Redefining the Perimeter

Zero-trust & Device-Bound Access Security

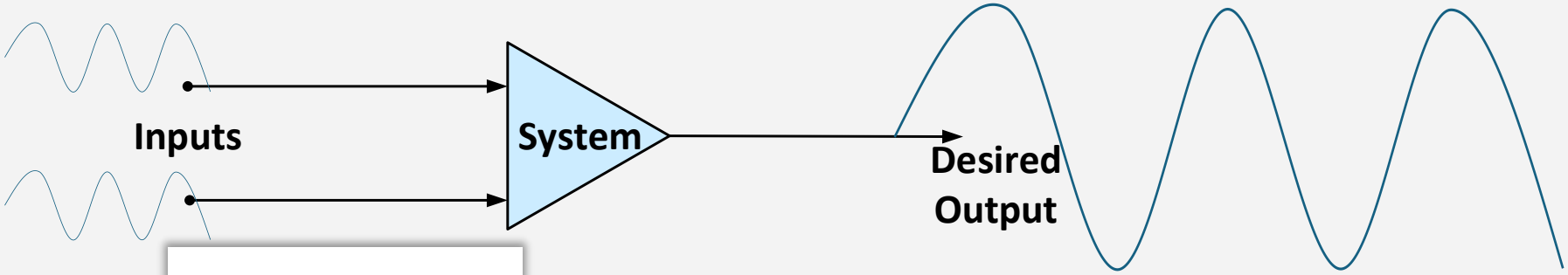
Our mission is to protect yours.

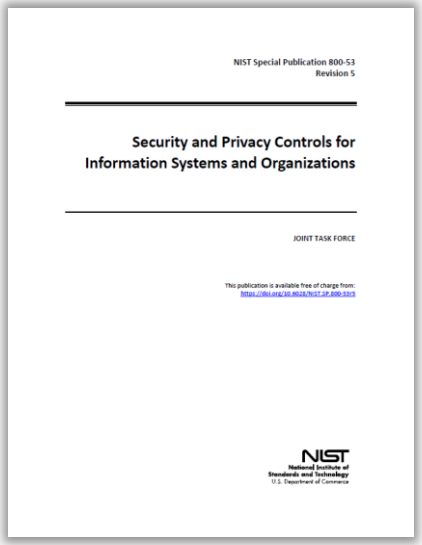
Introductions

- David Rihak, Peig
- Co-founder, Chief Product Manager
- Prior role: Digital Identity Architect, ADUCID. EU cross-border eID system design
- eIDAS eID assurance level substantial & high system architect
- 8 + years user authentication and digital identity system architecture experience

- Jim Matthews, Triangle Cyber
- Electrical Engineer, Architect, Systems Engineer/Integrator
- 35+ yrs DoD & Federal experience including DHS CISA, Missile Defense Agency, and US Navy
- Chief Architect, DHS CISA Cyber Analytic and Data System
- Former Raytheon Engineering Fellow
- Naval Surface Warfare Center Dahlgren Division (NSWCDD)

Building Cyber-Resilient Systems




NIST Special Publication 800-53
Revision 5

Security and Privacy Controls for
Information Systems and Organizations

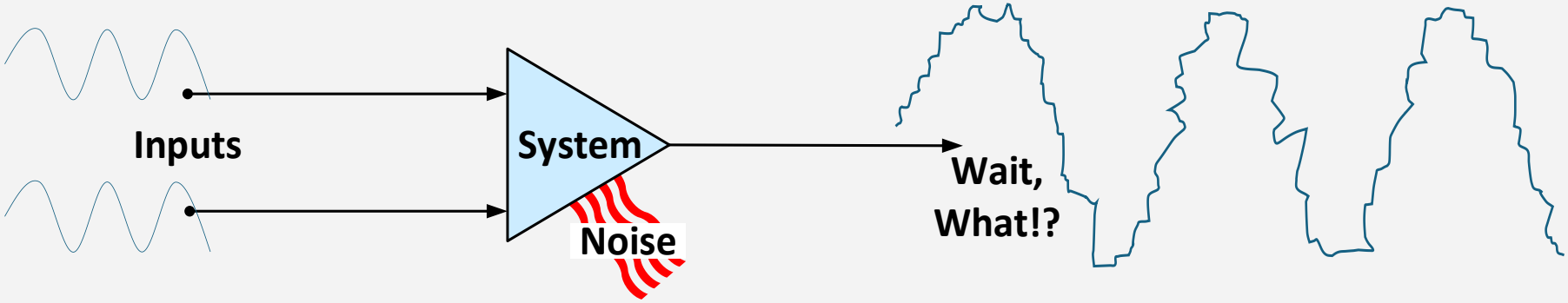
JOINT TASK FORCE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-53r5

