1

Architecting Passwordless Authentication with FIDO2

John Craddock
XTSeminars
Identity and security architect
www.xtseminars.co.uk, @john_craddock

2

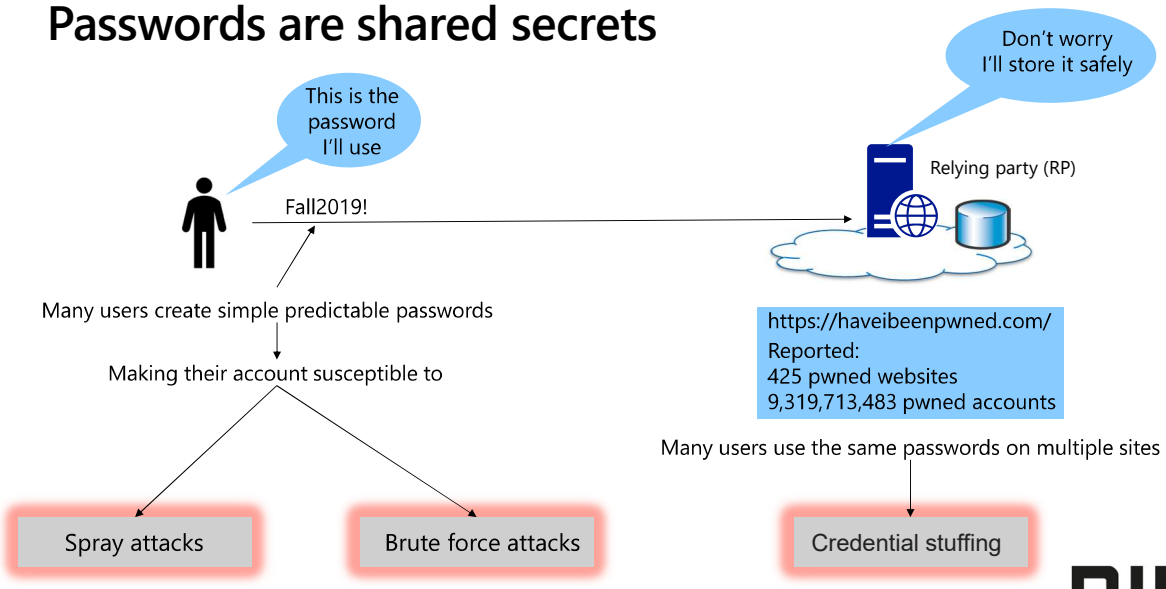
Agenda

- Passwords are a problem
- Going passwordless
- FIDO2 under the hood
- FIDO2 and Windows 10 Azure sign-in

XTSeminars

3

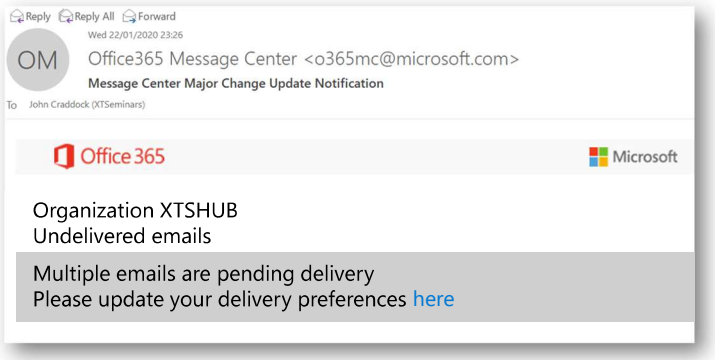
Passwords are shared secrets



XTSeminars

4

I'm not getting emails…

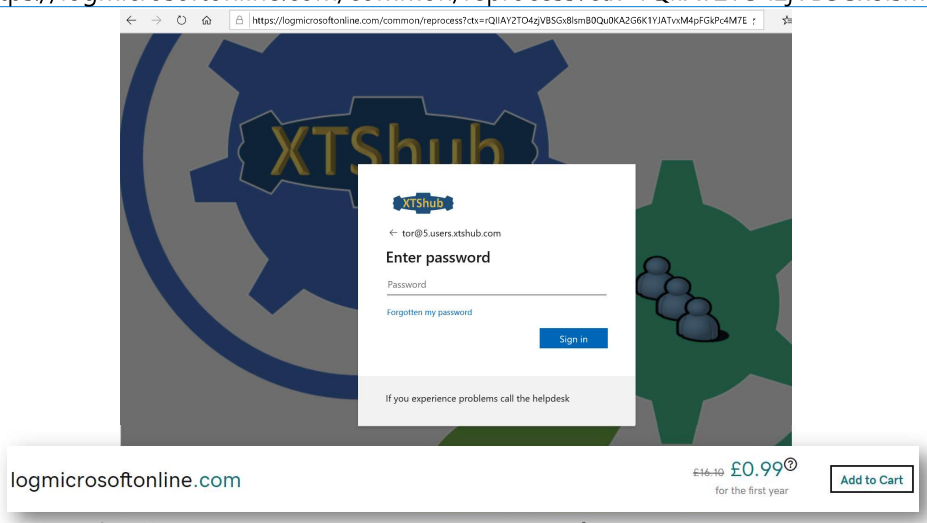


XTSeminars

5

Is there a problem?

https://logmicrosoftonline.com/common/reprocess?ctx=rQIIAY2TO4zjVBSGx8lsm



- Oops you just gave away your password

XTSeminars

6

Password resets

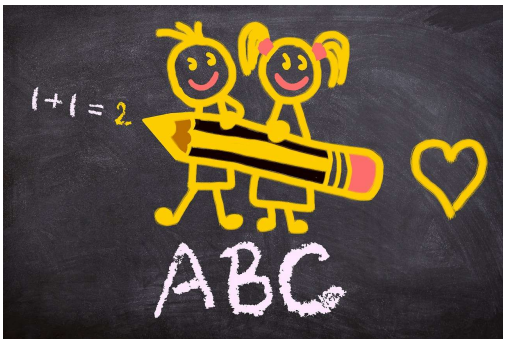
Question 1: what was the name of you first pet?

