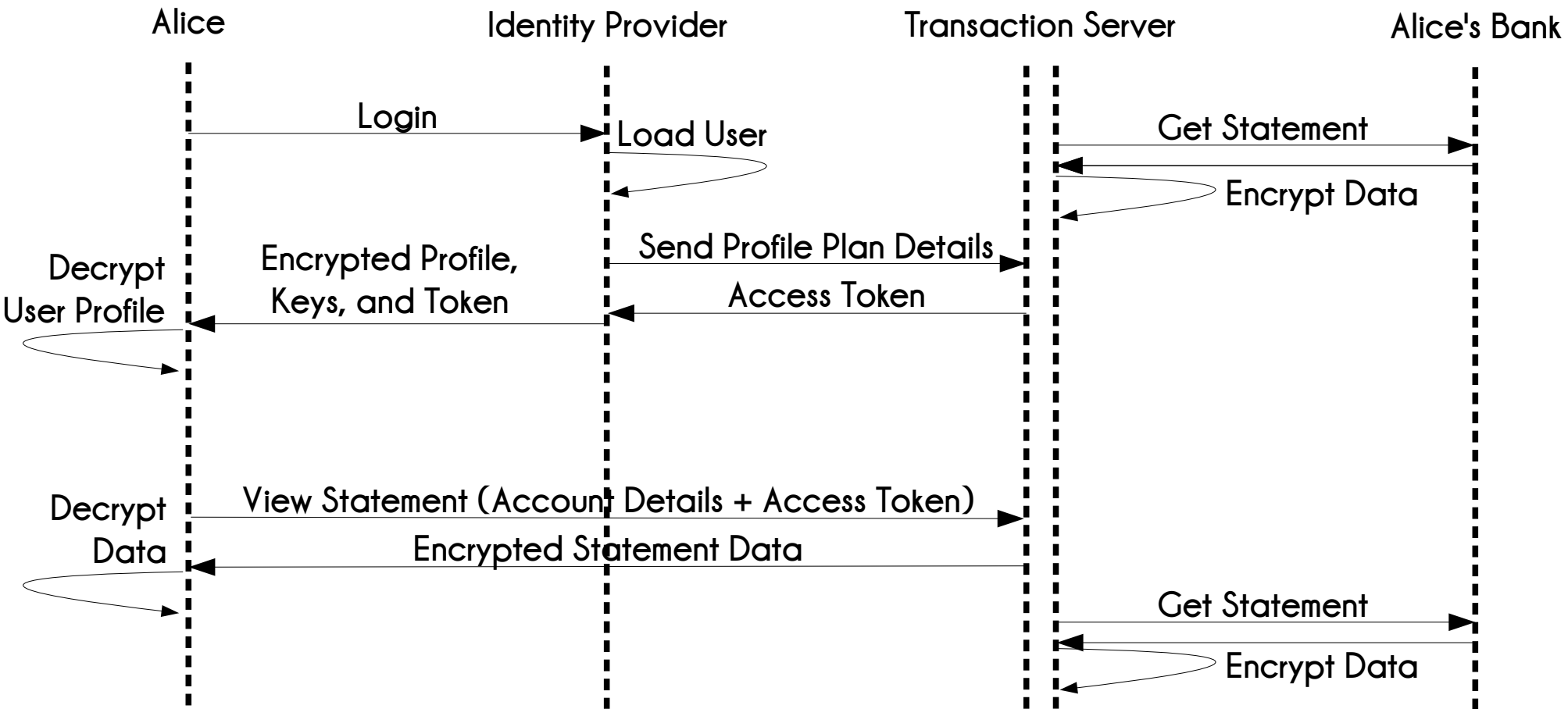
Software as a Service



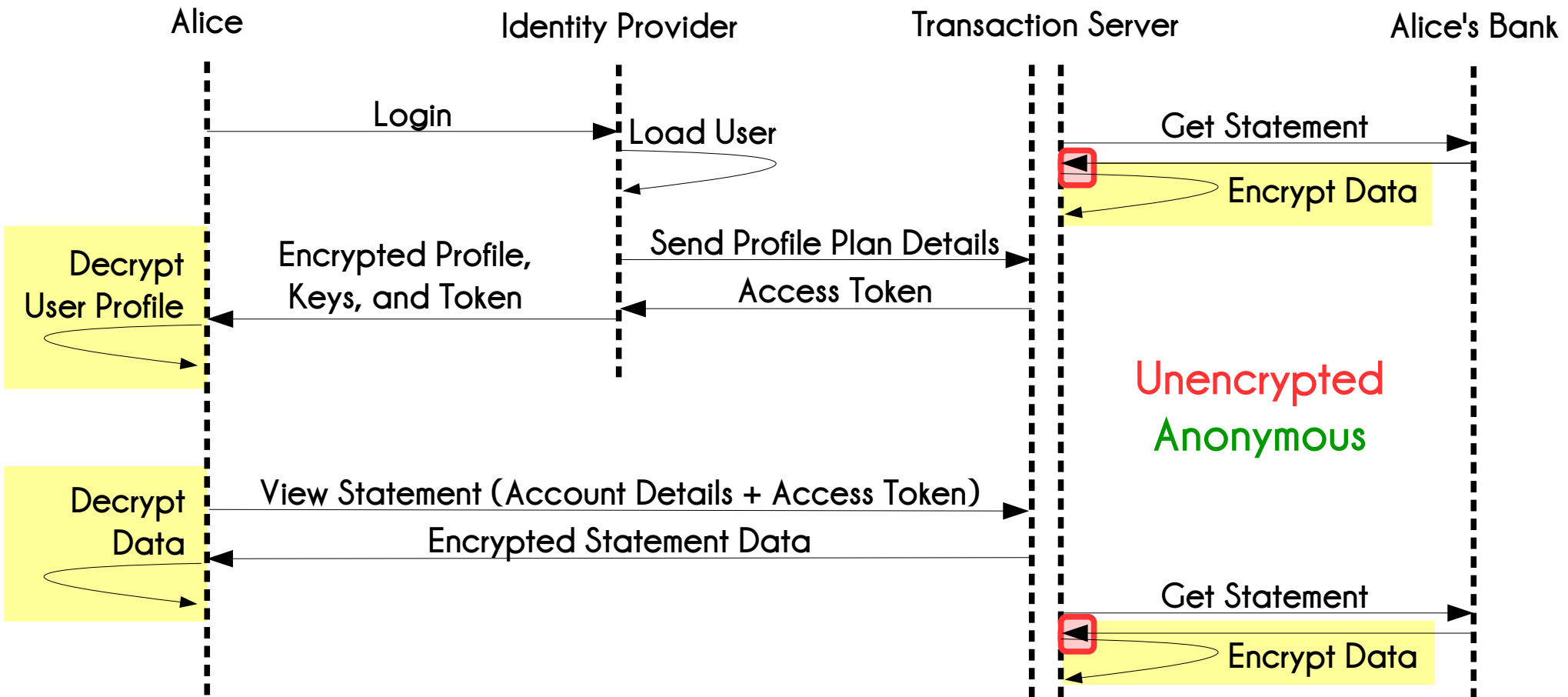
Software as a Service



Software as a Service

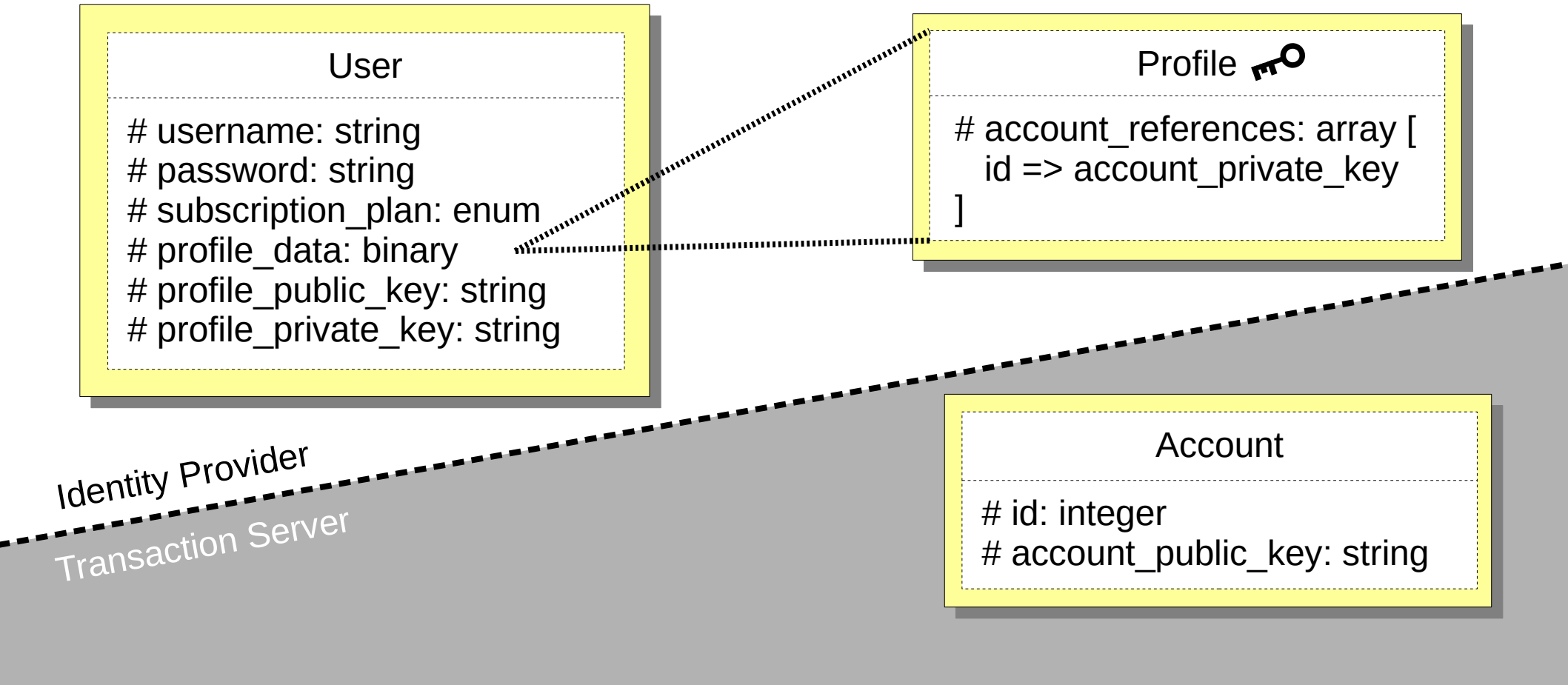


