ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

Passwordless

Sicurezza dell'Informazione

Nicolò Romandini

Post-doc @ DISI

nicolo.romandini@unibo.it

User Authentication

In most computer security contexts, user authentication is the fundamental building block and the primary line of defense

Identification step: Presenting an identifier to the security system (Identifiers should be assigned carefully, because authenticated identities are the basis for other security services, such as access control service)

Verification step: Presenting or generating authentication information that corroborates the binding between the entity and the identifier

Means of User Authentication

Something the individual knows (password and PIN)

Something the individual has (cryptographic keys, smart cards, and electronic/physical keys)

Something the individual is (recognition by fingerprint, retina, and face)

Something the individual does (recognition by voice pattern, handwriting characteristics, and typing rhythm)

Protocol Categories

Passive: Password

Active:

- One-time password
- Challenge/response
- Zero knowledge

Password-based Authentication

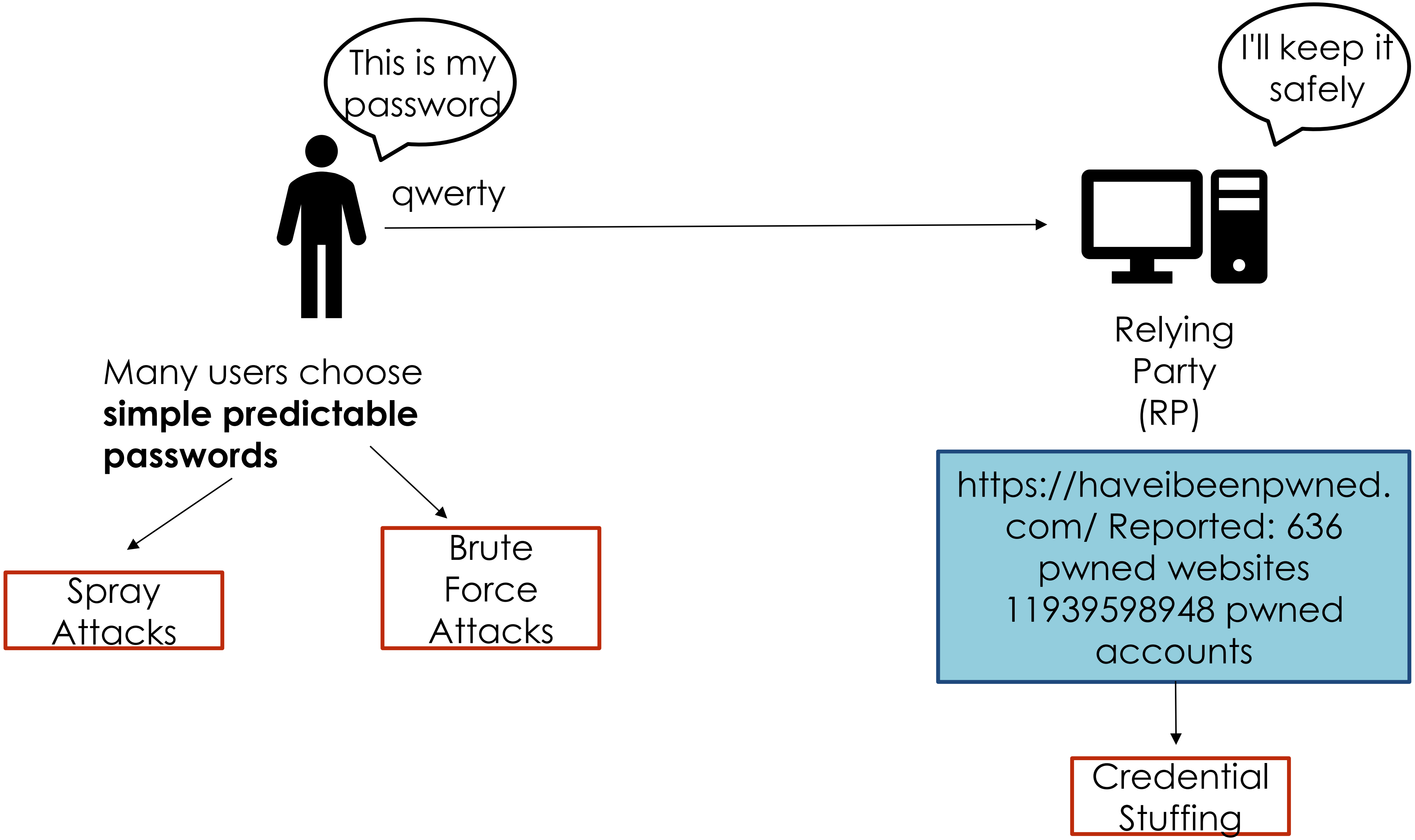
Passwords are the most common methods of authentication

- An average person has about 25 different online accounts, but only 54% of users use different passwords across accounts
- Many people choose convenience over security
- For developers, the complexity of passing those passwords securely through systems and storing them securely in hacker-proofed databases is a burdensome overhead

How to Choose a Good Password

- Do not use personal information
- Do not use made of characters that are close on the keyboard
- Use different kinds of characters
- Do not rely on simple manipulation (substitute letter with a number)
- Do not use password too short
- Update passwords periodically

Passwords Are Shared Secrets



This is my password

qwerty

I'll keep it safely

Relying Party (RP)

Many users choose **simple predictable passwords**

Spray Attacks

Brute Force Attacks

https://haveibeenpwned.com/ Reported: 636 pwned websites 11939598948 pwned accounts