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

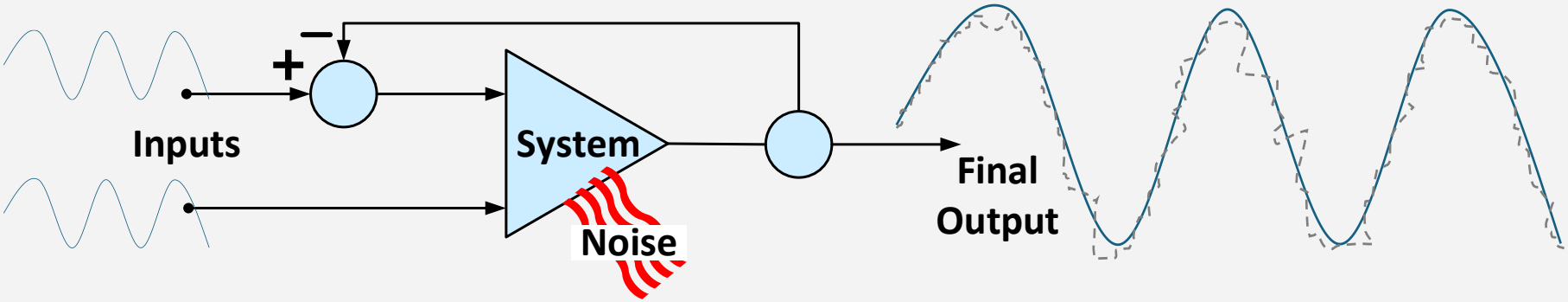
*Just implement 100% of the 1,000+ NIST SP 800-53 security controls *everywhere*, and we should be fine, right?*

A day in the life of a Cybersecurity Engineer..



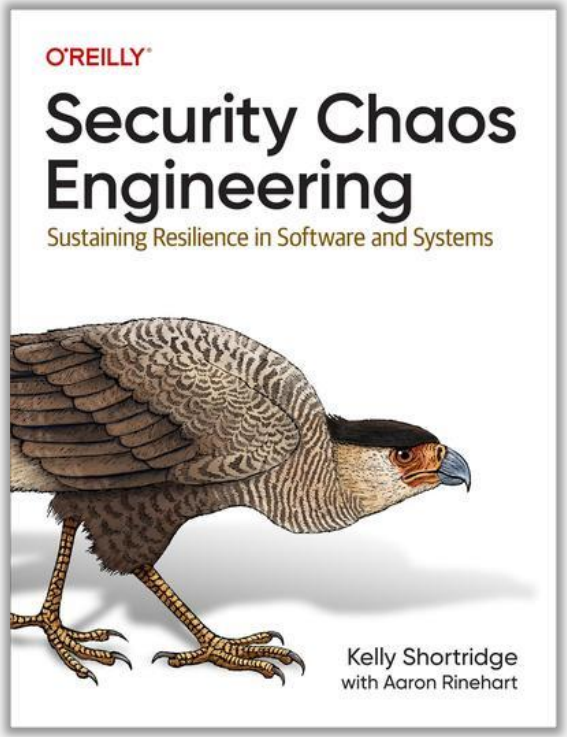
- ✓New Attacks
- ✓New Advisories
- ✓Updated vulnerability scanning tools
- ✓New Security Controls
- ✓Unexpected changes
- ✓Resource constraints

Feedback is the key…



- ✓Feedback allows you to adjust your inputs and leads to a more stable output
- ✓CISA/FBI/NSA/Vendor Advisories & Threat Reports

