How adaptive is the CAT?

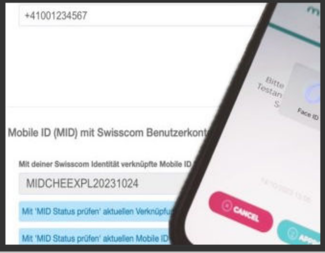
24.10.2023, H-P Waldegger

Who controls access to your sensitive customer data?

Authentication traditionally assured at point in time

Assurance level (LoA) categorization and path to password-less authentication

LoA 4



- username or ID
- centralized user certificate/public key (and processes)
- two auth factors bound/signed in user device
- cryptographically verified against centralized proof

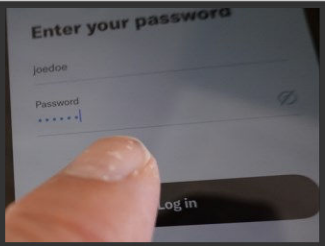
LoA 3

- username/password and
- two auth factors bound/signed in user device
- bound and cryptographically verified at backend

LoA 2

- username/password and
- second factor (e.g., OTP, mTAN)
- bound and verified at backend

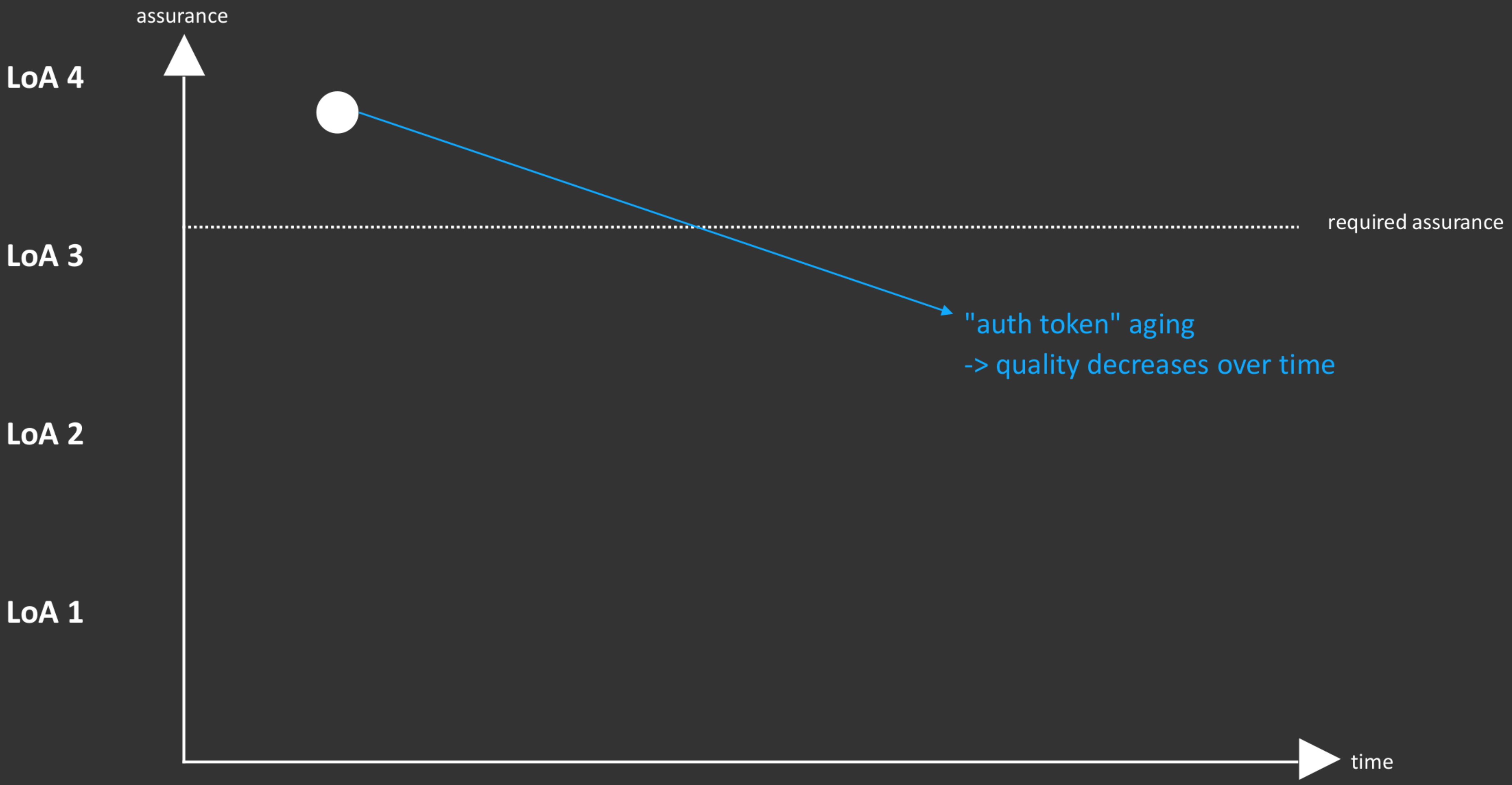
LoA 1



- username/password
- verified at backend

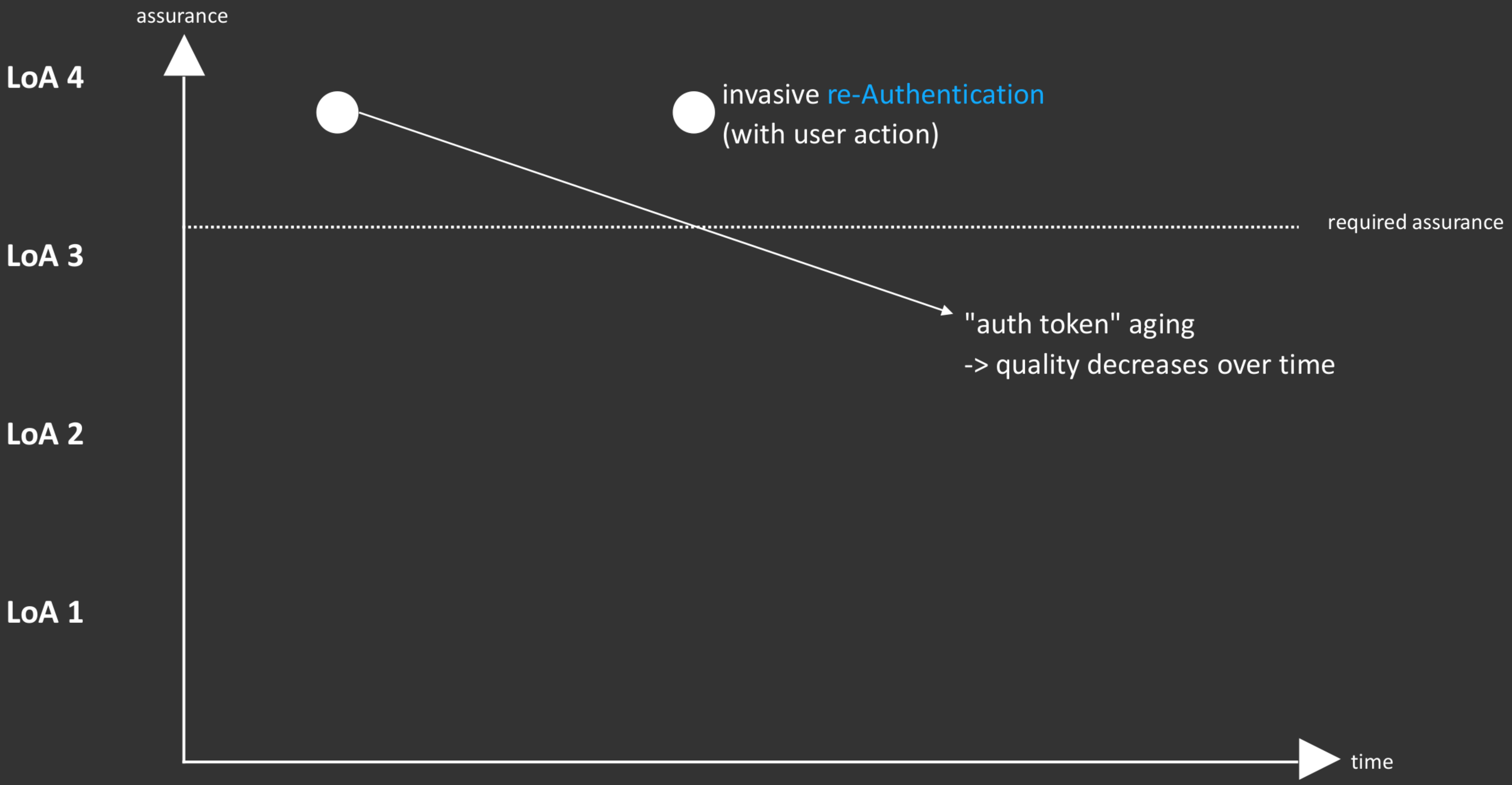
Authentication assured at point in time is subject to aging

Point-in-time authentication is rarely sufficient



Authentication assured at point in time is subject to aging

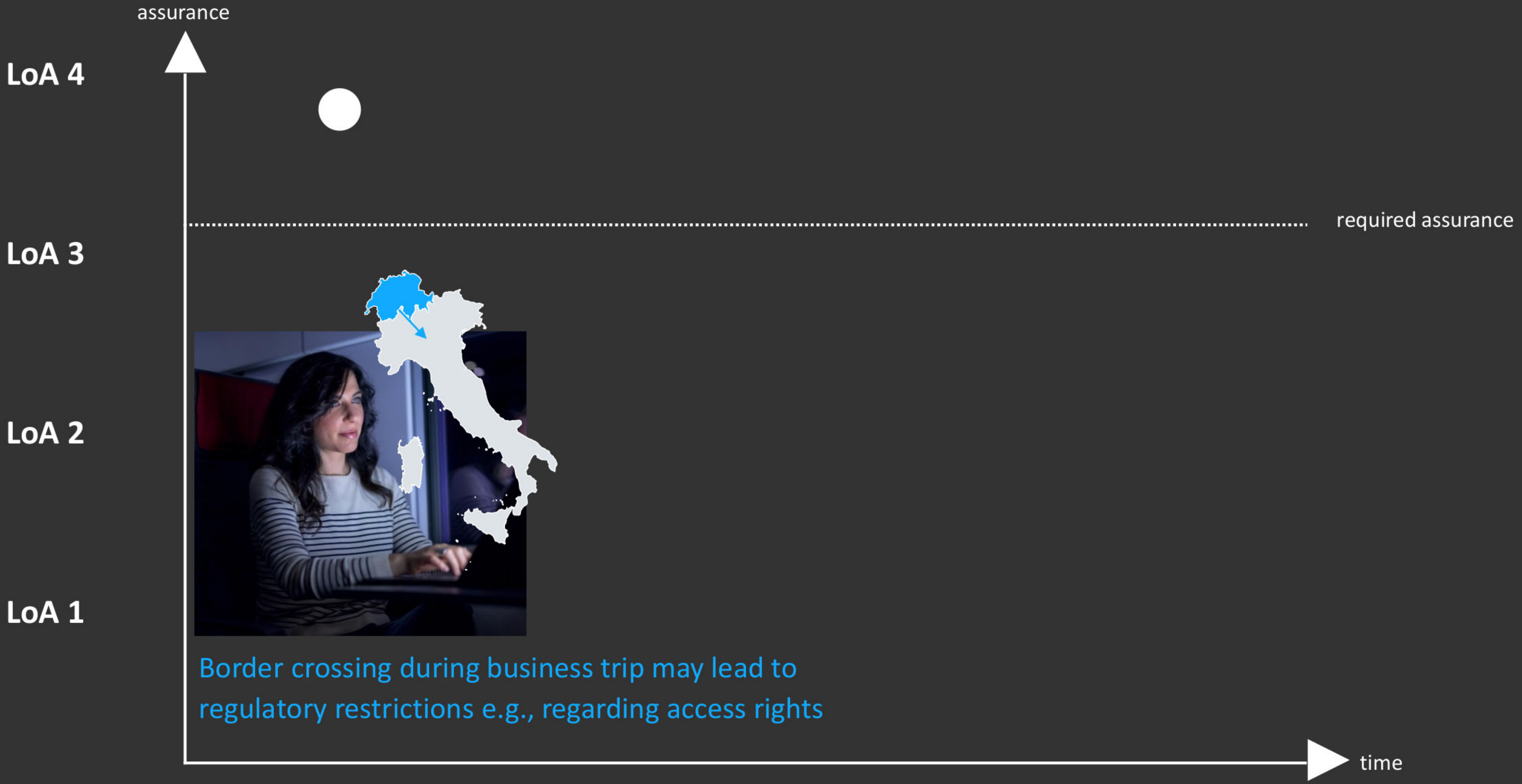
Periodic re-authentication necessary to get back to required assurance level