Credential Stuffing

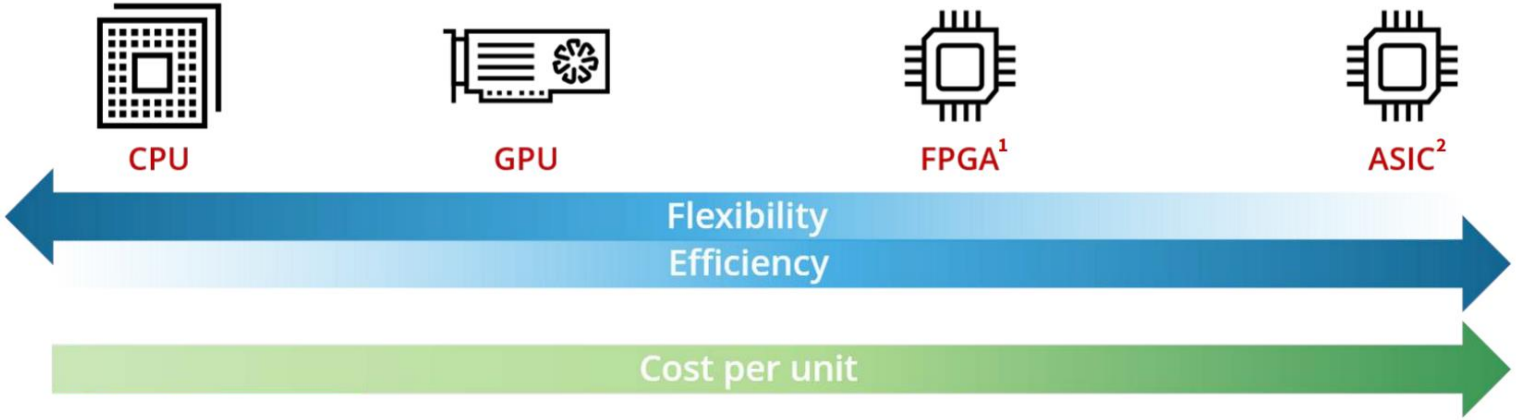
Dictionary and Brute-forcing

- Dictionary attacks check each word in a wordlist:
  - Smaller search-space
  - Require a wordlist quite complete

- Brute force attacks try every possible combination:
  - Bigger search-space
  - It may never end

How to Perform an Attack

- In real-world scenarios, these attacks may require days/weeks/months to provide some useful results
- Hardware resources play a key role
- Nowadays, credentials cracking can be optimized by running many instances in parallel



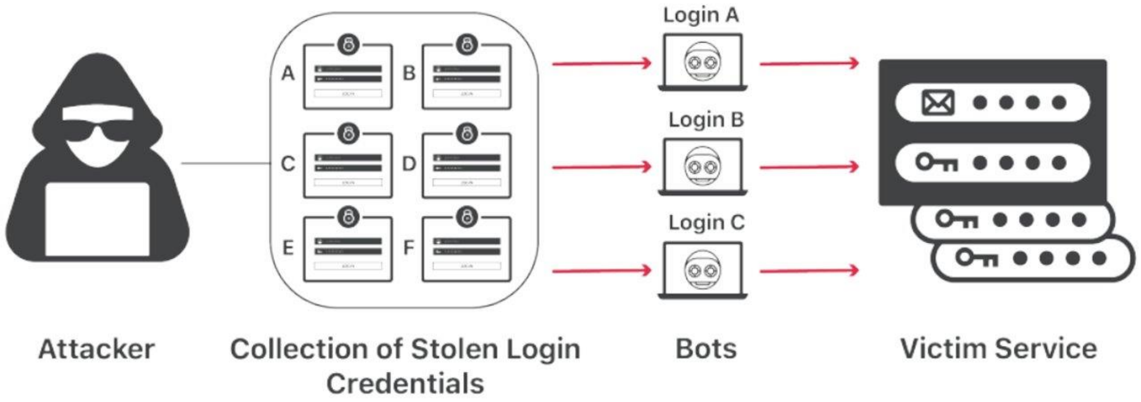
Protecting Credentials from Exposure (1/2)

- Passwords must be safely protected by online services

⚠ **Once an attacker gains access to the user database, all the user account can be easily compromised**

- Attackers also leverage **password reuse attacks** or **credential stuffing**

Same password for multiple services, what if it is leaked?



Protecting Credentials from Exposure (2/2)

- Leaked user data are usually sold on the dark web

Let's check if your account credentials have been leaked: https://haveibeenpwned.com/

- Due to the European General Data Protection Regulation (GDPR), companies that do not properly protect user data can be charged high fines!

Challenges

Educating users about password security is difficult

- **Multi-factor Authentication** (MFA) provides an extra layer of protection that eliminates 99.9% of sign-ins with compromised password succeding
  - In most cases, simple SMS MFA will be sufficient
  - Use simple solutions such as an authenticator app that sends push notifications
  - For high valuable accounts go for alternatives

How Do We Eliminate Passwords Being Compromised?

Eliminate shared secrets!!!

Towards Passwordless

Passwordless-authentication methods aim at overcoming these problems

- A user can log in to a system without providing any password or any other shared secret
- In most common implementations users enter a public identifier and then provide secure proof of identity through a registered device or token