Security Chaos Engineering



Feedback Loops and Learning Culture

"*Resilience depends on remembering failure and learning from it.*"

"*Feedback loops, in which outputs from the system are used as inputs in future operations, are therefore essential for system resilience.*"

Verizon DBIR “Winner“ in 2024 breaches

Use of stolen credentials

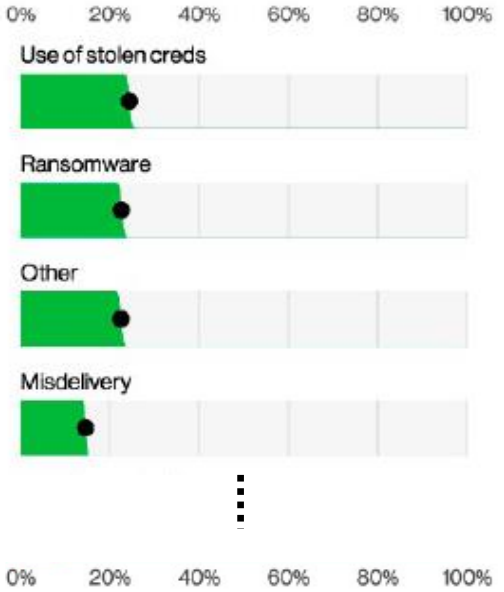


Figure 15. Top Action varieties in breaches (n=9,982)

CrowdStrike 2025 Global Threat Report

Recommendations

1 Secure the entire identity ecosystem

Adversaries increasingly target identities using credential theft, MFA bypass, and social engineering while covertly moving laterally between on-premises, cloud, and SaaS environments via trusted relationships. This allows them to impersonate legitimate users, escalate access, and evade detection.

Organizations should adopt phishing-resistant MFA solutions, such as hardware security keys, to prevent unauthorized access. Strong identity and access policies are essential, including just-in-time access, regular account reviews, and conditional access controls. Identity threat detection tools must monitor behavior across endpoints and on-premises, cloud, and SaaS environments to flag privilege escalation, unauthorized access, or backdoor account creation. Integrating these tools with XDR platforms ensures comprehensive visibility and a unified defense against adversaries.

Additionally, organizations should educate users to recognize vishing and phishing attempts while maintaining proactive monitoring to detect and respond to identity-based threats.

2 Eliminate cross-domain visibility gaps

Adversaries' growing use of hands-on-keyboard techniques and legitimate tools makes detection and response more difficult. Unlike traditional malware, these methods allow attackers to bypass traditional security measures by executing commands and using legitimate software to mimic normal operations.

To counter this, organizations must modernize their detection and response strategies. XDR and next-generation security information and event management (SIEM) solutions provide unified visibility across endpoints, networks, cloud environments, and identity systems, enabling analysts to correlate suspicious behaviors and see the full attack path.

Proactive threat hunting and threat intelligence further enhance detection by identifying potential attack patterns and providing insights into adversary tactics, techniques, and procedures. With real-time intelligence, organizations can stay informed about emerging threats, anticipate attacks, and prioritize critical security efforts.

3 Defend the cloud as core infrastructure

Cloud-focused adversaries are exploiting misconfigurations, stolen credentials, and cloud management tools to infiltrate systems, move laterally, and maintain persistent access for malicious activities like data theft and ransomware deployment.

Cloud-native application protection platforms (CNAPPs) with cloud detection and response (CDR) capabilities are critical to counter these threats.

These solutions provide operators with a unified view of their cloud security posture, helping them rapidly detect, prioritize, and remediate misconfigurations, vulnerabilities, and adversary threats. Additionally, enforcing strict access controls — such as role-based access and conditional policies — limits exposure to critical systems and ensures continuous monitoring for anomalies, including logins from unexpected locations.

Regular audits are also critical to maintaining security. Automated tools can uncover overly permissive storage settings, exposed APIs, and unpatched vulnerabilities. Frequent reviews of cloud environments ensure unused permissions and outdated configurations are addressed promptly.