Software as a Service



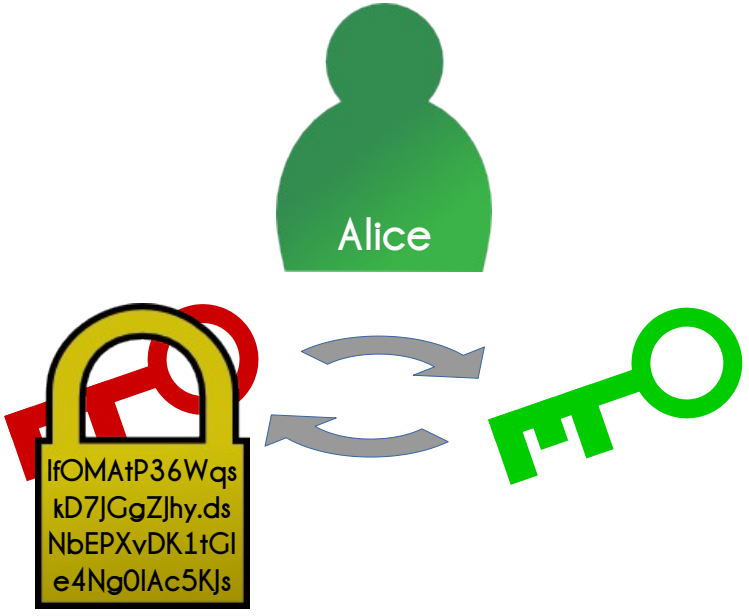
Profile Encryption

Profile Encryption

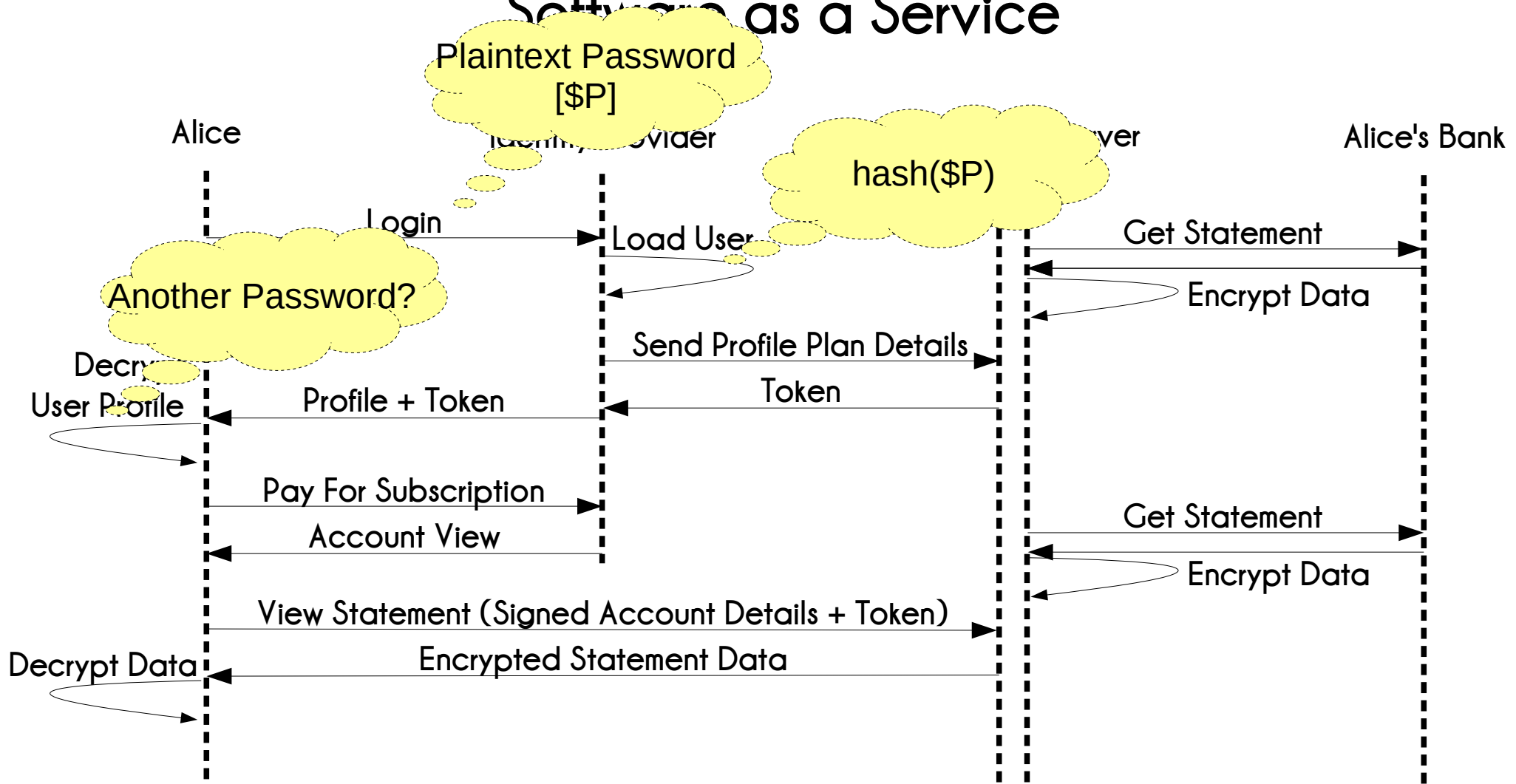


Public Private Keys

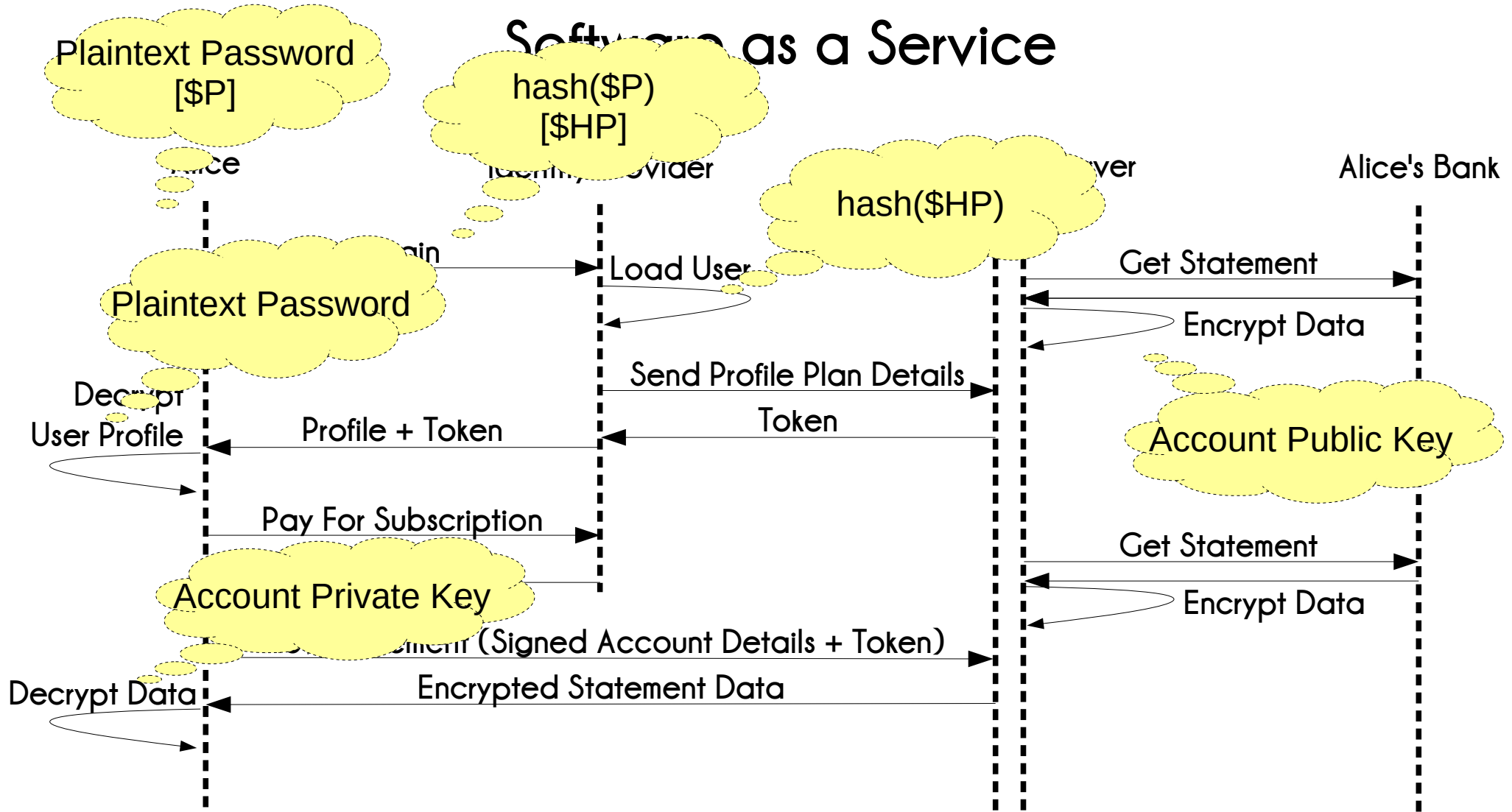