Benefits and Drawbacks

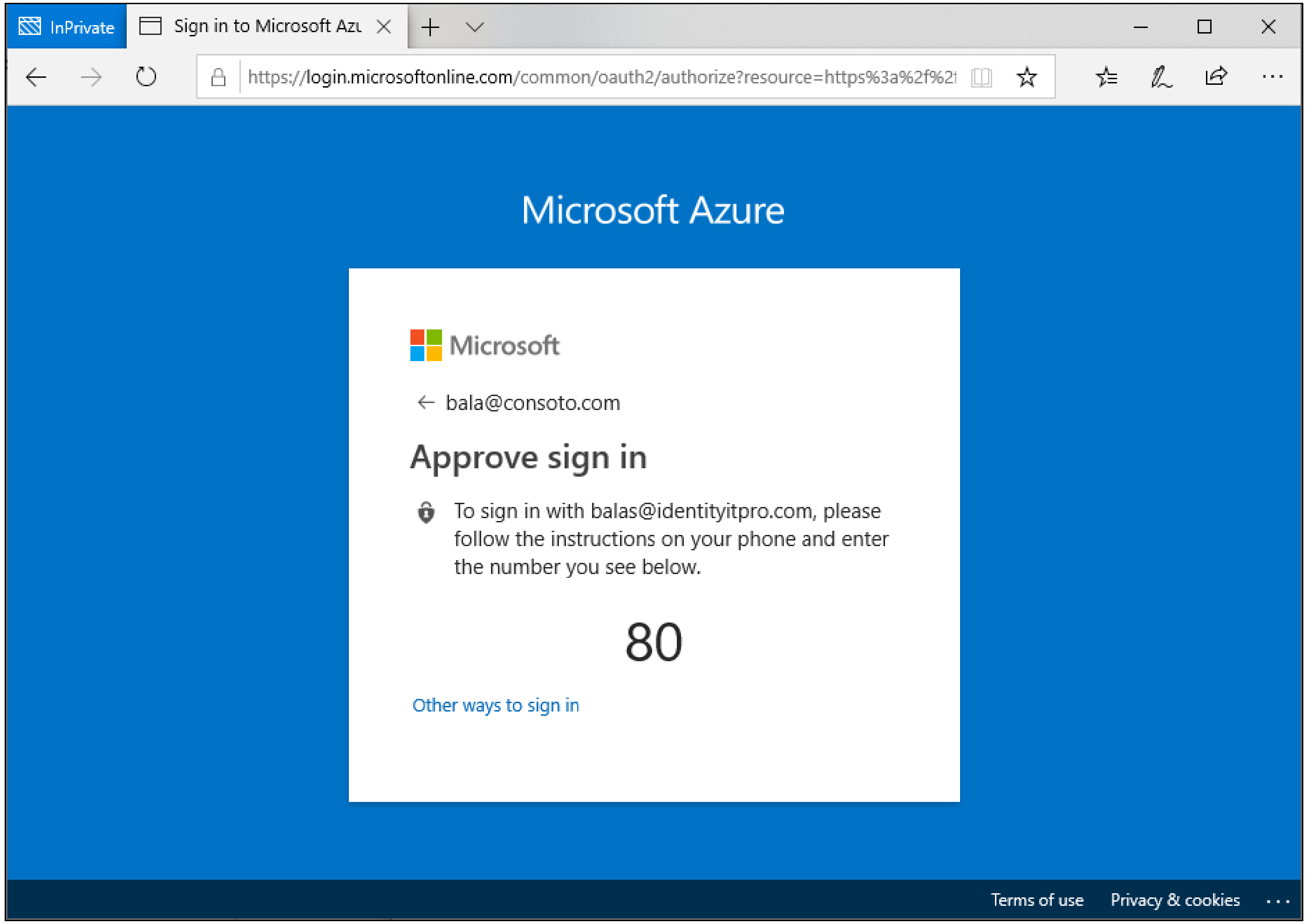
✓

- Greater security
- Better user experience
- Reduced IT costs
- Better visibility of credential usage

✗

- Implementation costs
- Training and expertise needed
- Single point of failure

Azure AD Passwordless Sign-in



InPrivate
Sign in to Microsoft Azu
https://login.microsoftonline.com/common/oauth2/authorize?resource=https%3a%2f%2f

Microsoft Azure

Microsoft

← bala@consoto.com

Approve sign in

To sign in with balas@identityitpro.com, please follow the instructions on your phone and enter the number you see below.

80

Other ways to sign in

Terms of use
Privacy & cookies
...

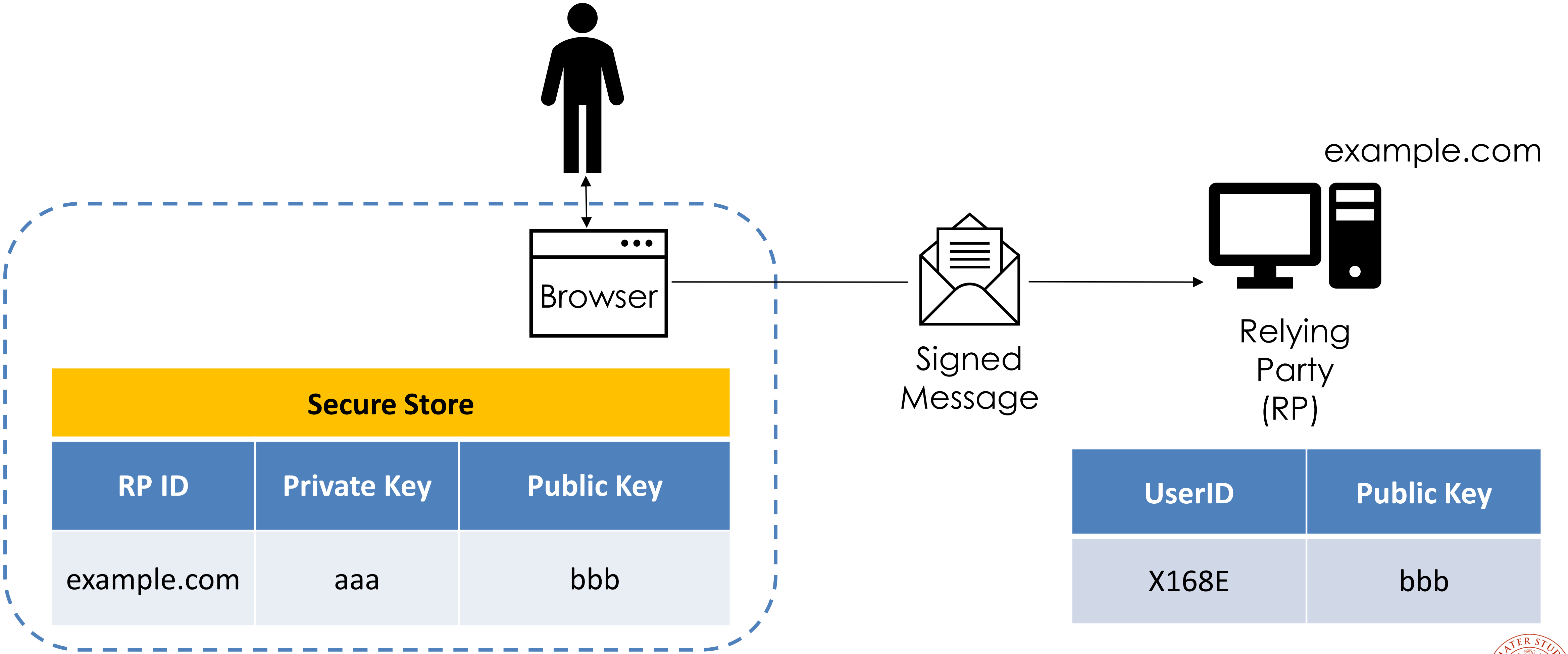
Standards for Being Scalable

- Fast IDentity Online (FIDO) Alliance founded in 2012, its mission was to create a passwordless authentication protocol

