



**Westfälische
Hochschule**

Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

A New Approach For FIDO UAF

→ Advantages of a cloud-based FIDO Client

Prof. Dr. (TU NN)

Norbert Pohlmann

Institute for Internet Security - if(is)

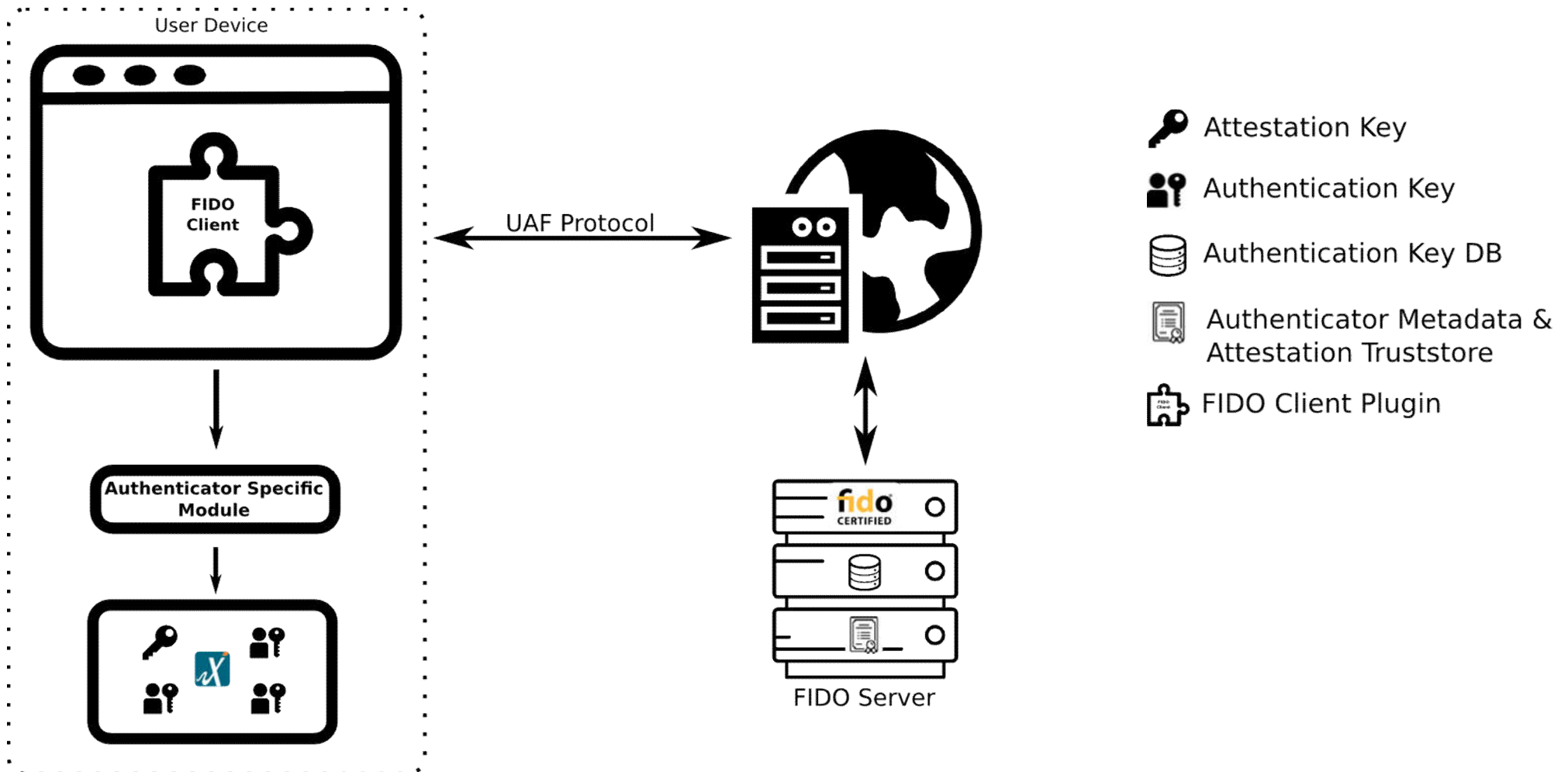
Westphalian University of Applied Sciences