Public Private Keys



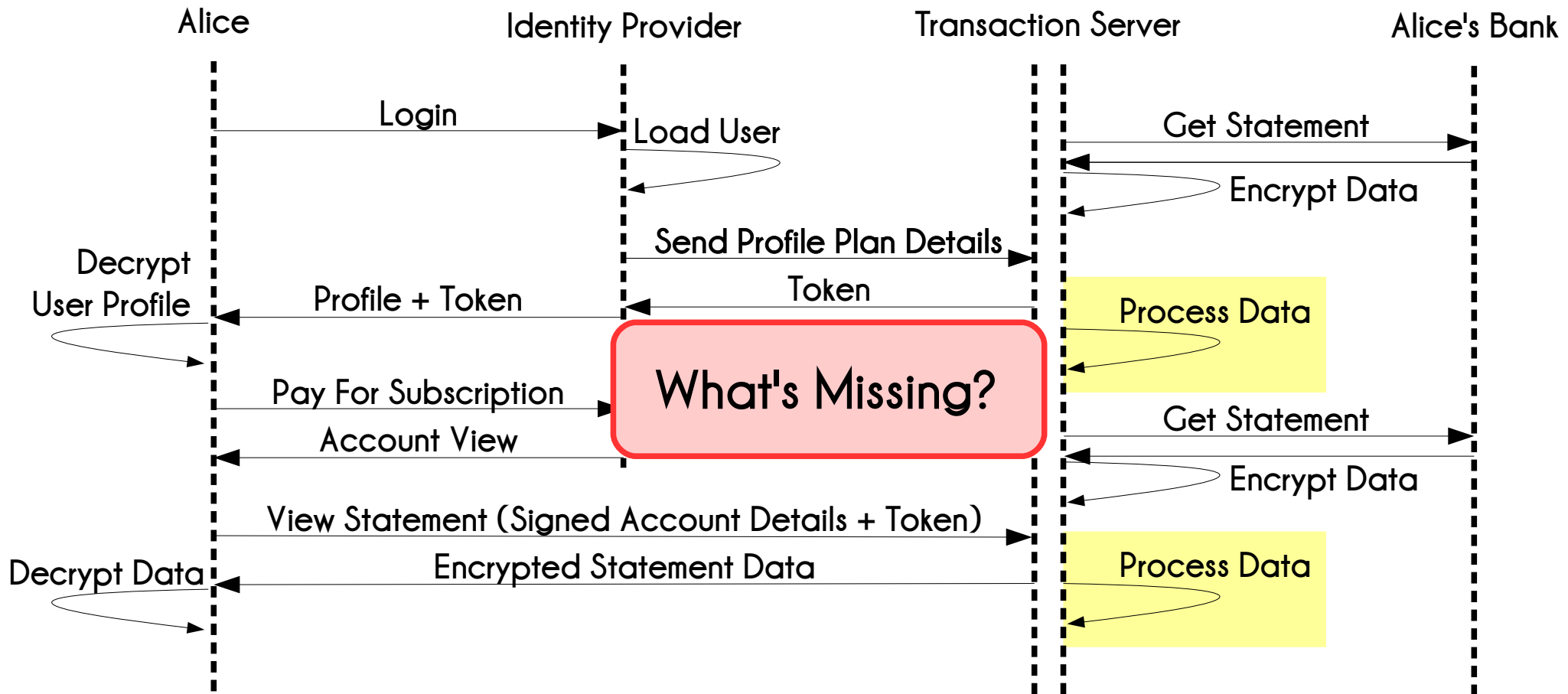
Software as a Service



Software as a Service



Software as a Service



Processing Encrypted Data