- In 2014, two passwordless protocols were published:
  - FIDO Universal Authentication Framework (FIDO UAF)
  - FIDO Universal 2nd Factor (FIDO U2F)

- In 2019, FIDO2 core Web Authentication protocol (WebAuthN) was adopted by the World Wide Web Consortium (W3C) as an Internet standard

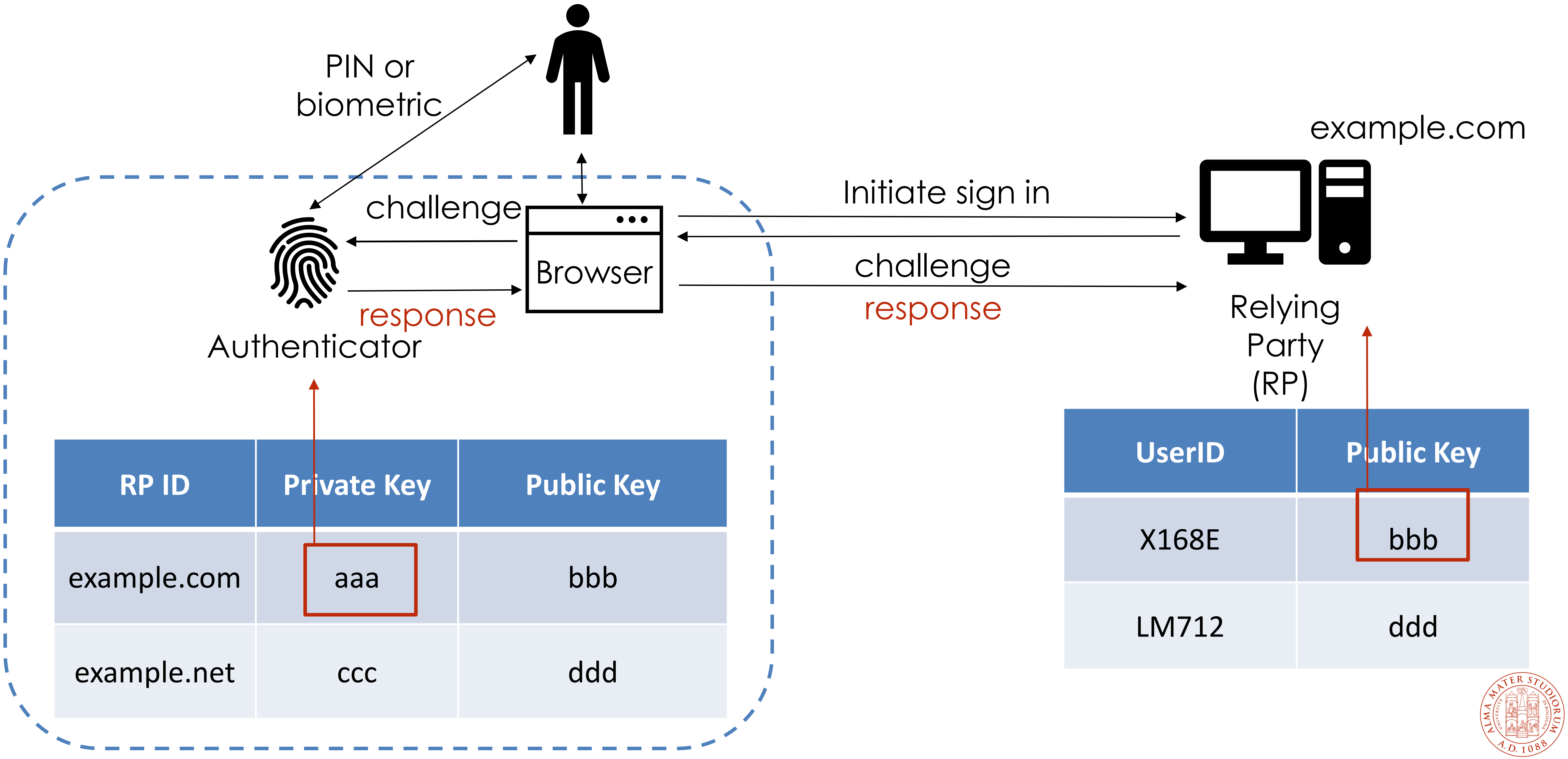
Use Asymmetric Encryption



Secure Store		
RP ID	**Private Key**	**Public Key**
example.com	aaa	bbb

UserID	Public Key
X168E	bbb

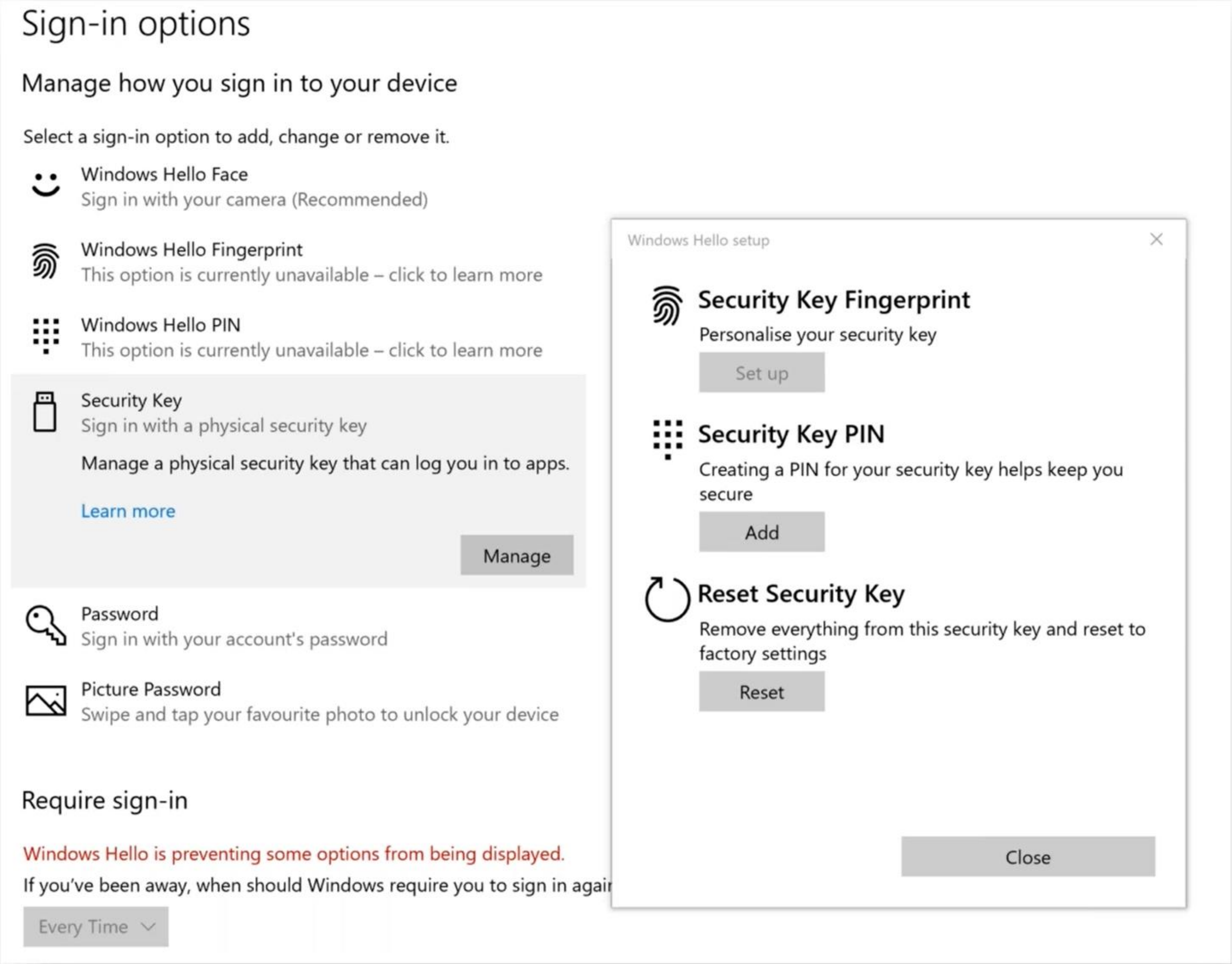
FIDO2 Authentication



RP ID	Private Key	Public Key
example.com	aaa	bbb
example.net	ccc	ddd

UserID	Public Key
X168E	bbb
LM712	ddd

Setting Up FIDO Security Key with Windows



Sign-in options

Manage how you sign in to your device

Select a sign-in option to add, change or remove it.

Windows Hello Face
Sign in with your camera (Recommended)

Windows Hello Fingerprint
