INFOTECH
[ IT & Communication ]

# 29. InfoTechDay

19.11.2024

HERZLICH WILLKOMMEN!

INFOTECH
[IT & Communication]

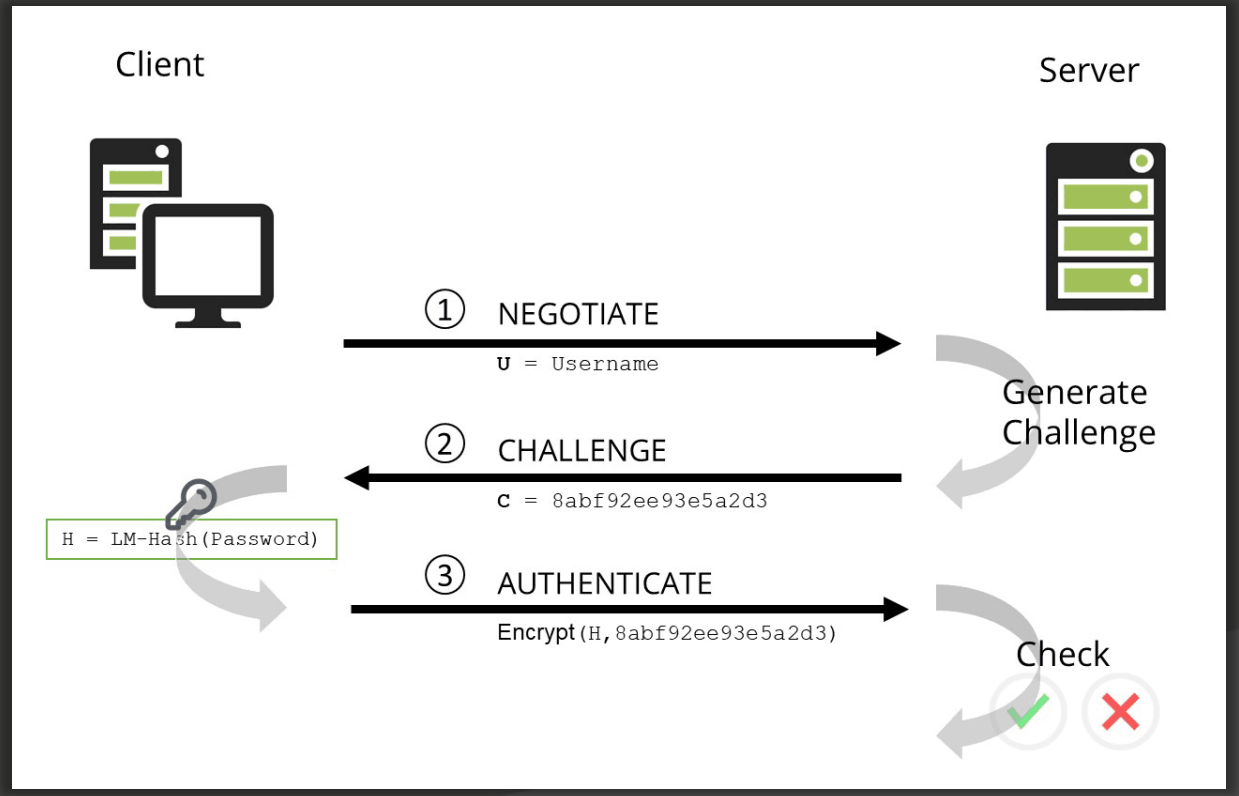
# Zukunftssichere Authentifizierung - gibt es diese?

**Dipl.-Ing. Franz Strasser**

Ihr Systemhaus.

# Active Directory Authentifizierung
# Windows New Technology LAN Manager (NTLM v1/v2)

INFOTECH
[ IT & Communication ]