- Resets send to an already compromised email alias
- Resets via Knowledge-Based Authentication (KBA) security questions and answers
  - Answers already known from pwned website or social media disclose

XTSeminars

7

Challenges



- Educating users about password security is difficult
- MFA is a must it will eliminate 99.9% of sign ins with *compromised* passwords succeeding
  - In most cases simple SMS MFA will be sufficient
  - For convenience or high value accounts go for alternatives
- Don't over prompt for MFA
  - With an authenticator app users get complacent and just approve

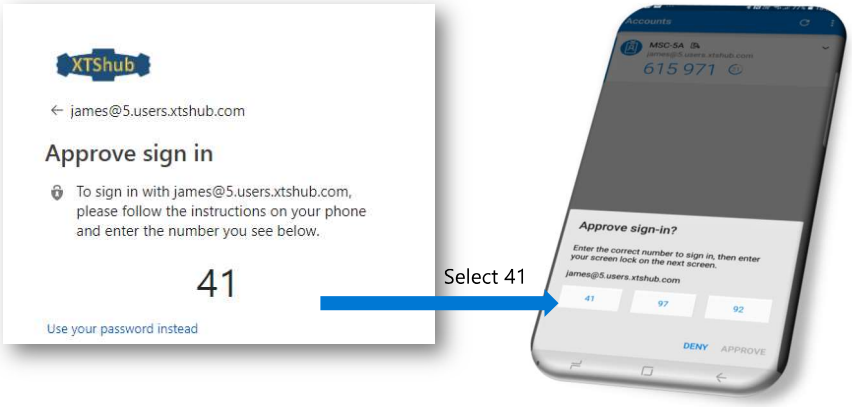
XTSeminars

8

How do we eliminate passwords being compromised?

9

Azure AD passwordless sign-in



XTSeminars

10

To be Internet scalable there must be standards

- Fast IDentity Online (FIDO) Alliance founded in July 2012
  - Mission to work on creating a passwordless authentication protocol
- December 2014 the Alliance published
  - The passwordless protocol FIDO Universal Authentication Framework (FIDO UAF)
  - The second-factor protocol FIDO Universal 2nd Factor (FIDO U2F)
- 2019 - FIDO2 core Web Authentication protocol (WebAuthN) adopted by the World Wide Web Consortium (W3C) as an Internet standard
- 2019 - Microsoft Hello certified as FIDO2 compliant
- Many vendors released FIDO2 security keys

XTSeminars

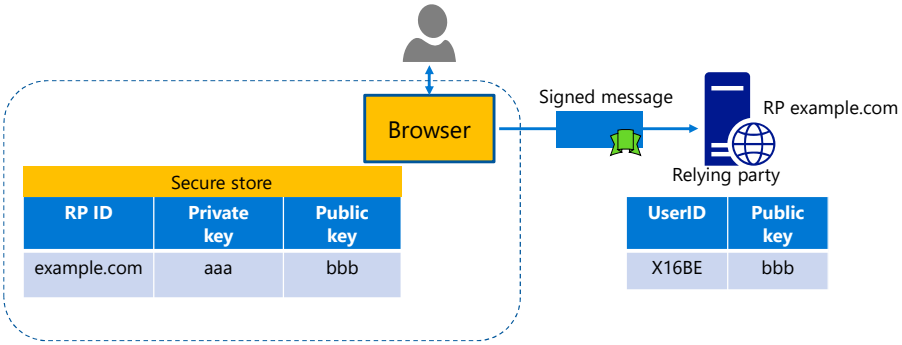
11

Proliferation of FIDO2 security keys

XTSeminars

12

Replaces shared secrets with asymmetric cryptography

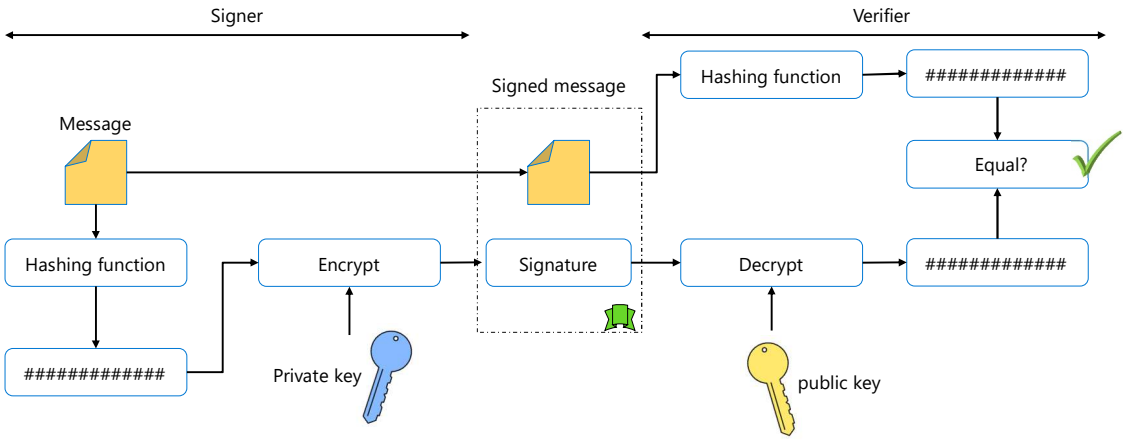


- The user signs a message with their private key
  - The private key never leaves the user's possession
- The RP can validate the signature with the user's public key
  - This proves the message has not been altered and the sender is the owner of the private key