This option is currently unavailable – click to learn more

Windows Hello PIN
This option is currently unavailable – click to learn more

Security Key
Sign in with a physical security key

Manage a physical security key that can log you in to apps.

Learn more

Manage

Password
Sign in with your account's password

Picture Password
Swipe and tap your favourite photo to unlock your device

Require sign-in

Windows Hello is preventing some options from being displayed.

If you've been away, when should Windows require you to sign in agai

Every Time

Windows Hello setup

Security Key Fingerprint
Personalise your security key

Set up

Security Key PIN
Creating a PIN for your security key helps keep you secure

Add

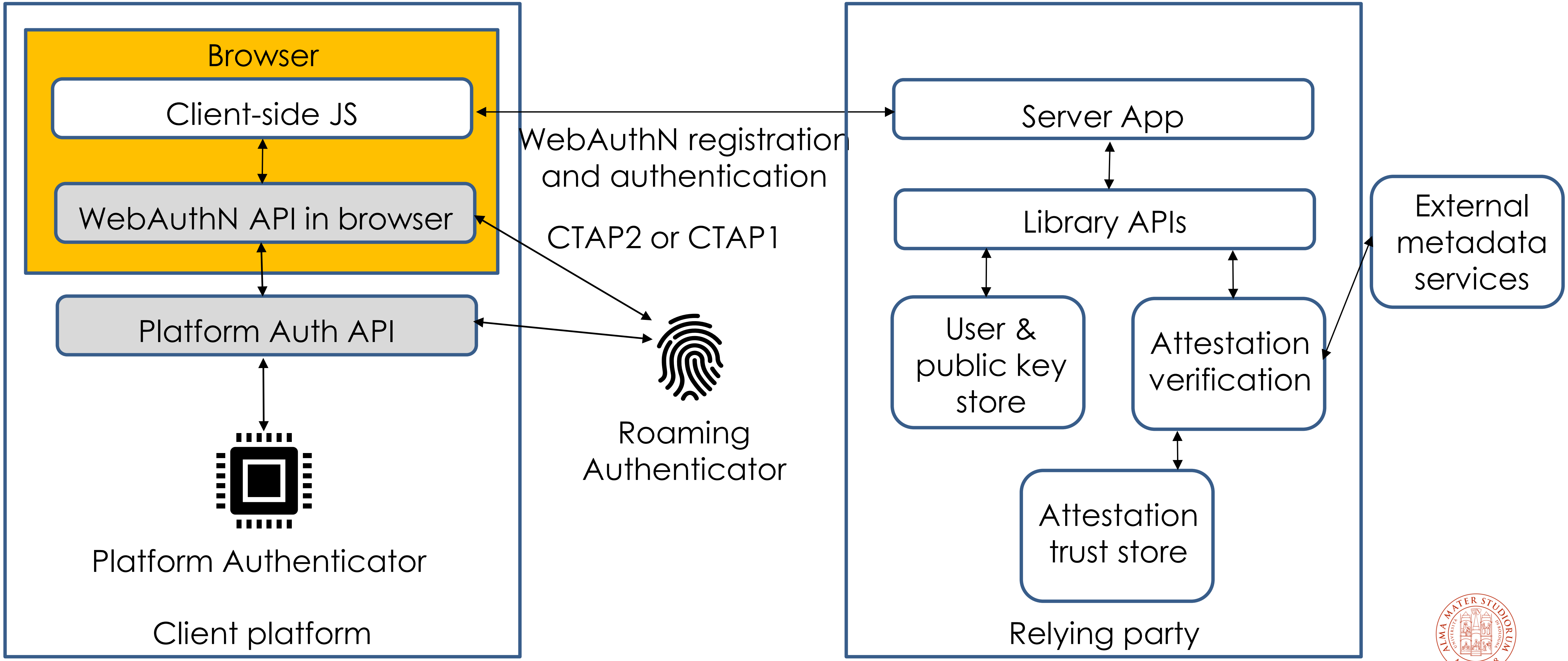
Reset Security Key
Remove everything from this security key and reset to factory settings

