FIDO2 einfach erklärt!

Michael Simon, Software Developer
cpsd it services GmbH, Linz

Inhalt

- Was ist FIDO2 ?
- Welche Möglichkeiten bietet FIDO2 ?
- Fallbeispiel: FIDO2 und Microsoft365
- Konfigurationsmöglichkeiten
- Registrierung eines neuen Tokens
- Anmeldung mit einem Token
- Was sind Passkeys?
- Die Authentisierungslösung von CPSD

Was ist FIDO2 ?

- **F**ast **ID**entity **O**nline
- Benutzeranmeldung auf Basis von asymmetrischer Kryptographie
- W3C-Web-Authentication-Standard (**WebAuthn**)
- Client to Authenticator Protocol (**CTAP2**)
- Der Benutzer vertraut dem Hersteller des Tokens

CPSD
ENCRYPTION EXPERTS

Welche Möglichkeiten bietet FIDO2 ?

- Anmeldung ohne Passwort
- 2. Faktor zusätzlich zum Passwort
- Verschiedene Hersteller und Token Formate
- Hardware Token können an mehreren Geräten verwendet werden
- Invalidieren von Anmeldedaten auf Basis des verwendeten Tokens (z.B. nach Bekanntwerden von Sicherheitslücken)

Fallbeispiel: FIDO2 und Microsoft365

- Einen Token zu einem Microsoft 365 Konto hinzufügen
- Einen Token zur Anmeldung an Microsoft 365 nutzen

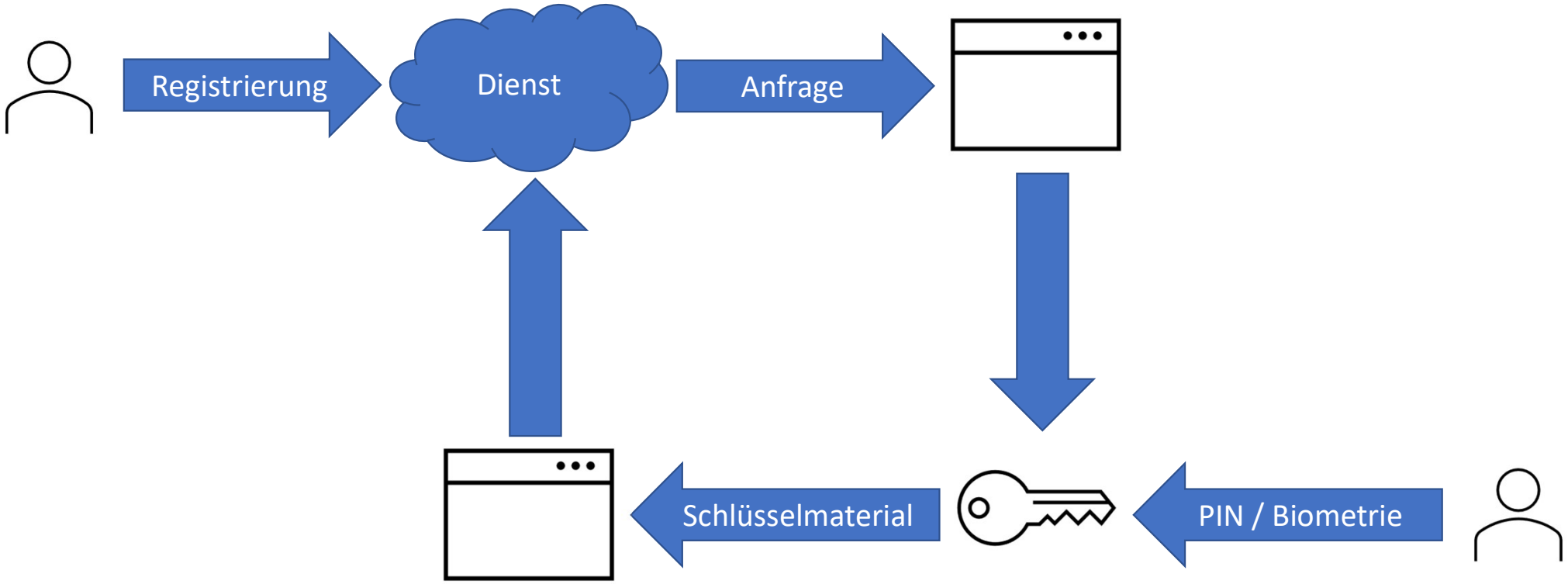
CPSD
ENCRYPTION EXPERTS

Konfigurationsmöglichkeiten

- Speichern des Schlüsselmaterials am Server oder am Token
- Benutzer Verifizierung mit PIN oder Biometrie
- Einzelne Token erlauben oder verbieten
- Über Erweiterungen werden dem Standard neue Möglichkeiten hinzugefügt