H-P Waldegger, swisscyberstorm.com, C1 Public

Authentication assured at point in time is subject to aging

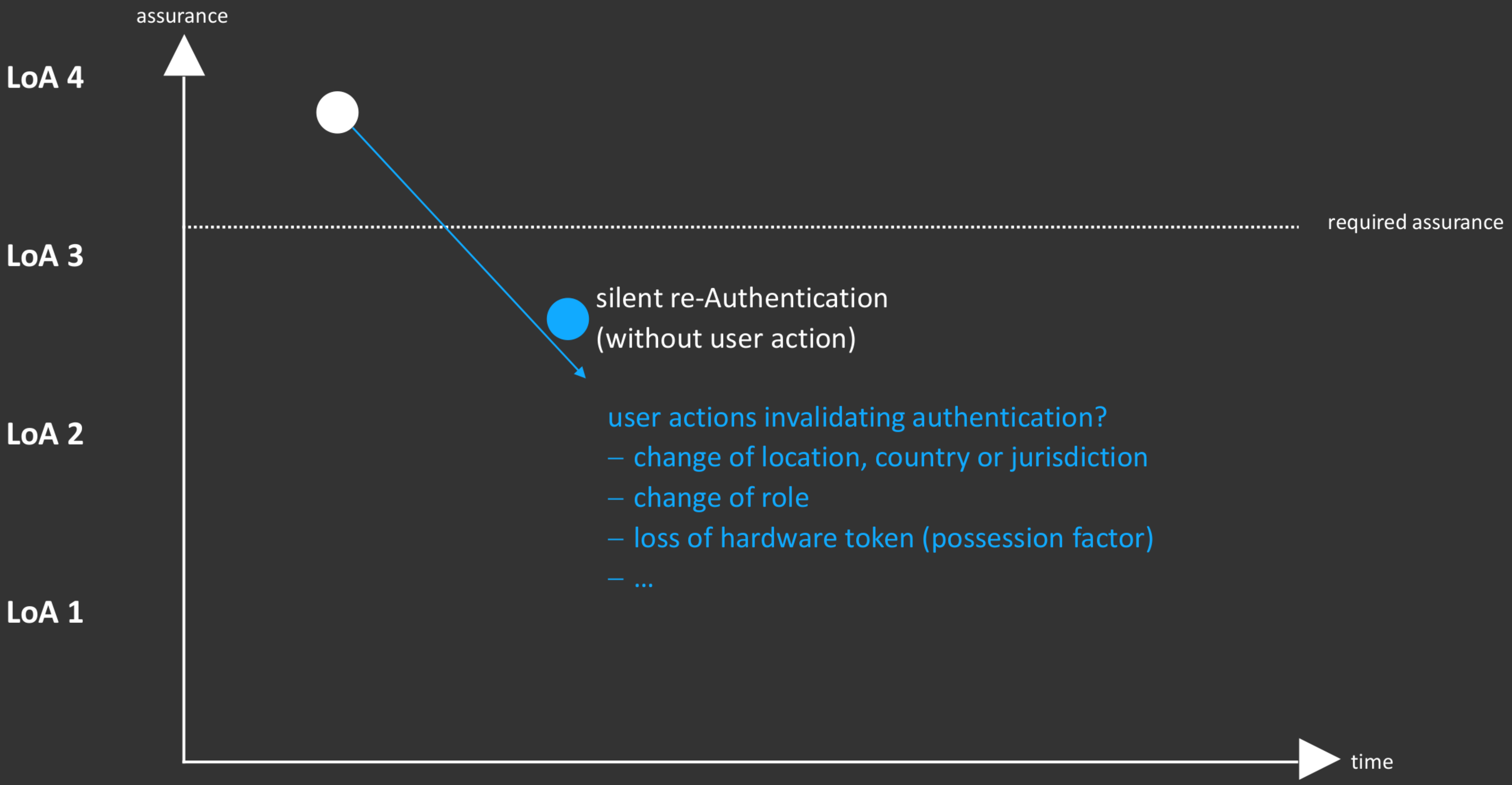
User-action may invalidate authentication or role assignment



Border crossing during business trip may lead to regulatory restrictions e.g., regarding access rights

Authentication assured at point in time is subject to aging

Frequent authentication requires adaptive strength to prevent user negligence



silent re-Authentication (without user action)