Reset

Close

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

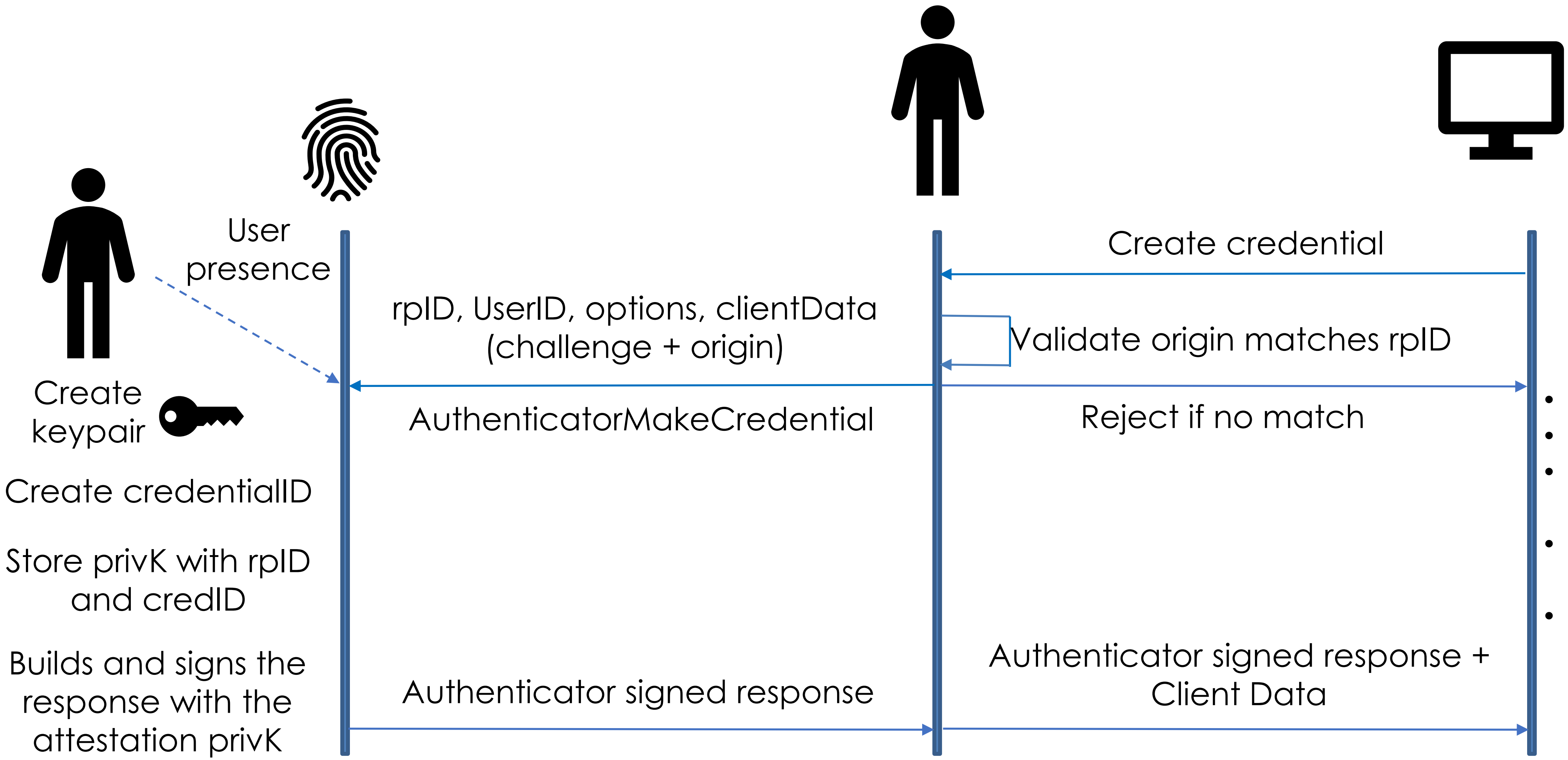
FIDO2 Components and Protocol



Registration Ceremony Parameters

- **Challenge**: random string of bytes, used to prevent replay attacks
- **rpID**: identifies the RP's domain (e.g, example.com)
- **User**: randomly generated id that is used to associate a credential with a user
- **PubKeyCredParams**: types of public keys that are acceptable to the RP
- **AuthenticatorSelection**:
  - The type of authenticator (roaming or platform)
  - If the authenticator private key should be residential
  - If user verification is required, preferred or discouraged
- **Timeout**: the user is required to respond within this time; otherwise, an error occurs
- **Attestation**: allows the RP to specify if attestation data is required. It enables the RP to verify the veracity and the security of the authenticator being used

Registration Ceremony



User presence

Create keypair

Create credentialID

Store privK with rpID and credID

Builds and signs the response with the attestation privK

Create credential

rpID, UserID, options, clientData (challenge + origin)

Validate origin matches rpID

AuthenticatorMakeCredential

Reject if no match

Authenticator signed response

Authenticator signed response + Client Data

- Verify origin
- Verify challenge
- Verify attestation signature
- Verify attestation root trust
- Store userID, credID and pubK

Attestation Metadata

- Fido Alliance Metadata Service (MDS)
  - Authenticator vendors can provide information about authenticators
  - Provides characteristics and capabilities of a particular authenticator
  - Allows risk-based decisions to be made about a particular authenticator

- Authenticators are identified by an Authenticator Attestation GUID (AAGUID)