→ **NTLM sollte NICHT mehr verwendet werden!**

# Active Directory Authentifizierung
# Windows New Technology LAN Manager (NTLM v1/v2)

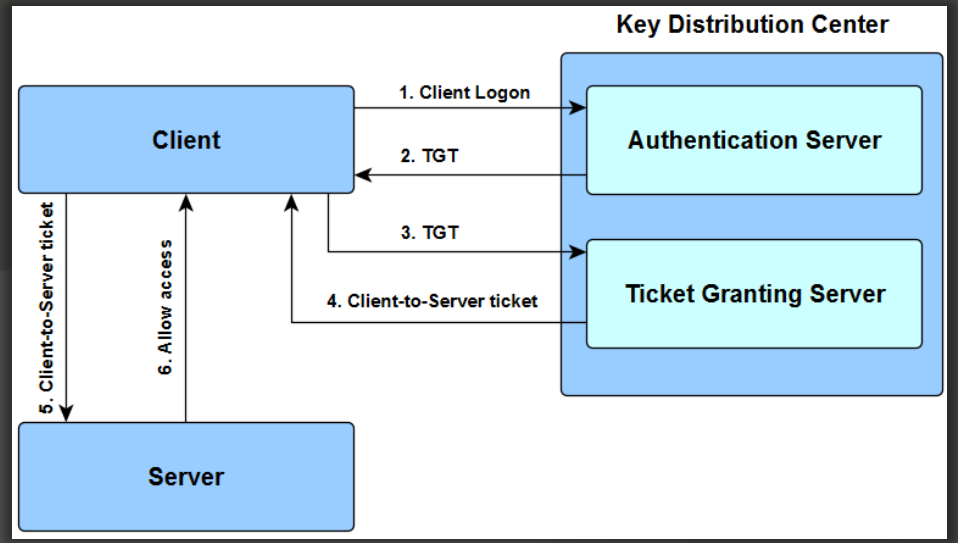
INFOTECH
[ IT & Communication ]

- **Wo wird NTLM verwendet?**
  - Als Fallback wenn Kerberos nicht funktioniert
  - Externe Geräte (kein Domain/DC Zugriff)
- **Wie wird NTLM-Verwendung reduziert?**
  - Abklärung ob NTLM erforderlich ist → Audit per GPO
  - NTLMv1 komplett deaktivieren → GPO
    (Send NTLMv2 response only. Refuse LM & NTLM)
  - NTLMv2 möglichst absichern (z.B. enforce 128-bit Enc, ...)

# Active Directory Authentifizierung
## Kerberos

INFOTECH
[ IT & Communication ]

- **Authentifizierung am Authentication Server (KDC/DC)**
  - Client schickt Anfrage mit UserID zum KDC
  - Ticket Granting Ticket (TGT) geht an Client
    - Verschlüsselt mit PW# (am KDC vorhanden)
- **Zugriff auf Ressourcen**
  - Client beantragt Zugriff beim KDC
    - KDC prüft TGT und Zugriffsrechte
  - Kerberos Ticket (ST) geht an Client
  - Client präsentiert ST an Server



# Active Directory Authentifizierung
# Zertifikatsbasierte Authentifizierung

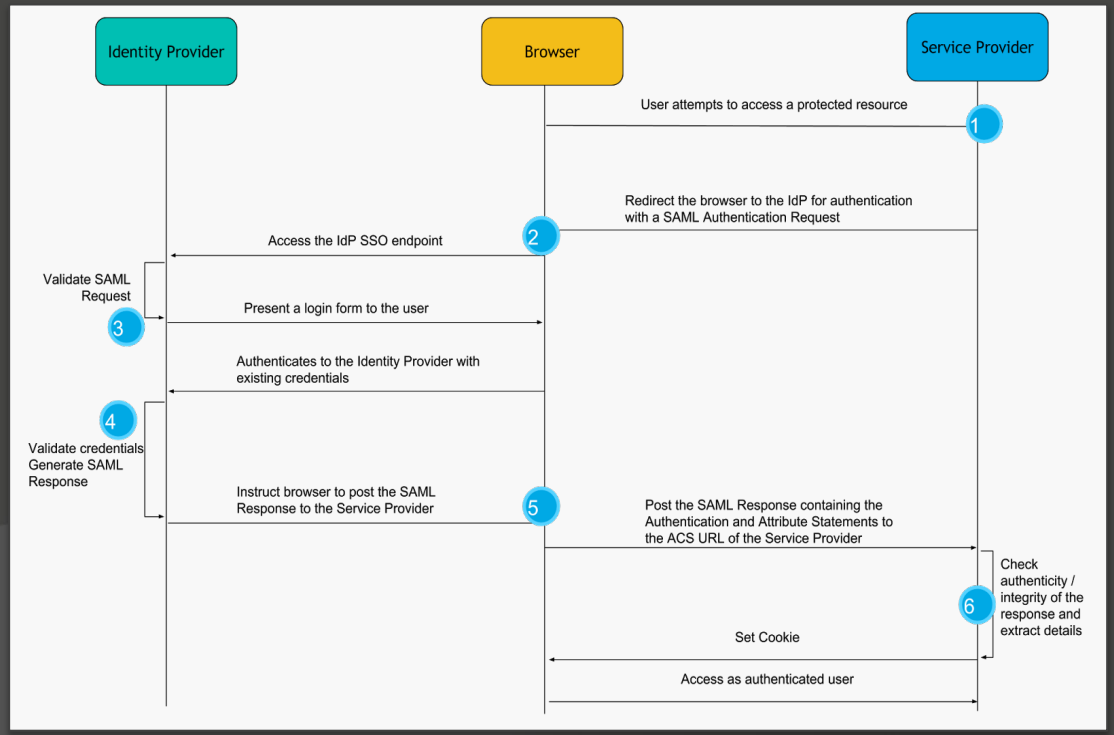
INFOTECH
[ IT & Communication ]