Processing Encrypted Data

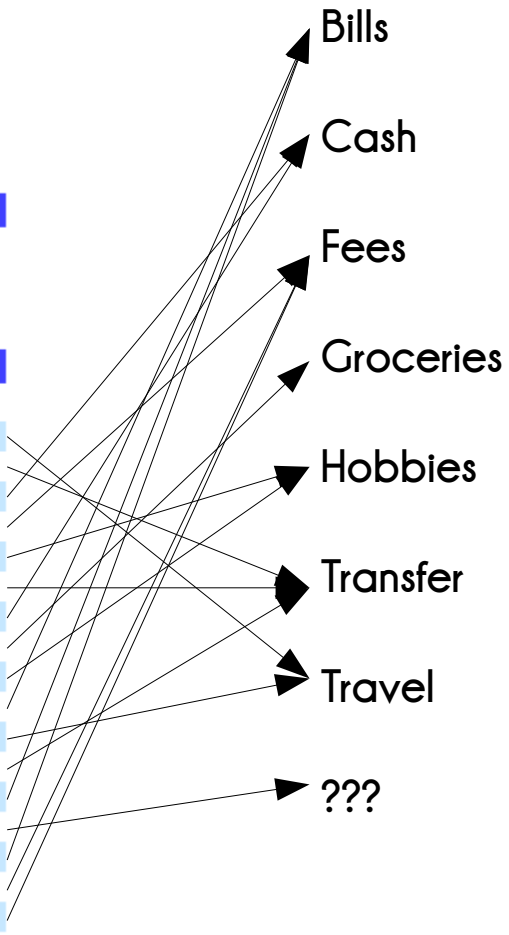
FIRST BANK OF WIKI
1425 JAMES ST, PO BOX 4000
VICTORIA BC V8X 3X4 1-800-555-5555

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



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	[redacted]

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

- Bills
- Cash
- Fees
- Groceries
- Hobbies
- Transfer
- Travel
- ???