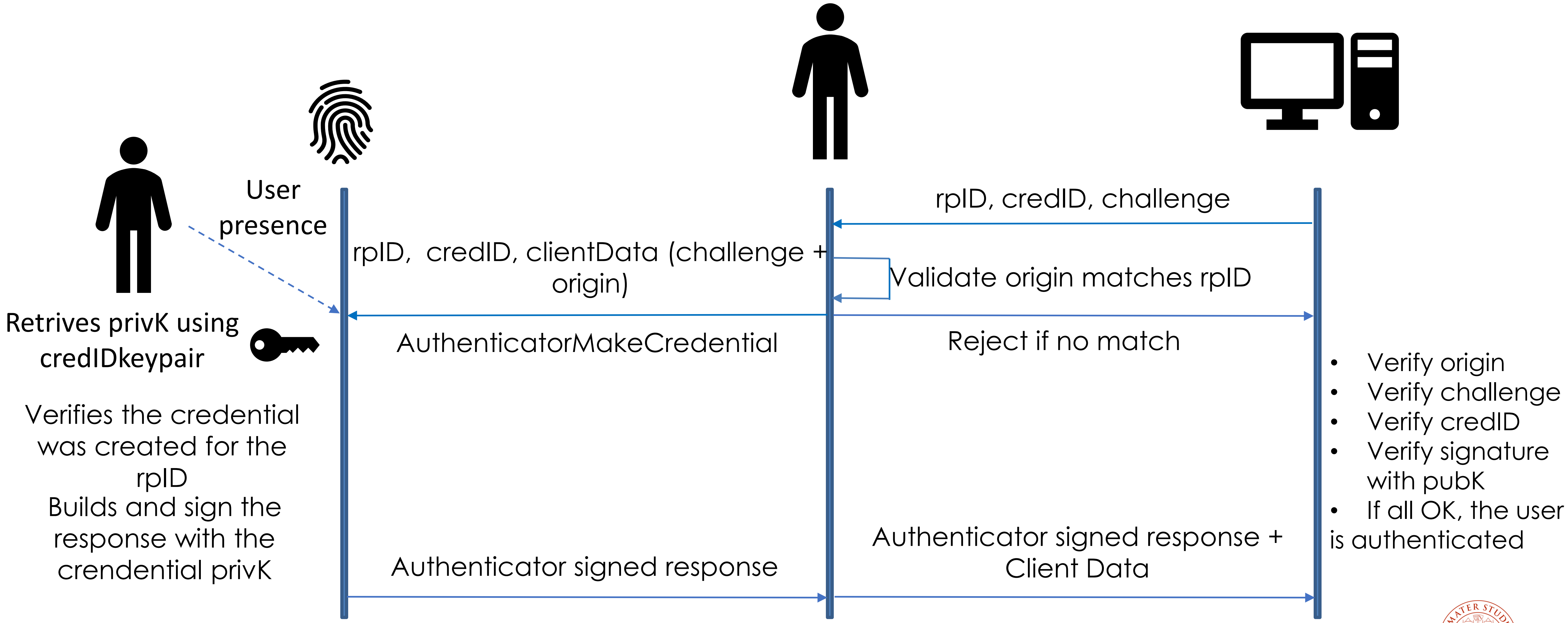
- During registration, the authenticator signs the response with an attestation private key embedded in the device

Identifying the User

- Registration includes binding a FIDO credential on a given authenticator to a specific user
  - Trust on First Use (TOFU)
  - Invitation
  - Identity Proofing
  - Binding to an existing credential

- Multiple authenticators can be registered on an account for recovery

Authentication Ceremony



User presence

rpID, credID, challenge

rpID, credID, clientData (challenge + origin)

Validate origin matches rpID

Retrives privK using credIDkeypair

AuthenticatorMakeCredential

Reject if no match

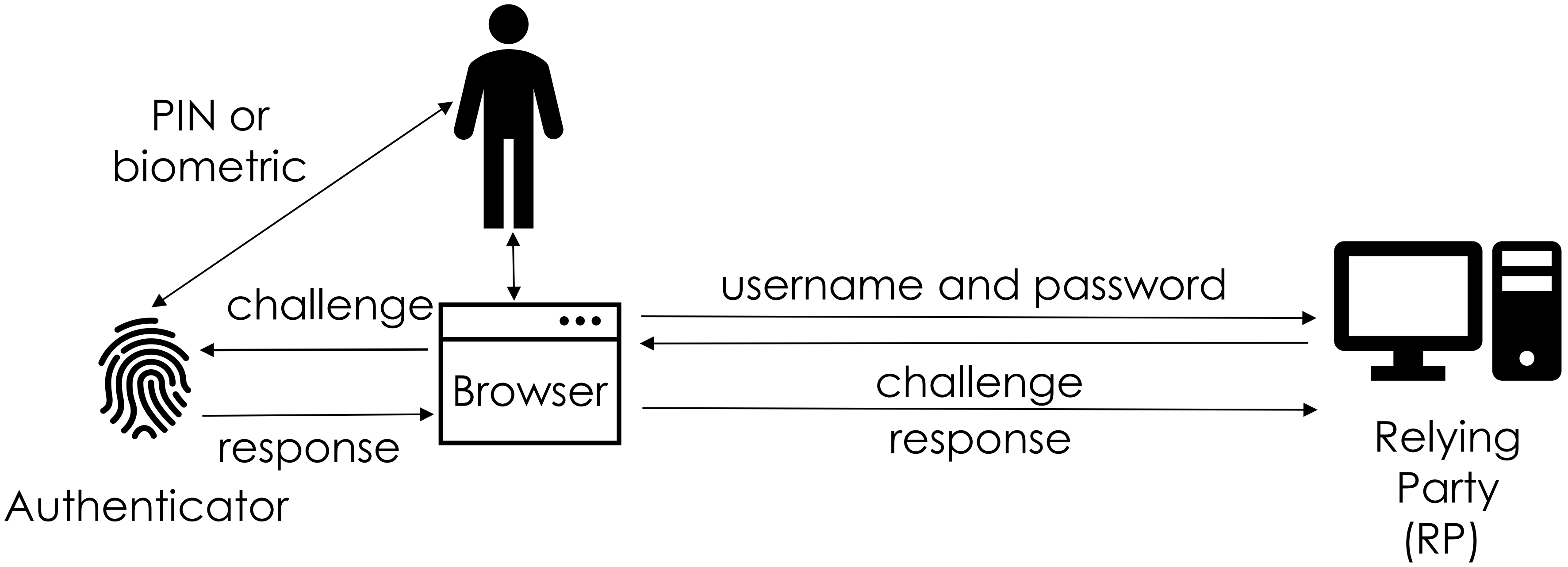
- Verify origin
- Verify challenge
- Verify credID
- Verify signature with pubK
- If all OK, the user is authenticated

Verifies the credential was created for the rpID
Builds and sign the response with the crendential privK