XTSeminars

13

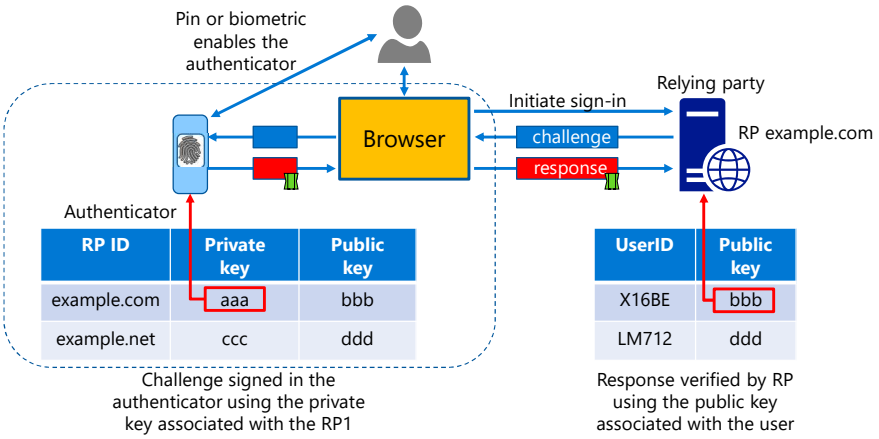
Crypto signing and verification



XTSeminars

14

FIDO2 Authentication

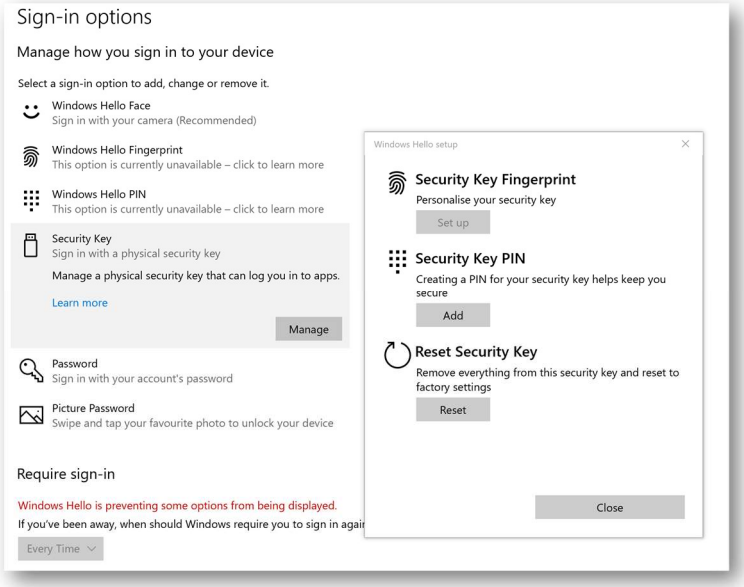


- The signed response is called an assertion

XTSeminars

15

Setting up a FIDO2 security key with Windows 10



XTSeminars

16

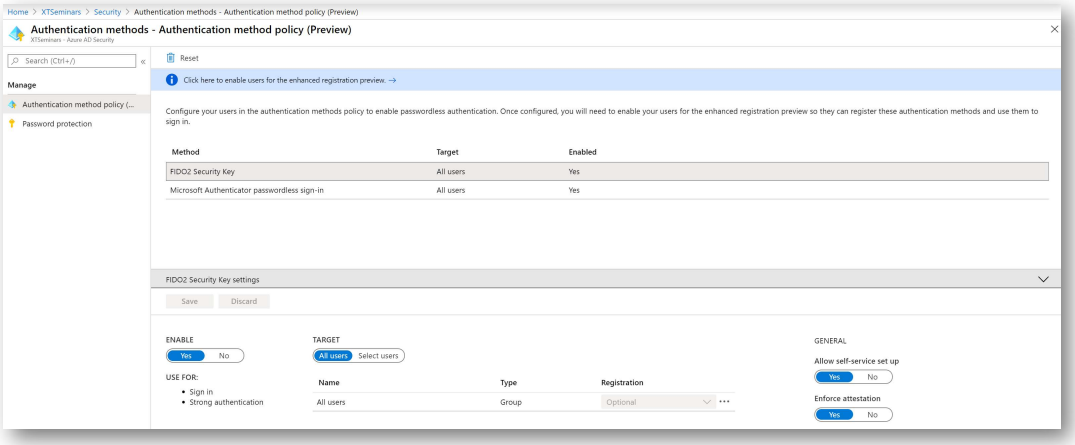
Top tip

- Windows 10 allows you to reset a key and clear all the credentials
- Go to "Sign-in options | Security Key | Manage | Reset“
- If you receive a message that the key cannot be reset
  - Perform the reset within 10 seconds of powering up the key

XTSeminars

17

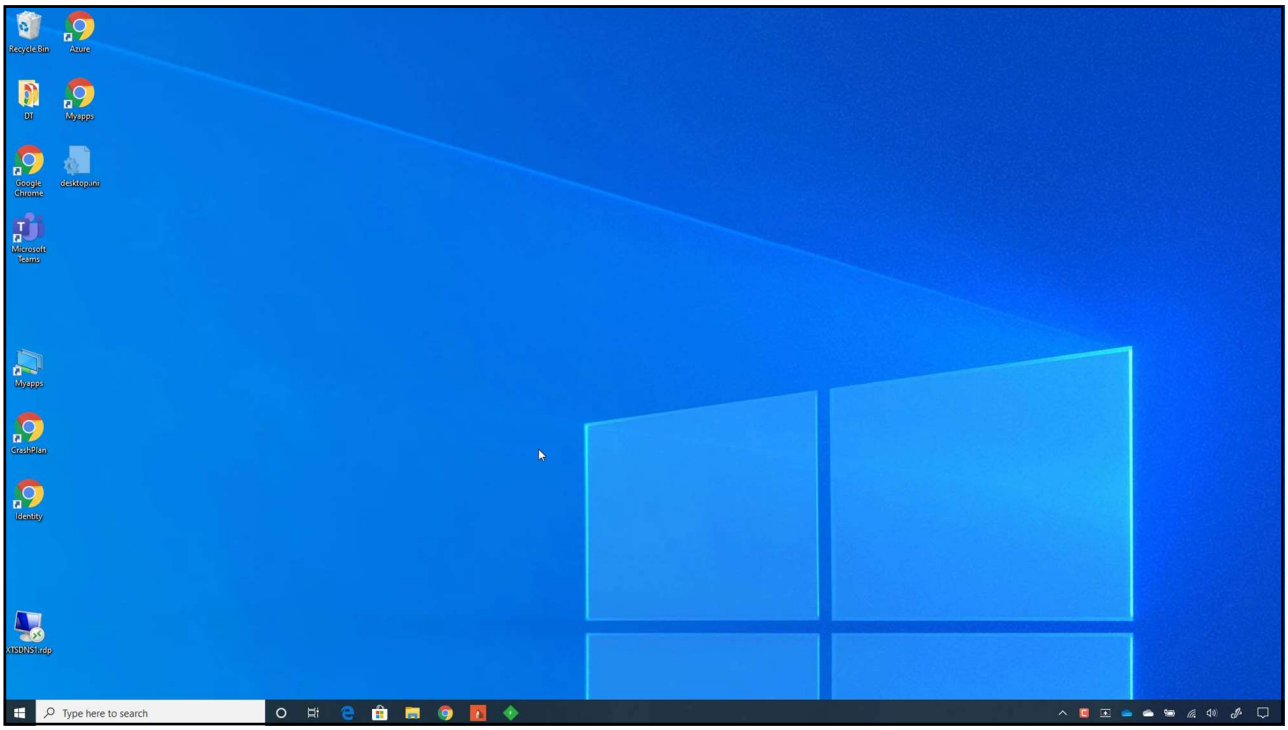
Enabling FIDO 2 security keys in Azure AD



