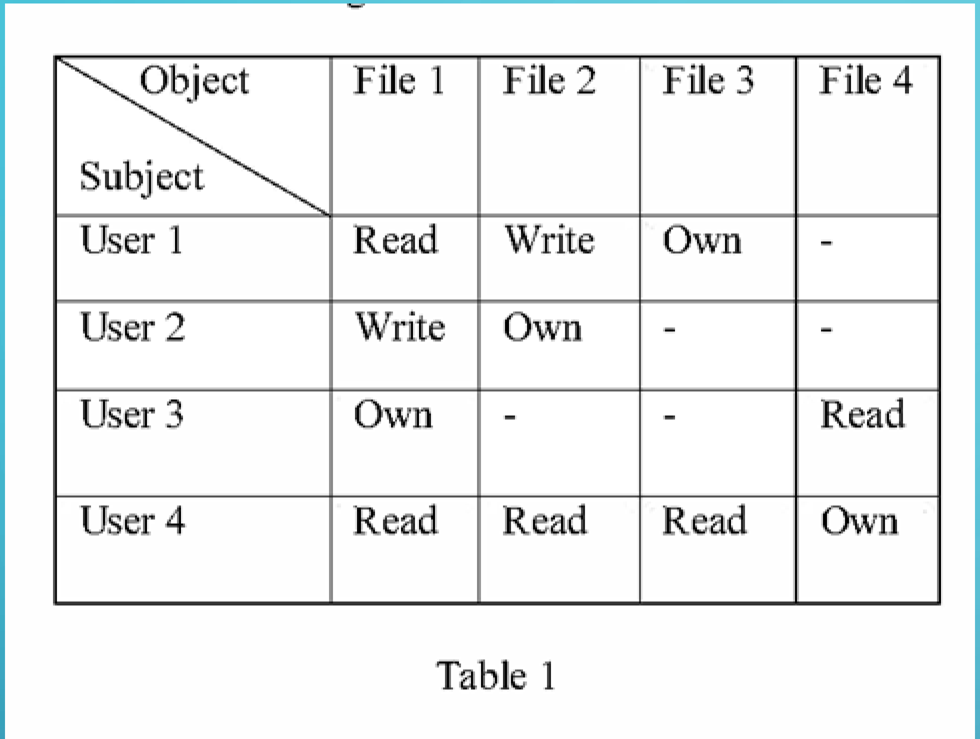
MULTI-FACTOR AUTHENTICATION AND AUTHENTICATION MECHANISMS

ACCESS CONTROL

Technique that regulates who can use what

ACCESS CONTROL MATRIX

Abstracting access control into a data structure



Object Subject	File 1	File 2	File 3	File 4
User 1	Read	Write	Own	-
User 2	Write	Own	-	-
User 3	Own	-	-	Read
User 4	Read	Read	Read	Own

Table 1

- ACM[U,O] -> What can the user access in object.
- ACLs.
- C-lists.

USER AUTHENTICATION

WHAT IS USER AUTHENTICATION?

- verifies the identity of a user attempting to gain access to a network or computing resource
- by authorizing a transfer of credentials during interactions on a network to confirm a user's authenticity
- is a method that keeps unauthorized users from accessing sensitive information

3 TASKS OF USER AUTHENTICATION

- Identification - Users have to prove who they are.
- Authentication - Users have to prove they are who they say they are.
- Authorization - Users have to prove they're allowed to do what they are trying to do.

AUTHENTICATION FACTOR

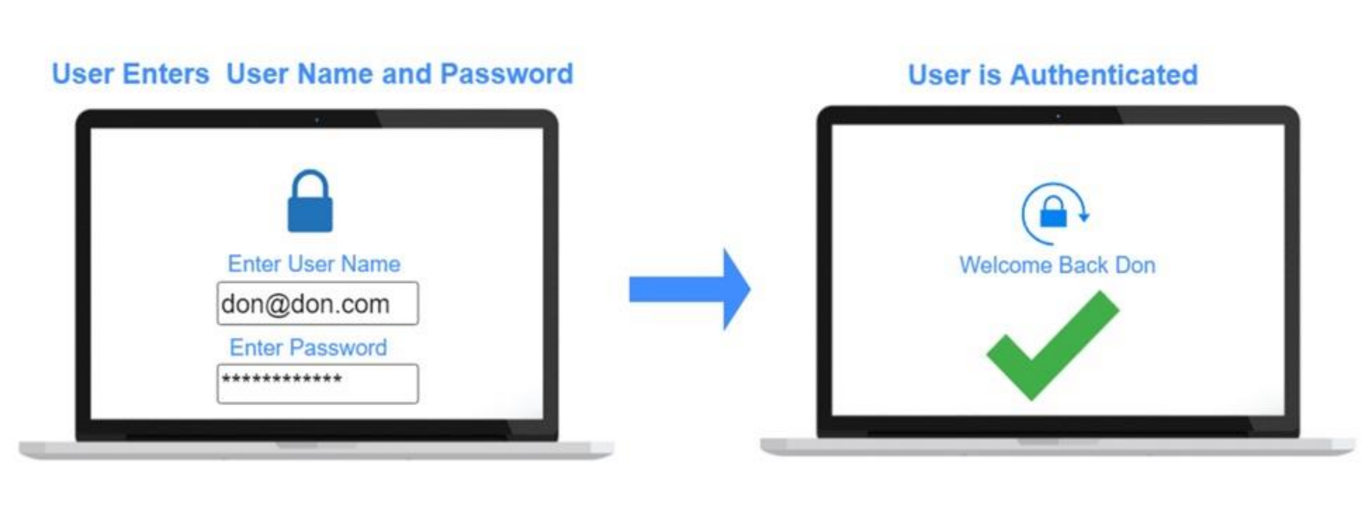
- special category of security credential that is used to verify the identity and authorization of a user attempting to gain access, send communications, or request data from a secured network