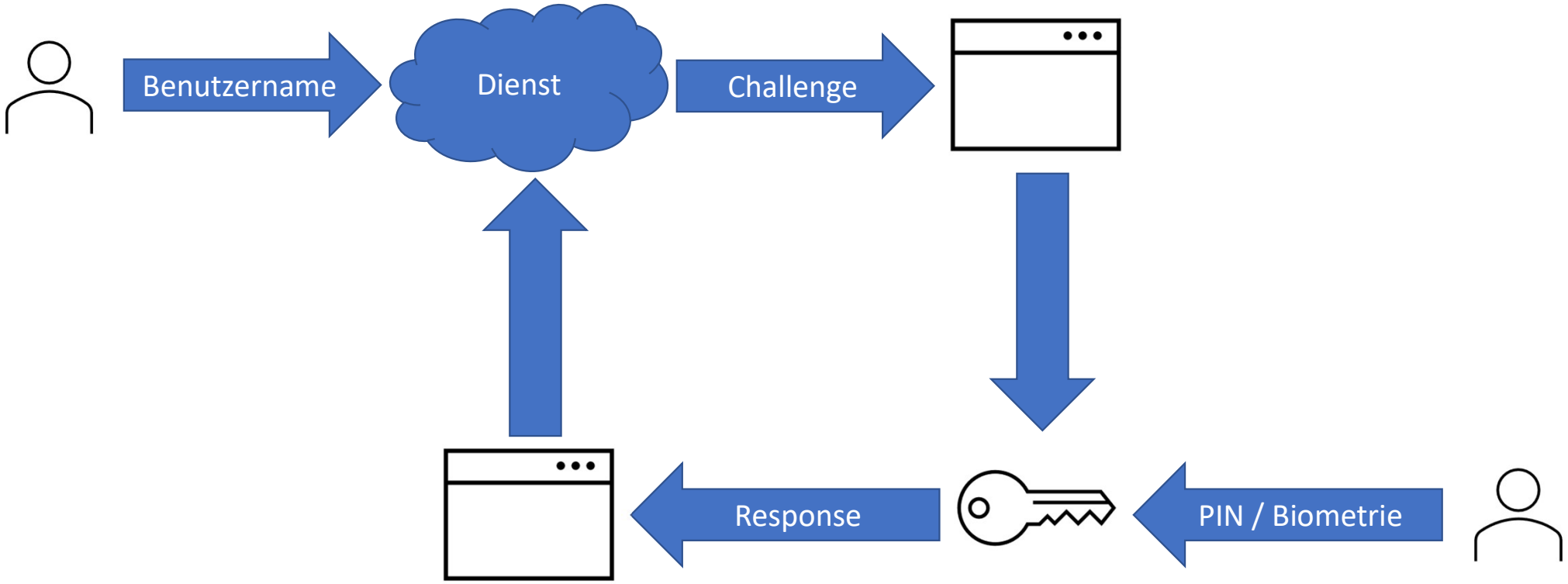
CPSD
ENCRYPTION EXPERTS

Die Registrierung eines Tokens



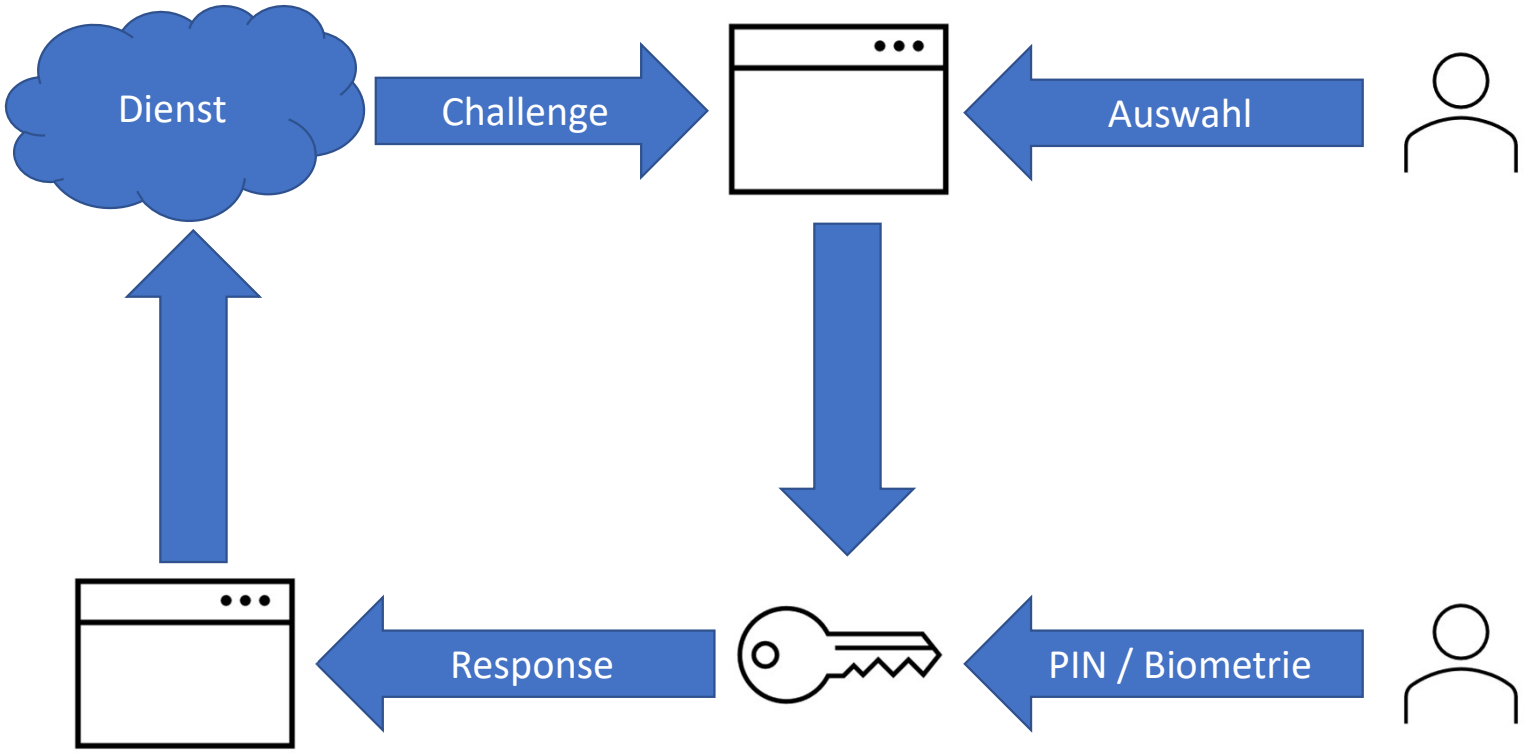
CPSD
ENCRYPTION EXPERTS

Die Anmeldung mit einem Token



CPSD
ENCRYPTION EXPERTS

Die Anmeldung mit einem Token



CPSD
ENCRYPTION EXPERTS

Was sind Passkeys?

- Bauen auf FIDO2 Standard auf
- Verwenden keine Hardware Token
- Das Schlüsselmaterial kann auf mehreren Geräten verwendet werden
- Der Benutzer vertraut dem Hersteller des Betriebssystems

