Distributed Systems:

- Security -

Anca Jurcut
E-mail: anca.jurcut@ucd.ie

School of Computer Science and Informatics
University College Dublin
Ireland

From the Previous Lecture…

- Essential to protect communication channels and interfaces of systems with shared resources - hold information that might be subject to attack
  - E.g. e-mail, financial transactions

- Security protocols, policies and mechanisms are designed to protect such resources

- Two kinds of Security mechanisms:
  - Shared key/Secret key cryptography
  - Public key cryptography

From the Previous Lecture…

- Secret key cryptography - symmetric - same key used for encryption and decryption
  - A and B share same key - can exchange encrypted information without risk
  - problem: how to exchange keys?
- Public key cryptography - asymmetric - different keys used for encryption and decryption - knowledge of one does not reveal the other
  - one key made public, anyone can send messages to the holder of corresponding private key - holder of private key can sign messages and certificates

From the Previous Lecture…

- RSA most widely used asymmetric encryption algorithm
  - should be used with 768-bit keys or greater
- secret key encryption (symmetric) algorithms **out-perform** public key encryption (asymmetric) algorithms by several orders of magnitude
  - asymmetric algorithms only used in hybrid protocols to establish a secure channels that use shared keys for subsequent exchanges
- *Kerberos* is a well designed scheme for authenticating users and the protection of services within an organisation
  - we will now take a closer look at Kerberos...

Distributed Systems: Case Study: Kerberos

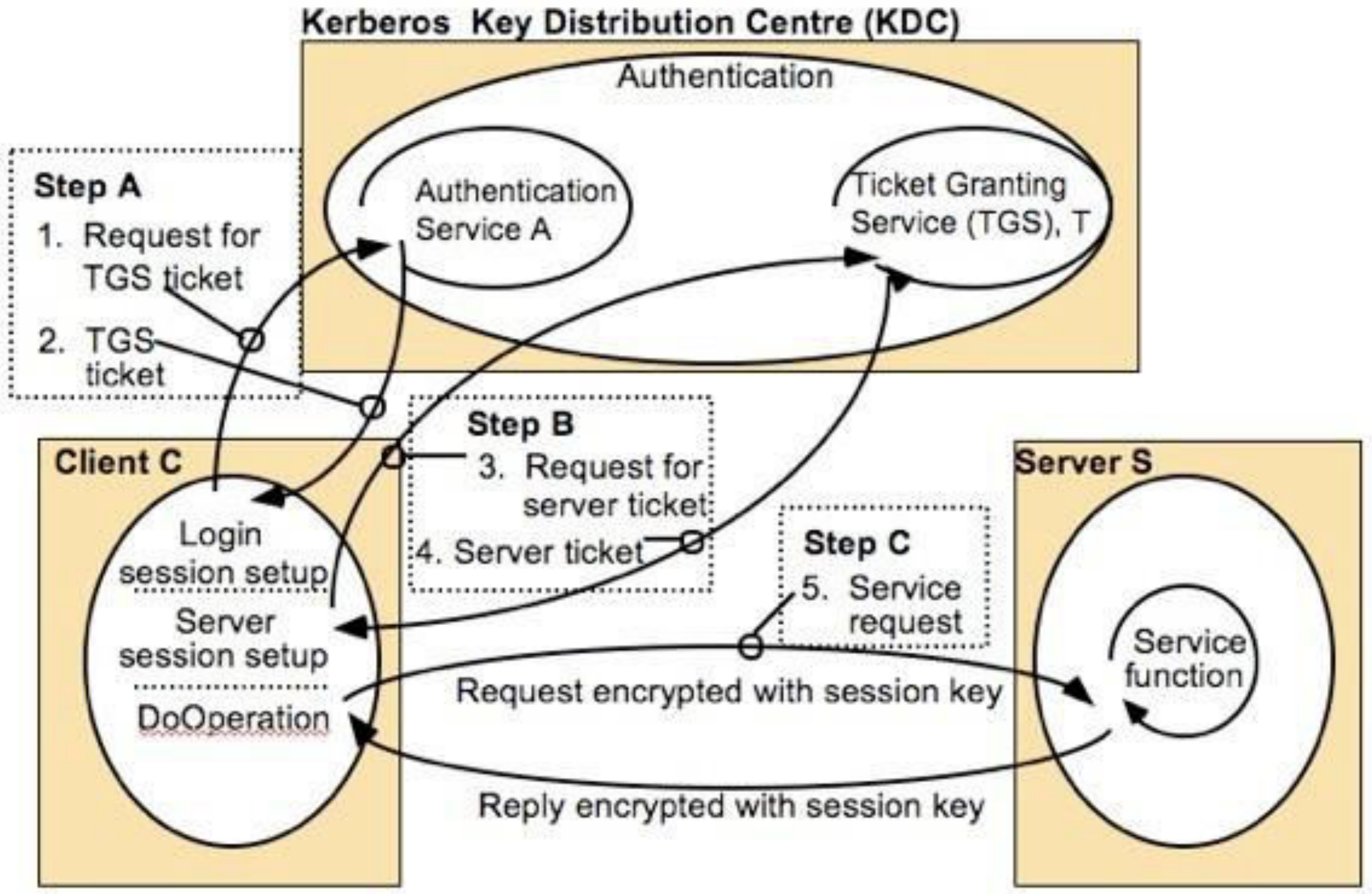
Introduction

- Kerberos is a computer network authentication protocol
  - allows nodes to communicate over non-secure network to prove their identity to one another in a secure manner
- Developed by MIT in the 1980’s and soon to become an Internet Standard.
  - The default authentication service for Windows 2000.
- Shared secret-based strong 3rd party authentication
- provides single sign-on capability
- Passwords never sent across network

Adopts Mediated Authentication

- A trusted third party mediates the authentication process -
  - called the **Key Distribution Centre (KDC)**
- Each user and service shares a secret key with the KDC
- KDC generates a session key - securely distributes it to the communicating parties
- communicating parties prove to each other that they know each other

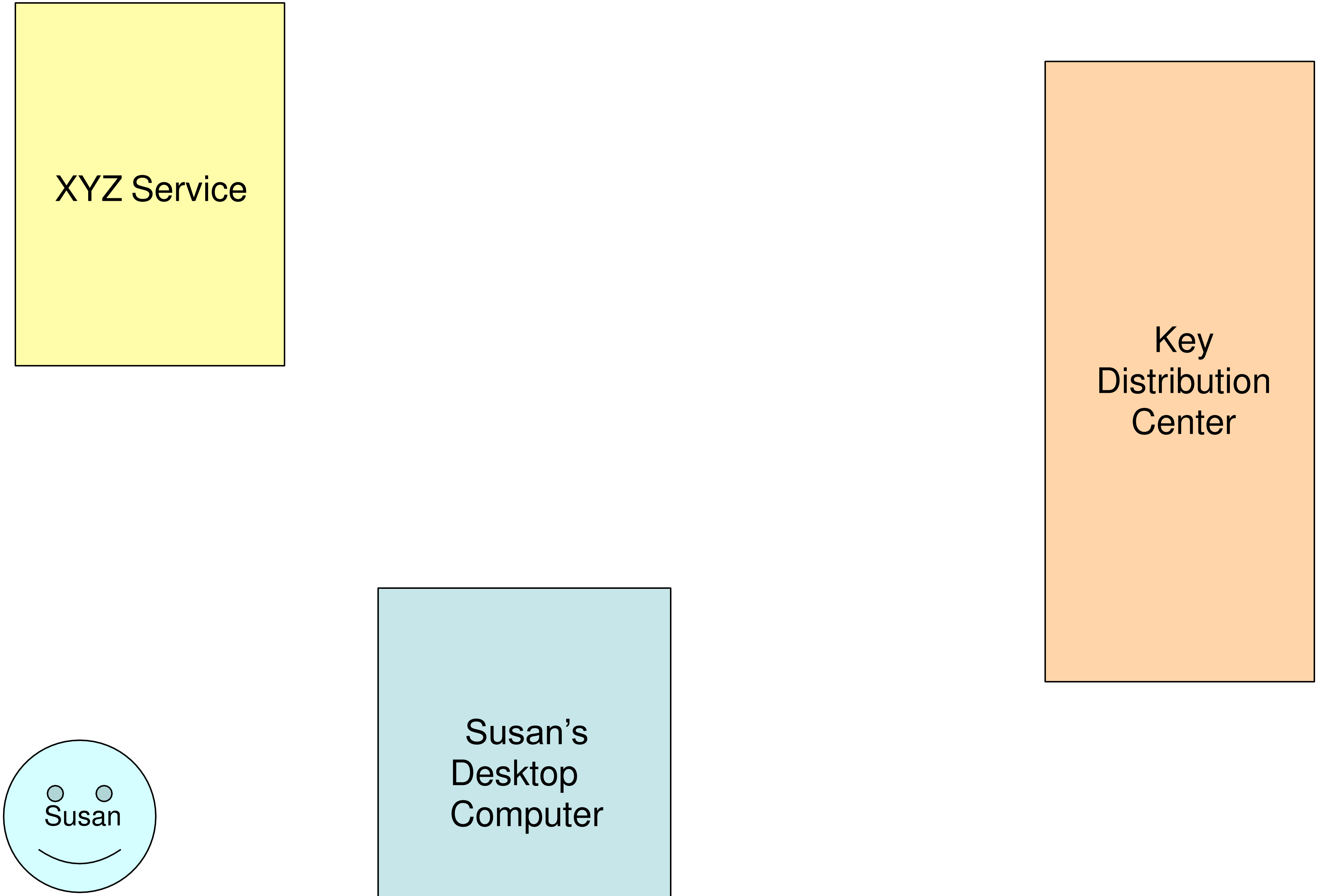
Kerberos System Architecture


Kerberos Key Distribution Centre (KDC)
Authentication
Authentication Service A
Ticket Granting Service (TGS), T
Step A
1. Request for TGS ticket
2. TGS ticket
Client C
Login session setup
Server session setup
DoOperation
Step B
3. Request for server ticket
4. Server ticket
Step C
5. Service request
Server S
Service function
Request encrypted with session key
Reply encrypted with session key

Kerberos

- Employs three types of security objects:
  - **Ticket:** a token issued to a client for presentation to a particular server. Includes the client id, server id, start time, expiry time, and session key.
  - **Authentication:** a token created by a client to prove the user's identity.
  - **Session Key:** a secret key, randomly generated by Kerberos, and issued to a client for use when communicating with a particular server.

- Lets look at an example...

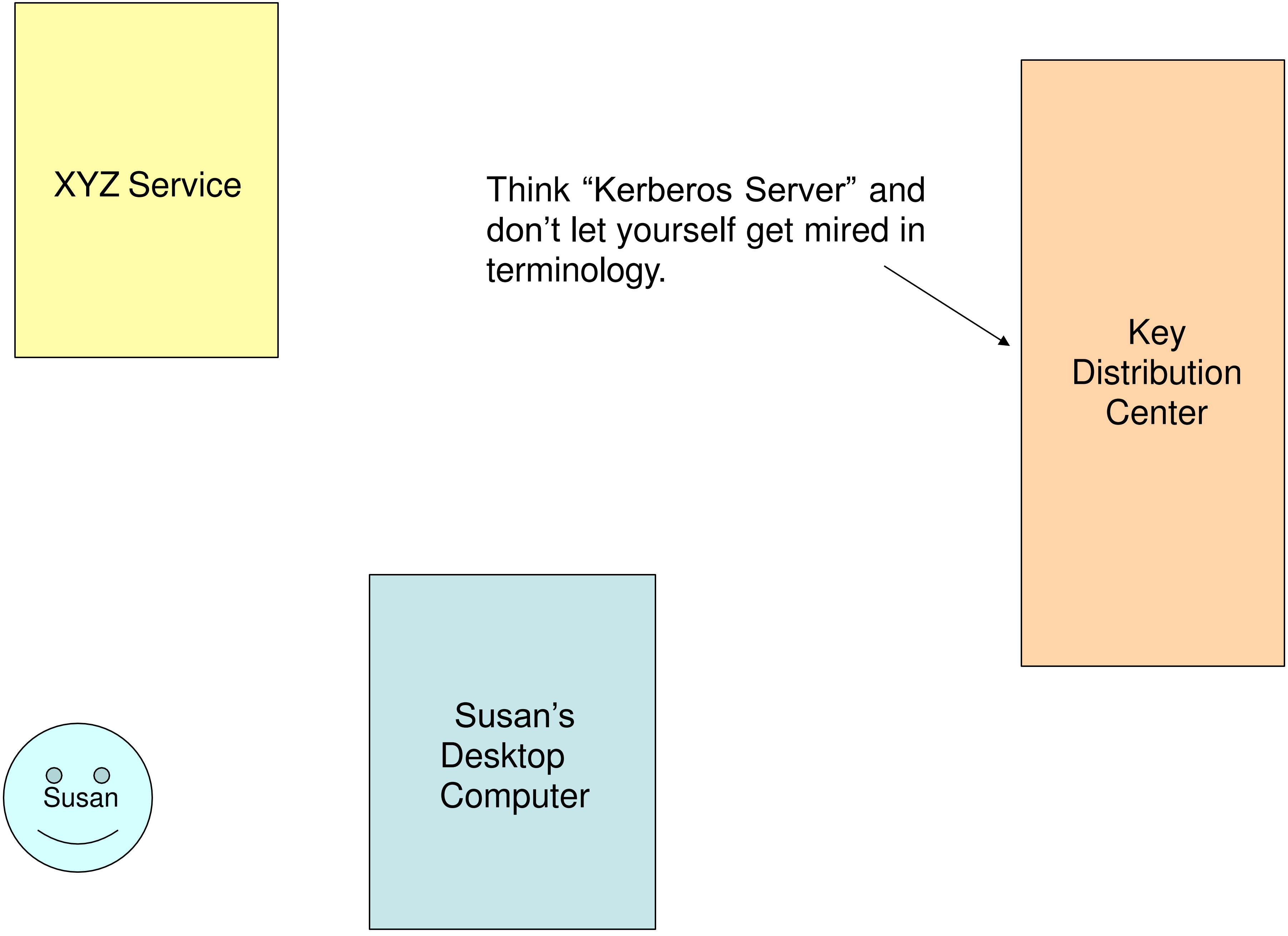


XYZ Service

Key Distribution Center

Susan

Susan’s Desktop Computer



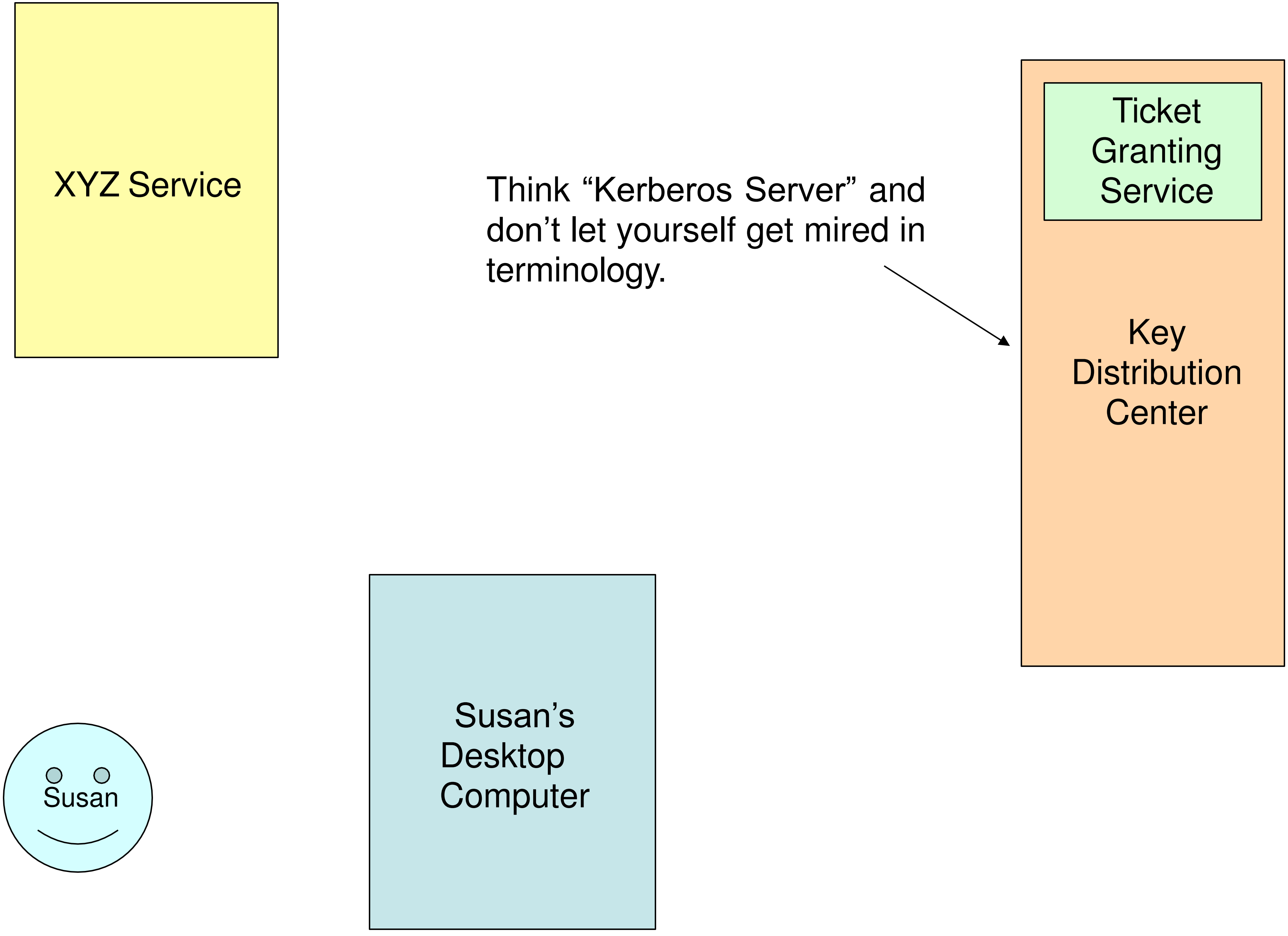
XYZ Service

Think “Kerberos Server” and don’t let yourself get mired in terminology.