4 Prioritize vulnerabilities with an adversary-centric approach

Adversaries are increasingly exploiting publicly disclosed vulnerabilities and using exploit chaining, combining multiple vulnerabilities to gain rapid access, escalate privileges, and bypass defenses. These multi-stage attacks often rely on public resources like POC exploits and technical blogs, enabling adversaries to craft effective and hard-to-detect payloads.

To counter these threats, organizations must prioritize regular patching or upgrading of critical systems, especially frequently targeted internet-facing services like web servers and VPN gateways. Monitoring for subtle signs of exploit chaining, such as unexpected crashes or privilege escalation attempts, can help detect attacks before they progress.

Tools like Falcon Exposure Management, built with native AI prioritization, enable teams to reduce noise and focus on the vulnerabilities that matter most, specifically those affecting critical and high-risk systems. By adopting proactive security approaches, discovering exposures across the attack surface, and leveraging automation, organizations can mitigate sophisticated threats and limit adversary opportunities.

5 Know your adversary and be prepared

When a cyberattack unfolds in minutes — or even seconds — being prepared can be the difference between containment and catastrophe. An intelligence-driven approach enables security teams to move beyond reactive defense by understanding which adversary is targeting them, how they operate, and what their objectives are. With threat intelligence, adversary profiling, and tradecraft analysis, security teams can prioritize resources, adapt defenses, and actively hunt for threats before they escalate. CrowdStrike's threat intelligence doesn't just detect known threats — it anticipates new and evolving tradecraft, ensuring defenders are always one step ahead. By seamlessly integrating intelligence into security workflows, organizations can accelerate response times, disrupt adversaries, and turn intelligence into action.

Though technology is critical to detect and stop intrusions, the end user remains a crucial link in the chain to stop breaches. Organizations should initiate user awareness programs to combat the continued threat of phishing and related social engineering techniques. For security teams, practice makes perfect. Encourage an environment that routinely performs tabletop exercises and red/blue teaming to identify gaps and eliminate weaknesses in your cybersecurity practices and response.