Processing Encrypted Data

Bills

Cash

Fees

Groceries

Hobbies

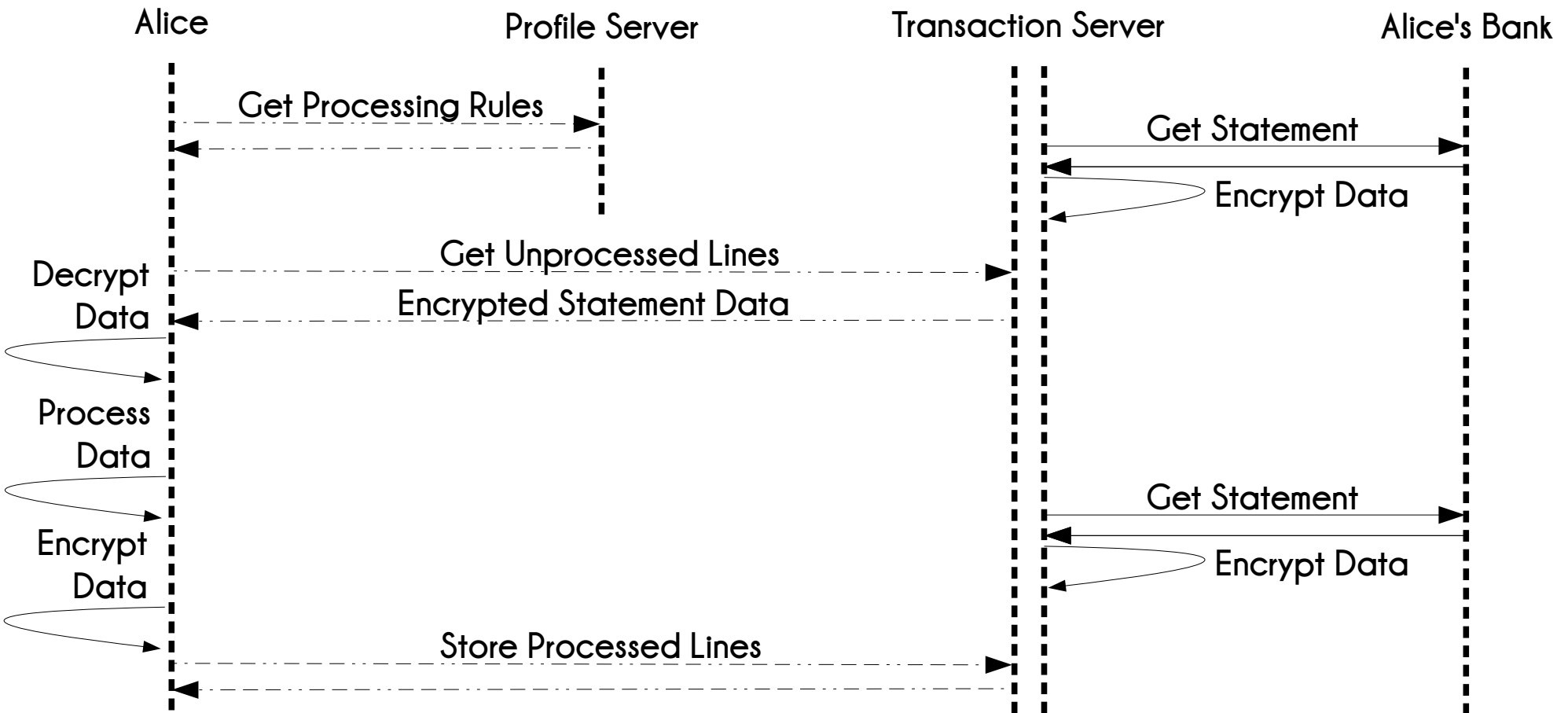
Transfer

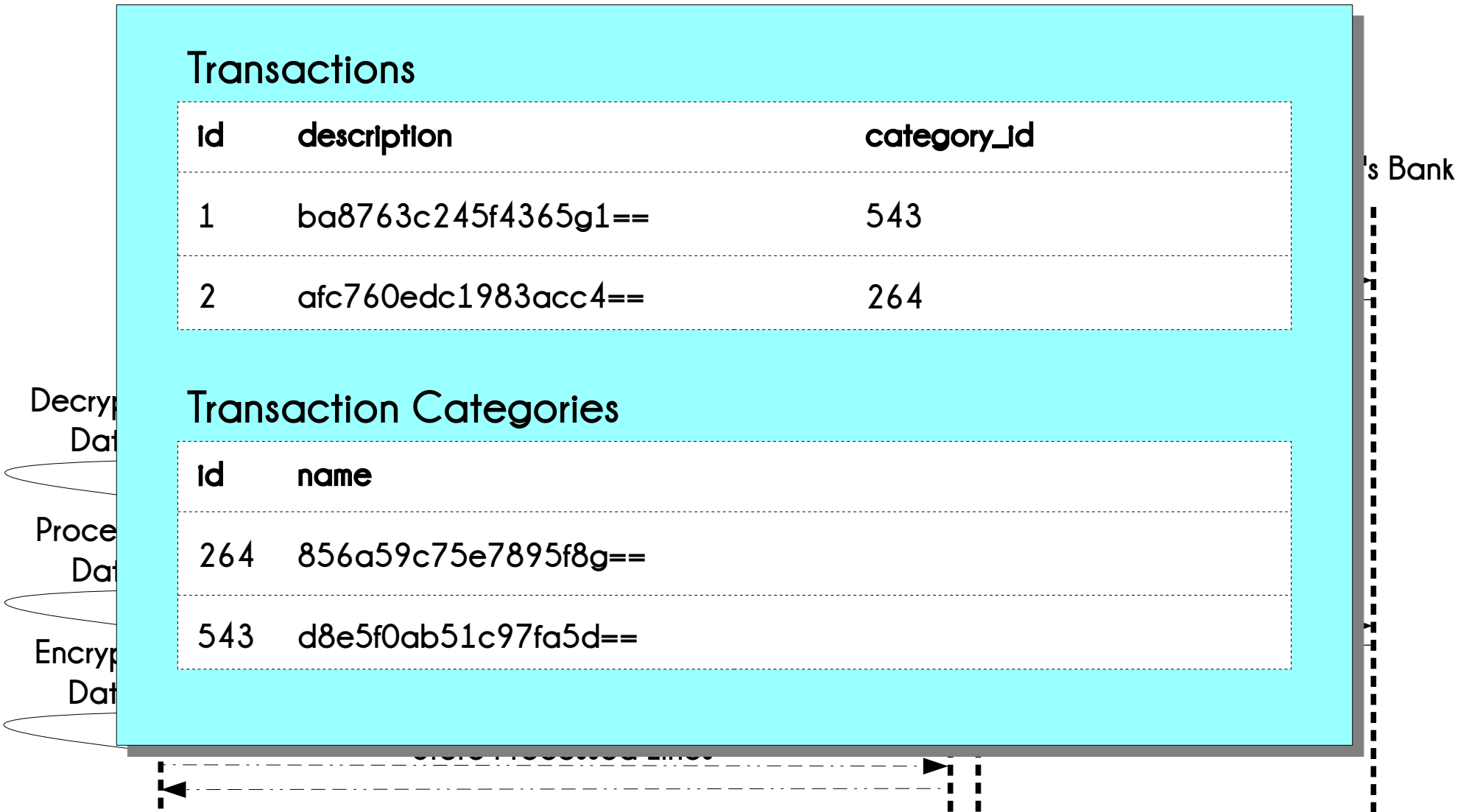
Travel

???