Key Distribution Center

Susan

Susan’s Desktop Computer



XYZ Service

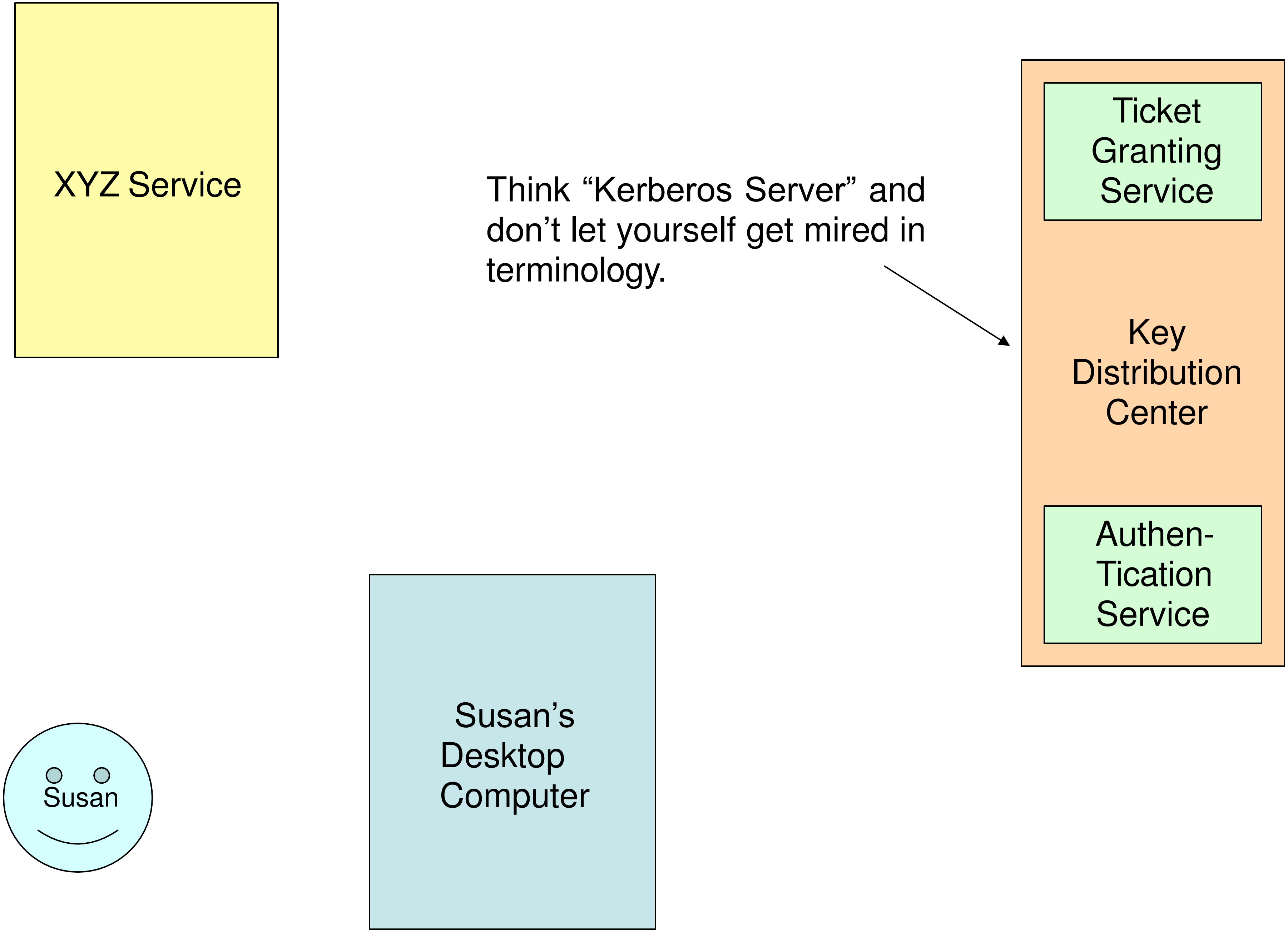
Think “Kerberos Server” and don’t let yourself get mired in terminology.

Ticket Granting Service

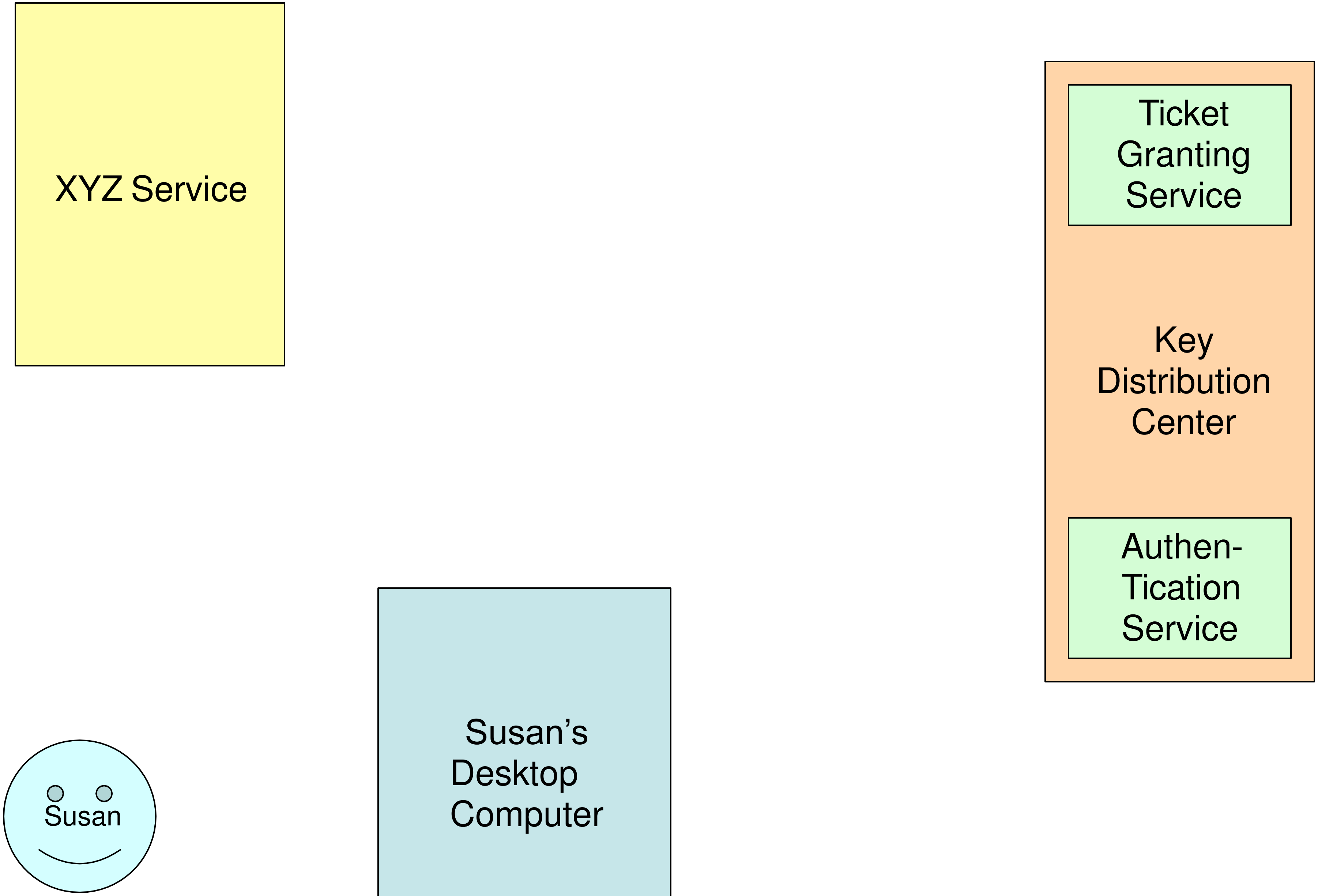
Key Distribution Center

Susan’s Desktop Computer

Susan



Think “Kerberos Server” and don’t let yourself get mired in terminology.



XYZ Service

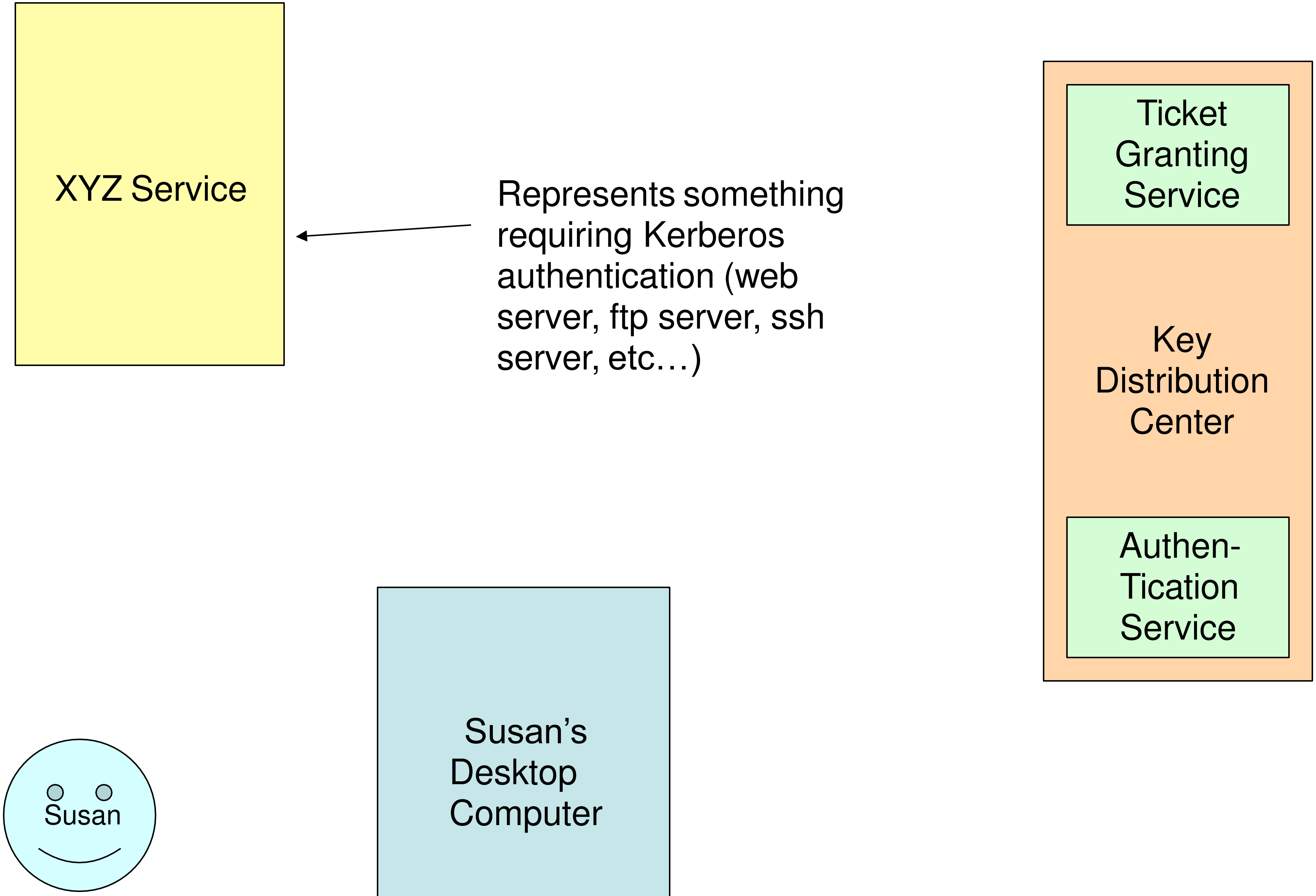
Ticket Granting Service

Key Distribution Center

Authen-Tication Service

Susan

Susan’s Desktop Computer



XYZ Service

Represents something requiring Kerberos authentication (web server, ftp server, ssh server, etc…)