- SmartCard = X.509 Zertifikat
- PrivateKey auf der SmartCard
- Beim Zugriff wird ein PIN benötigt
- Support auf diversen Plattformen (Windows, Mac, Linux, iOS, Android)
- Phising-resistente Authentifizierung
- Voraussetzung: Public Key Infstructure (PKI)

# Moderne Authentifizierung
# Security Assertion Markup Language (SAML)

INFOTECH
[ IT & Communication ]

- **Single Sign-On (SSO) gegen zentralen Identity Provider (IdP)**
- **Basiert auf Assertions (XML Format)**
- **Zugriff auf Ressourcen:**
  1. Zugriffsversuch beim Service Provider (SP)
  2. Umleitung auf IdP → Login
  3. Umleitung auf SP mit SAML-Response
- **SP und IdP müssen sich kennen**



# Moderne Authentifizierung
# Security Assertion Markup Language (SAML)

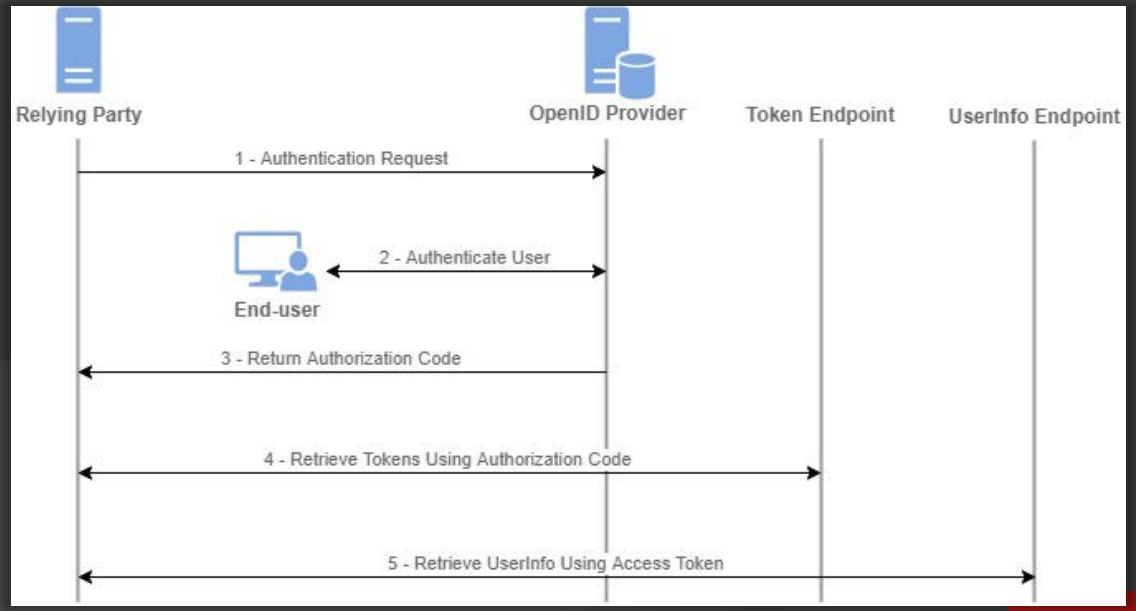
INFOTECH
[ IT & Communication ]

- **Wo wird SAML eingesetzt?**
  - De-Facto Standard im Enterprise-Bereich
  - Identity Providers:
    - Microsoft Entra ID und ADFS
    - Okta
    - Google
    - Shibboleth
    - ...
  - Anwendungen:
    - M365 Dienste
    - Slack
    - Citrix Virtual Apps and Desktops
    - ...
    - ...