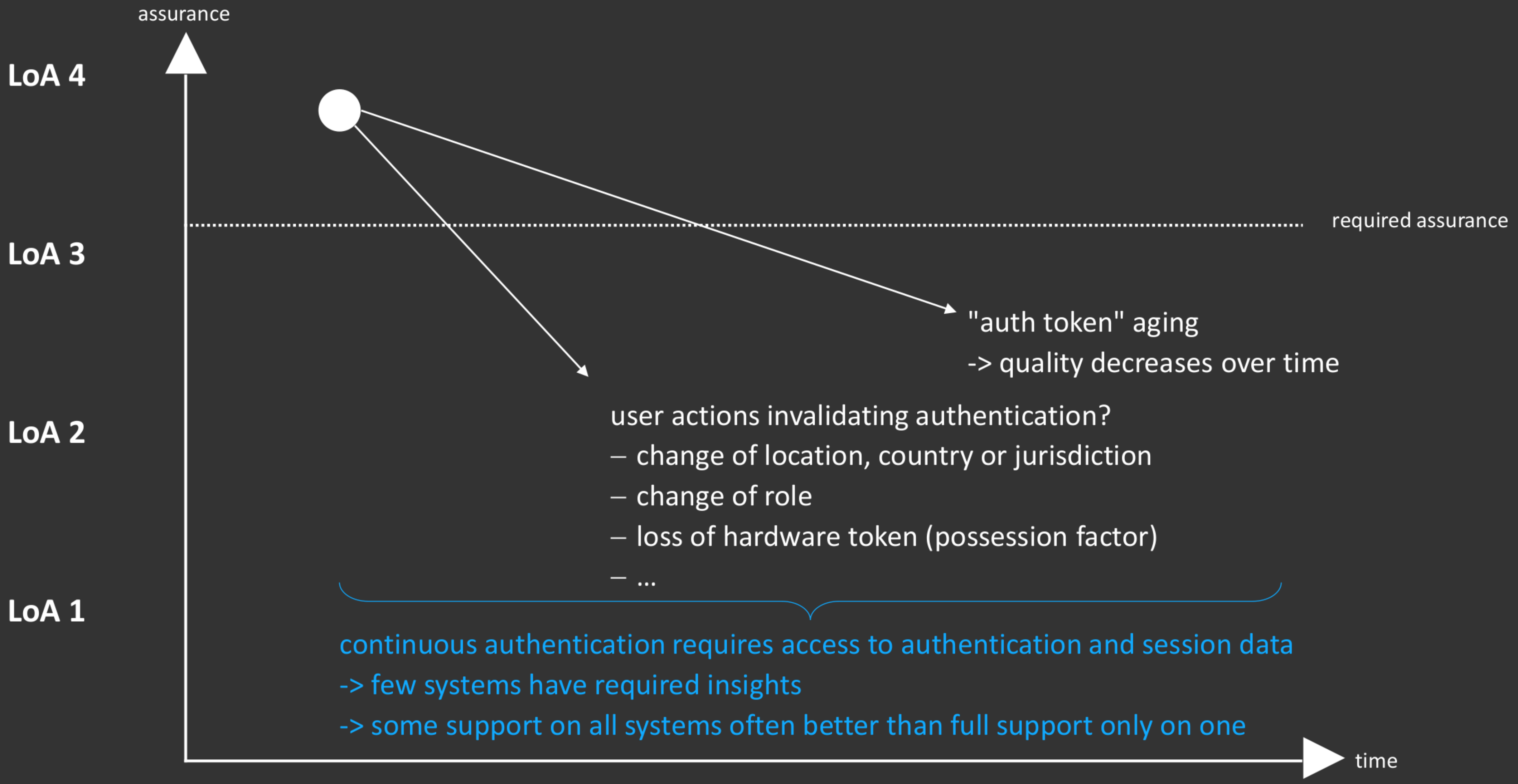
user actions invalidating authentication?

- change of location, country or jurisdiction
- change of role
- loss of hardware token (possession factor)
- …

H-P Waldegger, swisscyberstorm.com, C1 Public

Authentication assured at point in time is subject to aging

Human Factor: How often can someone re-authenticate without getting negligent?



"auth token" aging
-> quality decreases over time

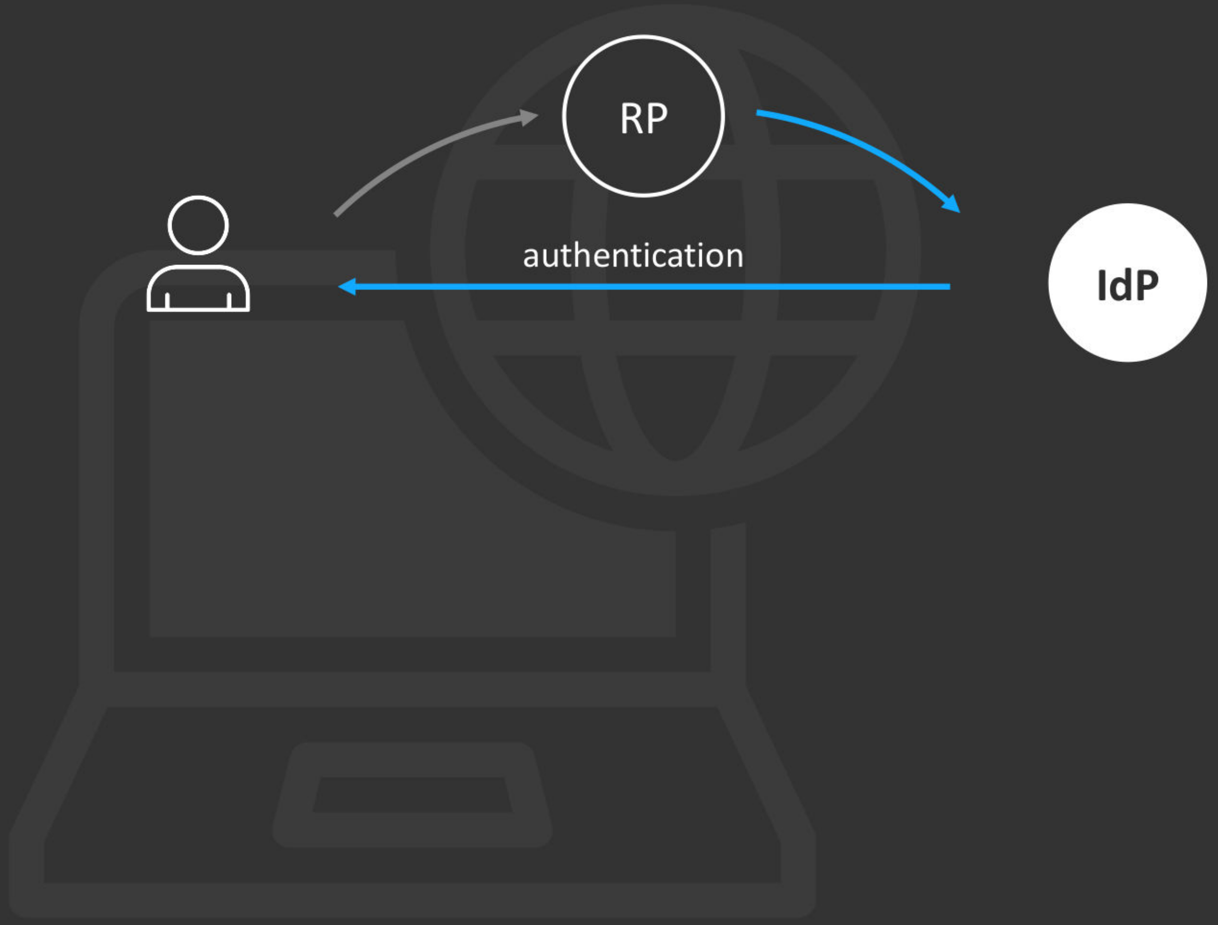
user actions invalidating authentication?