Client Side Processing

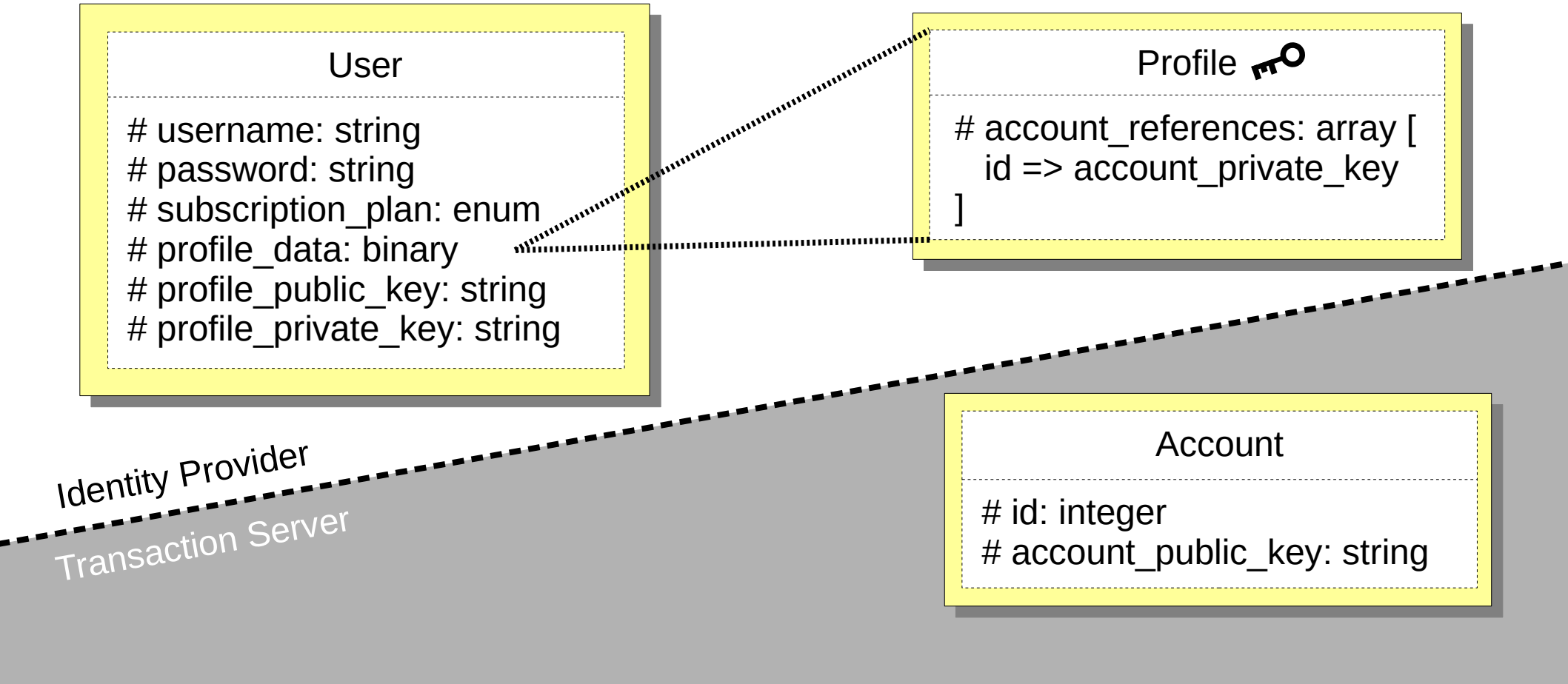
Client Side Processing



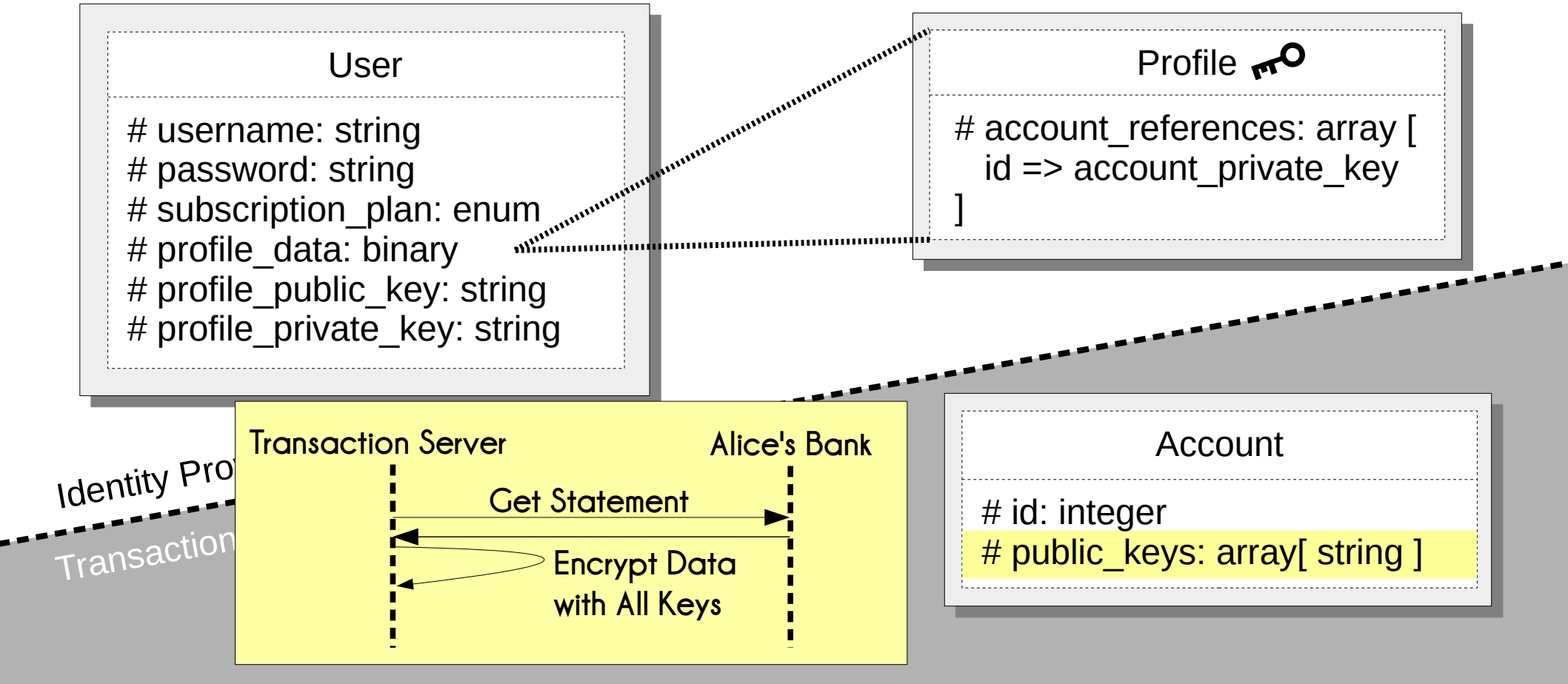

Transactions
id
description
category_id
1
ba8763c245f4365g1==
543
2
afc760edc1983acc4==
264
Transaction Categories
id
name
264
856a59c75e7895f8g==
543
d8e5f0ab51c97fa5d==
's Bank
Decryp
Dat
Proce
Dat
Encryp
Dat