FIVE AUTHENTICATION FACTOR CATEGORIES

- Knowledge: Something the user knows, like username, password, or a PIN.
- Possession: Something the user has, like a safety token.
- Inherence : Something the user is, which can be demonstrated with fingerprint, retina verification, or voice recognition.
- Location: Based on the user's physical position.
- Time: A time-based window of opportunity to authenticate like OTP (TOTP)

SINGLE FACTOR AUTHENTICATION (SFA)

- is a method of logging users into resources by having them present only one way of verifying their identity
- Username and password is the dominant form of SFA



ADVANTAGES

- Ease of Use

convenience and simplicity are among the significant reasons this authentication method became so popular

- Cost of Implementation

simple and relatively straightforward to set into place

DISADVANTAGES

- Low Protection Levels

doesn’t offer solid and reliable security and main issue is that there’s only one authentication factor

- The Security is on the User

simpler the password, the easier the hackers can get in and

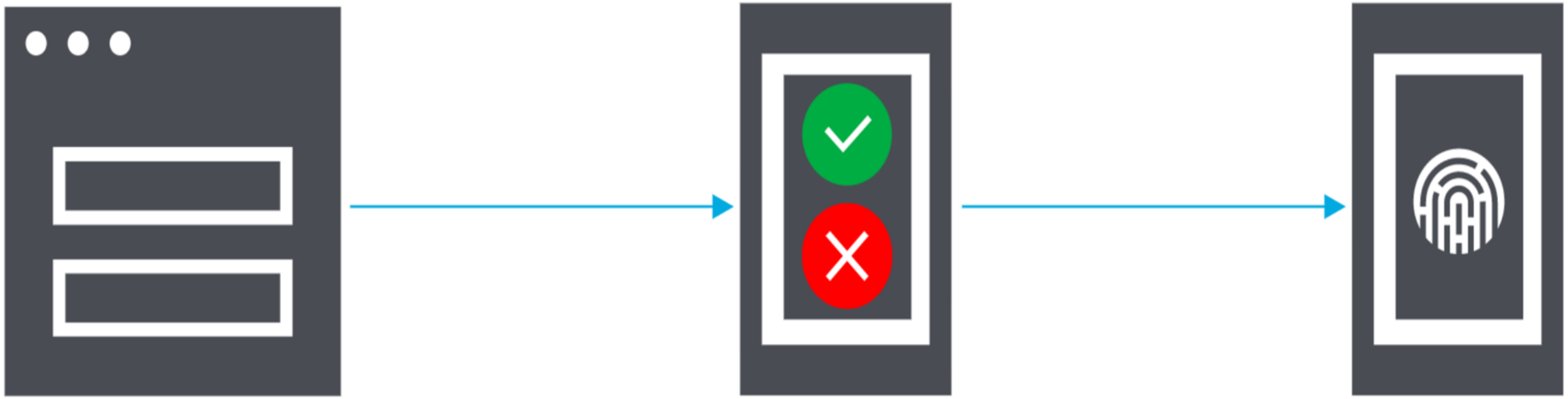
primary factor determining how secure his account will be, based on the strength of his password

MULTI-FACTOR AUTHENTICATION(MFA)

WHAT IS MFA ?

MULTI-FACTOR AUTHENTICATION (MFA) IS A SECURITY PROCESS THAT REQUIRES USERS TO RESPOND TO REQUESTS TO VERIFY THEIR IDENTITIES BEFORE THEY CAN ACCESS WEBSITES OR OTHER ONLINE APPLICATIONS.

IT IS AN AUTHENTICATION METHOD THAT REQUIRES THE USER TO **PROVIDE TWO OR MORE VERIFICATION FACTORS** TO GAIN ACCESS TO A RESOURCE.