- change of location, country or jurisdiction
- change of role
- loss of hardware token (possession factor)
- ...

continuous authentication requires access to authentication and session data
-> few systems have required insights
-> some support on all systems often better than full support only on one

Continuous authentication is a challenge in federated systems

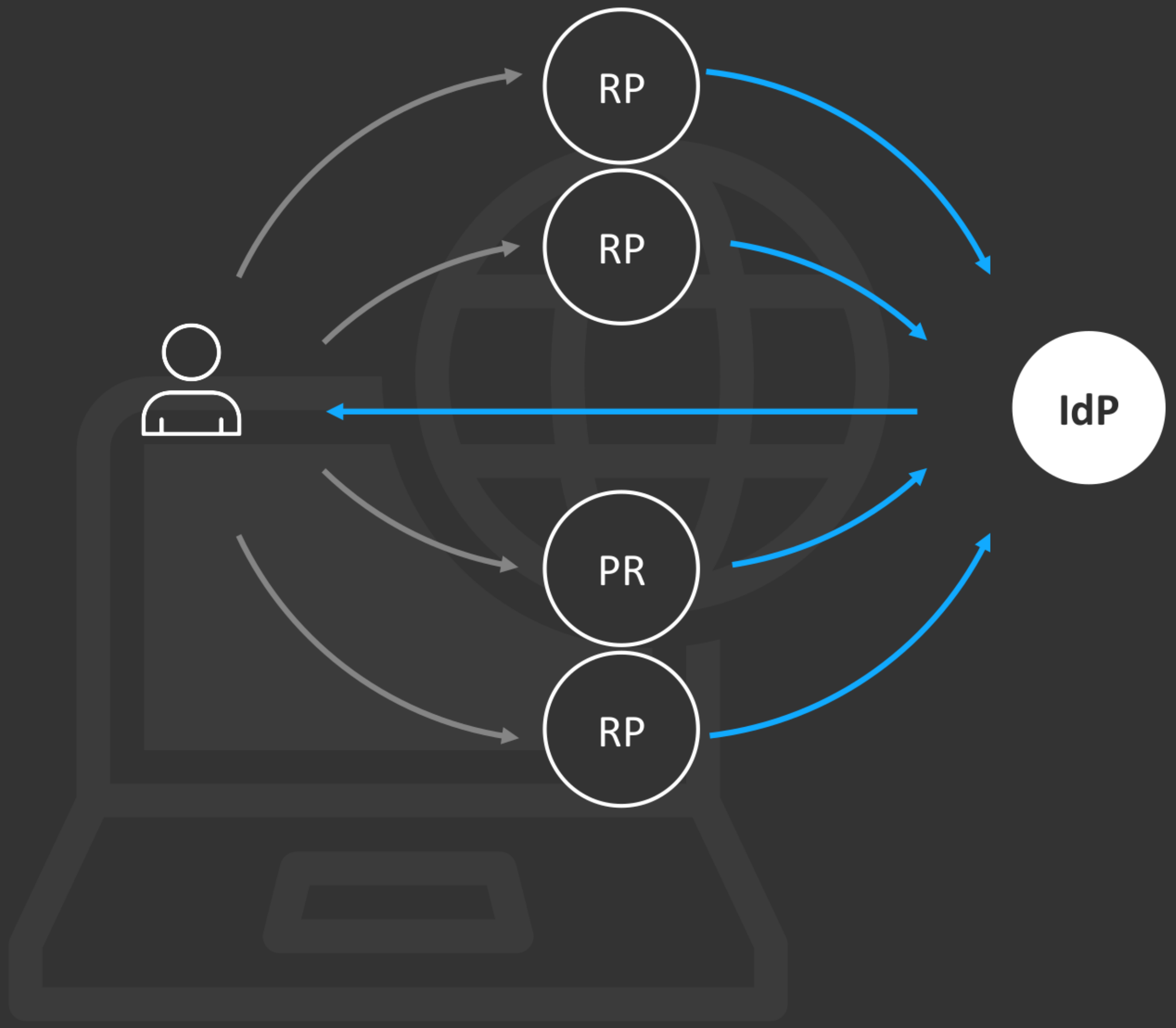
IdP (authentication system) and RP (enforcement point) need to cooperate



In distributed/federated environments relying party (RP) and the authenticating system (IdP) need to co-operate to support continuous authentication.