# Moderne Authentifizierung
# OpenID Connect (OIDC)

INFOTECH
[ IT & Communication ]

- **Baut auf OAuth2 auf (Open Authorization)**
  - Reines Autorisierungsprotokoll
- **Erweiterung um Authentifizierung + SSO**
- **Workflow ähnlich zu SAML**
  - JSON statt XML
- **Optimiert für Web und mobile Apps**
- **Wird immer mehr eingesetzt**
  - Grund: „einfacher“ als SAML



# Zweifaktor- / Mehrfaktor-Authentifizierung

## Legacy

INFOTECH
[IT & Communication]

- **Etwas wissen | haben | ausmachen**
- **OATH (Initiative For Open Authentication)**
  - 4-8 stelliger wechselnder PIN
  - TOTP → TimeBased
  - HOTP → HashBased
- **Push**
  - Aktive Meldung am Smartphone (o.Ä.) bei Login

# Zweifaktor- / Mehrfaktor-Authentifizierung

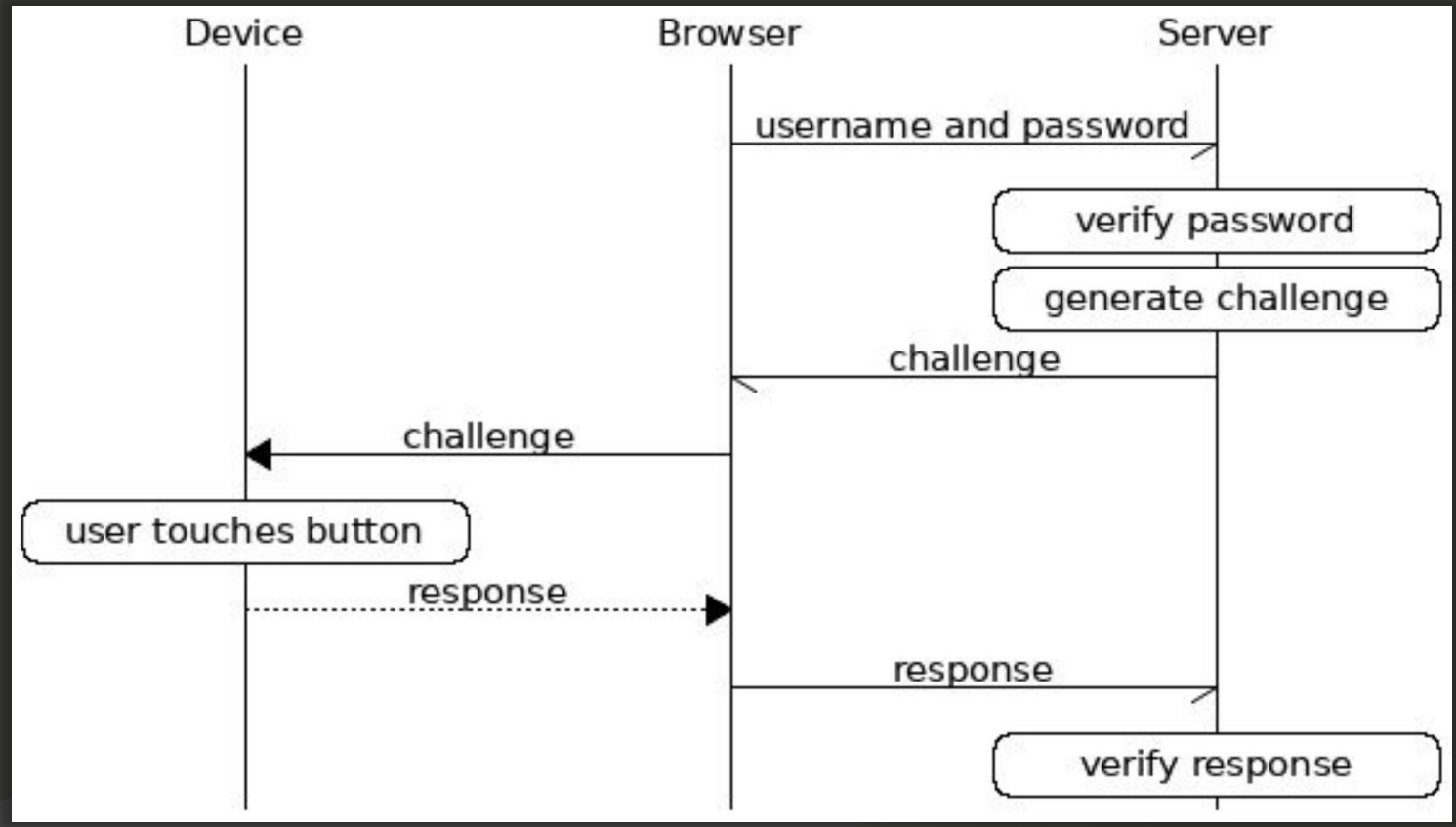
## **FIDO U2F** (CTAP1)