Step 1: User name and password entered

Step 2: Pin from phone app entered

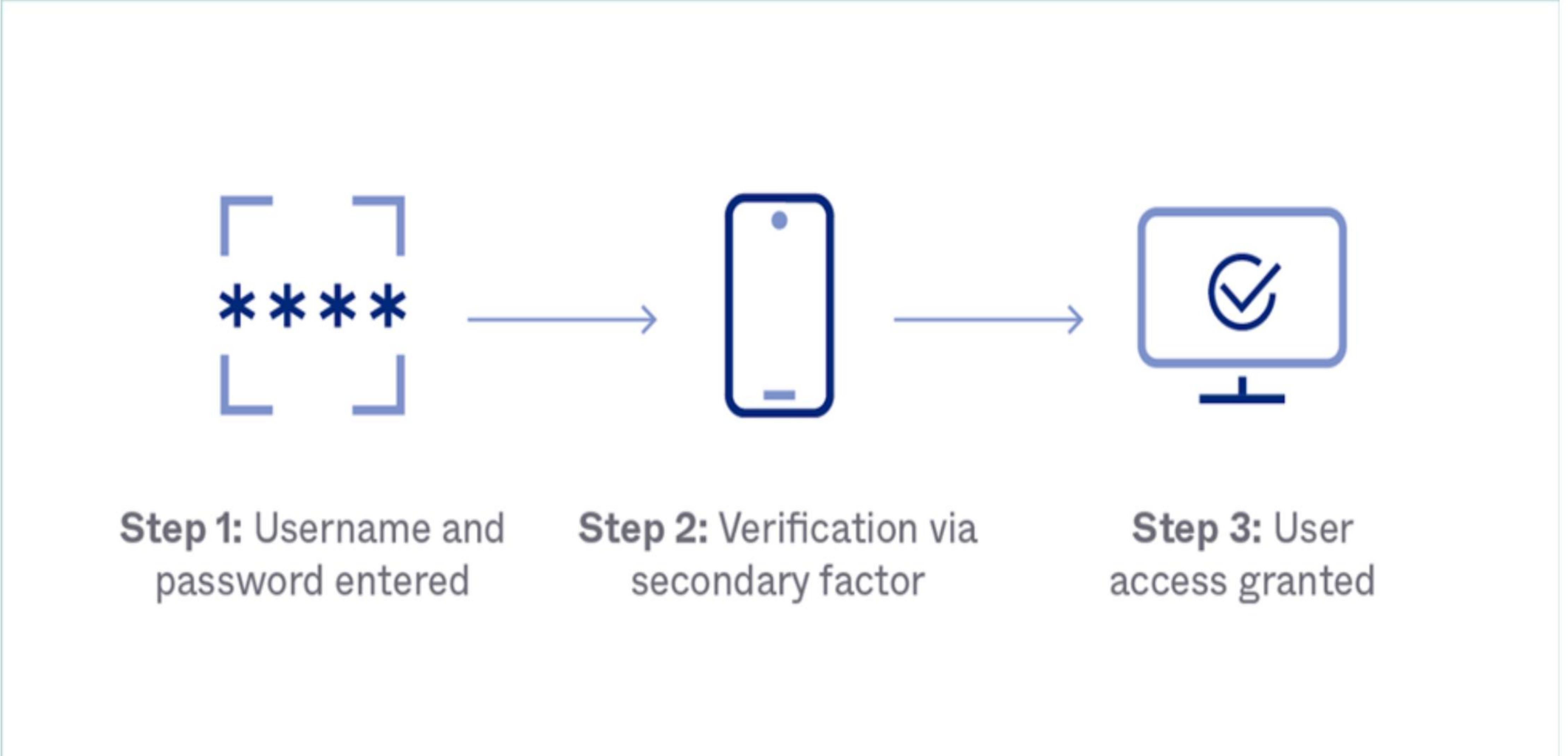
Step 3: Fingerprint verified

WHY MFA NEEDED ?

- DIGITAL WORLD - Reuse Passwords
- SINGLE FACTOR AUTHENTICATION IS UNRELIABLE
- PRONE TO VARIOUS ATTACKS

TWO FACTOR AUTHENTICATION [2FA]

- TWO-FACTOR AUTHENTICATION (2FA) IS A SPECIFIC TYPE OF MULTI-FACTOR AUTHENTICATION (MFA) THAT STRENGTHENS ACCESS SECURITY BY REQUIRING **TWO AUTHENTICATION FACTORS** TO VERIFY YOUR IDENTITY.
- THE **STANDARD 2FA** INCLUDES THE PROVISION OF USER CREDENTIALS (**KNOWLEDGE**) AND AN ONE-TIME AUTHENTICATION CODE VIA SMS (**POSSESSION**).
- PROTECTS AGAINST PASSWORD BRUTE-FORCE ATTACKS AND SECURES YOUR LOGINS AND DATA.