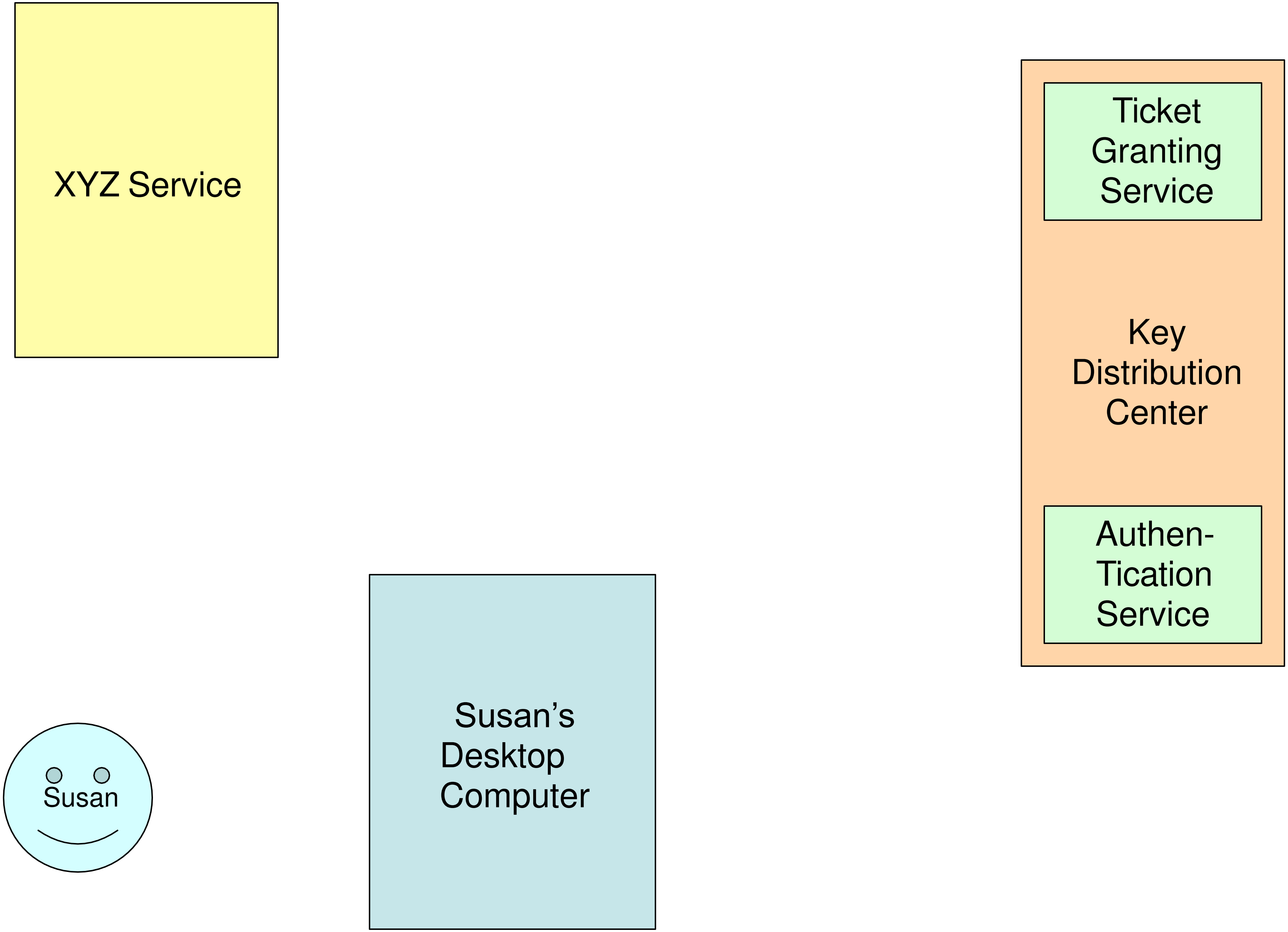
Ticket Granting Service

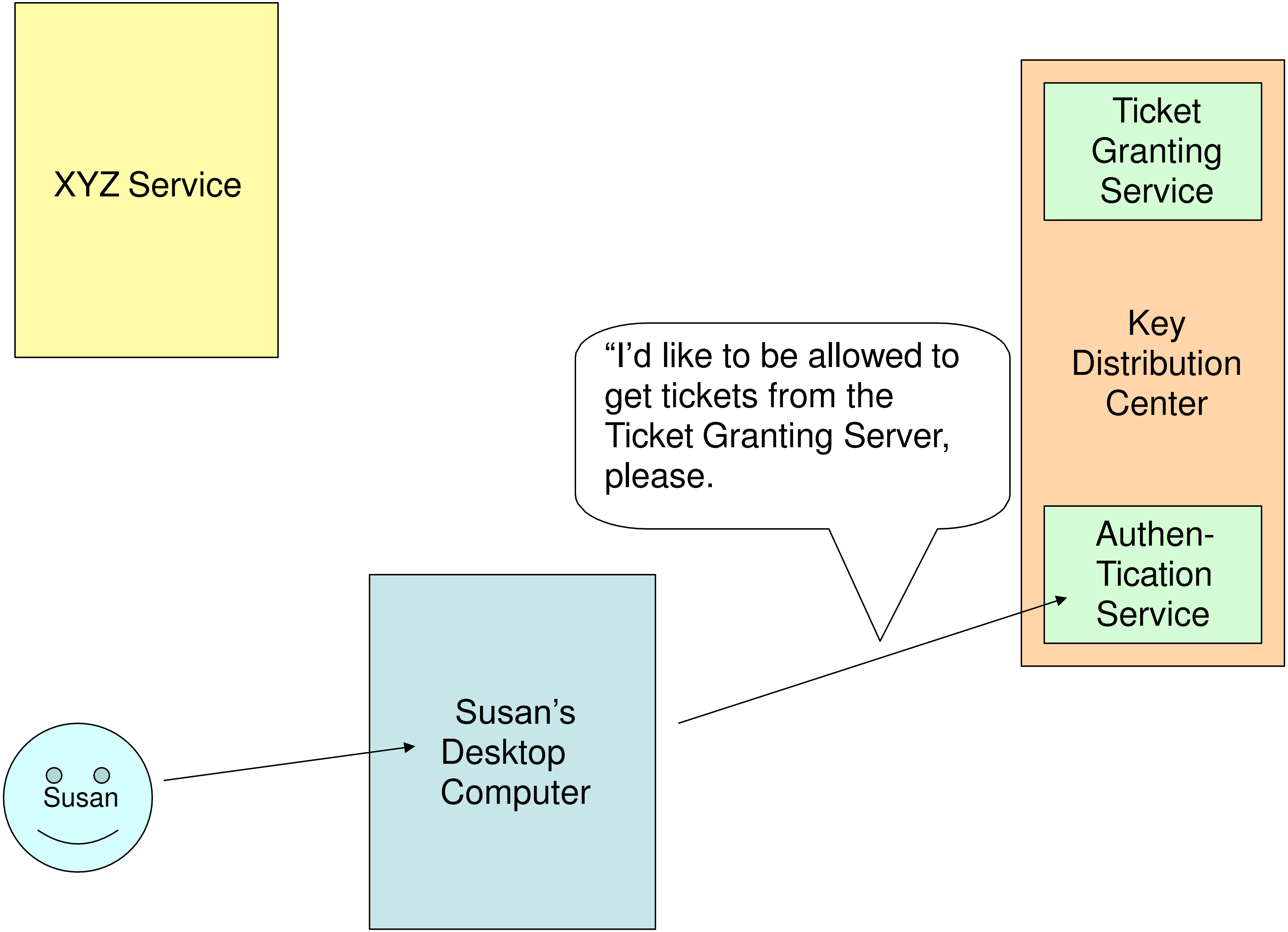
Key Distribution Center

Authen-Tication Service

Susan's Desktop Computer

Susan


XYZ Service
Ticket Granting Service
Key Distribution Center
Authen- Tication Service
Susan's Desktop Computer
Susan



XYZ Service

Ticket Granting Service

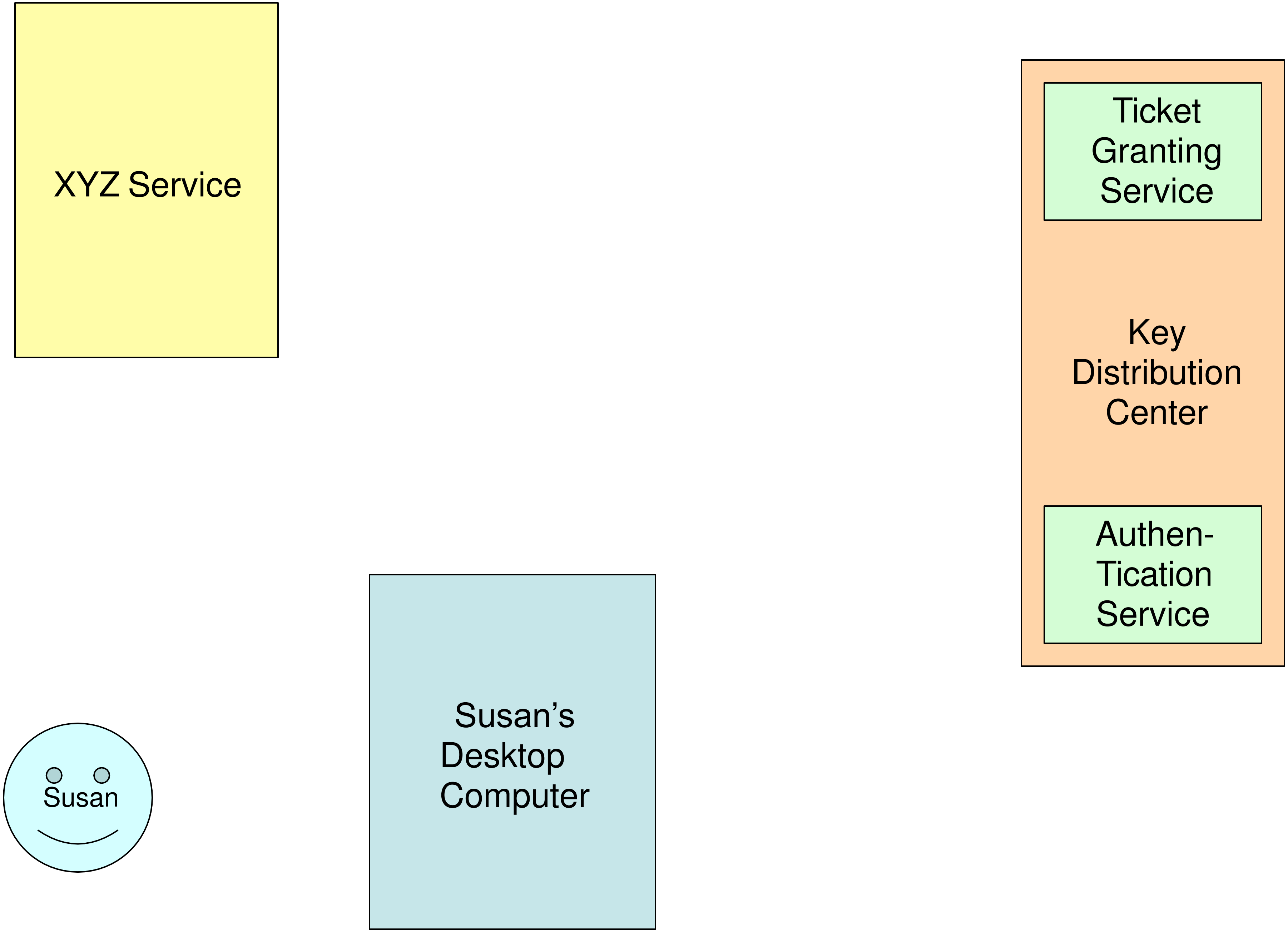
Key Distribution Center

Authen-Tication Service

“I’d like to be allowed to get tickets from the Ticket Granting Server, please.

Susan’s Desktop Computer

Susan



XYZ Service

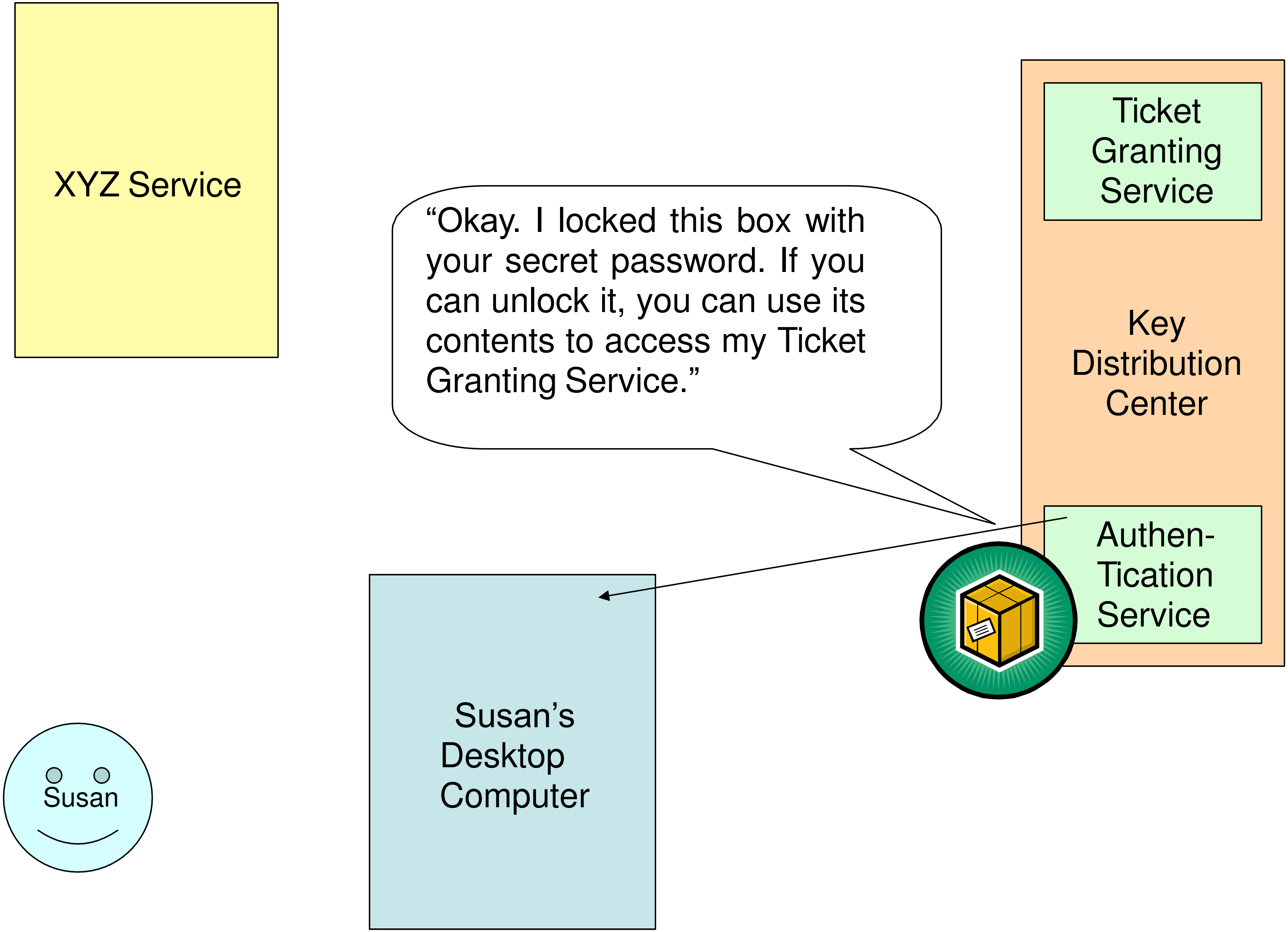
Ticket Granting Service

Key Distribution Center

Authen-Tication Service

Susan

Susan’s Desktop Computer



XYZ Service

“Okay. I locked this box with your secret password. If you can unlock it, you can use its contents to access my Ticket Granting Service.”

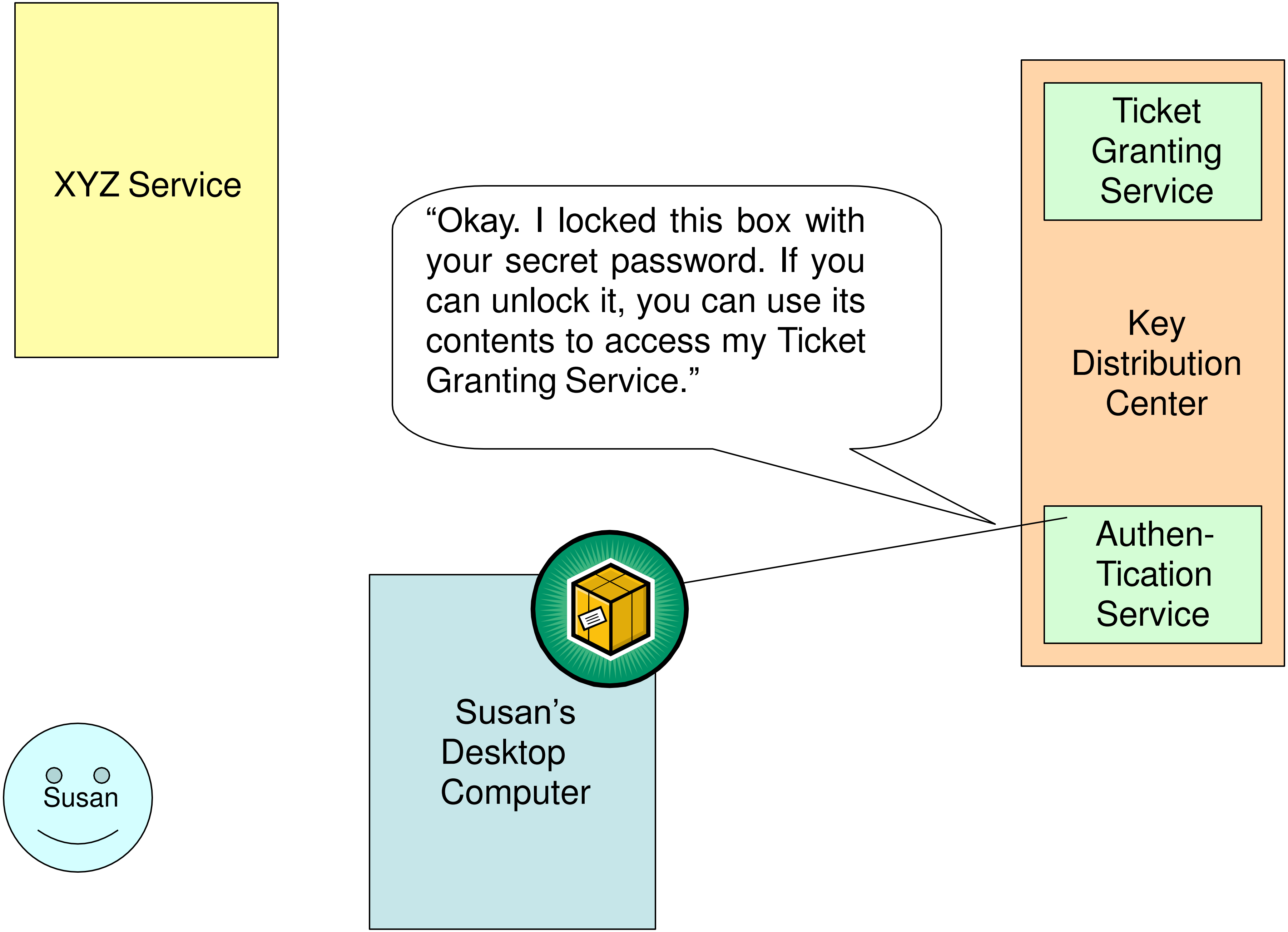
Ticket Granting Service

Key Distribution Center

Authen-Tication Service

Susan’s Desktop Computer

Susan



XYZ Service

“Okay. I locked this box with your secret password. If you can unlock it, you can use its contents to access my Ticket Granting Service.”