- In the future policies will be added
  - MFA
  - SSPR
  - Password

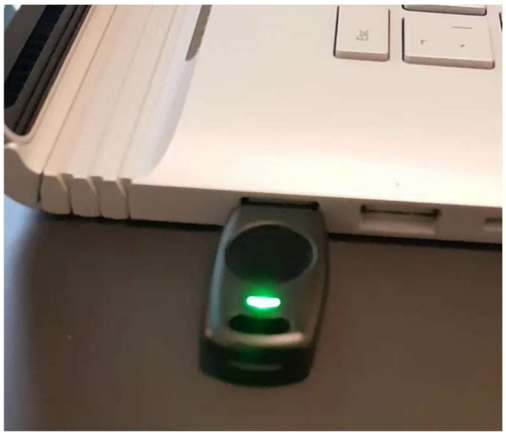
XTSeminars

18



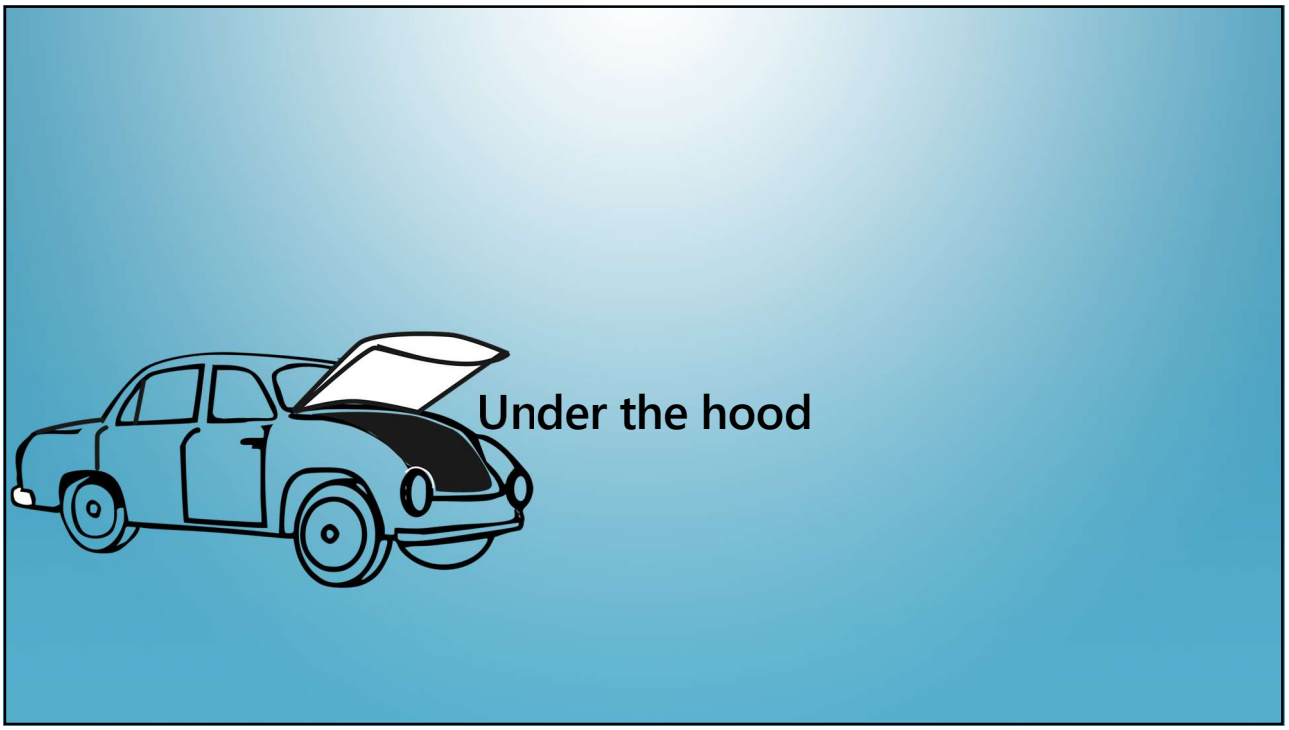
19

eWBM Goldengate G310



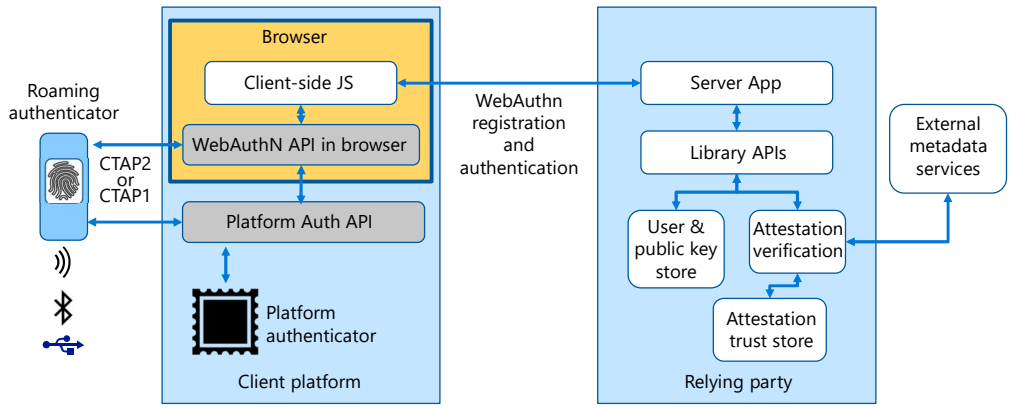
XTSeminars

20



21

FIDO2 components and protocols



XTSeminars

22

Two Ceremonies

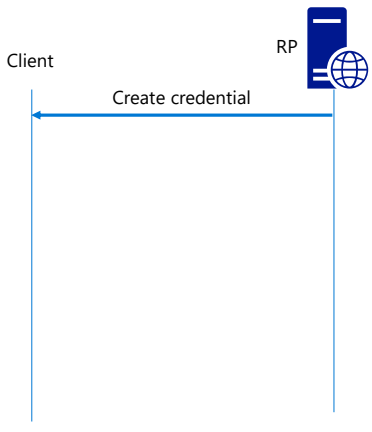
Registration

Authentication

XTSeminars

23

Registration ceremony



XTSeminars

24

Create Credential parameters include

Challenge: Random string of bytes, used to prevent replay attacks

RPId: Identifies the RP's domain

User: Randomly generated id that is used to associate a credential with a user

pubKeyCredParams: Specifies the cryptographic types of public keys that are acceptable to the RP

authenticatorSelection:

- The type of authenticator - cross-platform (roaming) or platform (bound)
- If the authenticator private key should be residential
  - Required for passwordless authentication
- If user verification to the authenticator is required, preferred or discouraged

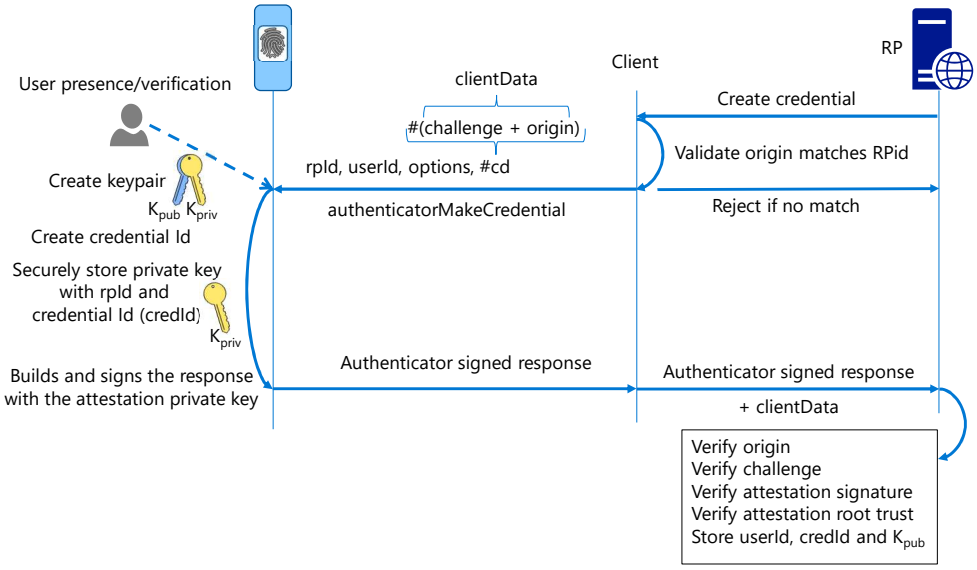
timeout: The user is required to respond within this time; otherwise, an error occurs.

attestation: Allows the RP to specify if attestation data is required. Attestation data allows the RP to verify the veracity and the security of authenticator being used

XTSeminars

25

Registration ceremony



XTSeminars

26

Attestation metadata

- FIDO Alliance Metadata Service (MDS)
  - Authenticator vendors can publish Metadata Statements
    - Trusted source of 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 that is burnt into the device

XTSeminars

27

Verifying the attestation signature

- The attestation signature signs the attestation data and the users public key
- Verification of the signature confirms that the public key has not been substituted by a man-in-the-middle attack
  - The signing certificate's public key is used to verify the signature,
    - The certificate chain is verified as well as the certificate revocation list
  - Some RPs will rely on the veracity of the TLS channel and allow self-attestations (surrogate-attestations)
    - Self-attestations use a self-signed certificate
  - Microsoft Azure AD has a "Force Attestation" option which can be switched to No to allow self-signed certs

XTSeminars

28

AAGUIDS & Metadata

Product Name or Laser Marking	Firmware	FIDO2 AAGUID
YubiKey 4 (Series)	All	N/A
YubiKey 5 (USB-A, No NFC)	5.1.X	cb69481e-8ff7-4039-93ec-0a2729a154a8
YubiKey 5 (USB-A, No NFC)	5.2.X	ee882879-721c-4913-9775-3dfcce97072a
YubiKey 5 NFC	5.1.X	fa2b99dc-9e39-4257-8f92-4a30d23c4118
YubiKey 5 NFC	5.2.X	2fc0579f-8113-47ea-b116-bb5a8db9202a
YubiKey 5 Nano	5.1.X	cb69481e-8ff7-4039-93ec-0a2729a154a8
YubiKey 5 Nano	5.2.X	ee882879-721c-4913-9775-3dfcce97072a


```
{
    deviceId: "1.3.6.1.4.1.41482.1.7",
    displayName: "YubiKey 5 Series security key",
    transports: 4,
    deviceUrl: "https://support.yubico.com/support/solutions/articles/15000014180-yubikey-5c",
    imageUrl: "https://developers.yubico.com/U2F/Images/YK5-series.png",
  - selectors: [
      - {
            type: "x509Extension",
          - parameters: {
                key: "1.3.6.1.4.1.45724.1.1.4",
              - value: {
                    type: "hex",
                    value: "cb69481e8ff7403993ec0a2729a154a8"
                }
            }
        }
    ]
},
```


Section from Yubico metadata

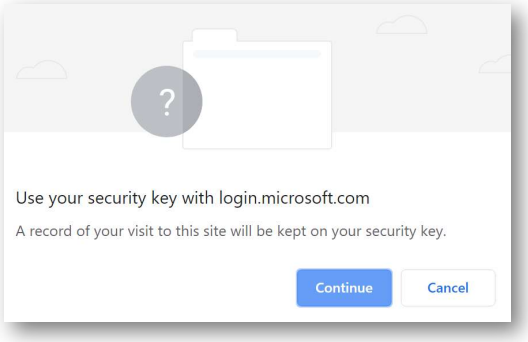
Product	VID	PID	AAGUID
Goldengate 310	0x311F	0x4A1A	95442b2e-f15e-4def-b270-efb106facb4e
Goldengate 320	0x311F	0x4C2A	87dbc5a1-4c94-4dc8-8a47-97d800fd1f3c