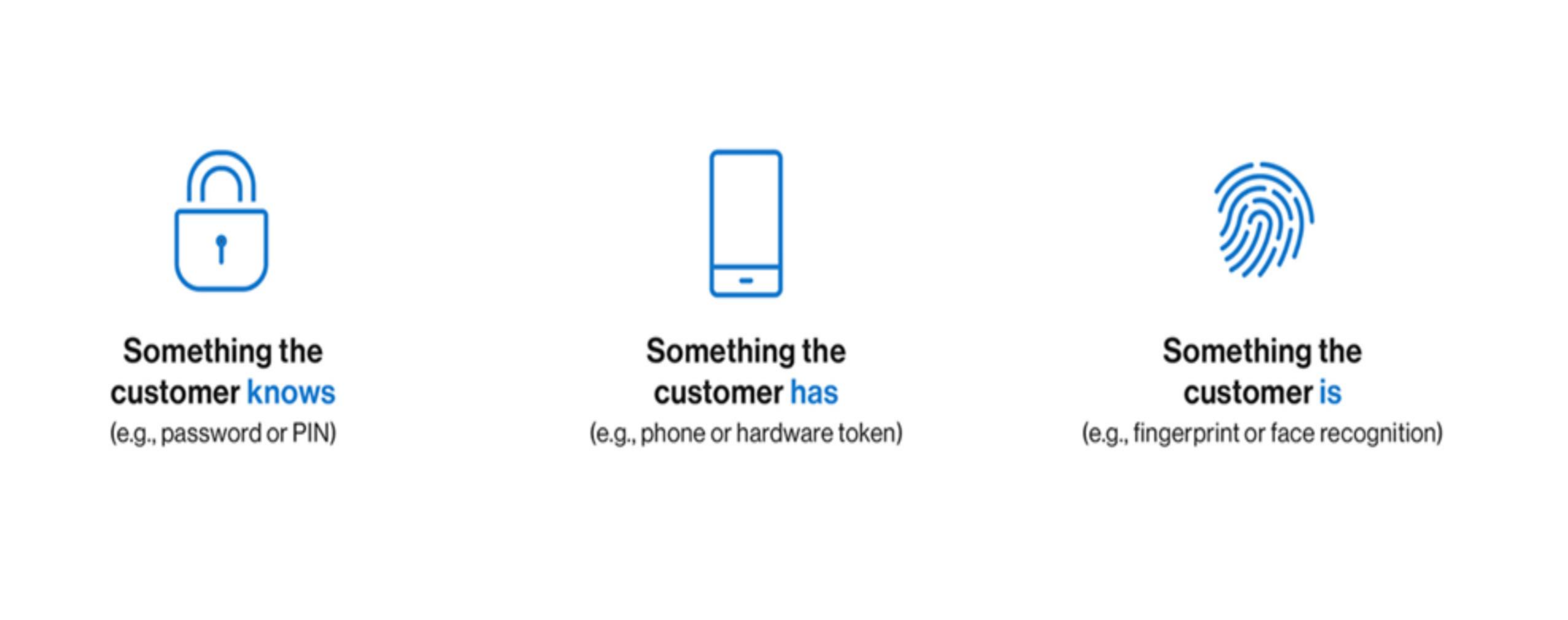
Step 1: Username and password entered

Step 2: Verification via secondary factor

Step 3: User access granted

THREE FACTOR AUTHENTICATION [3FA]

- **THREE LAYERS OF AUTHENTICATION FACTORS** TO VERIFY YOUR IDENTITY.
- 3FA = KNOWLEDGE(LOGIN DETAILS) + POSSESSION(OTP) + INHERENCE(BIOMETRICS)
- PROVIDES MORE SECURITY THAN 2FA