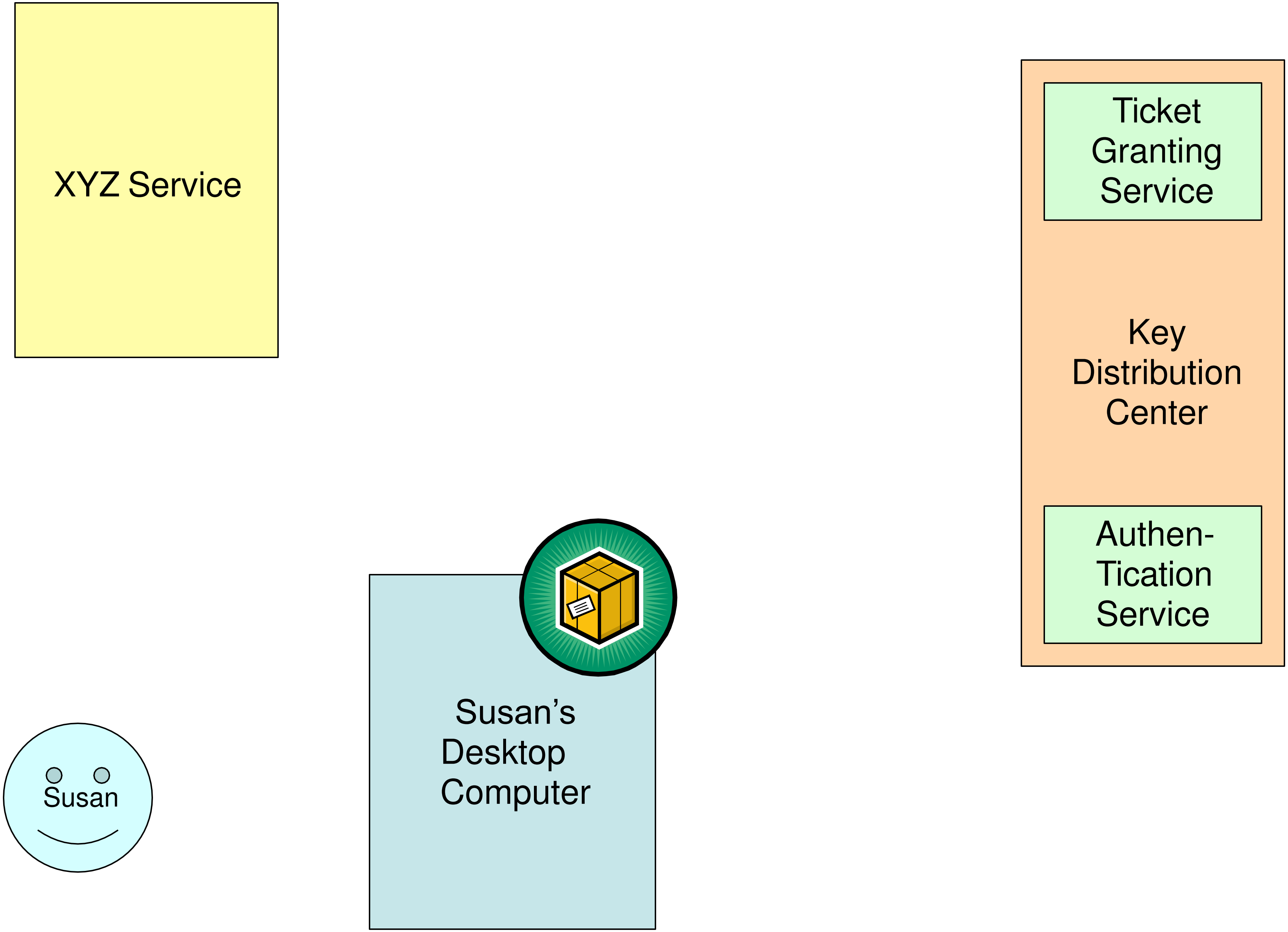
Ticket Granting Service

Key Distribution Center

Authen-Tication Service

Susan’s Desktop Computer

Susan



XYZ Service

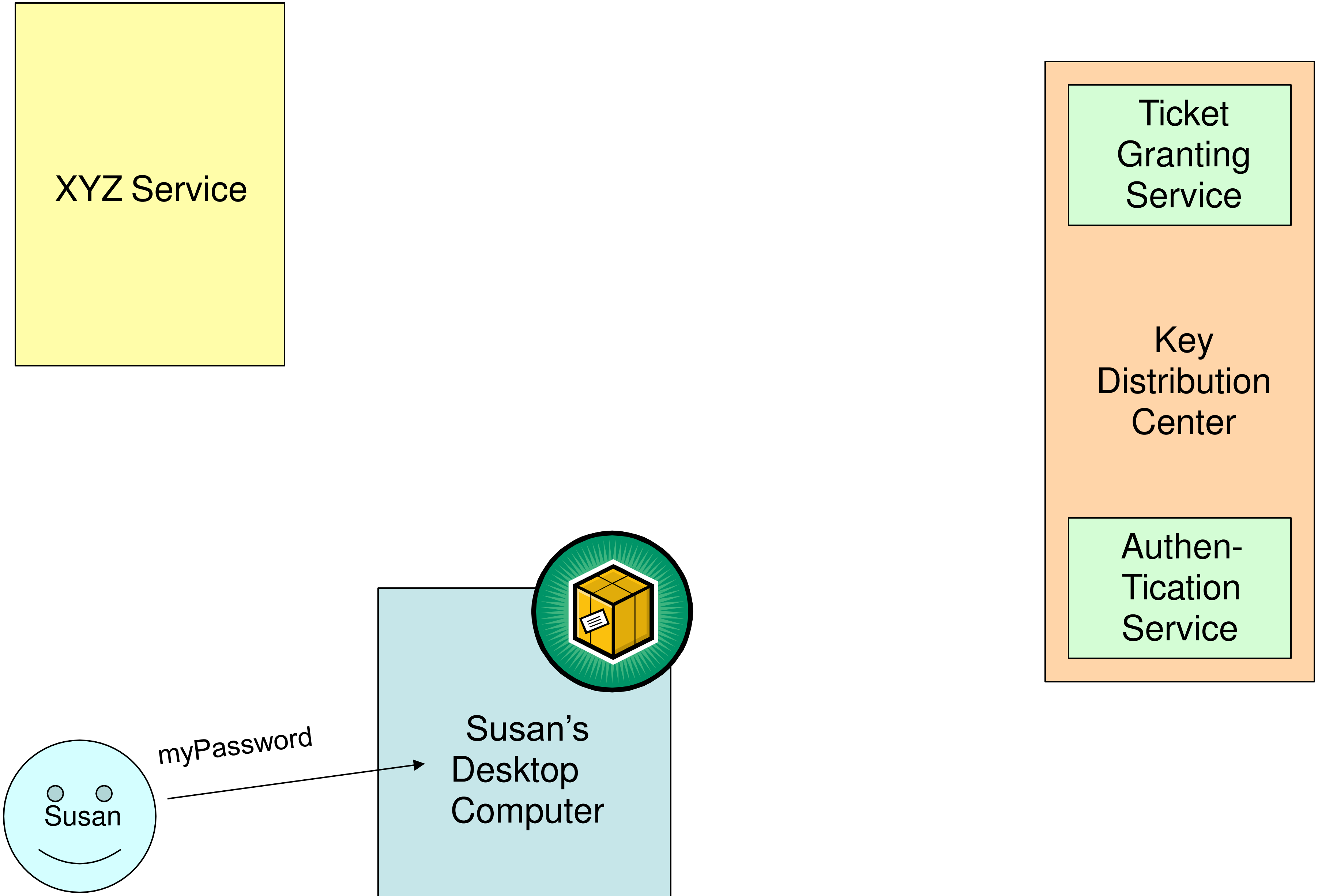
Ticket Granting Service

Key Distribution Center

Authen-Tication Service

Susan's Desktop Computer

Susan



XYZ Service

Ticket Granting Service

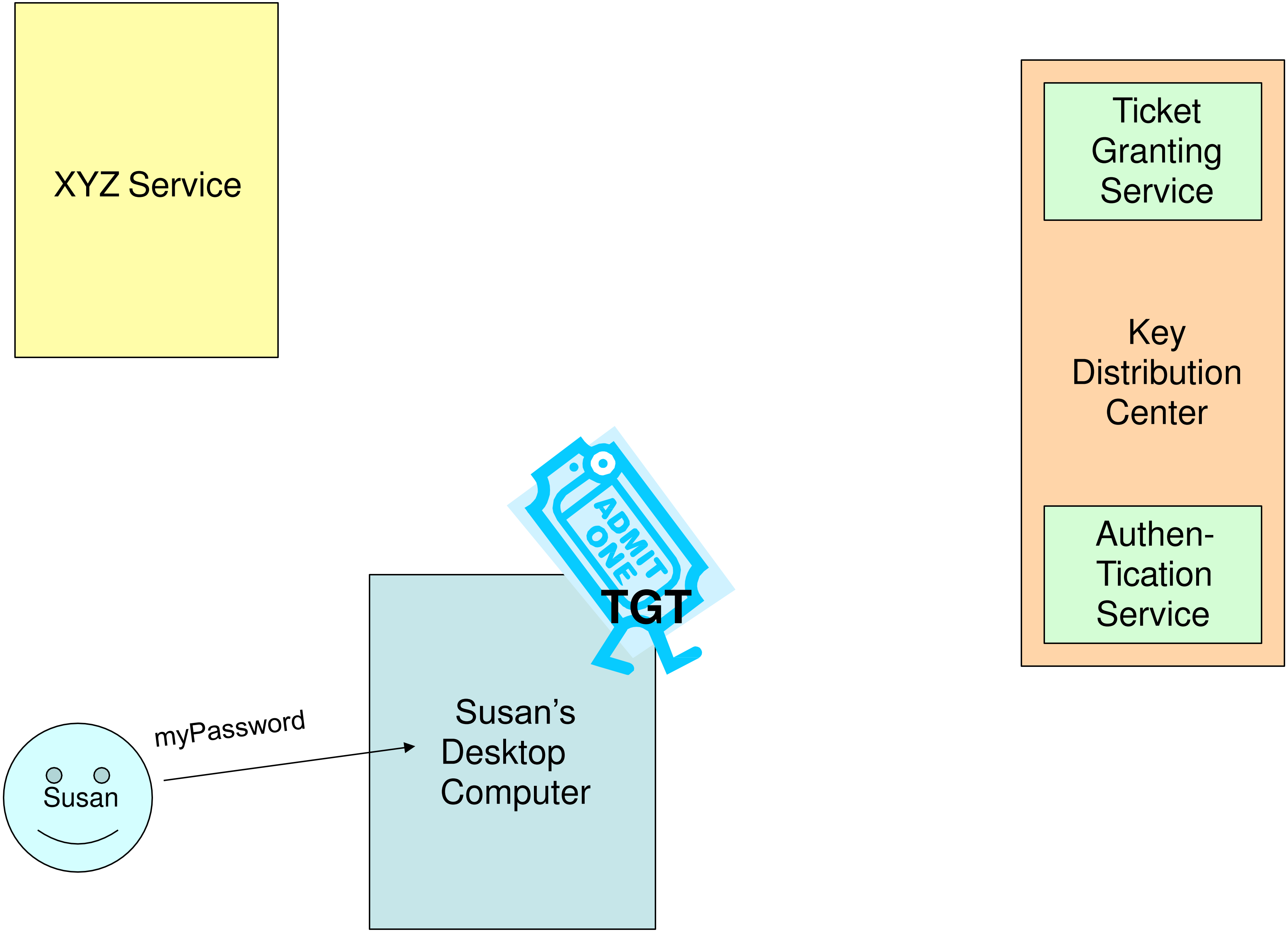
Key Distribution Center

Authen-Tication Service

Susan's Desktop Computer

myPassword

Susan



XYZ Service

Ticket Granting Service

Key Distribution Center

Authen-Tication Service

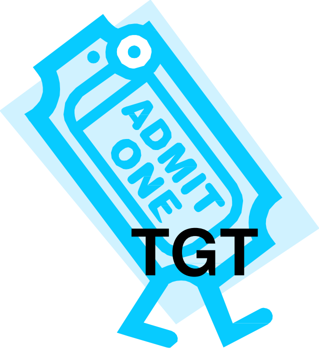
ADMIT ONE

TGT

Susan's Desktop Computer

myPassword

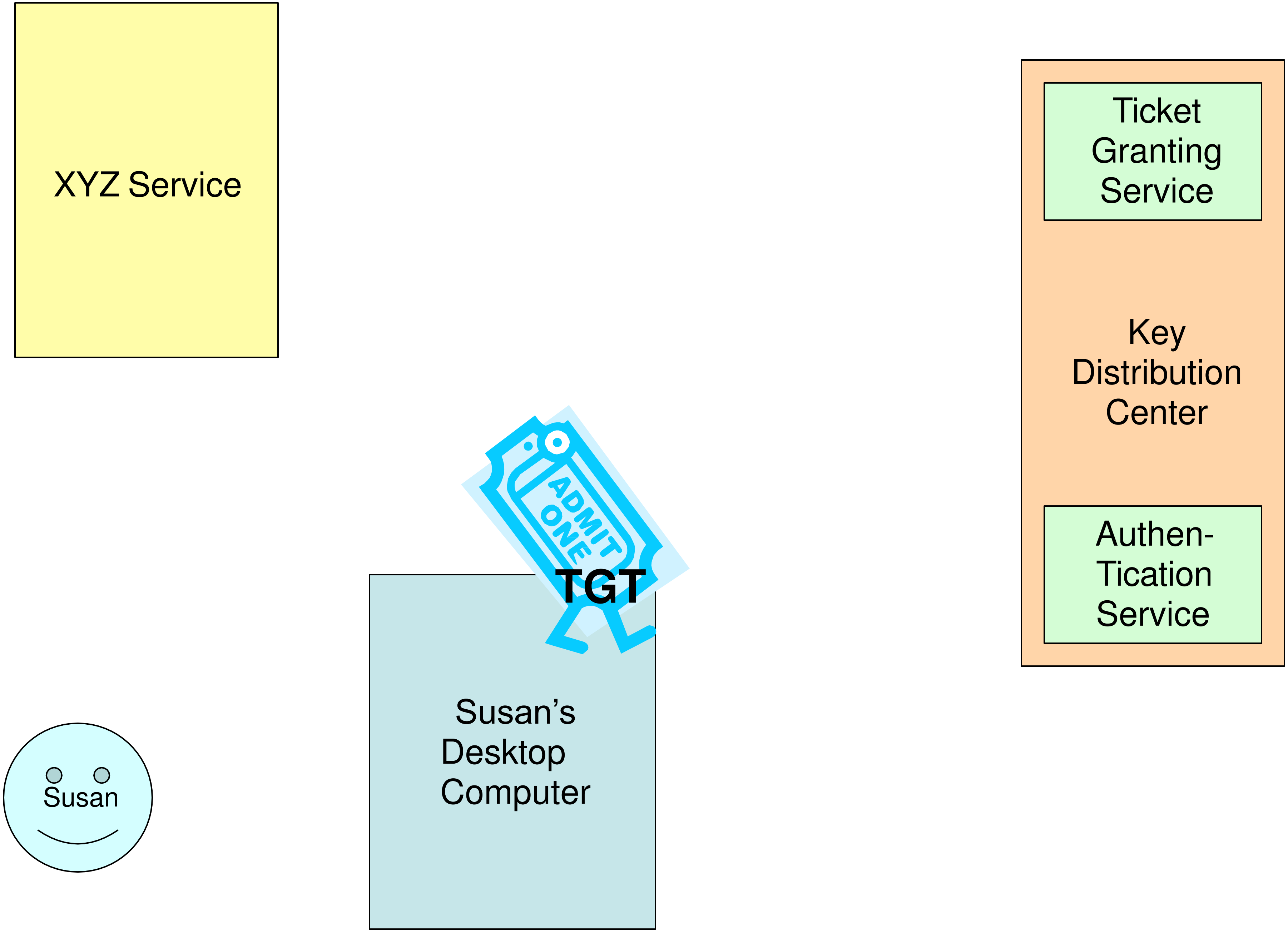
Susan



Because Susan was able to open the box (decrypt a message) from the Authentication Service, she is now the owner of a shiny “Ticket-Granting Ticket”.

The Ticket-Granting Ticket (TGT) must be presented to the Ticket Granting Service in order to acquire “service tickets” for use with services requiring Kerberos authentication.

The TGT contains no password information.