Continuous authentication is a challenge in federated systems

IdP in strong position to reduce authentication requests requiring user interaction

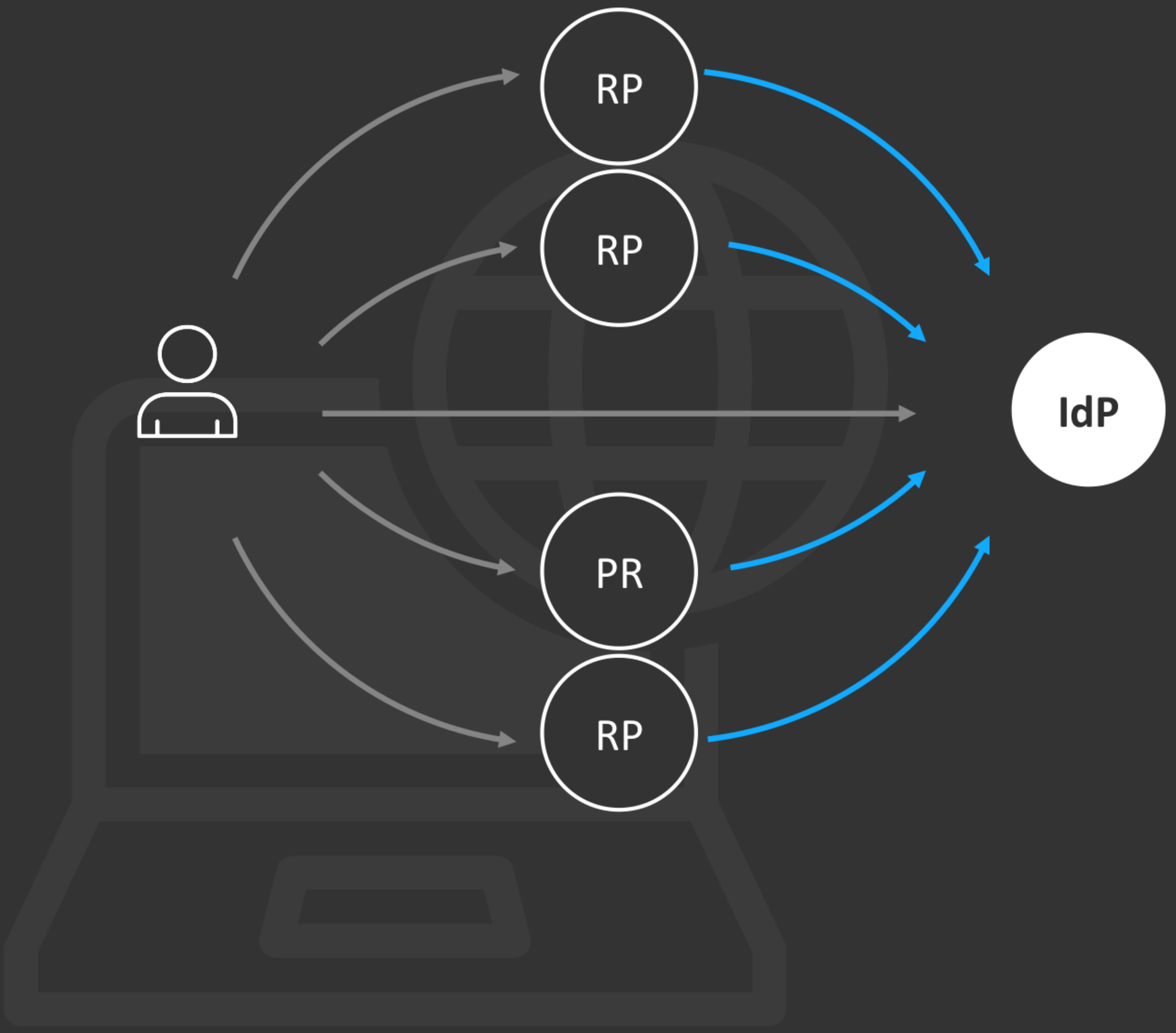


In a complex (B2B) environment with different relying parties (RP), the authenticating system (IdP) has good insight of the user overall status.