Something the customer knows

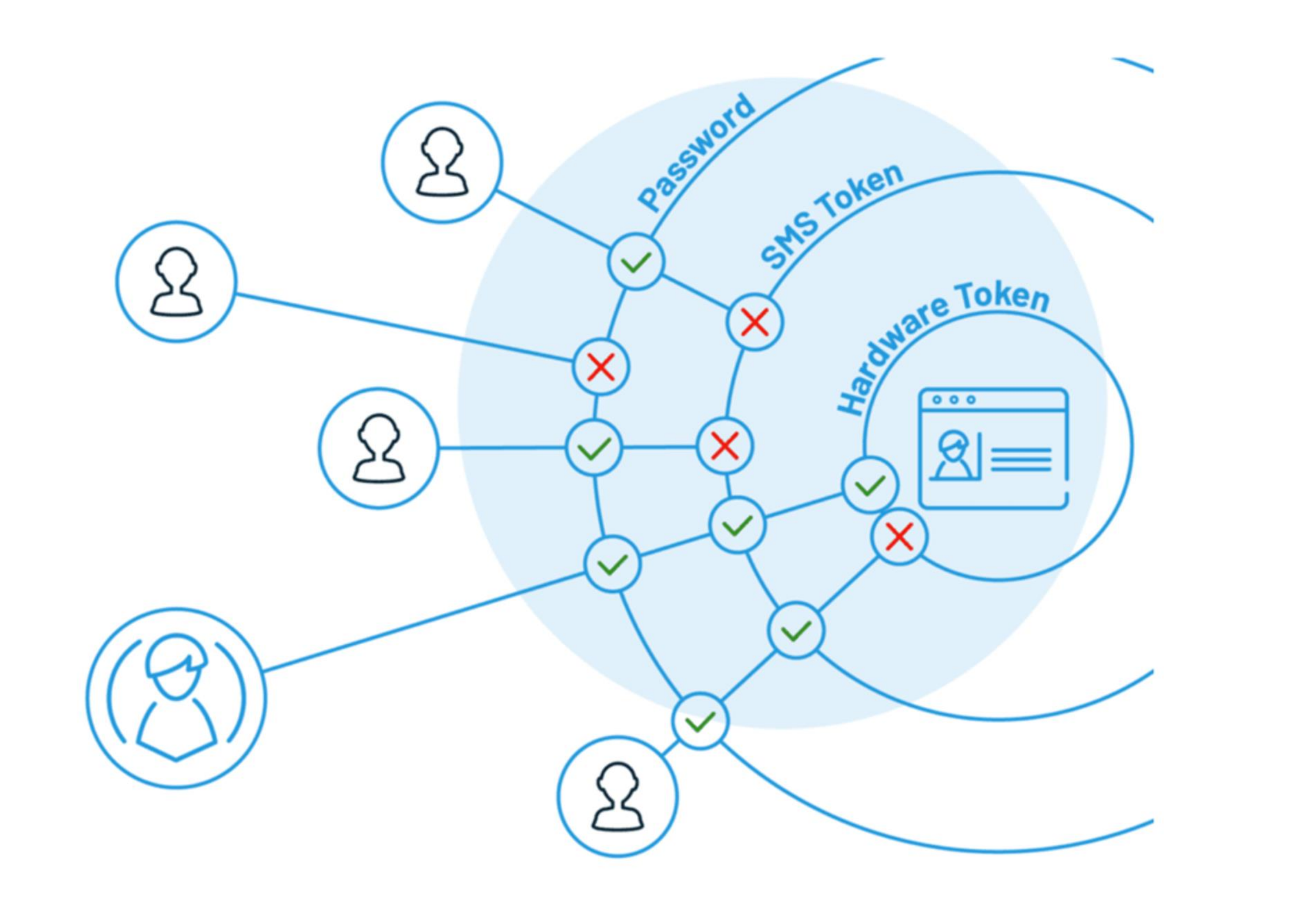
(e.g., password or PIN)

Something the customer has

(e.g., phone or hardware token)

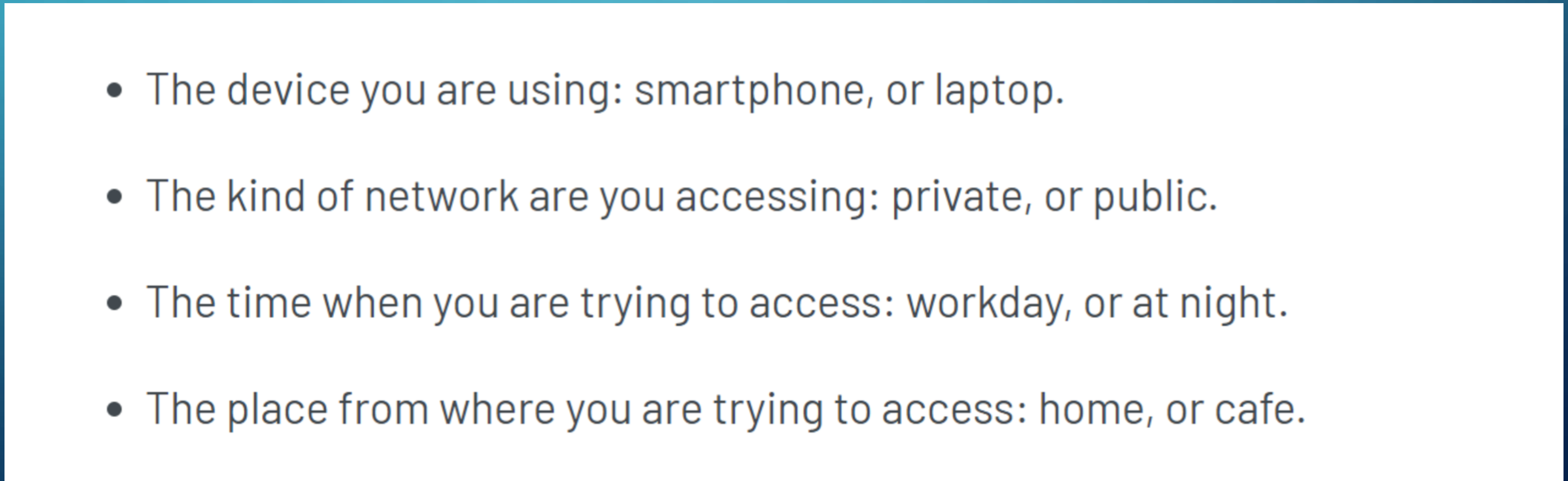
Something the customer is

(e.g., fingerprint or face recognition)