XYZ Service

Ticket Granting Service

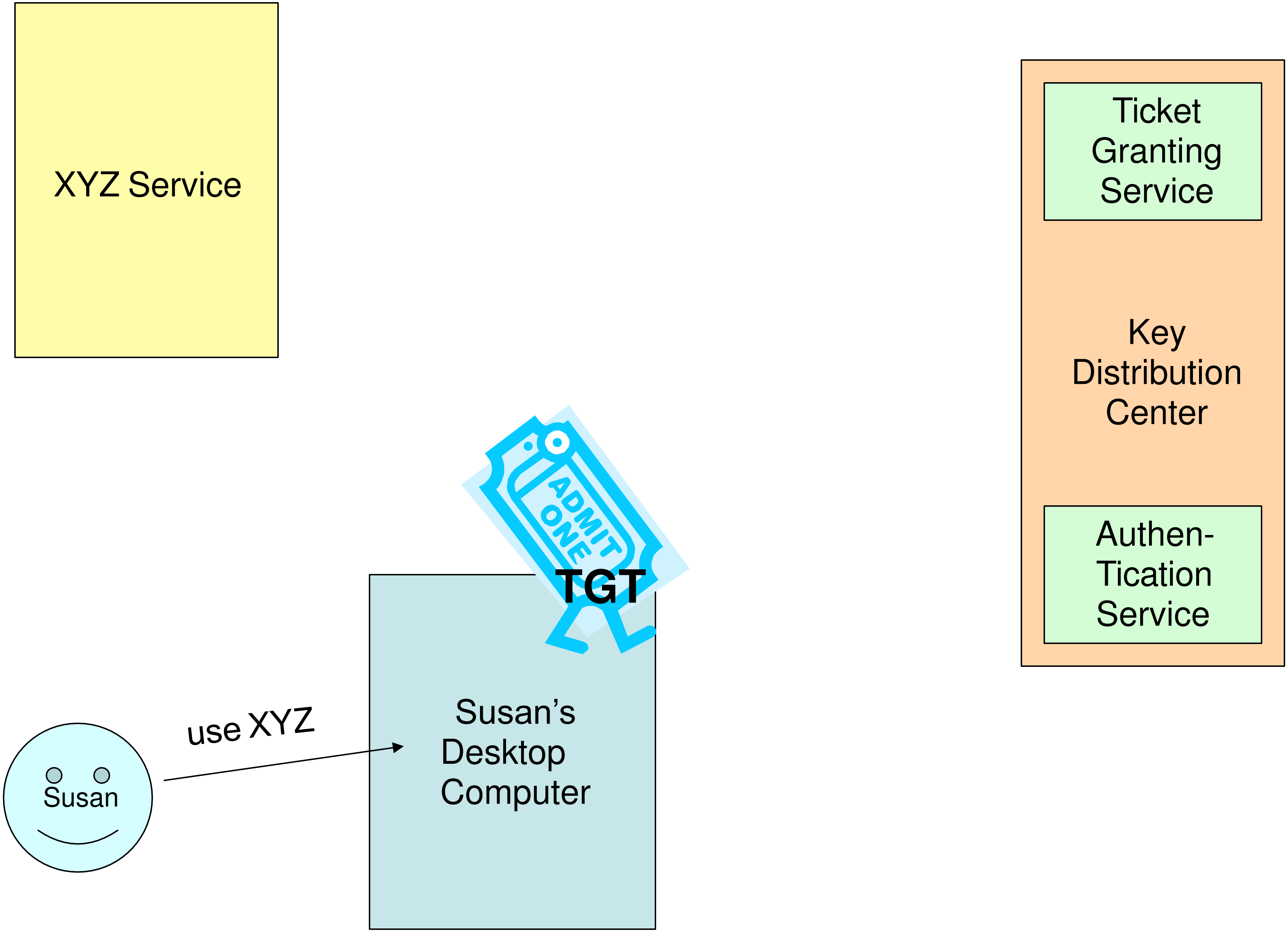
Key Distribution Center

Authen- Tication Service

TGT

Susan’s Desktop Computer

Susan



XYZ Service

Ticket Granting Service

Key Distribution Center

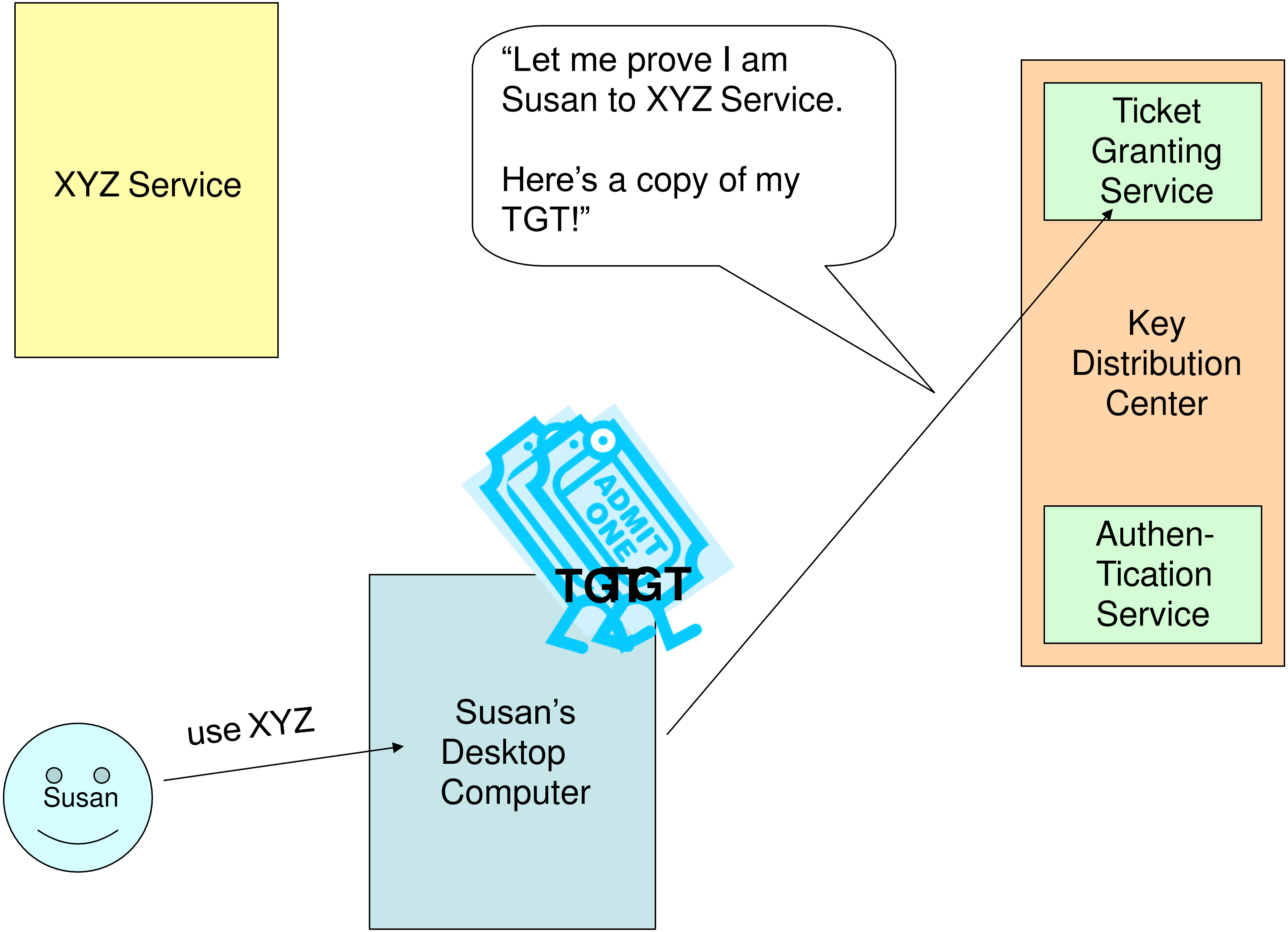
Authen-Tication Service

TGT

Susan's Desktop Computer

use XYZ

Susan



“Let me prove I am Susan to XYZ Service.

Here’s a copy of my TGT!”

XYZ Service

Ticket Granting Service

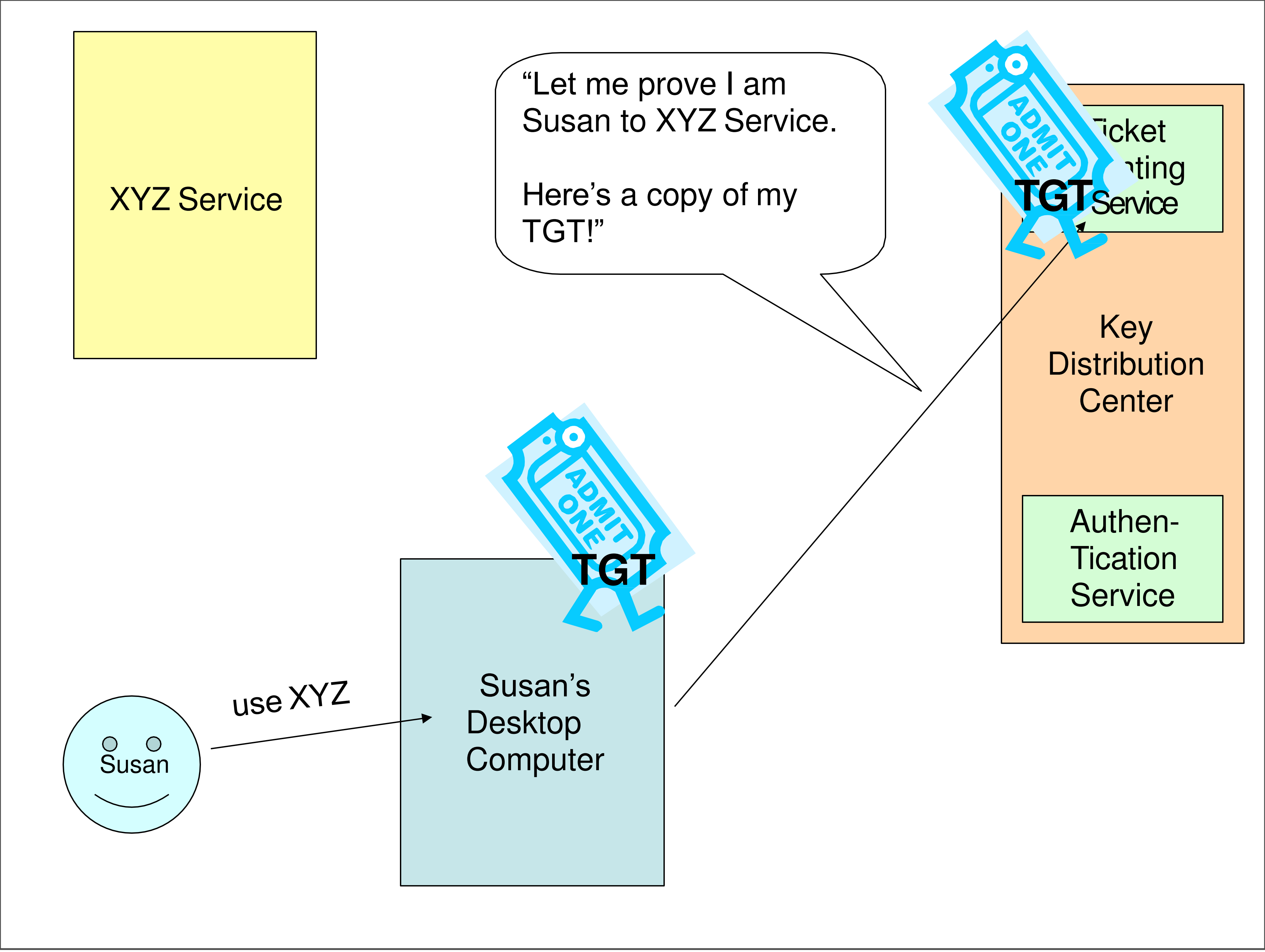
Key Distribution Center

Authen-Tication Service

Susan’s Desktop Computer

use XYZ

Susan



XYZ Service

“Let me prove I am Susan to XYZ Service.

Here’s a copy of my TGT!”