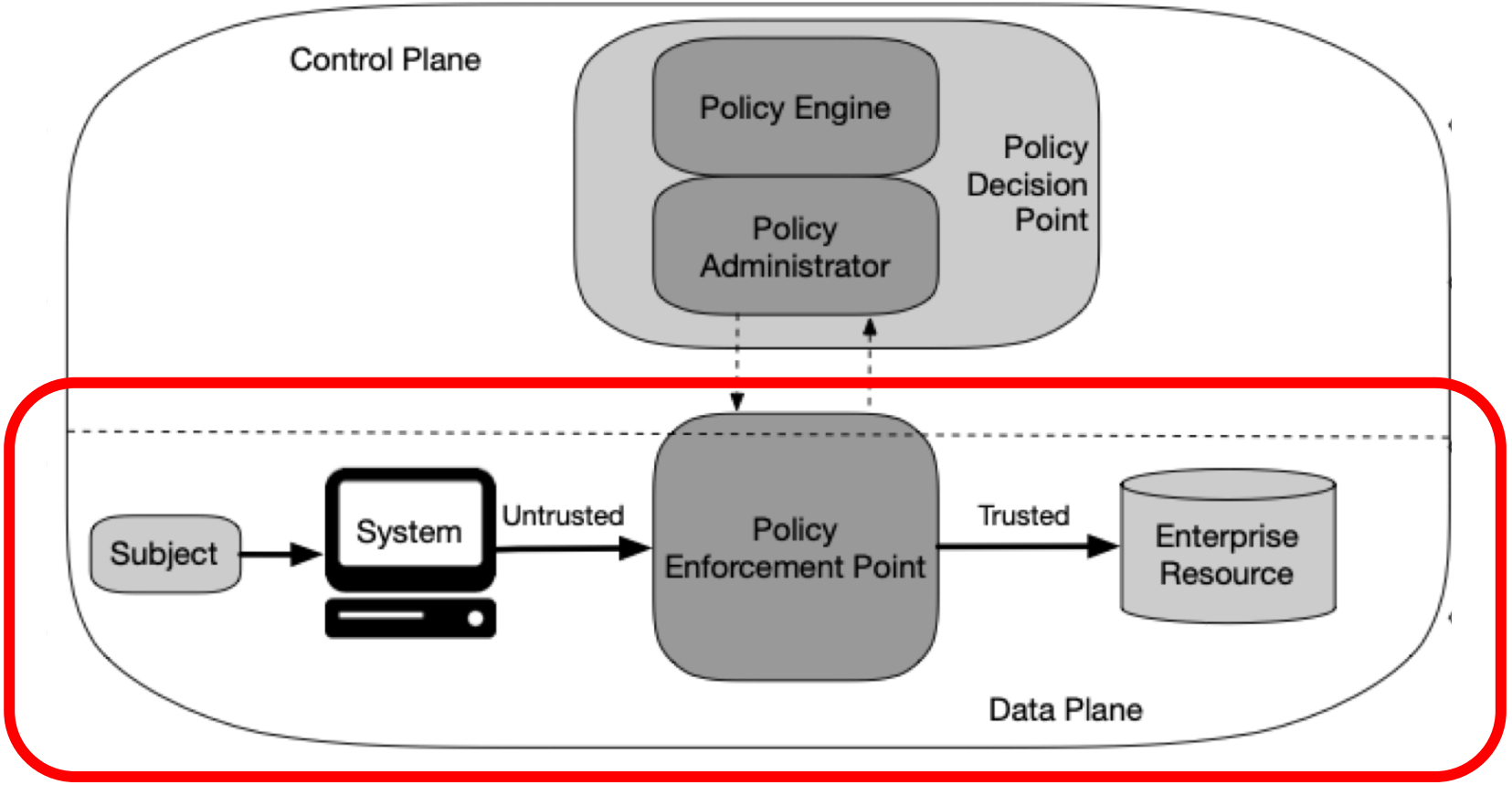
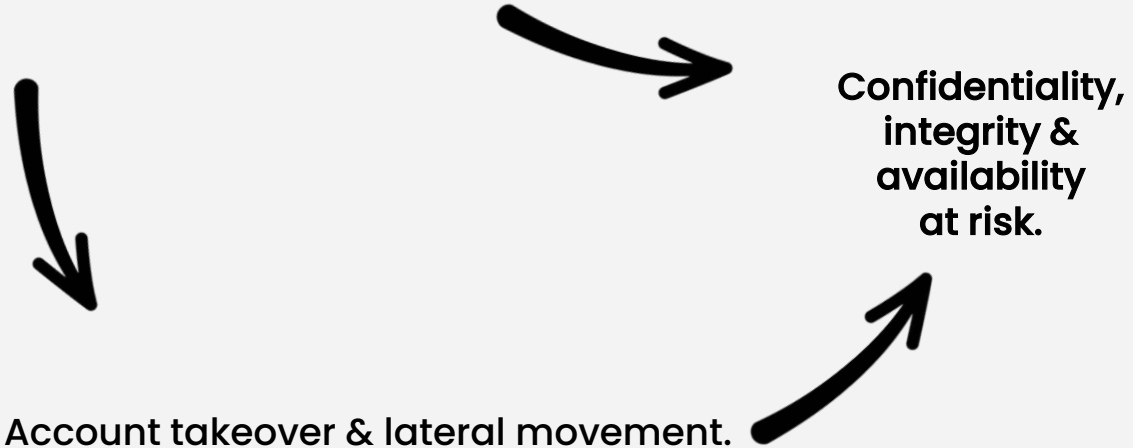
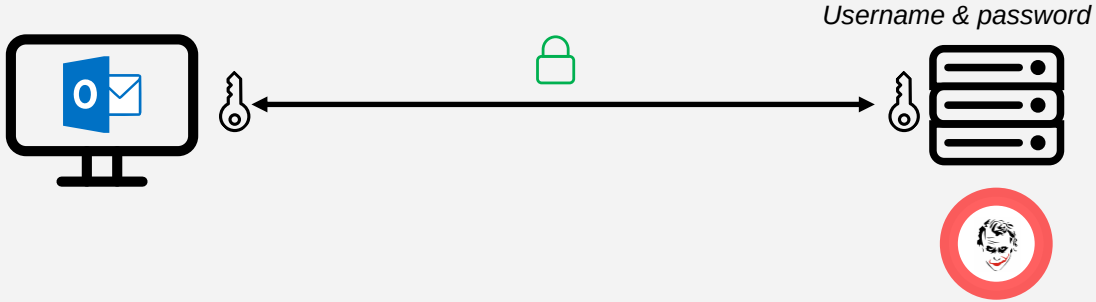