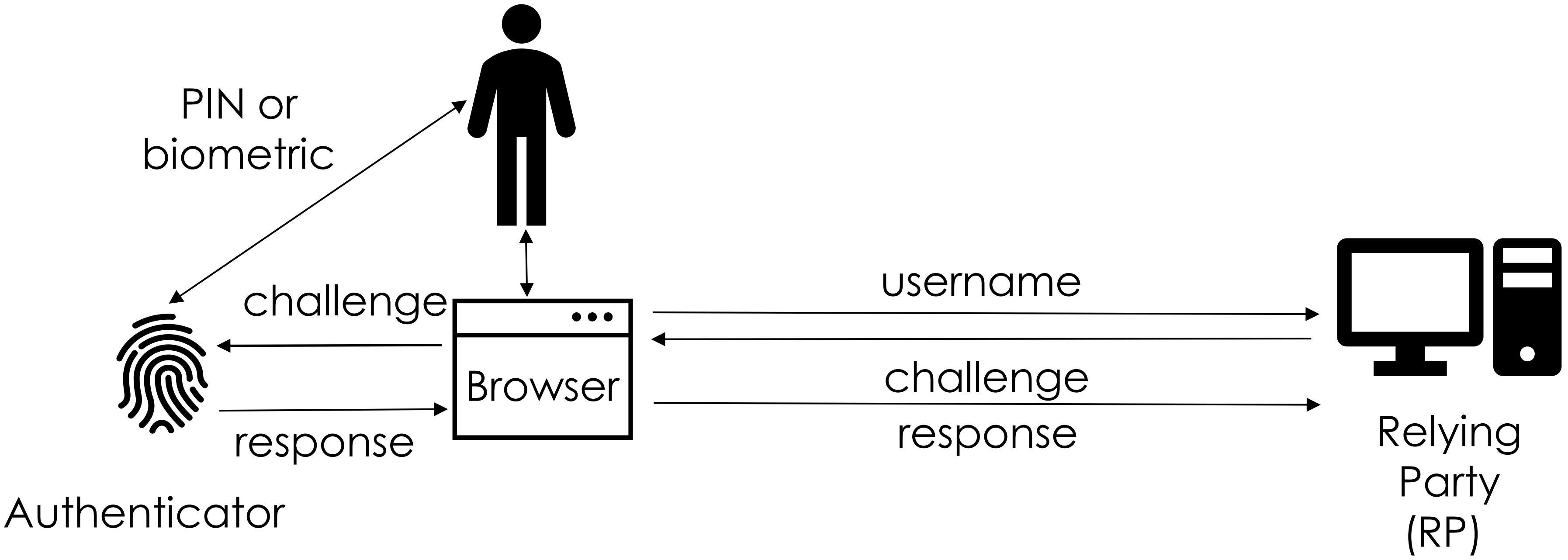
Authenticator signed response

Authenticator signed response + Client Data

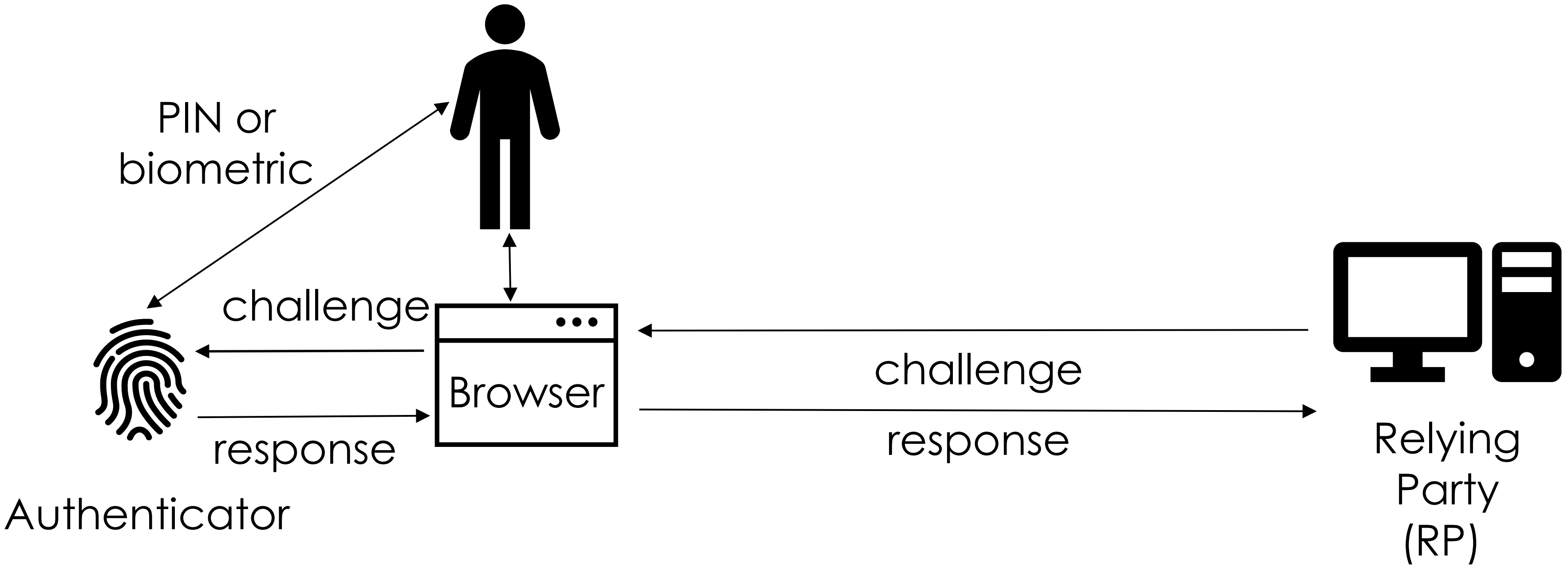
Two Factor Authentication



Passwordless



Nameless Passwordless



To Sum Up

- User isn't required to create a password, a unique cryptographic key pair is created for each site
- Any social engineering attacks will not be successful without the authenticator
- All credentials are scoped for a particular relying party
- An attacker won't gain any benefits by using the user's public keys

Online Examples

- https://webauthn.me/
- https://webauthn.io/
- https://www.passwordless.dev/