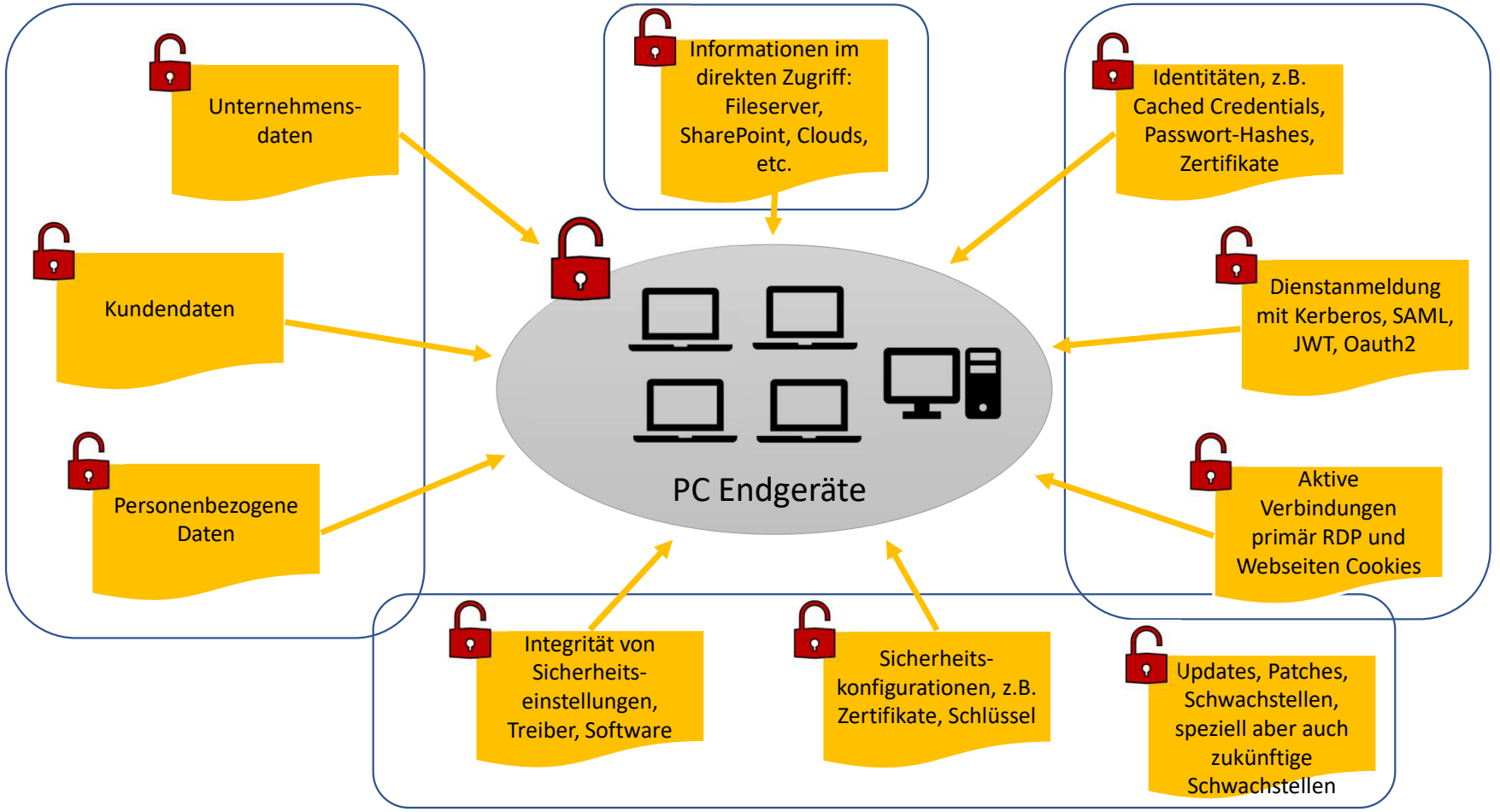
Authentisierung von CPSD

Mag. Rainer Altmüller, Geschäftsführer

Die Authentisierungslösung von CPSD

- Mit dem Produkt Secure Disk for BitLocker bietet CPSD eine Pre-Boot-Authentisierung für Windows PCs.
- Als 1-Faktor Authentisierung (1FA) oder Multi-Faktor-Authentisierung (MFA) einsetzbar
- Unterstützt Kunden bei der Go-Passwordless Umsetzung

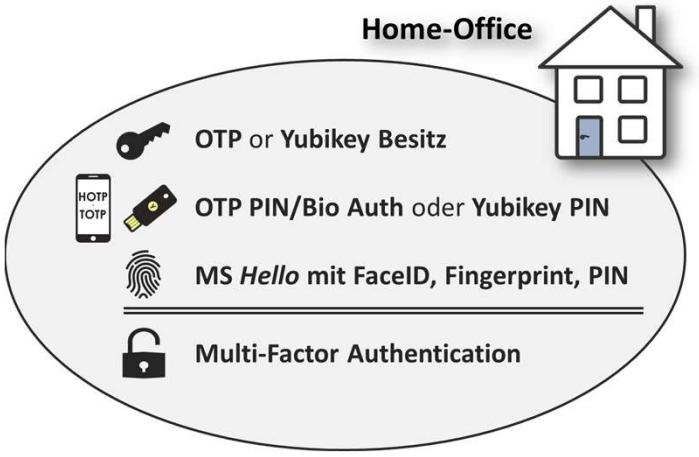
Warum muss ein PC geschützt sein?



Der kryptographische Pre-Boot-Schutz durch ***Secure Disk for BitLocker*** bietet eine zusätzliche Security-Maßnahme für **alle 10 Angriffsszenarien!**

Use-Case: Home-Office

So funktioniert 100% Password-less mit Secure Disk for BitLocker



1. Aktivieren Sie Secure Boot
2. Aktivieren Sie BitLocker mit TPM
3. Installieren Sie die Secure Disk for BitLocker
4. Fügen Sie Microsoft BitLocker einen CPSD Secure Disk MFA Protector hinzu, z.B. OTP oder YubiKey
5. Nach dem Secure Disk MFA Boot nutzen Sie Microsoft Hello for Business zur Entsperrung der Bildschirmsperre und Energiesparmodus
6. Alle dahinterliegenden IT-Dienste inkl. der Cloud-Dienste sind geschützt!

About CPSD

- 2002 in Linz gegründet
- Software Entwicklung und Integration von Kryptographie und Authentisierung
- 15 Mitarbeiter im Unternehmensverbund
- Kontakt:

  - Rainer Altmüller
    Tel: +43 732 781584-10
    E-Mail: rainer.altmueller@cpsd.at

  - Michael Simon
    Tel: +43 732 781584-0
    E-Mail: michael.simon@cpsd.at