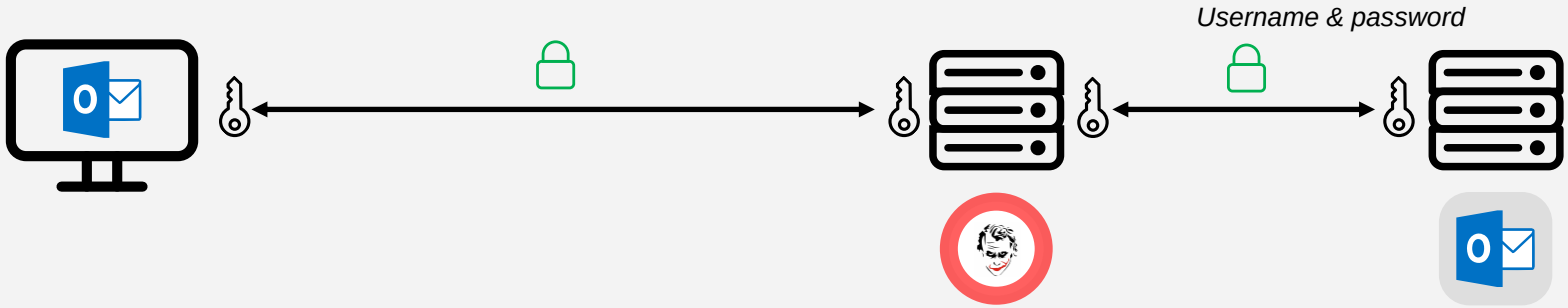
Figure 2: Core Zero Trust Logical Components

Threat: Use of Stolen CREDENTIALS

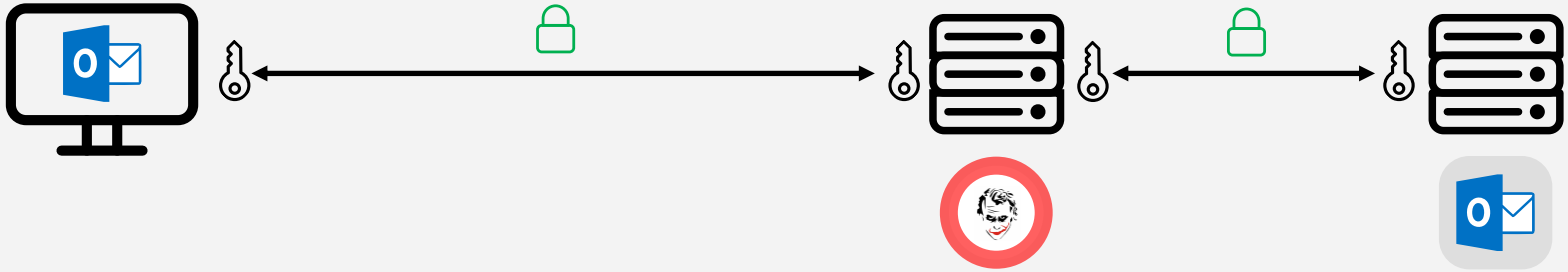
- **Reuse** for other “websites”.
- Social engineering, phishing.
- **CREDENTIALS** & **persistent session cookies!**