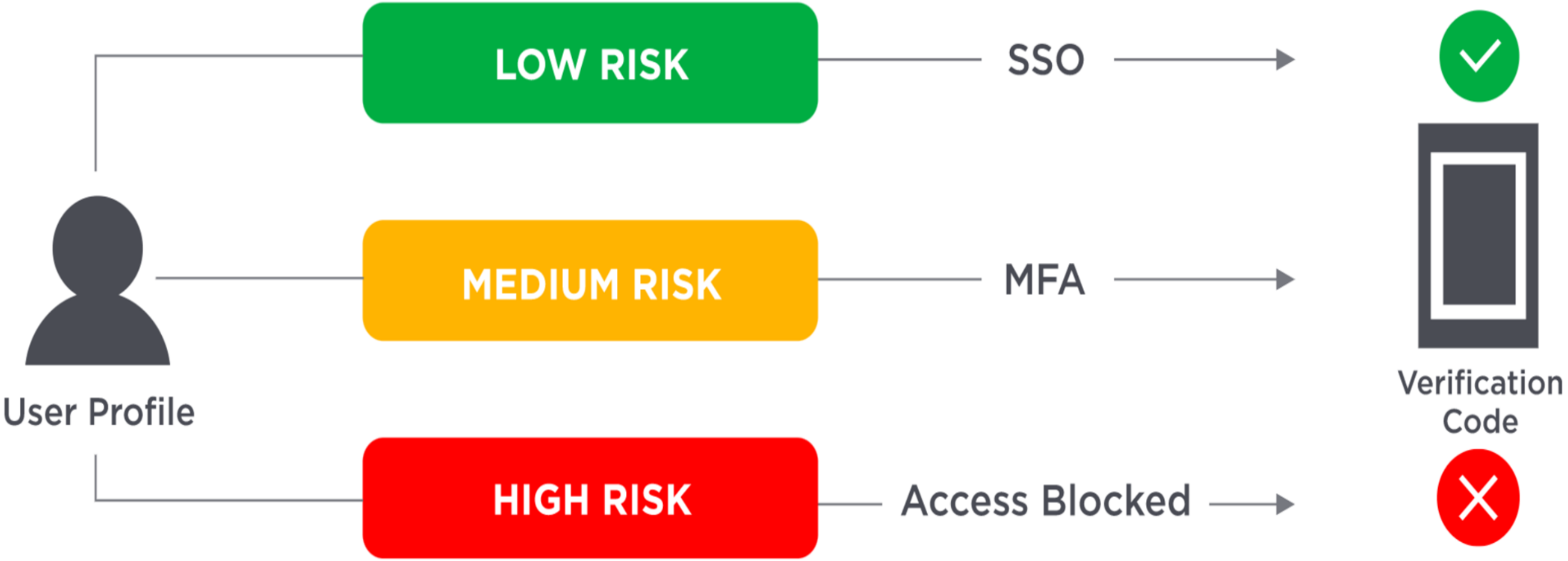

Password
SMS Token
Hardware Token

ADAPTIVE AUTHENTICATION

- ALSO REFERRED TO AS RISK-BASED AUTHENTICATION
- BY CONSIDERING CONTEXT AND BEHAVIOR WHEN AUTHENTICATING AND OFTEN USES THESE VALUES TO ASSIGN A LEVEL OF RISK ASSOCIATED WITH THE LOGIN ATTEMPT



- The device you are using: smartphone, or laptop.
- The kind of network are you accessing: private, or public.
- The time when you are trying to access: workday, or at night.
- The place from where you are trying to access: home, or cafe.



User Profile

LOW RISK

SSO

MEDIUM RISK

MFA

HIGH RISK

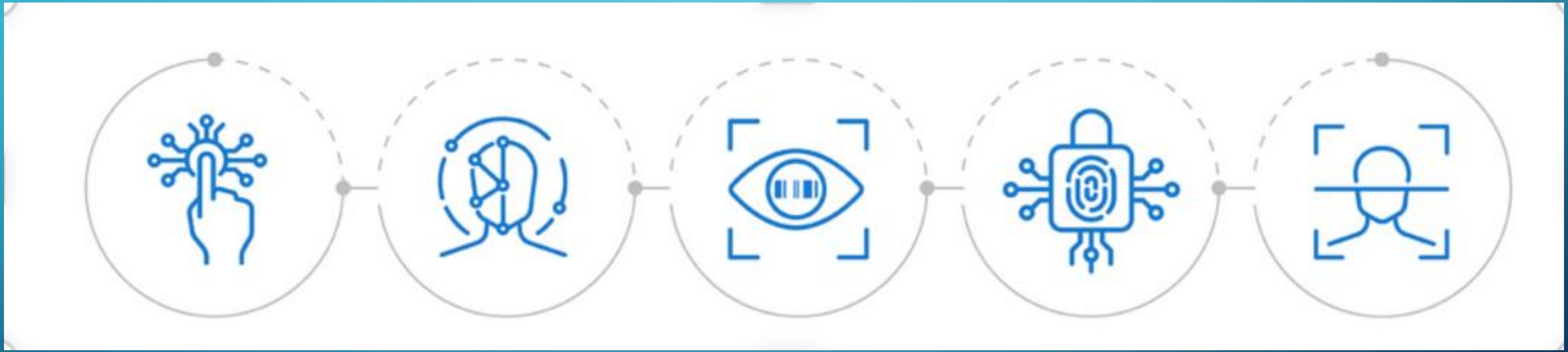
Access Blocked

Verification Code

BENEFITS OF MFA:

- BETTER SECURITY
- IMPROVED CUSTOMER TRUST
- INCREASED FLEXIBILITY

BUT STILL NOT 100% SECURE !



DIRECTORY SERVICE AUTHENTICATION

WHAT IS DIRECTORY SERVICE?

DS is an IT infrastructure for storing and mapping resource information that are accessed frequently on daily basis.

DS acts as a centralized database which stores resource information which are distributed across location.

DIRECTORY SERVICE AUTHENTICATION

Directory service Authentication (also called as authentication login domain) to provide a single sign-on for groups of users instead of maintaining individual local login accounts.

Each user in a group is assigned the same role (for example, Infrastructure administrator).

DIRECTORY AUTHENTICATION

Authentication is the process of validating users. During authentication, the server asks itself, “Is the user who he or she says they are?” Each DSA has one or more authentication levels. The authentication levels assigned to a DSA define what credentials a user must present to bind to and query that DSA.

DIRECTORY SUPPORTS THREE LEVELS OF AUTHENTICATION

- Anonymous authentication
- Clear-password authentication
- SSL authentication

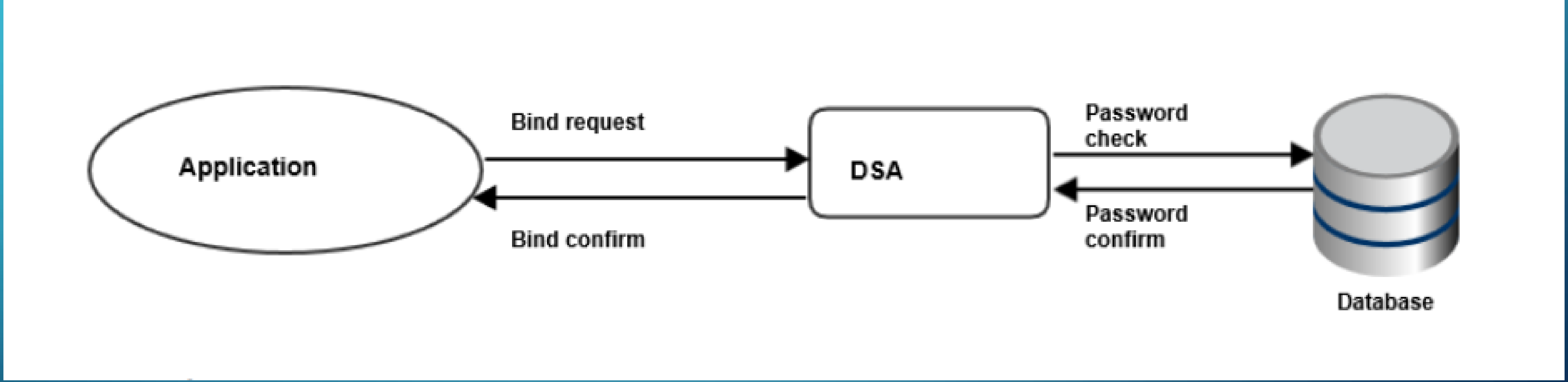
ANONYMOUS AUTHENTICATION

- Anonymous authentication lets users connect to a directory without providing credentials. This is useful for public directory services, because user identification is usually not important.

CLEAR –PASSWORD AUTHENTICATION

- Clear-password authentication allows users to connect or bind to a directory by providing a username and password.
- In password authentication, the user must supply a password for each server, and the administrator must keep track of the name and password for each user, typically on separate servers.

HOW A CONNECTION IS ESTABLISHED WITH CLEAR-PASSWORD AUTHENTICATION



AUTHENTICATION FAILS AND THE BIND IS REFUSED IN THE FOLLOWING CASES:

- The entry named by the user cannot be found.
- The entry named by the user name does not contain a password attribute.
- The password provided does not match the password value of the attribute in the entry named by the user name.

SSL AUTHENTICATION

Strong authentication uses SSL certificates to protect LDAP and X.500 access by encrypting data with Secure Sockets Layer (SSL) security. When certificate-based authentication is used, all communication on the binding set up by the bind use SSL encryption. SSL certificate based authentication is typically used in environments where personal or company data requires protection.

Example:

Online Banking Environment.