INFOTECH
[ IT & Communication ]

- **Fast IDentity Online**
  **Universal 2nd Factor**

- **Schutz vor:**
  - MITM
  - Phishing
  - Cloning

- **Problem: Passwort erforderlich**



# Einschub: Passwörter

## Top 200 Most Common Passwords (NordPass)

INFOTECH
[ IT & Communication ]

- **International:**
  - 123456 (und Varianten)
  - password
  - qwerty123
  - secret
  - …
  - iloveyou (ca. 200.000 mal)
  - TimeLord12
  - …
- **Österreich**
  - 123456 (und Varianten)
  - Abcd1234
  - g00dpa
  - password
  - …
  - hallo123
  - michael
  - …

Quelle: NordPass (https://nordpass.com/most-common-passwords-list/)

# Zweifaktor- / Mehrfaktor-Authentifizierung
# FIDO 2

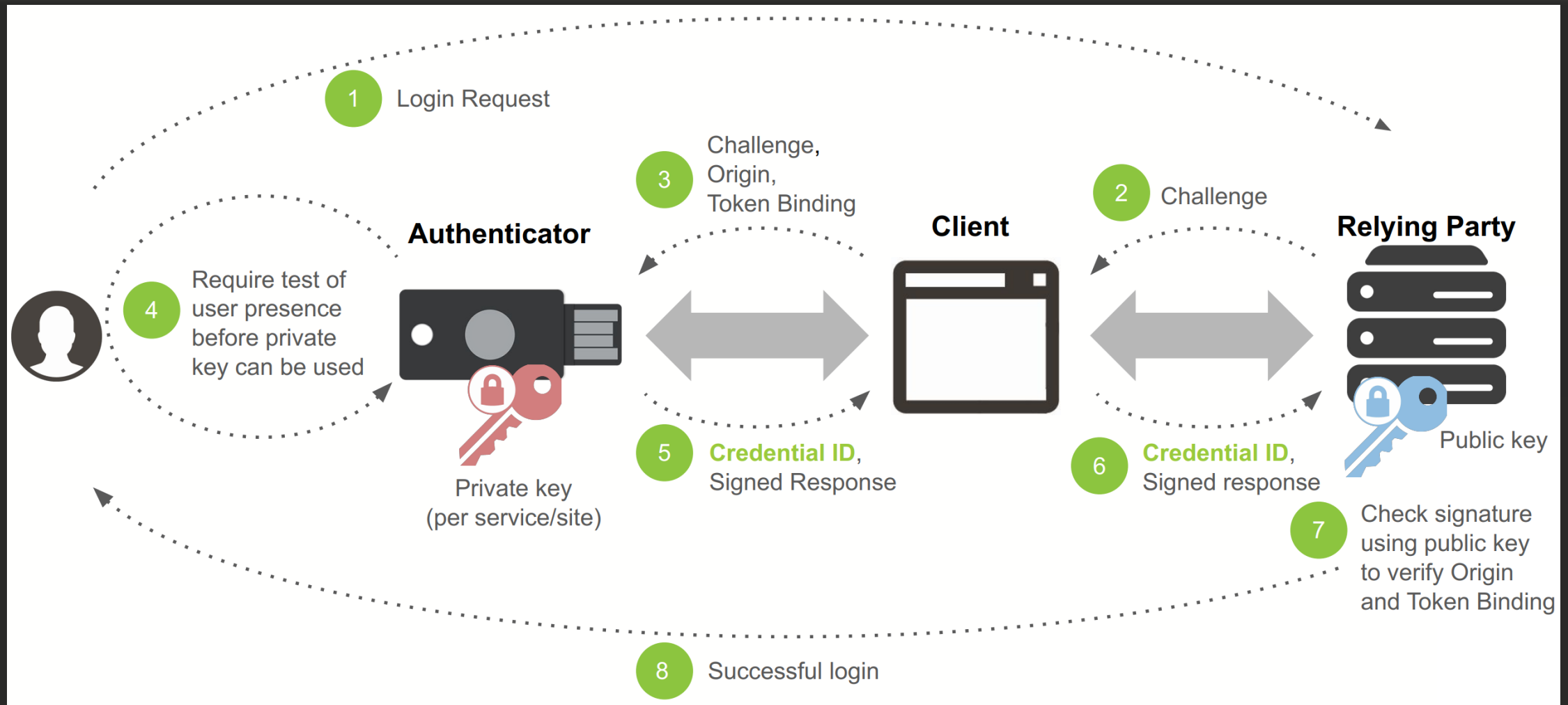
INFOTECH
[ IT & Communication ]