H-P Waldegger, swisscyberstorm.com, C1 Public

Continuous authentication is a challenge in federated systems

IdP and RP need to cooperate – protocols and semantics yet to be finalized

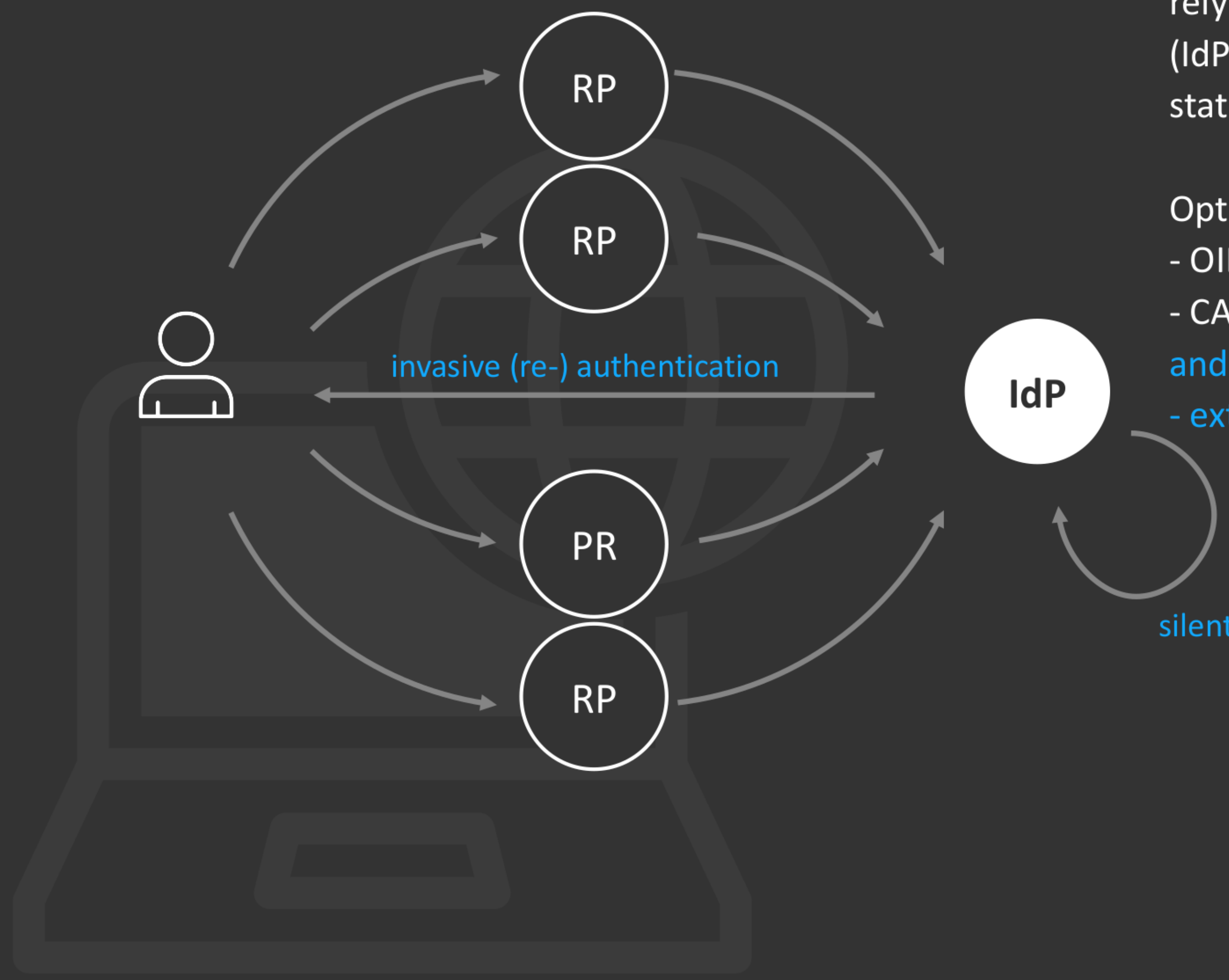


In a complex (B2B) environment with different relying parties (RP), the authenticating system (IdP) has better insight of the user overall status.

Options to share information, e.g.:
- OIDC attributes (claims)
- CAEP protocol? (on watch list)

Continuous authentication is a challenge in federated systems

Re-authentication without user-interaction can keep required assurance level



In a complex (B2B) environment with different relying parties (RP), the authenticating system (IdP) has better insight of the user overall status.

Options to share information, e.g.:
- OIDC attributes (claims)
- CAEP protocol? (on watch list)

and
- extended definition of assurance levels

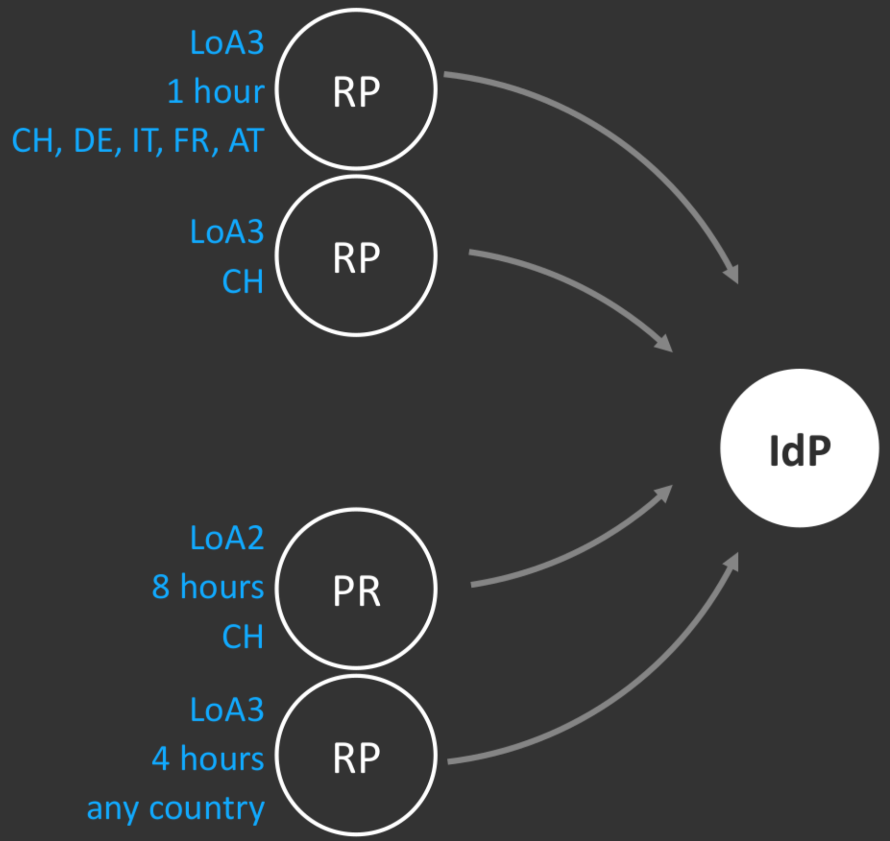
What about the adaptive part?

Extended definition of assurance level allows RP to remain in control of risk level

LoA 4	always authenticate LoA4 (no silent execution)
LoA 3	OK (silent), if • LoA3 or higher during last x minutes and • same country (if requested) else re-authenticate LoA3
LoA 2	OK (silent), if • LoA2 or higher during last x minutes and • same country (if requested) else re-authenticate LoA2
LoA 1	OK (silent), if • LoA1 or higher during last x minutes and • same country (if requested) else re-authenticate LoA1

What about the adaptive part?

Each RP can adapt re-authentication to own risk level or compliance requirement



LoA 4 always authenticate LoA4
(no silent execution)

LoA 3 OK (silent), if

- LoA3 or higher during last x minutes and
- same country (if requested)

else re-authenticate LoA3

LoA 2 OK (silent), if

- LoA2 or higher during last x minutes and
- same country (if requested)

else re-authenticate LoA2

LoA 1 OK (silent), if

- LoA1 or higher during last x minutes and
- same country (if requested)

else re-authenticate LoA1

What about the adaptive part?