eWBM

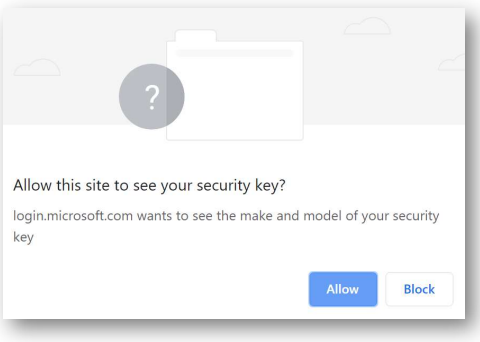
XTSeminars

29

FIDO2 via a browser



Resident keys



Attestation

XTSeminars

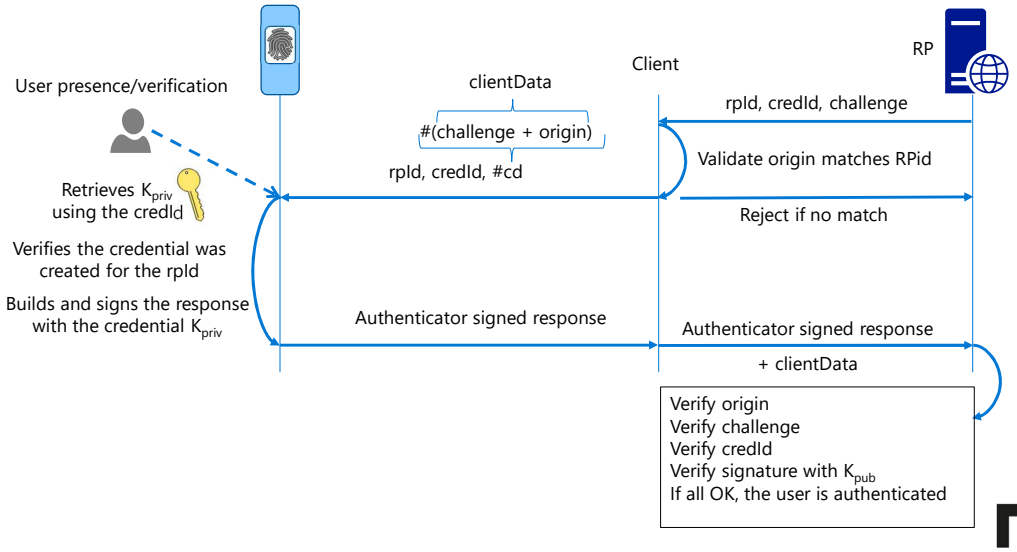
30

Identifying the user

- Registration includes binding a FIDO credential on an given authenticator to a specific user
  - Trust on First Use (TOFU)
    - Only assures that the user registering the credential can authenticate to the RP
  - Invitation
    - Invitation sent to user in advance of registration
  - Identity Proofing
    - User documents/presence may be required
  - Binding to an existing credential
    - Sign-in, possibly with MFA, before registering credential and authenticator
- Multiple authenticators can be registered on an account for recovery

XTSeminars

Authentication ceremony



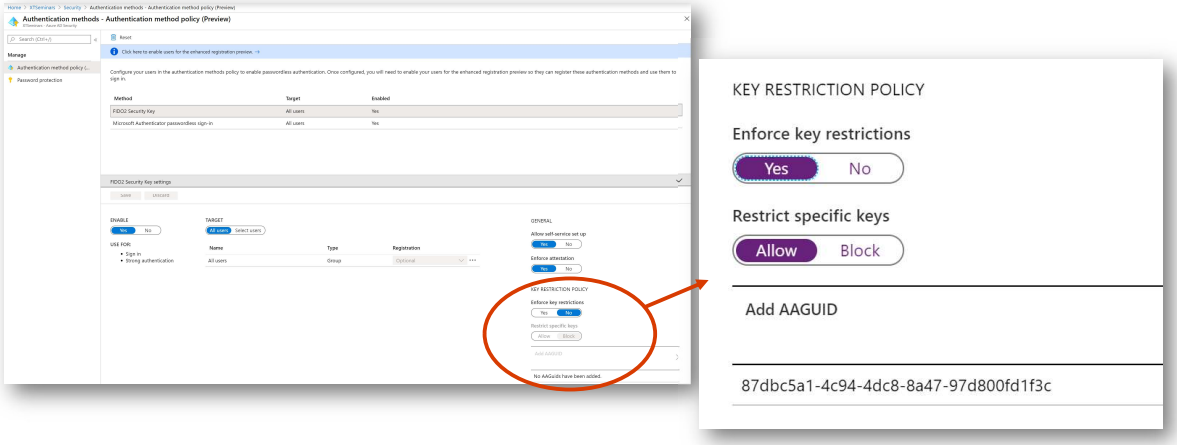
XTSeminars

Demo…

Registration and authentication

33

White and black listing authenticators



XTSeminars

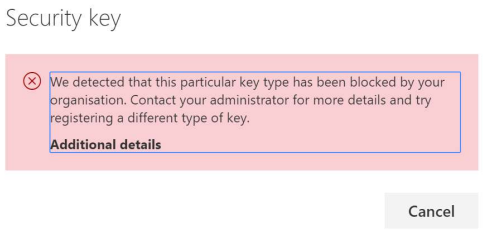
34

Demo…

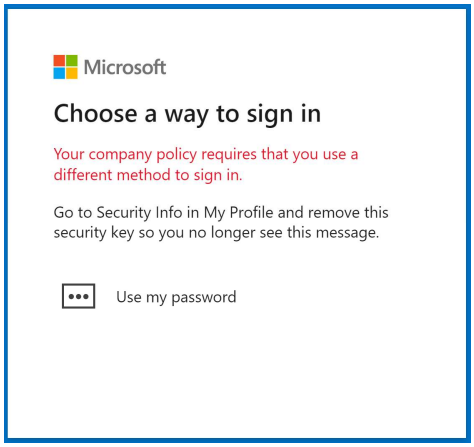
Blocked authenticator

35

Blocked security keys



During registration



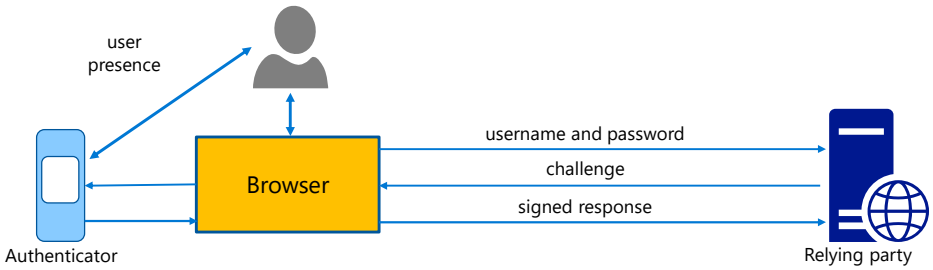
During authentication if the policy has changed between registration and authentication