Ticket
nting
Service

ADMIT ONE

TGT

Key Distribution Center

Authen-
Tication
Service

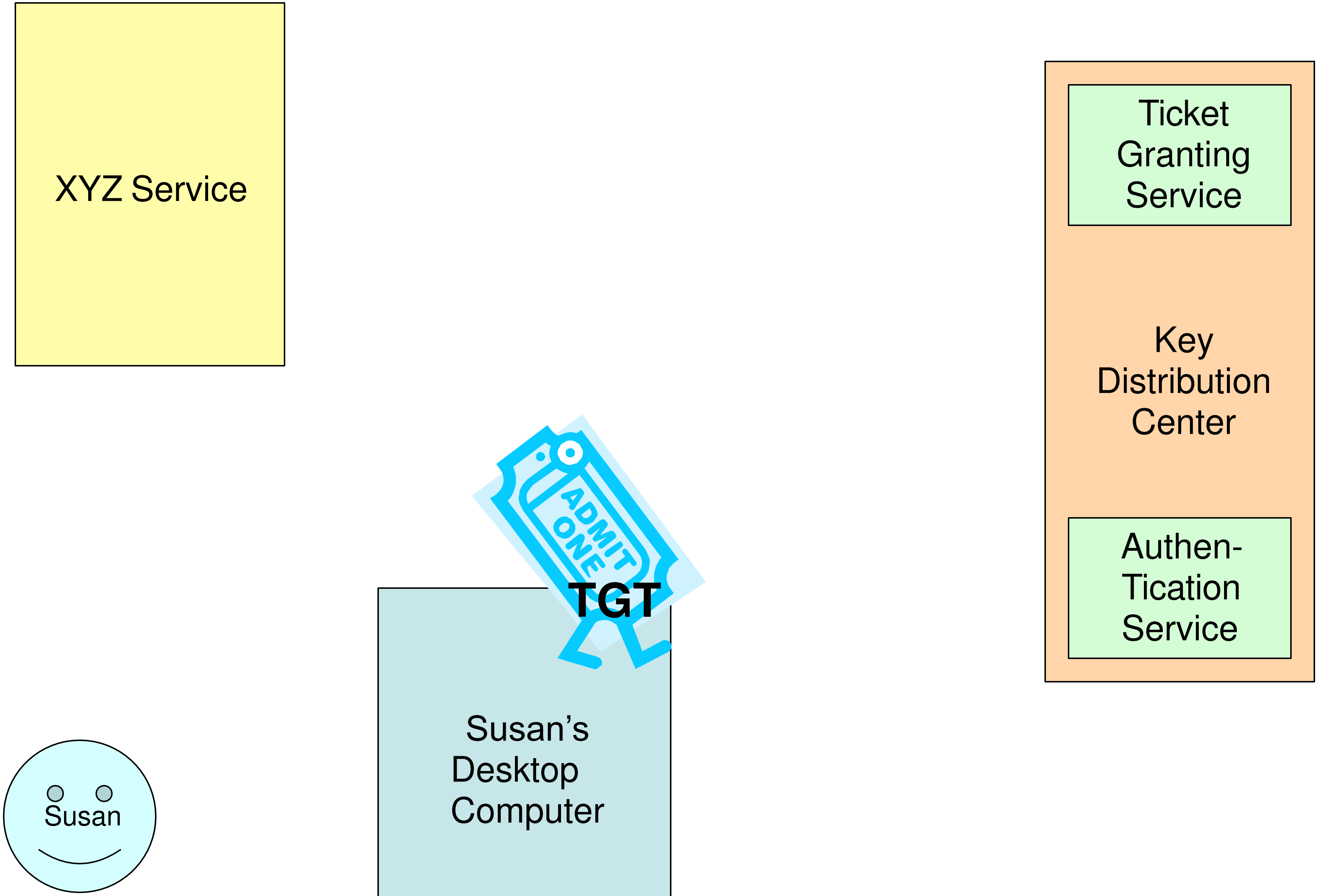
ADMIT ONE

TGT

Susan’s Desktop Computer

use XYZ

Susan



XYZ Service

Ticket Granting Service

Key Distribution Center

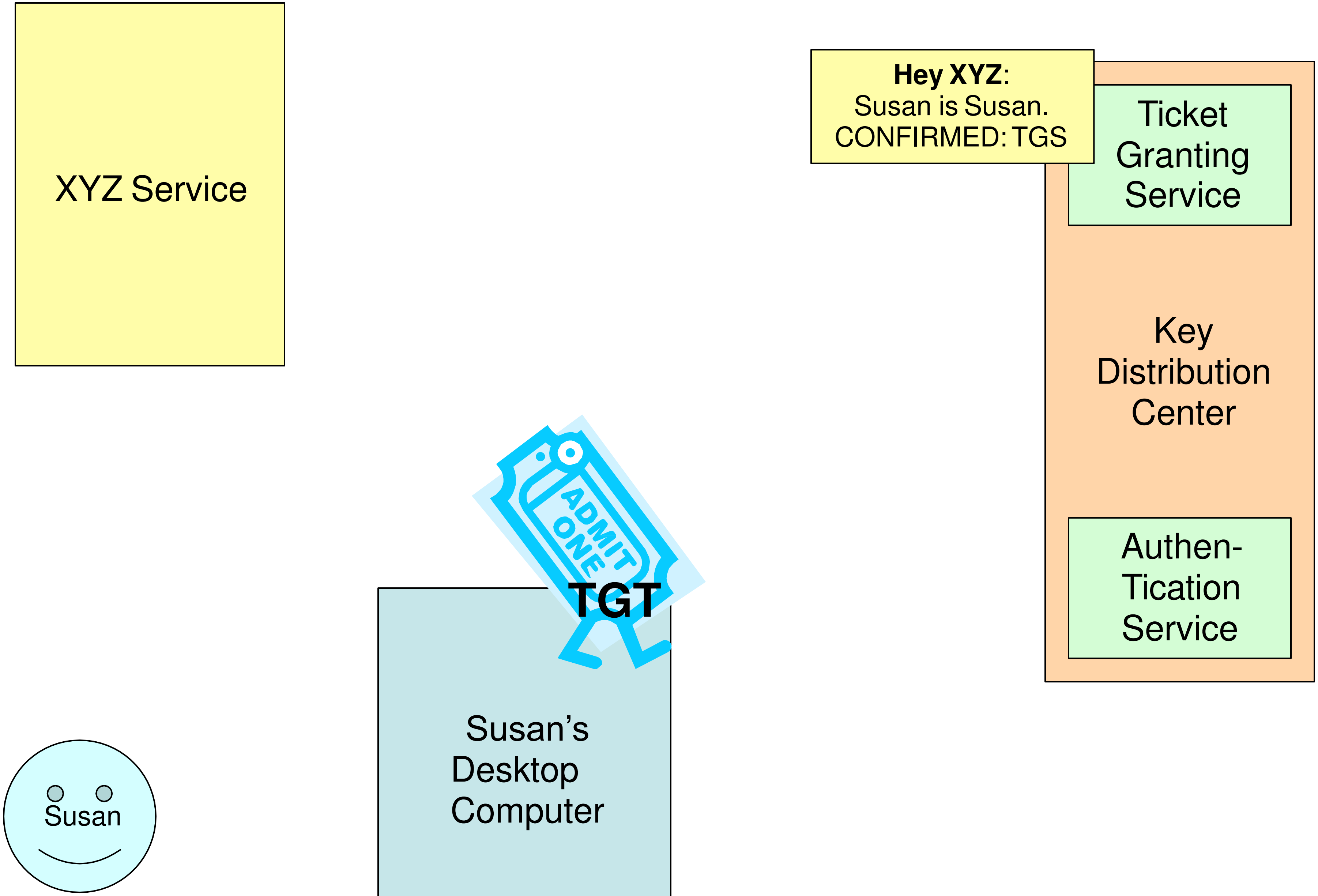
Authen-Tication Service

ADMIT ONE

TGT

Susan's Desktop Computer

Susan



XYZ Service

Hey XYZ:
Susan is Susan.
CONFIRMED: TGS

Ticket Granting Service

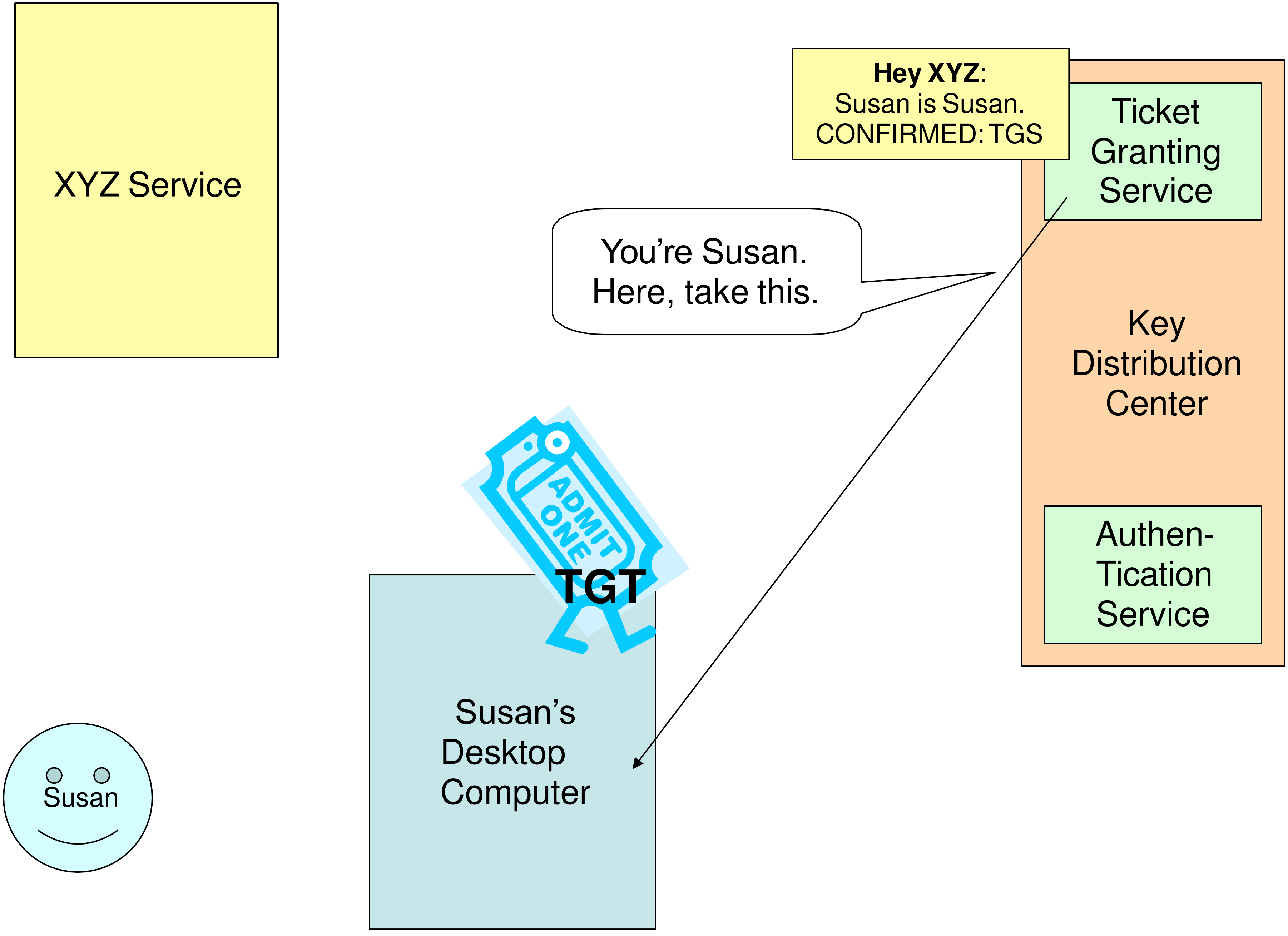
Key Distribution Center

Authen-Tication Service

TGT

Susan's Desktop Computer

Susan



XYZ Service

Hey XYZ:
Susan is Susan.
CONFIRMED: TGS

Ticket Granting Service

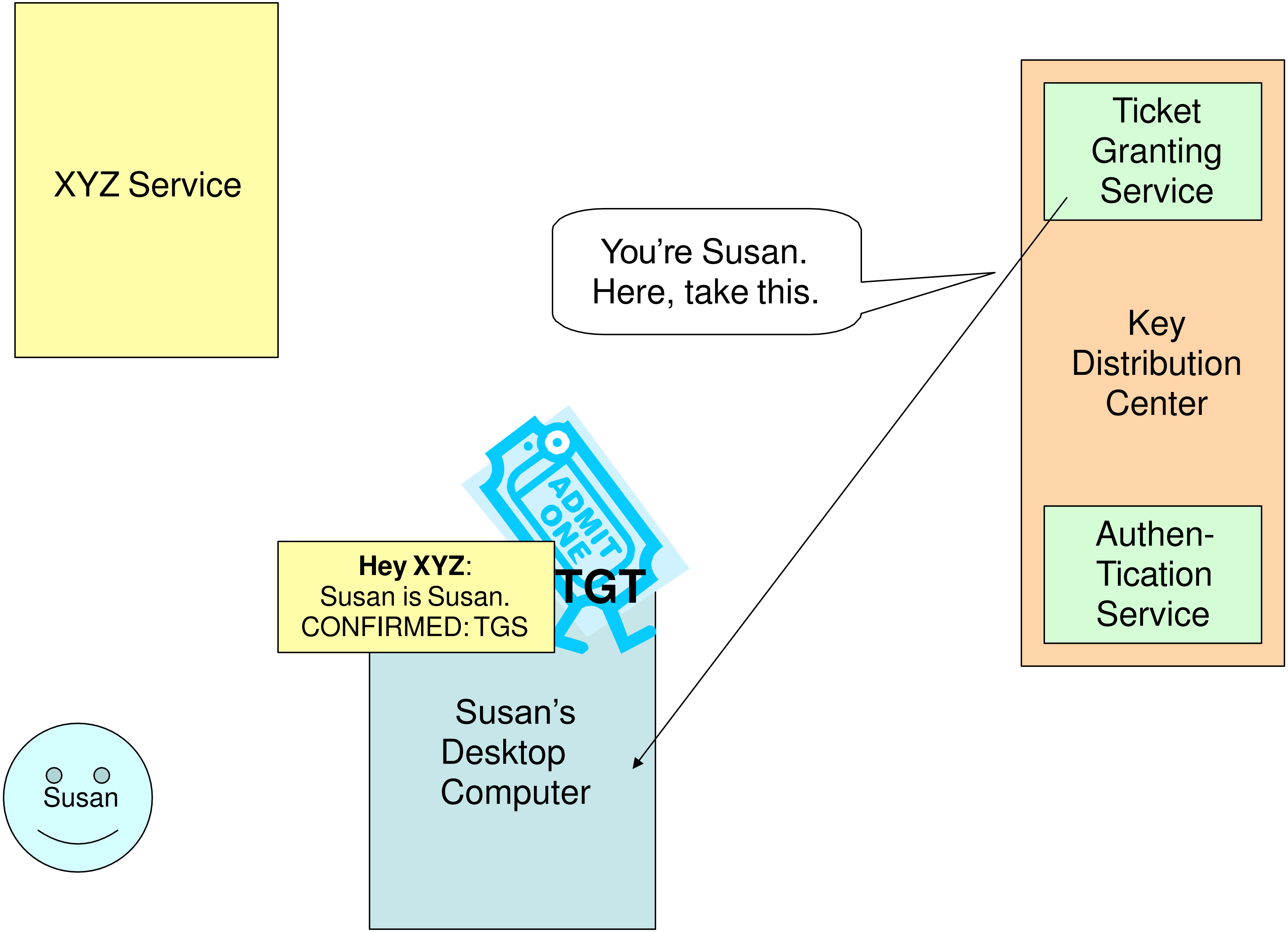
You're Susan.
Here, take this.

Key Distribution Center

Authen-Tication Service

Susan's Desktop Computer

Susan



XYZ Service

You’re Susan.
Here, take this.

Ticket Granting Service

Key Distribution Center

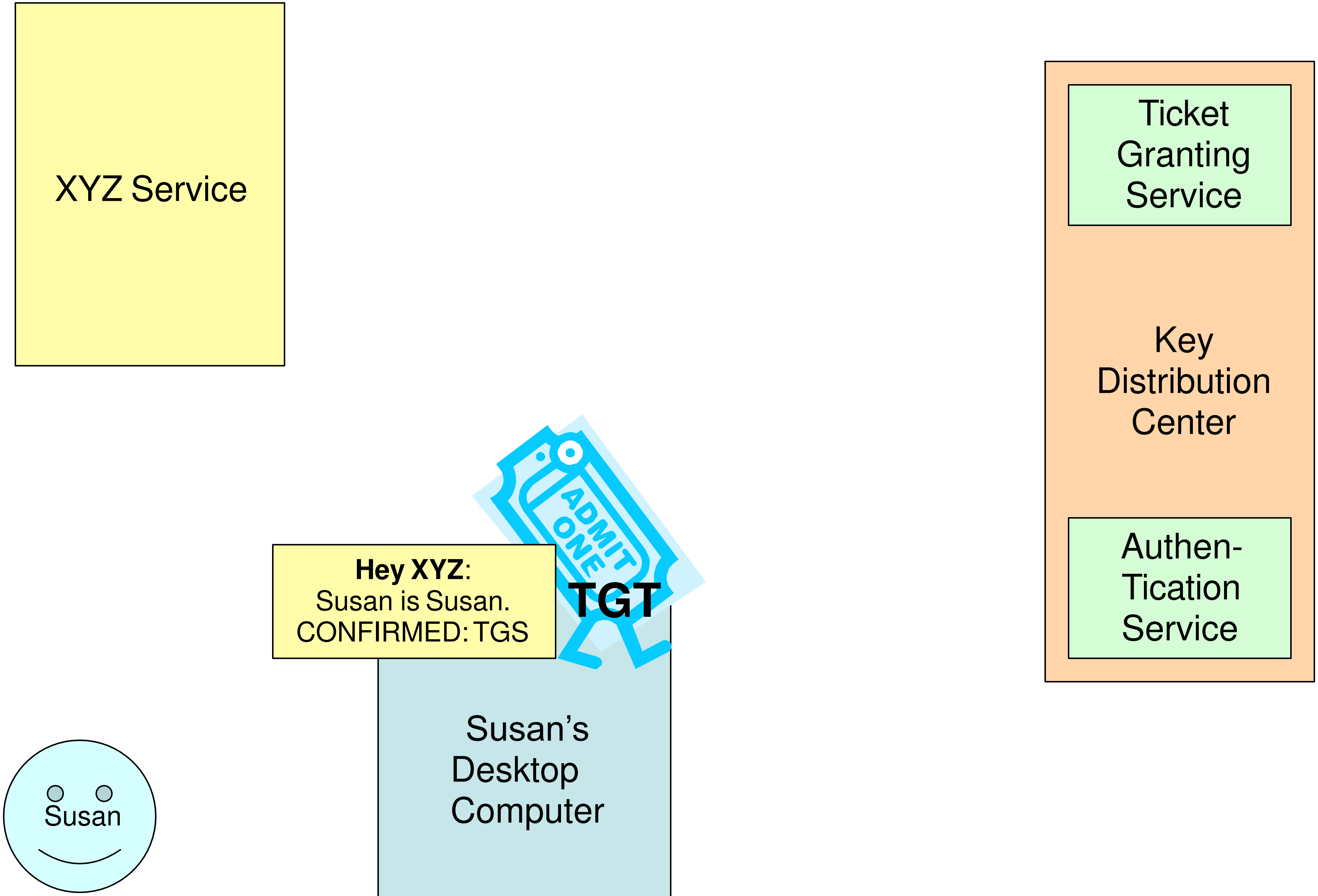
Authen-Tication Service

Hey XYZ:
Susan is Susan.
CONFIRMED: TGS

TGT

Susan’s Desktop Computer

Susan



XYZ Service

Ticket Granting Service

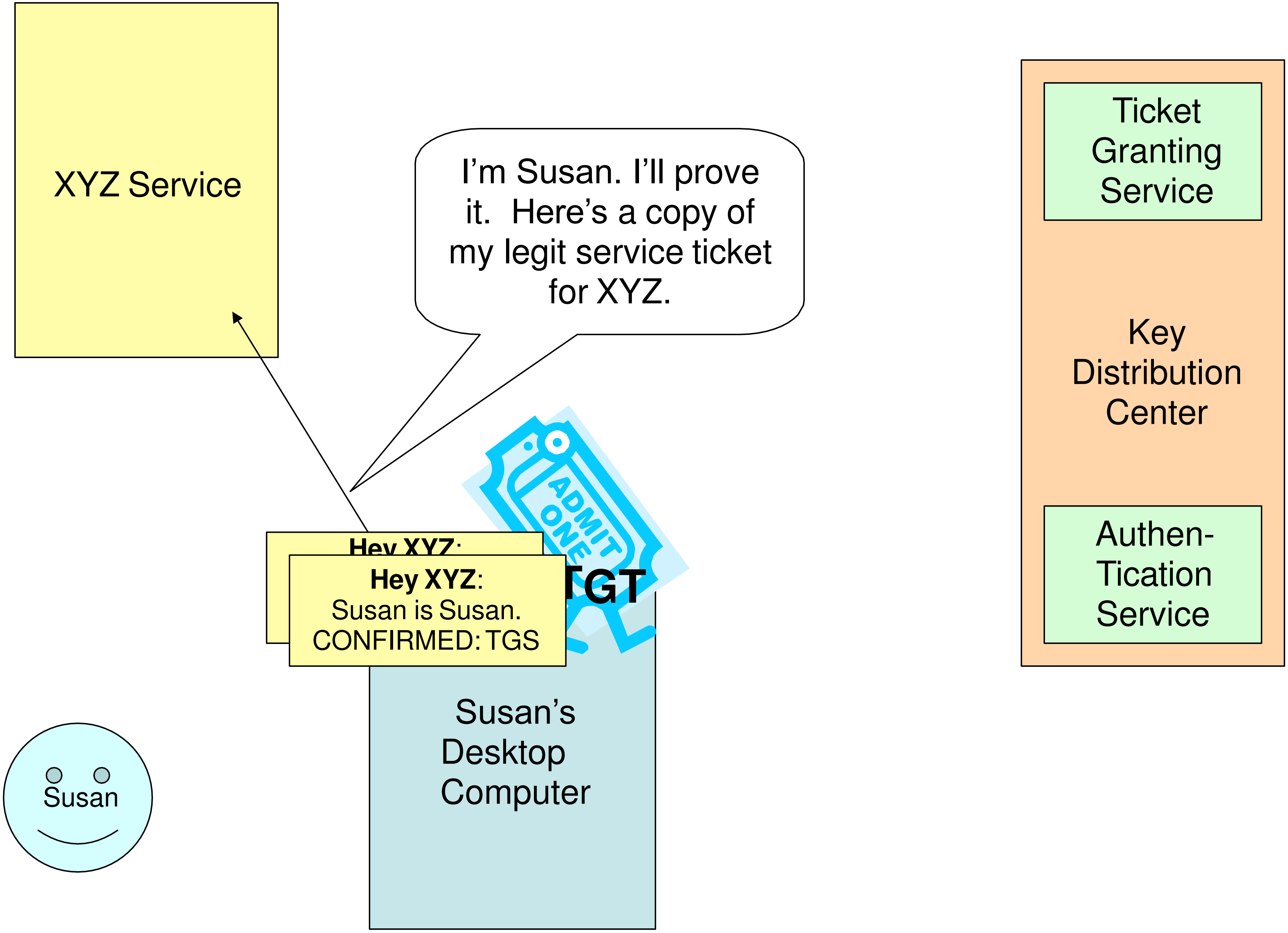
Key Distribution Center

Authen-Tication Service

Hey XYZ:
Susan is Susan.
CONFIRMED: TGS

Susan's Desktop Computer

Susan



XYZ Service

I’m Susan. I’ll prove it. Here’s a copy of my legit service ticket for XYZ.

Hey XYZ:

Hey XYZ:
Susan is Susan.
CONFIRMED: TGS

ADMIT ONE

TGT

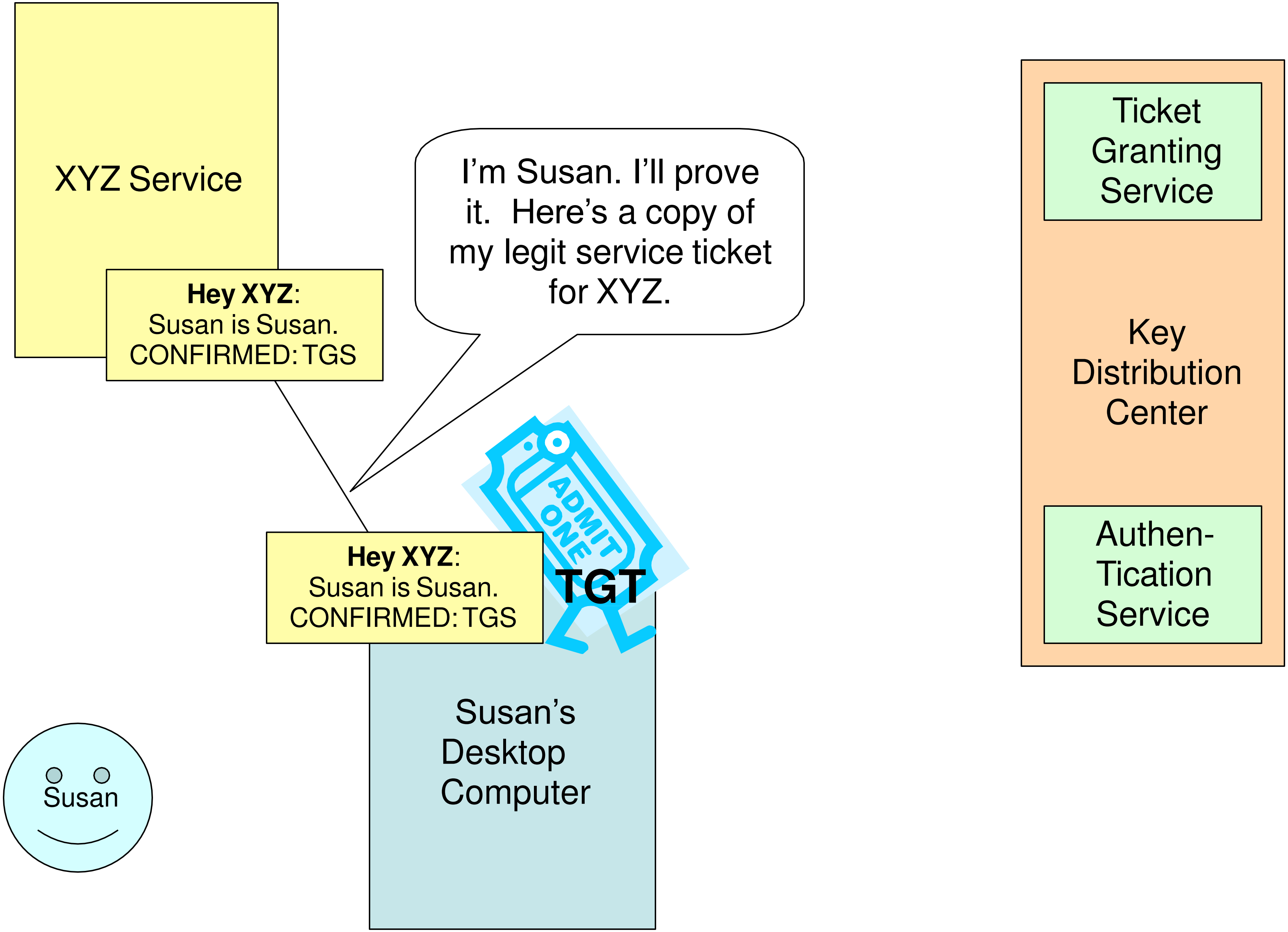
Susan’s Desktop Computer

Susan

Ticket Granting Service

Key Distribution Center

Authen-Tication Service



XYZ Service

Hey XYZ:
Susan is Susan.
CONFIRMED: TGS

I'm Susan. I'll prove it. Here's a copy of my legit service ticket for XYZ.