Sharing Data Anonymously Between Users

Sharing Data Anonymously Between Users



Sharing Data Anonymously Between Users

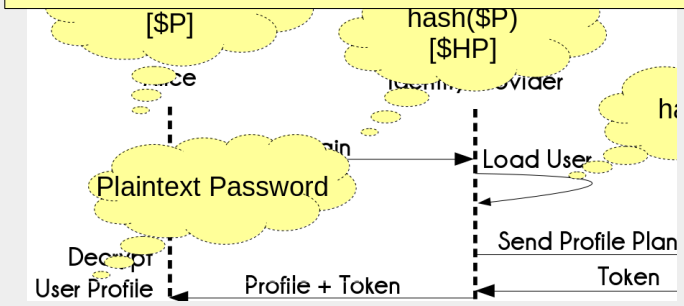


The Issues

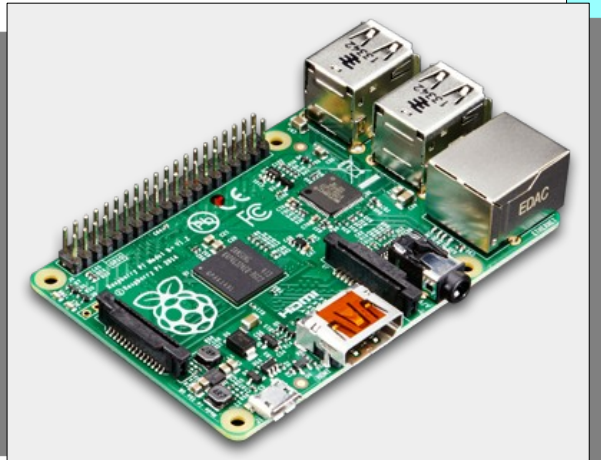
The Issues

$2y$10$pXB4mVRxGk1E
64oaojzMWO1grT0ClDFV
hFvJAr0mVFzH3S3sOWFwu

60 chars - starts with $2y$ - ...



Private Keys on Profile Server



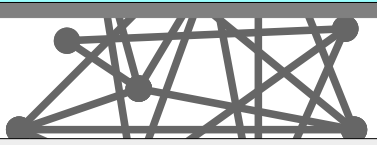
Processing Done Client Side

Transactions

id	description	category_id
1	ba8763c245f4365g1==	543
2	afc760edc1983acc4==	264

Transaction Categories

id	name
264	856a59c75e7895f8g==
543	d8e5f0ab51c97fa5d==



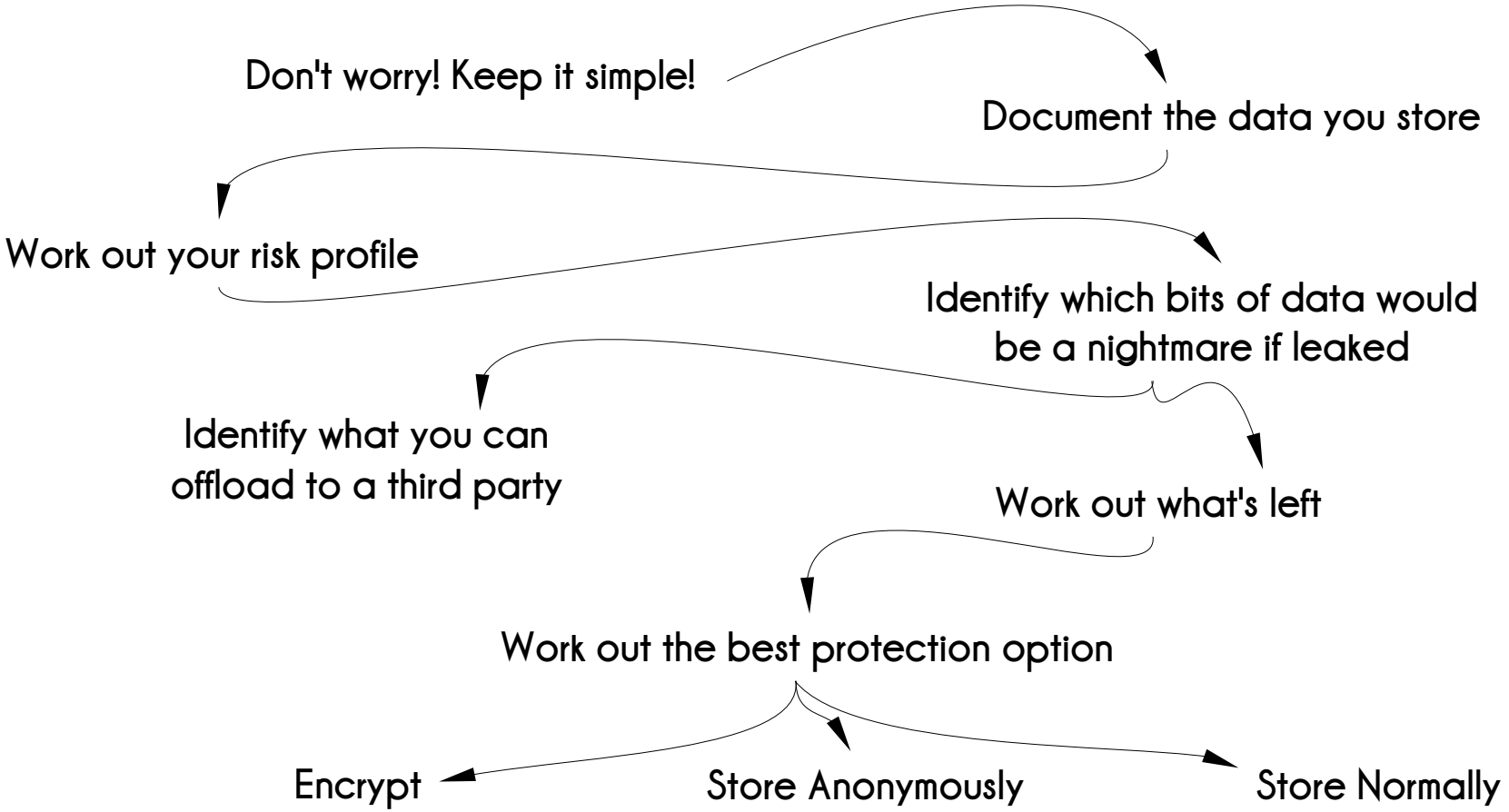
Account

id: integer
public_keys: array[string]

Graphing

Where to Start?

Where to Start?



It's better to protect a bit of your data **today**

than all your data tomorrow

for tomorrow never comes...

Thanks!
Questions?

Zero Knowledge

You Can't Leak What You Don't Know

Ben Dechrai
Developer Evangelist
Auth0

@bendechrai