Further topics of interest being investigated to support continuous adaptive trust

Behavioral Factors (Something the user does)

- Keystroke Dynamics
- Mouse Movement Patterns
- Navigational Patterns
- Touch Dynamics
- Gait Analysis

Location Factors

- GPS
- IP Address Monitoring
- WiFi Network

Temporal Factors

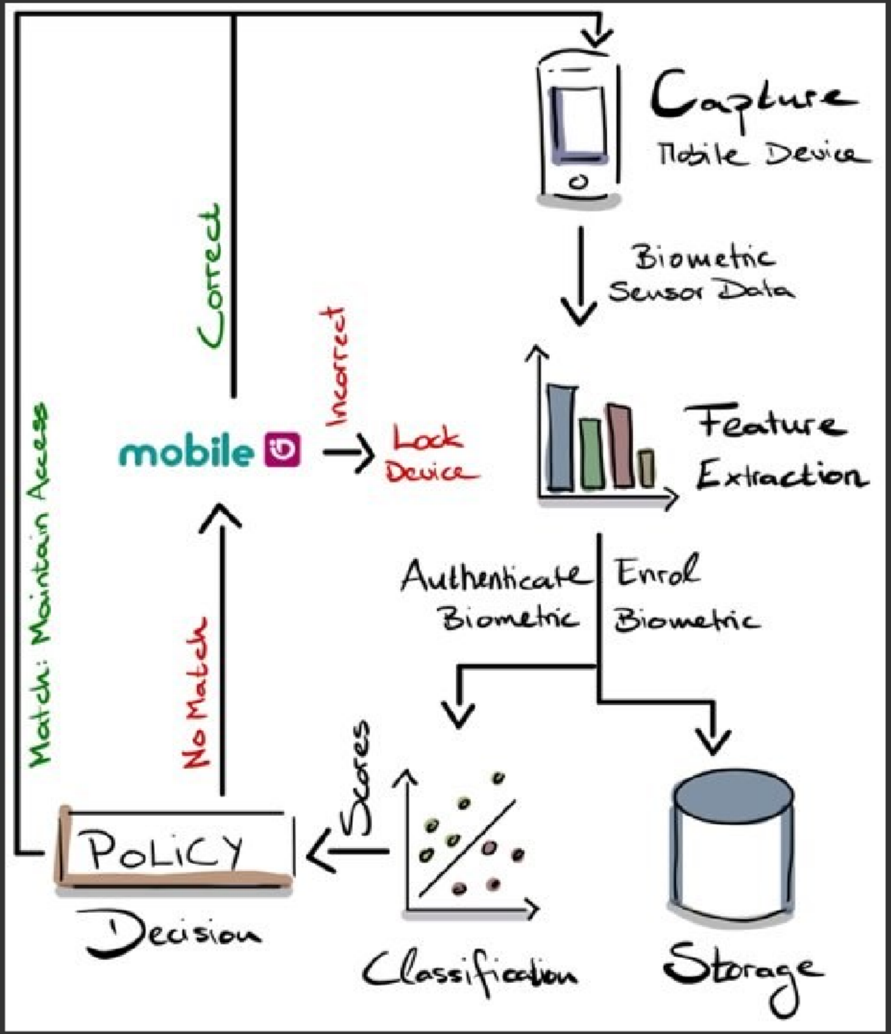
- Time of Activity

Device Factors

- Device Profiling
- Browser or App Profiling

Environmental Factors

- Ambient Sound or Light
- Temperature



Questions?

Innovators of Trust
trustworthy, committed, curious

And regarding trust: We return confidence scores offering full transparency

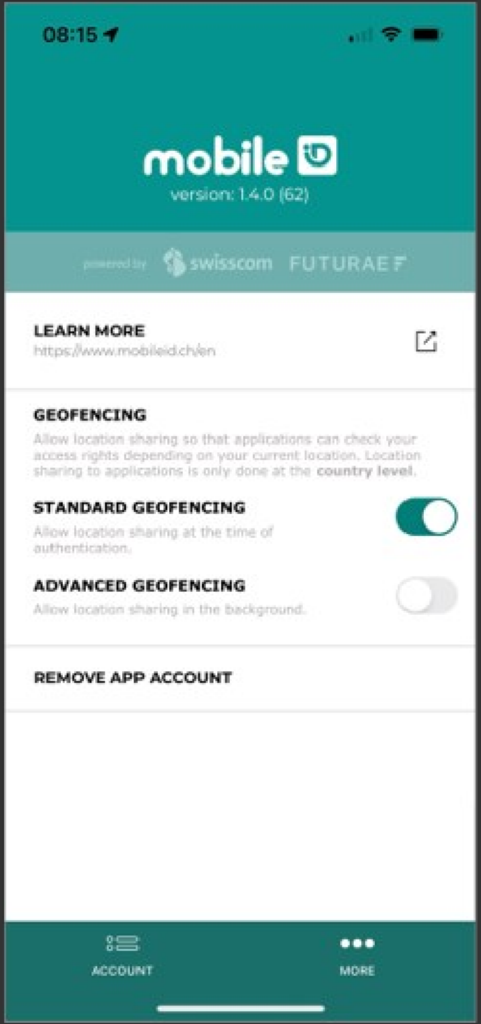
Current state of technical PoC to validate flow and clarify privacy options

Phase 1: Initial Authentication
Initially, the user attempts to log in to the Relying Party. Dependent on user history, they may be prompted via Mobile-ID OpenID Connect (OIDC) to confirm an MFA authentication on the mobile device. After successful user authentication (a) the Relying Party receives an Access Token from Mobile-ID OIDC and b) there is an active session between the user and the Relying Party.

Phase 2: Continuous Authentication
Using the Access Token, the Relying Party can continuously obtain user information from the OIDC */userinfo* endpoint. This process does not require user interaction and can be done silently in the background. The information (claims; related to the SIM or APP location) retrieved from the OIDC service allows the Relying Party to further determine whether or not a user re-authentication is required to keep the user session active.

CAUTH confidence scores

- device confidence
- location confidence



version: 1.4.0 (62)

LEARN MORE
https://www.mobileid.ch/en

GEOFENCING
Allow location sharing so that applications can check your access rights depending on your current location. Location sharing to applications is only done at the **country level**.

STANDARD GEOFENCING
Allow location sharing at the time of authentication.

ADVANCED GEOFENCING
Allow location sharing in the background.

REMOVE APP ACCOUNT

H-P Waldegger

Manager Cyber Security, Swisscom B2B

hans-peter.waldegger@swisscom.com
+41-58-223 44 16

Go for strong authentication!
https://www.swisscom.ch/mobileid

Contact

Cyber Security for the connected world.

More information on www.swisscom.ch/security