Ticket Granting Service

Key Distribution Center

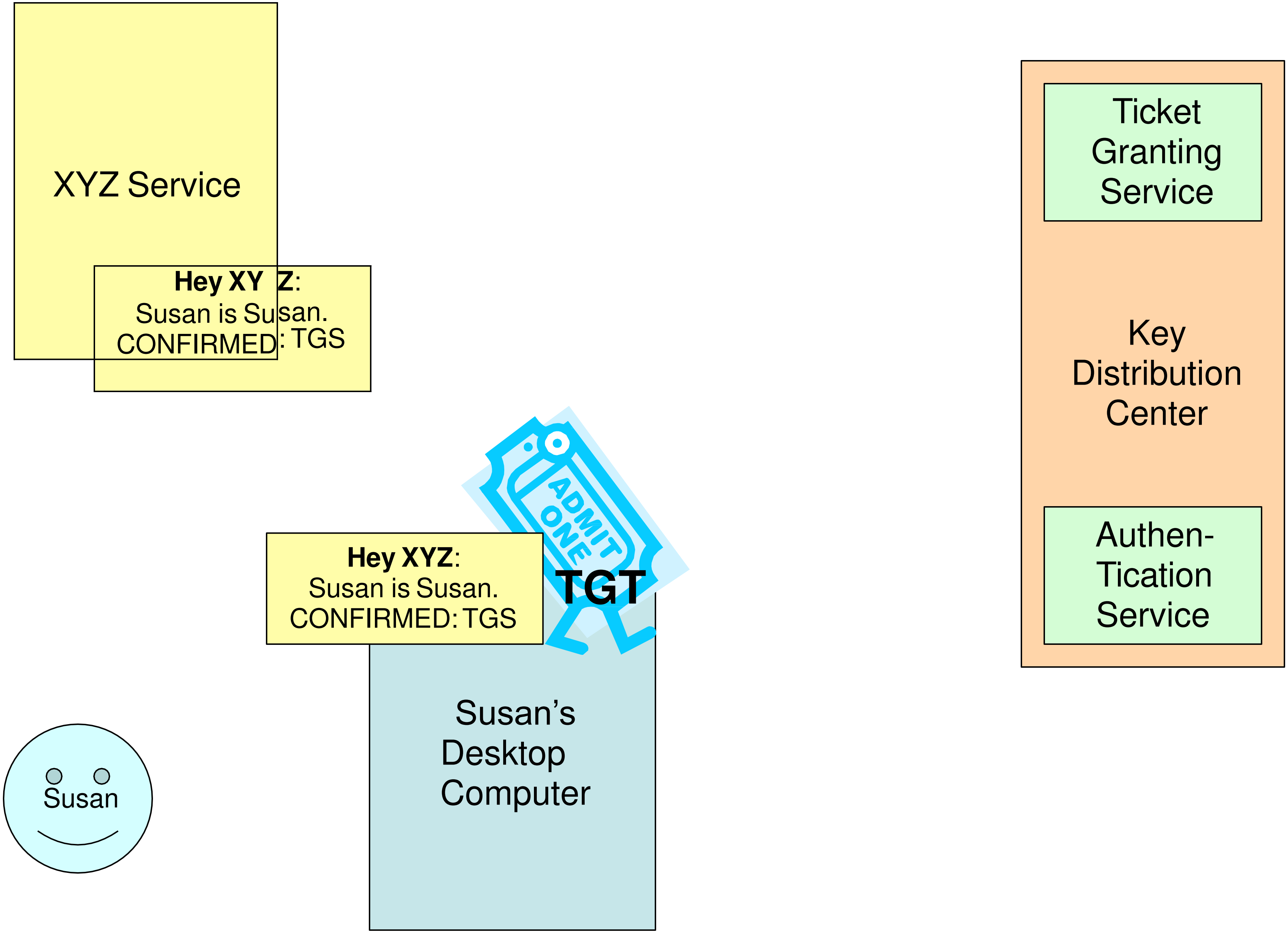
Authen-Tication Service

Hey XYZ:
Susan is Susan.
CONFIRMED: TGS

TGT

Susan

Susan's Desktop Computer



XYZ Service

Hey XYZ:
Susan is Susan.
CONFIRMED: TGS

Ticket Granting Service

Key Distribution Center

Authen-Tication Service

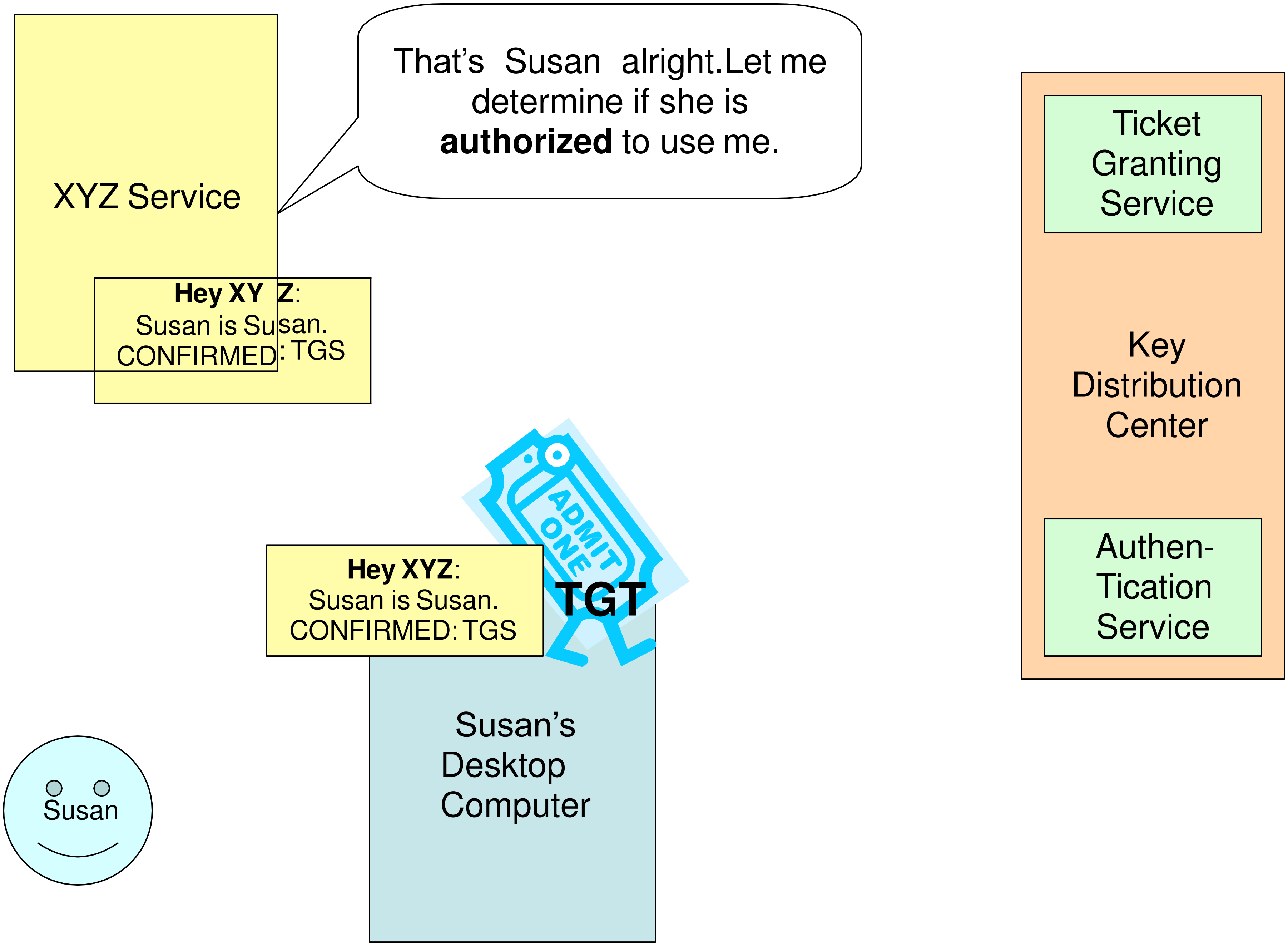
ADMIT ONE

TGT

Hey XYZ:
Susan is Susan.
CONFIRMED: TGS

Susan's Desktop Computer

Susan



That's Susan alright. Let me determine if she is **authorized** to use me.

XYZ Service

Hey XYZ:
Susan is Susan.
CONFIRMED: TGS

Ticket Granting Service

Key Distribution Center

Authen-Tication Service

ADMIT ONE

TGT

Hey XYZ:
Susan is Susan.
CONFIRMED: TGS

Susan's Desktop Computer

Susan

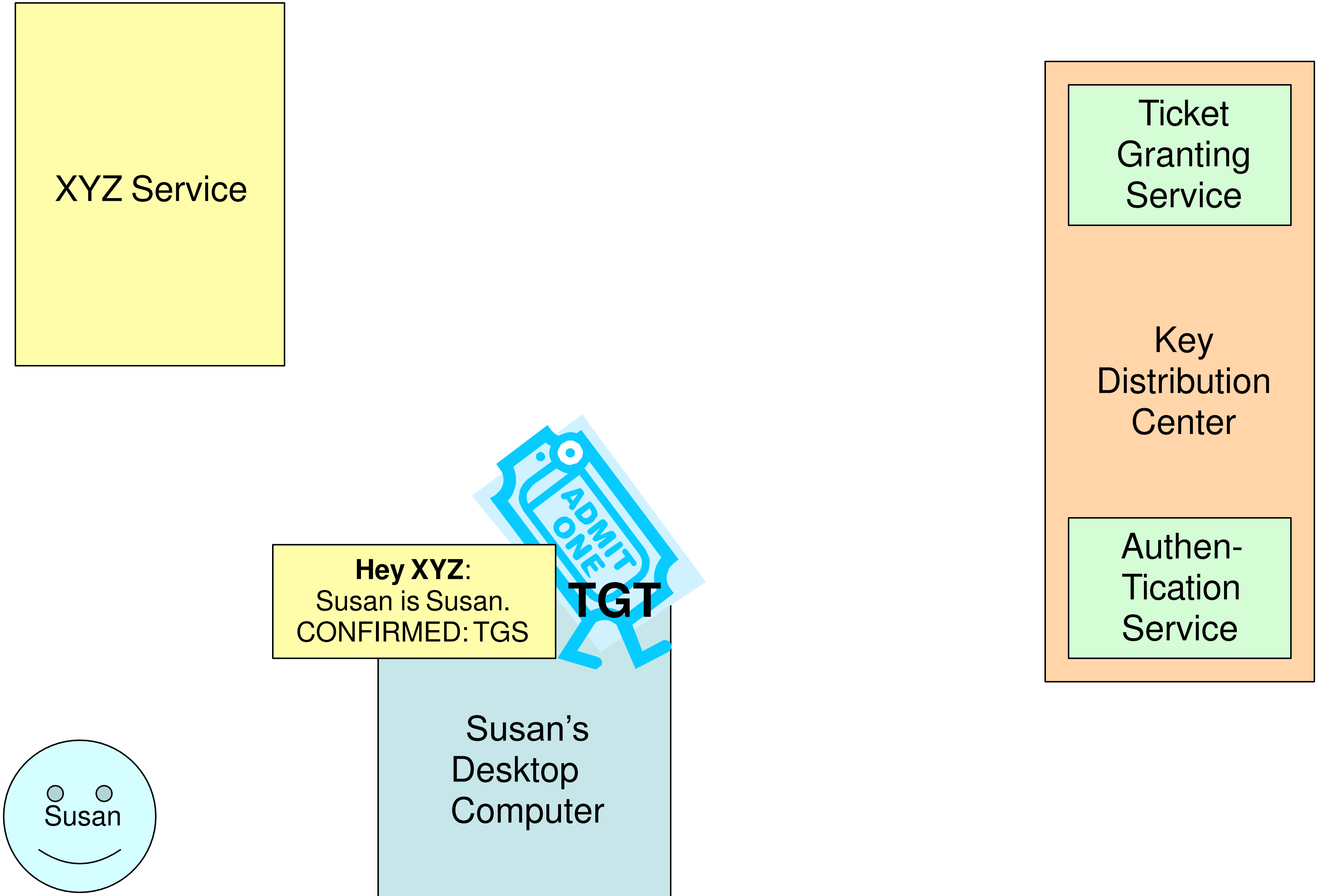
Authorization checks are performed by the XYZ service…

Just because Susan has **authenticated** herself does not inherently mean she is **authorized** to make use of the XYZ service.

One remaining note:

Tickets (your TGT as well as service-specific tickets) have expiration dates configured by your local system administrator(s). An expired ticket is unusable.

Until a ticket's expiration, it may be used repeatedly.