Gelsenkirchen, Germany www.if-is.net



FIDO

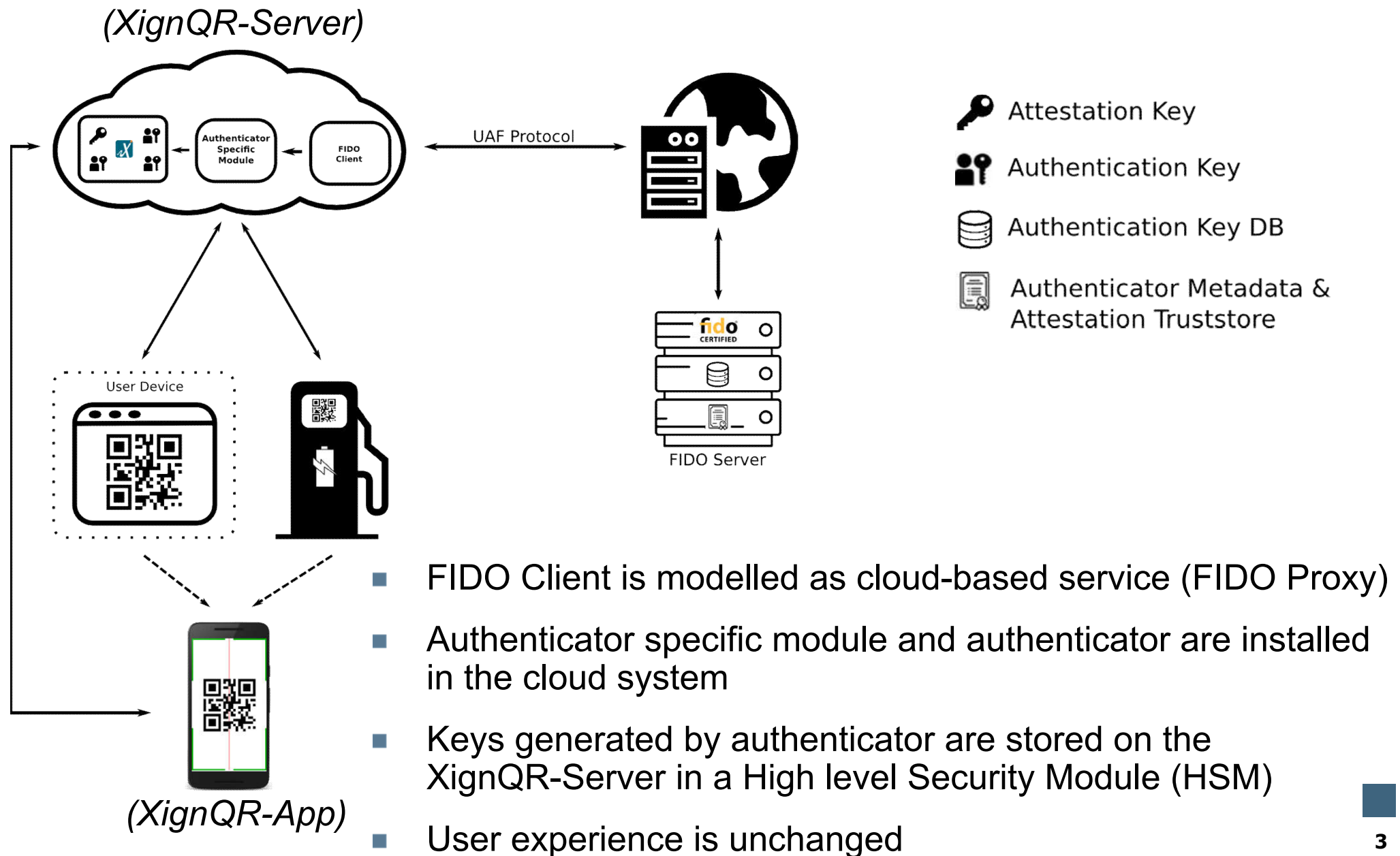
→ The classic approach



- FIDO Client is browser extension/plugin
- Authenticator specific module and authenticator are installed in the user's system
- Keys generated by authenticator are stored in the user's system (ideally in TPM)

FIDO

→ A new approach (XignQR)



FIDO – A new approach

→ Advantages

- Usable with any browser (Independent of browser vendors)
- Does not rely on plugins or extensions, therefore usable with public terminals
- Keys are stored in a secure environment (no requirement for TPM as secure key storage)
- Loss of user device not so fatal (keys are stored in cloud-system's HSM)
- Authenticator needs to be registered only once

FIDO – A new approach

→ New Use Cases

- The alternative approach enables new use cases in scenarios other than web authentication
 - Terminals without displays (charging stations, ...)
 - Physical access management (smart home, industrial Internet, ...)
 - Mobile transactions (mobile commerce, ...)
 - ...

FIDO – A new approach

→ Requirements for alternative scenarios

- There where are no displays involved:
 - Authentication and transaction confirmation by XignQR and static QR Code
 - XignQR (Smartphone-XignApp) displays transaction data and receives user's confirmation
 - XignQR System delivers FIDO assertions on behalf of user to FIDO Server
 - XignApp communicates with FIDO Client Proxy in cloud-system



**Westfälische
Hochschule**

Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

A New Approach For FIDO UAF

→ Advantages of a cloud-based FIDO Client

Thank you for your attention!
Questions?

Prof. Dr. (TU NN)

Norbert Pohlmann

Institute for Internet Security - if(is)
Westphalian University of Applied Sciences
Gelsenkirchen, Germany www.if-is.net

if(is)
internet security.