WHAT IS A CERTIFICATE? WHO ISSUE’S THE CERTIFICATE

A certificate provides generally recognized proof of someone's or something's identity.

CAs, validate identities and issue certificates.

CA binds a particular public key to the name of the entity the certificate identifies

It always includes the digital signature of the issuing CA

CONTENTS OF A CERTIFICATE:

Data Section:

- The certificate's serial number.
- Information about the user's public key
- The DN of the CA that issued the certificate.
- The period during which the certificate is valid (for example, between 11:00 a.m. on April 3, 2022 and 1:00 p.m. April 3, 20022).
- Subject name(user's DN).

Signature Section:

- The cryptographic algorithm, or cipher, used by the issuing CA to create its own digital signature.
- The CA's digital signature, obtained by hashing all of the data in the certificate together and encrypting it with the CA's private key.

SSL AUTHENTICATION HAS TWO PARTS:

- The SSL connection
- The directory connection (using a bind)

HOW AN SSL CONNECTION IS ESTABLISHED

1. The client sends a bind request, including a certificate.

2. DSA validates the connection request by checking the validity dates and checking the issuer of the certificate against the configured trusted roots.

3. If the certificate details are correct, the DSA establishes an SSL connection with the client application.

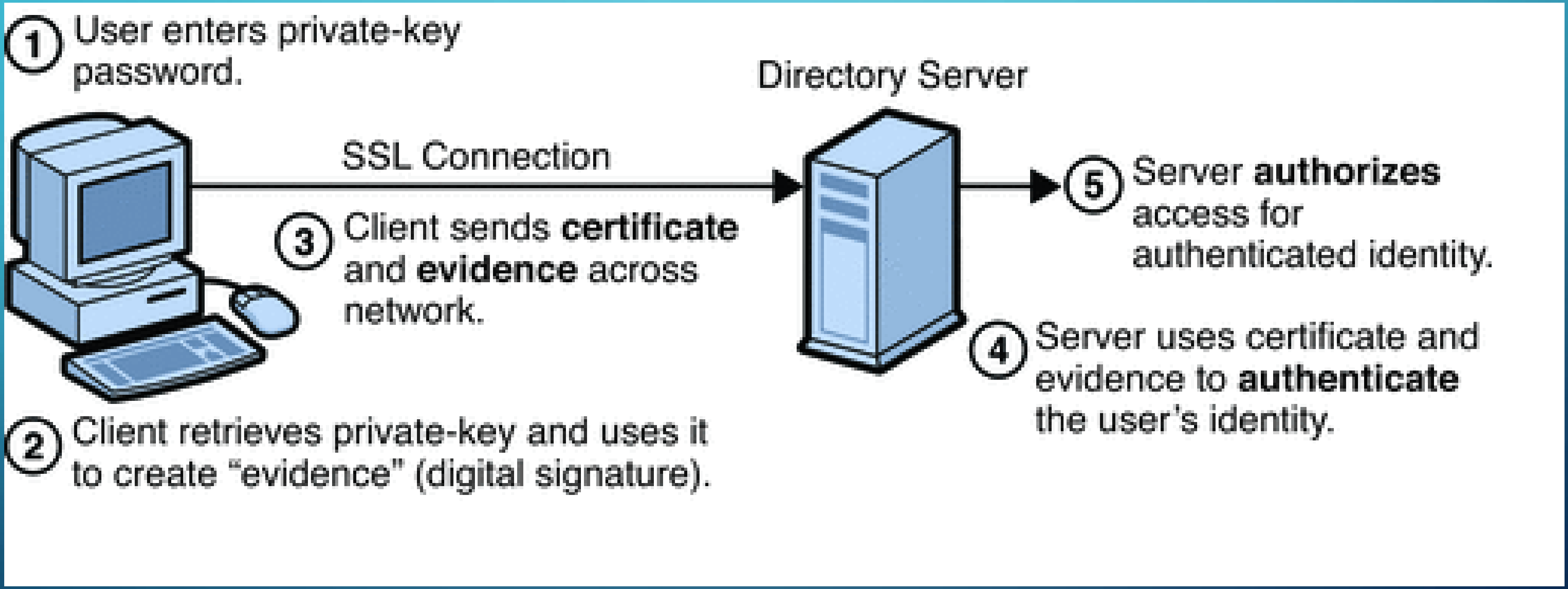
HOW A DIRECTORY CONNECTION IS ESTABLISHED:

1. The client sends a bind request to the directory.

2. The DSA checks the directory entry named by the subject DN contained in the certificate.

3. If the DN named in the subject DN of the certificate match those in the directory, then the DSA accepts the bind request.

ADAVANTAGES OF SSL AUTHENTICATION



1. User enters private-key password.

2. Client retrieves private-key and uses it to create "evidence" (digital signature).

3. Client sends **certificate** and **evidence** across network.

4. Server uses certificate and evidence to **authenticate** the user's identity.

5. Server **authorizes** access for authenticated identity.