- **Passwortlose Authentifizierung möglich**
  - PIN oder Biometrie
- **Kein Benutzername mehr**
- **CTAP2 = Protokoll zwischen Browser und FIDO2-Gerät**
- **WebAuthn = Protokoll zwischen Browser und Server**
- **Login auf**
  - diverse Websites (Azure, Okta, Google, Apple, PayPal, ...)
  - diverse Passwort-Manager (Bitwarden, 1Password, Passbolt, ...)
  - Windows

# Zweifaktor- / Mehrfaktor-Authentifizierung

## FIDO 2

INFOTECH
[IT & Communication]



# Zweifaktor- / Mehrfaktor-Authentifizierung
# Windows Hello for Business

INFOTECH
[ IT & Communication ]

- Eigenständige Authentifizierungsmethode
- An Gerät gebunden (TPM) => 1. Faktor
- 2. Faktor: PIN, Fingerabdruck, Gesicht oder Iris
- Kann auf FIDO2 kompatiblen Websites verwendet werden
- Nachteil: nur Windows-Geräte

# Zusammenfassung

INFOTECH
[IT & Communication]

- **Schwache Authentifizierung**
  - Single-Factor (UN+PW, SMS, etc.)
- **Starke Authentifizierung**
  - Multi-Factor (TOTP/HOTP, etc.)
- **Starke passwortlose Authentifizierung**
  - Push Notifications
- **Starke passwortlose und Phishing-resistente Authentifizierung**
  - FIDO2
  - Windows Hello For Business
  - Zertifikatsbasierte Authentifizierung

# Vergleich / Bewertung von Microsoft

INFOTECH
...ication]

| Authentication method combination | MFA strength | Passwordless MFA strength | Phishing-resistant MFA strength |
|---|---|---|---|
| FIDO2 security key | ✓ | ✓ | ✓ |
| Windows Hello for Business | ✓ | ✓ | ✓ |
| Certificate-based authentication (Multi-Factor) | ✓ | ✓ | ✓ |
| Microsoft Authenticator (Phone Sign-in) | ✓ | ✓ | |
| Temporary Access Pass (One-time use AND Multi-use) | ✓ | | |
| Password + something you have[1] | ✓ | | |
| Federated single-factor + something you have[1] | ✓ | | |
| Federated Multi-Factor | ✓ | | |
| Certificate-based authentication (single-factor) | | | |
| SMS sign-in | | | |
| Password | | | |
| Federated single-factor | | | |

Quelle: https://learn.microsoft.com/en-us/entra/identity/authentication/concept-authentication-strengths#built-in-authentication-strengths

# Was nehmen wir vom Vortrag mit?

# Infotech Kaffeetassen!

INFOTECH
[ IT & Communication ]

- **Welche Authentifizierungsmethode sollte in Microsoft ActiveDirectory NICHT mehr verwendet werden?**
  - NTLM
- **Wie nennt man die Möglichkeit, eine Identität bei verschiedenen Diensten zu verwenden und sich nur einmal anmelden zu müssen?**
  - Single-SignOn (SSO)
- **Was wird bei FIDO2 zusätzlich zum Gerät noch benötigt?**
  - PIN oder Biometrie

INFOTECH
[IT & Communication]

# Zukunftssichere Authentifizierung - Ja, die gibt‘s!

**Dipl.-Ing. Franz Strasser**

Ihr Systemhaus.

INFOTECH

[ IT & Communication ]

Ihr Systemhaus.