XYZ Service

Hey XYZ:
Susan is Susan.
CONFIRMED: TGS

TGT

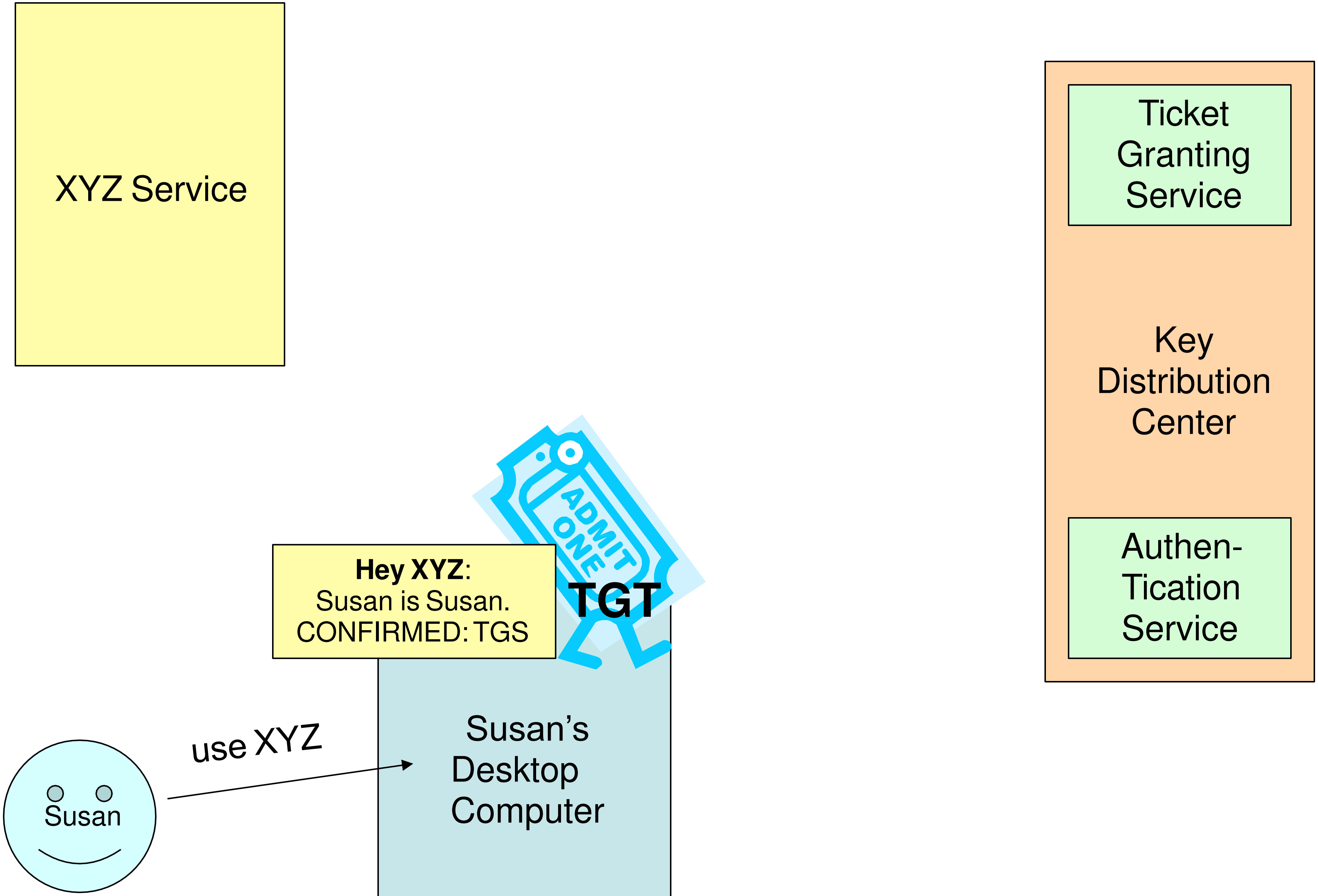
Susan's Desktop Computer

Susan

Key Distribution Center

Ticket Granting Service

AuthenTication Service



XYZ Service

Ticket Granting Service

Key Distribution Center

Authen-Tication Service

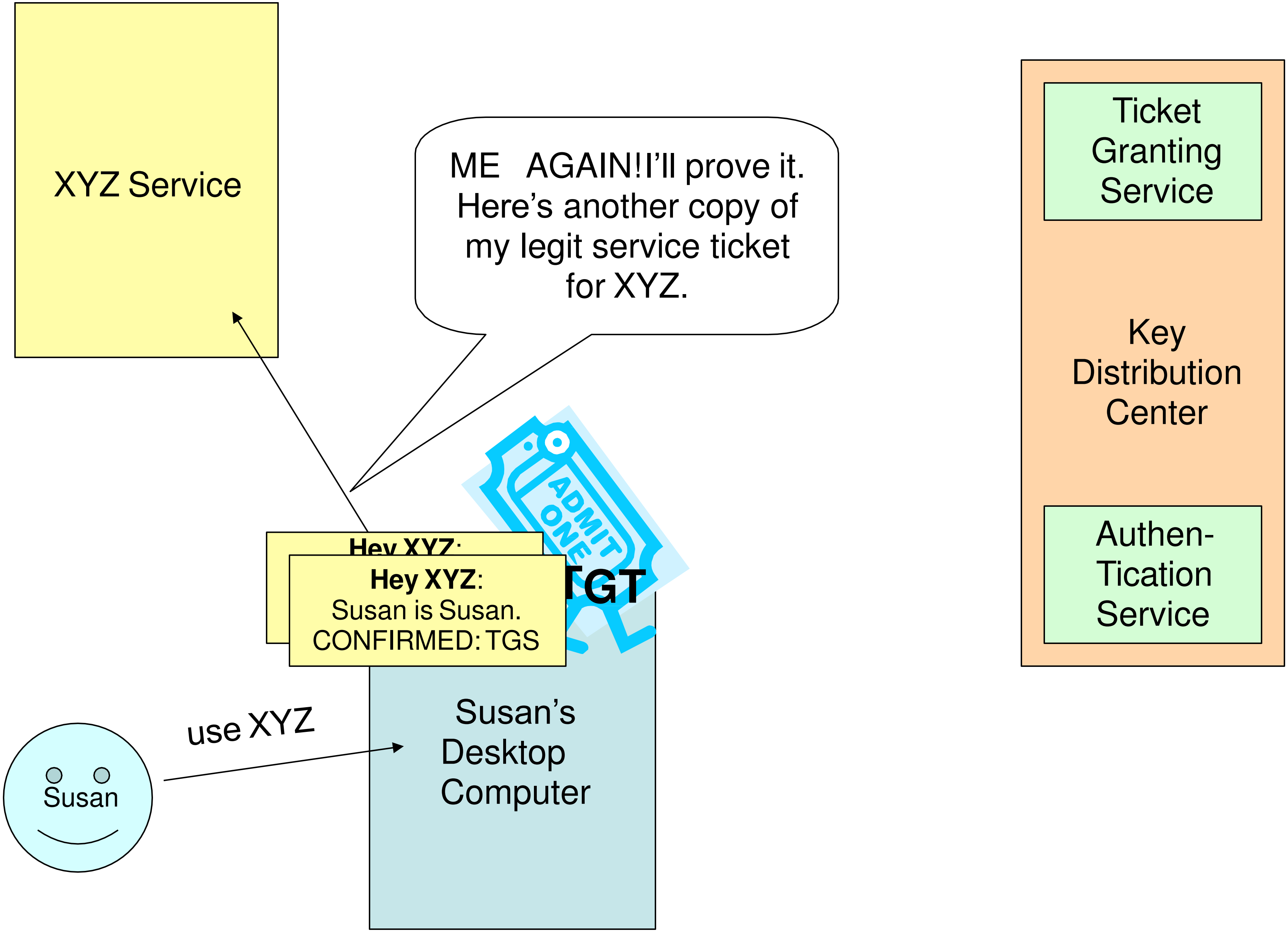
Hey XYZ:
Susan is Susan.
CONFIRMED: TGS

TGT

use XYZ

Susan

Susan's Desktop Computer



XYZ Service

ME AGAIN!I’ll prove it. Here’s another copy of my legit service ticket for XYZ.

Hey XYZ:

Hey XYZ:
Susan is Susan.
CONFIRMED: TGS

ADMIT ONE

TGT

use XYZ

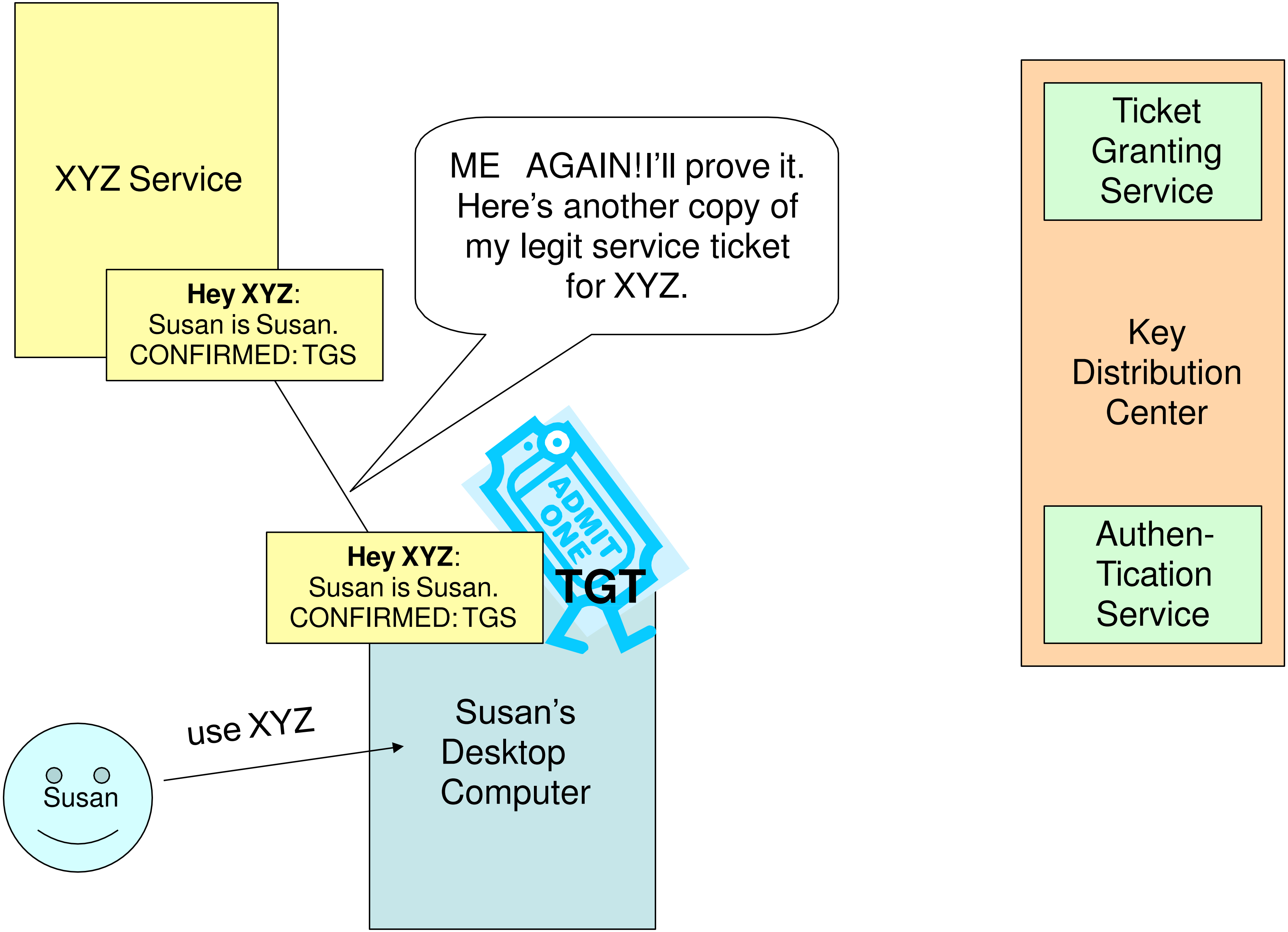
Susan

Susan’s Desktop Computer

Ticket Granting Service

Key Distribution Center

Authen-Tication Service



XYZ Service

Hey XYZ:
Susan is Susan.
CONFIRMED: TGS

ME AGAIN! I'll prove it. Here's another copy of my legit service ticket for XYZ.

Hey XYZ:
Susan is Susan.
CONFIRMED: TGS

use XYZ

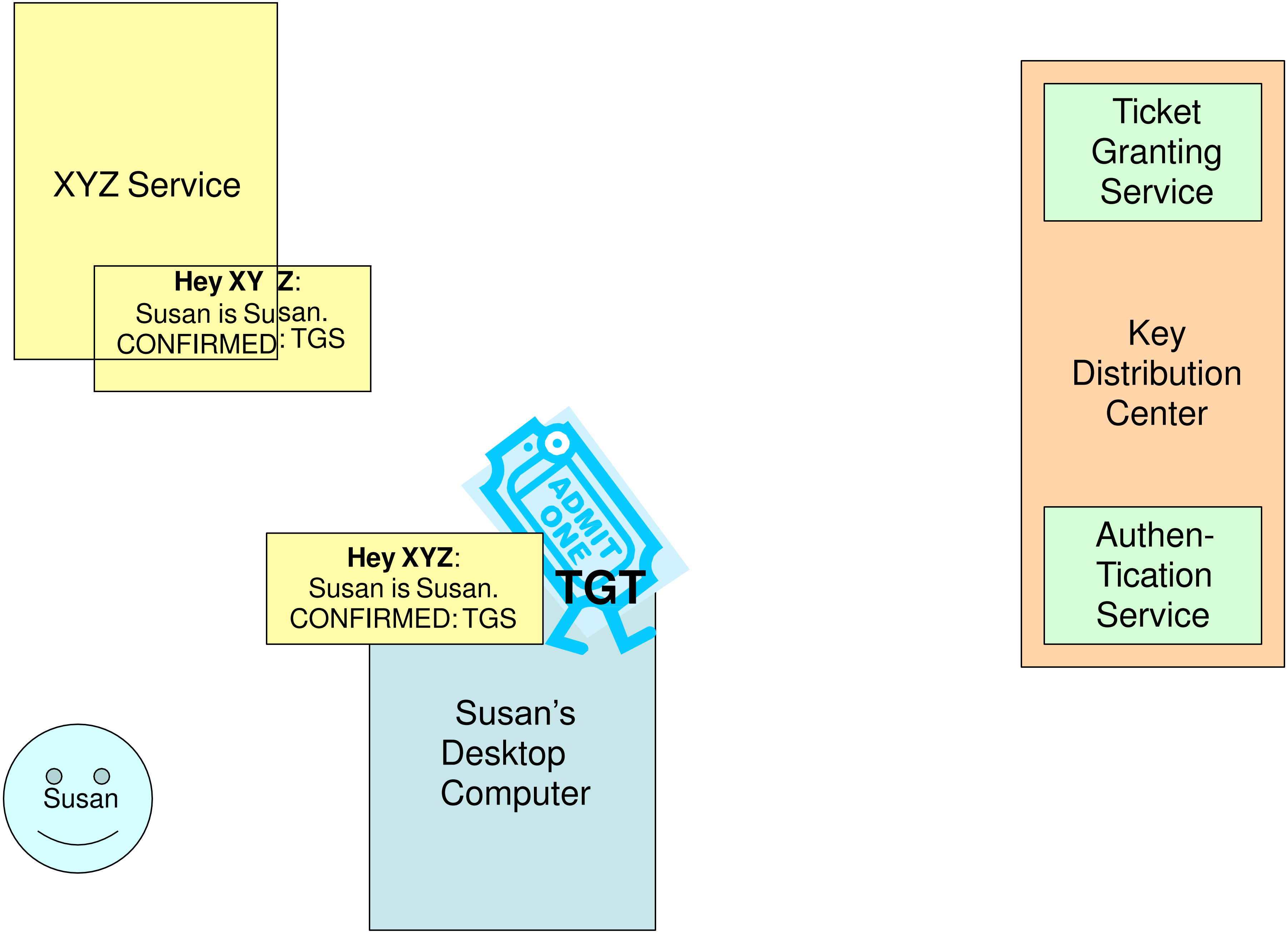
Susan

Susan's Desktop Computer

Key Distribution Center

Ticket Granting Service

Authen- Tication Service



XYZ Service

Hey XYZ:
Susan is Susan.
CONFIRMED: TGS

Hey XYZ:
Susan is Susan.
CONFIRMED: TGS

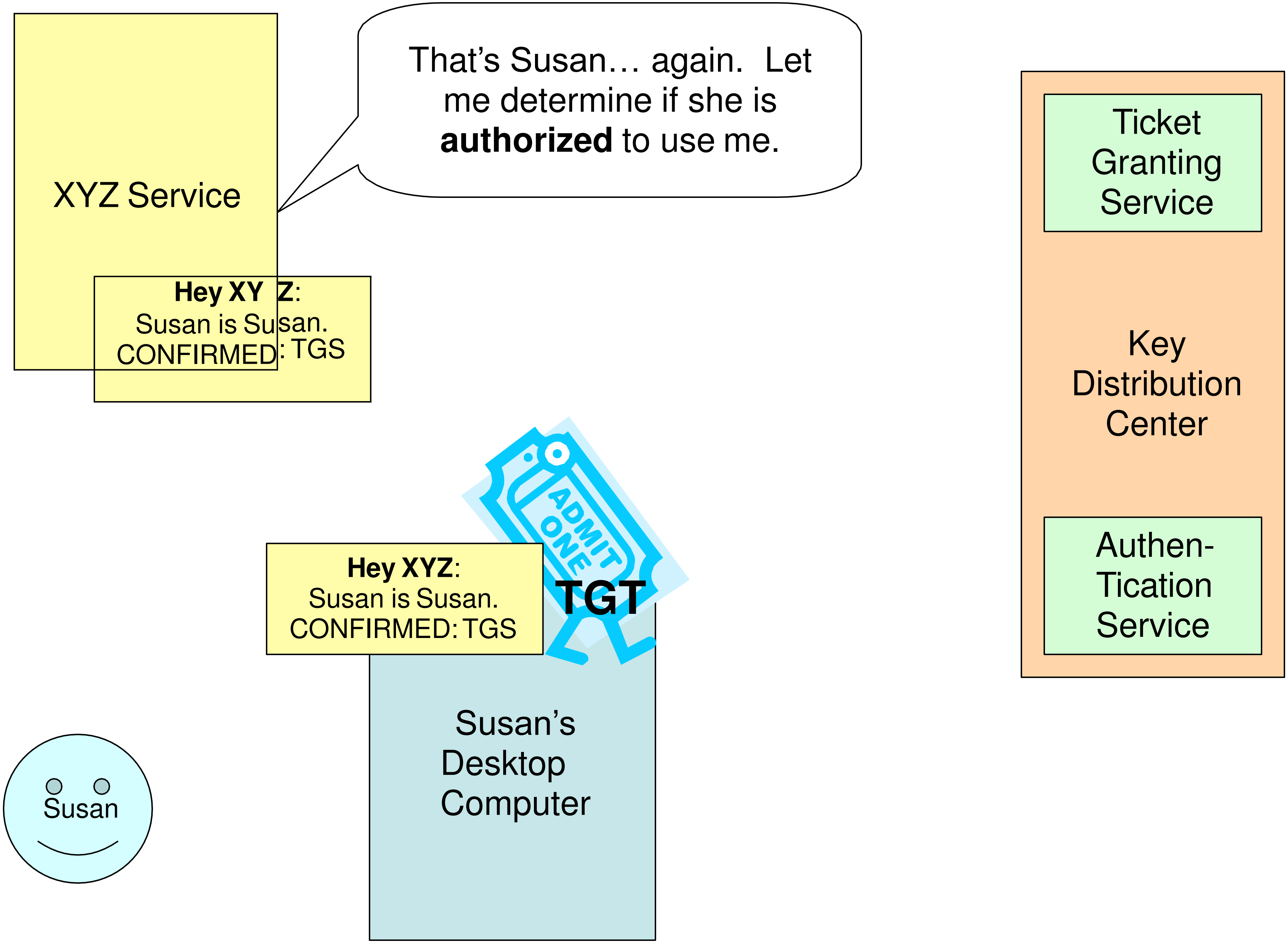
Susan

Susan's Desktop Computer

Ticket Granting Service

Key Distribution Center

Authen-Tication Service



That’s Susan… again. Let me determine if she is **authorized** to use me.

XYZ Service

Hey XYZ:
Susan is Susan.
CONFIRMED: TGS

Ticket Granting Service

Key Distribution Center

Authen-Tication Service

ADMIT ONE

TGT

Hey XYZ:
Susan is Susan.
CONFIRMED: TGS

Susan’s Desktop Computer

Susan

Further Reading

- An Introduction to Kerberos : http://www.upenn.edu/computing/pennkey/docs/kerbpres/200207Kerberos.htm
- MIT Kerberos Site : http://web.mit.edu/kerberos/
- The Moron's Guide to Kerberos : http://www.isi.edu/~brian/security/kerberos.html
- Kerberos: The Definitive Guide : http://www.oreilly.com/catalog/kerberos/cover.html