XTSeminars

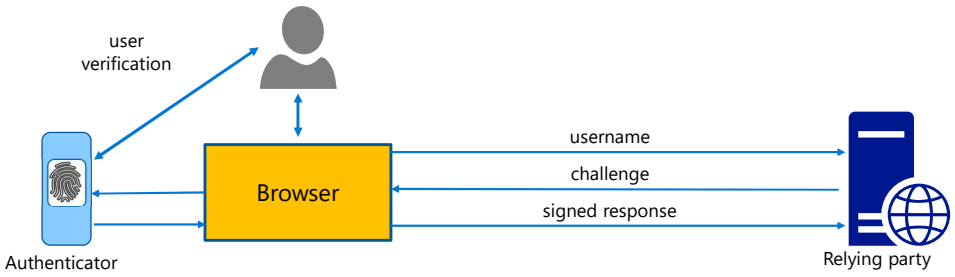
36

Usage scenarios

Second factor authentication



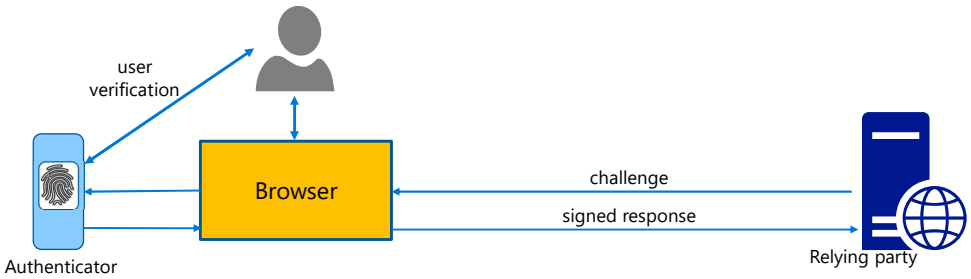
Passwordless



XTSeminars

39

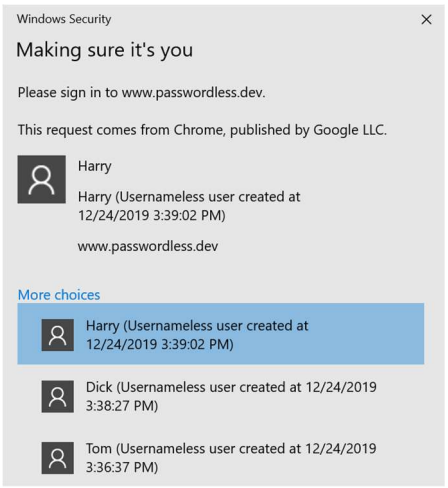
Nameless and Passwordless



XTSeminars

40

Multiple names registered for the same resource



- The user chooses

XTSeminars

41

Windows 10 sign in with a FIDO2 security key

42

AAD Joined and hybrid AAD joined devices

One to one
Windows Hello for Business

One to many
FIDO2 security key

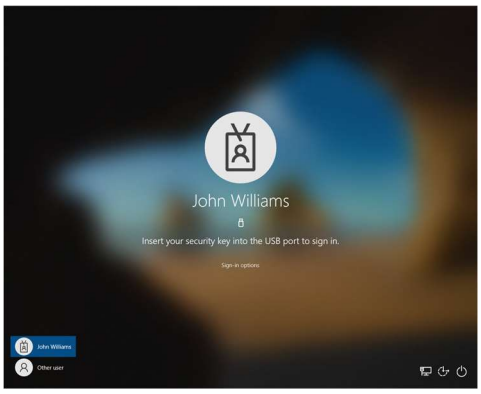
XTSeminars

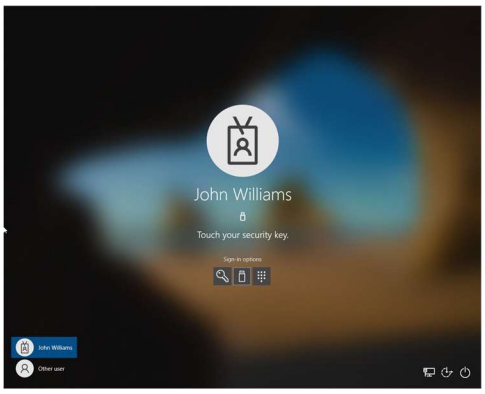
Windows 10 FIDO2 sign-in

- Microsoft security key requirements
  - Resident keys
  - Client PIN for keys that don't have a biometric interface
  - HMAC-secret for offline sign-in
  - Multiple accounts per RP
- Sign-in with a security key is enabled via
  - Intune
  - Group policy
  - Creating a provisioning package using the Windows Configuration Designer app

XTSeminars

Sign in





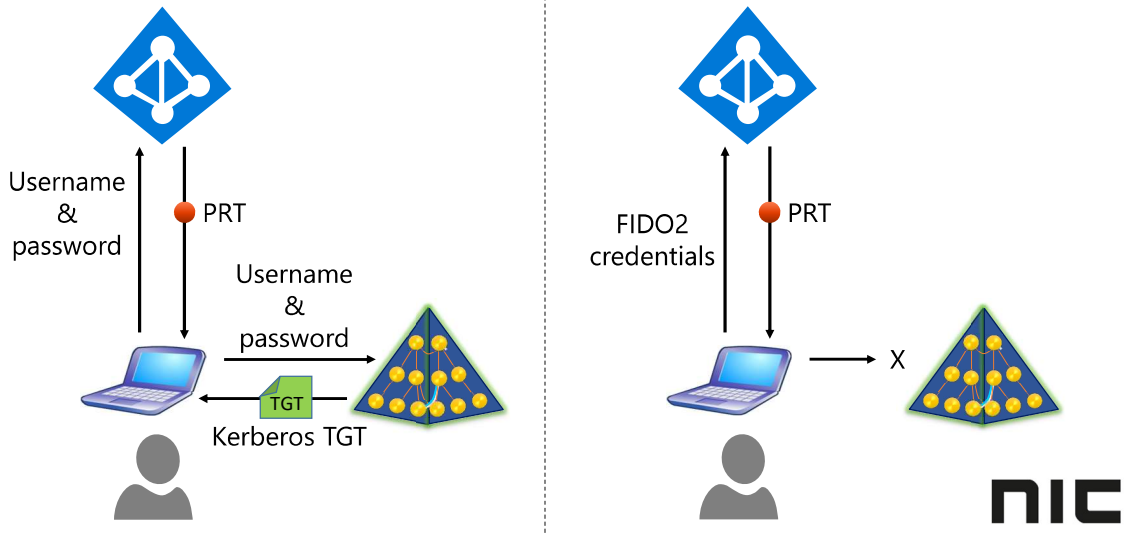
XTSeminars

45

SSO to on-premises

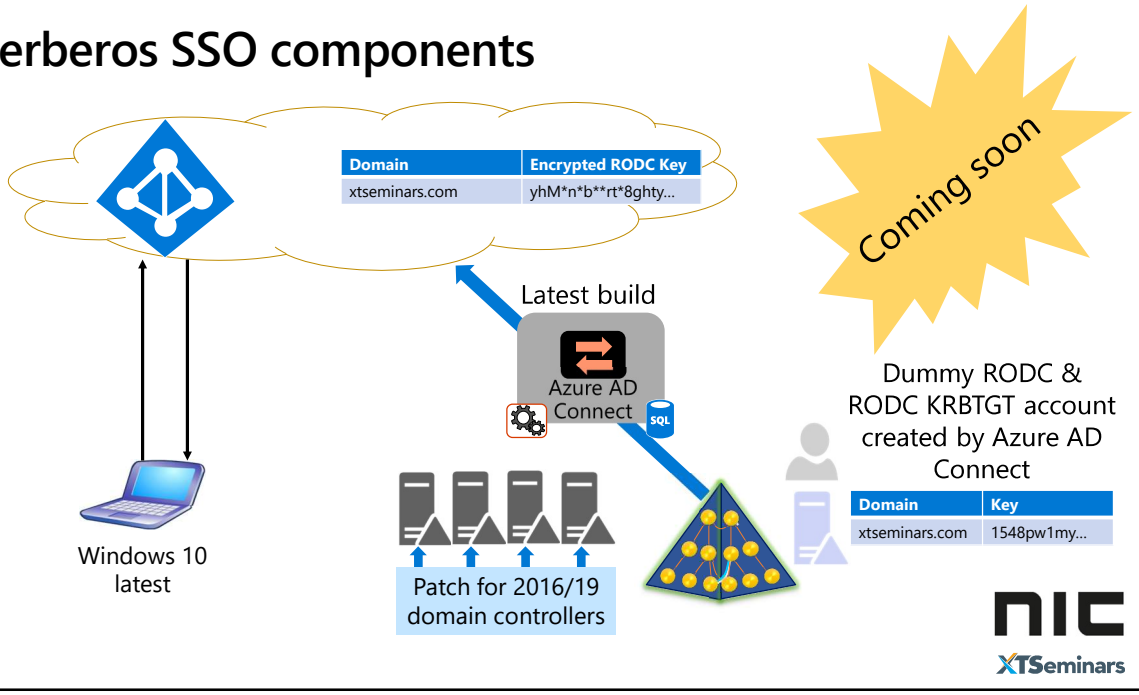
46

Windows sign-in to Azure AD and on-premises



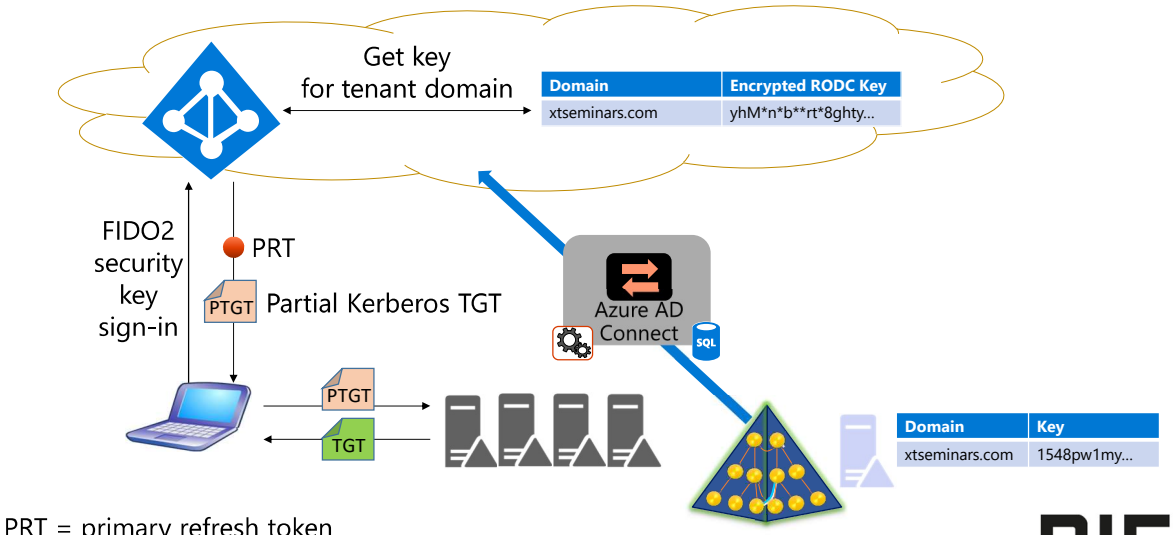
47

Kerberos SSO components



48

Sign-in with FIDO2



PRT = primary refresh token
TGT = ticket granting ticket

XTSeminars

49

Now we can live in a world without passwords

50

In summary

- A user is required to create the password
  - Not any longer a unique cryptographic key pair is created for each site
- Users reveal their passwords via phishing attacks
  - Even if a user gave away their PIN via social engineering, an attack is not going to succeed without the authenticator
  - All credentials are scoped for a particular relying party, eliminating phishing attacks via fake websites
- The target system holds a database of usernames, passwords and possibly KBA questions and answers
  - Gaining access to the user's public keys has no benefit to a hacker

51

If you want to play…

- https://webauthn.me/
- https://webauthn.io
- https://webauthnsample.azurewebsites.net/
- https://www.passwordless.dev/overview

52

Join me for a masterclass

Identity masterclass

Auth Protocols Troubleshooting masterclass

Follow me!
@john_Craddock
www.xtseminars.co.uk

Public masterclasses: UK, The Netherlands, Switzerland, Norway, Sweden, Finland, USA
Onsite masterclasses: as requested

www.xtseminars.co.uk for details

XTSeminars