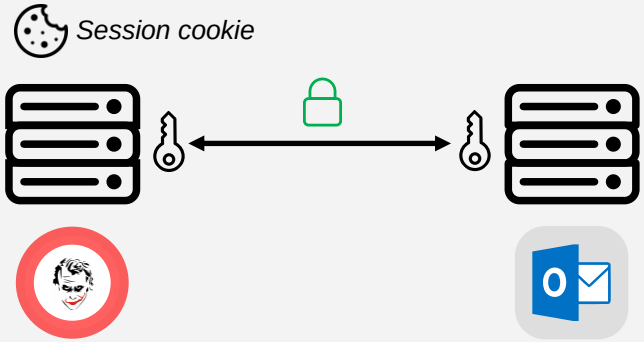



Username & password


Username & password

Dude's authenticator




Session cookie

MFA doesn’t prevent use of stolen credentials

MFA (theoretically) reduces time of access

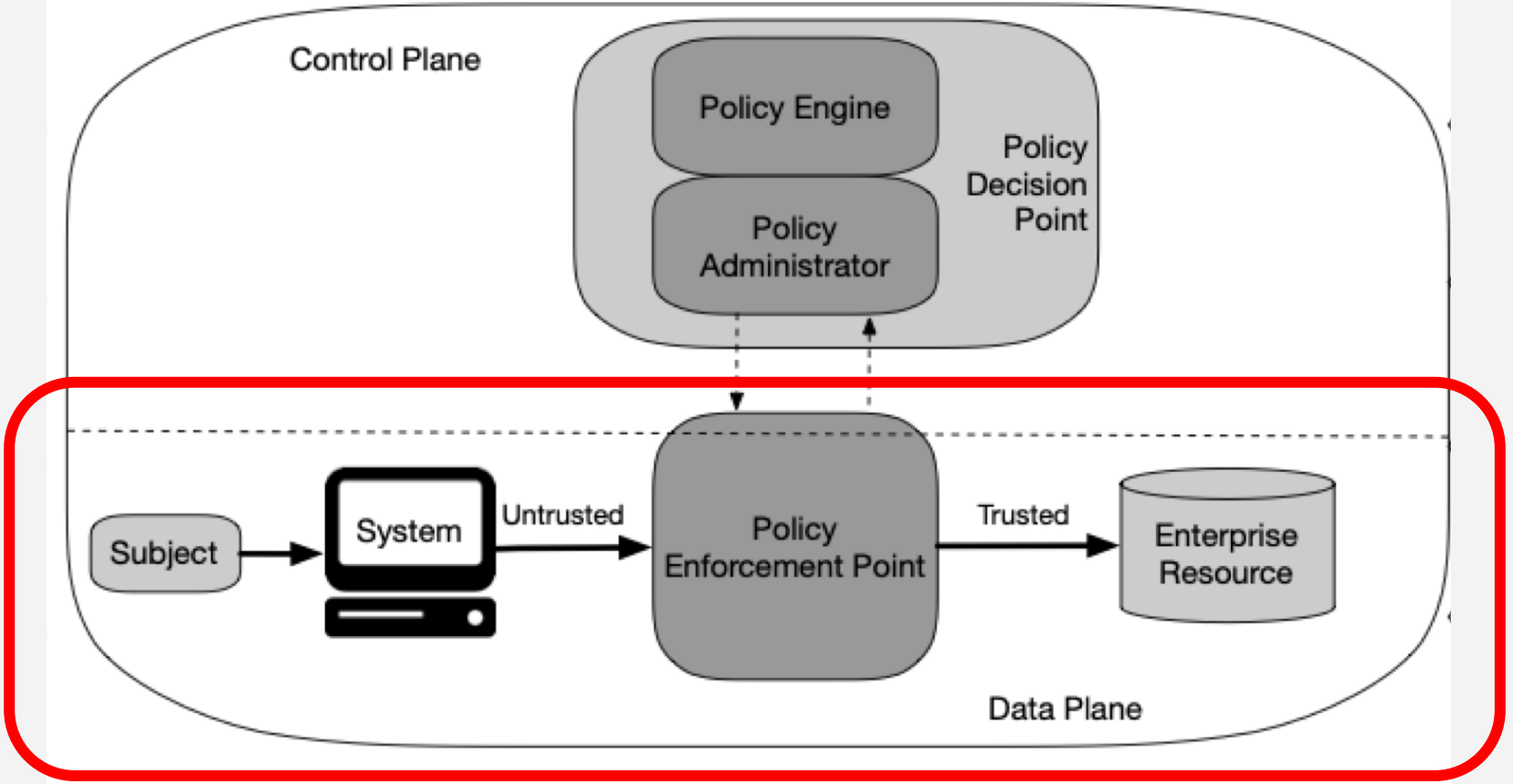


Figure 2: Core Zero Trust Logical Components

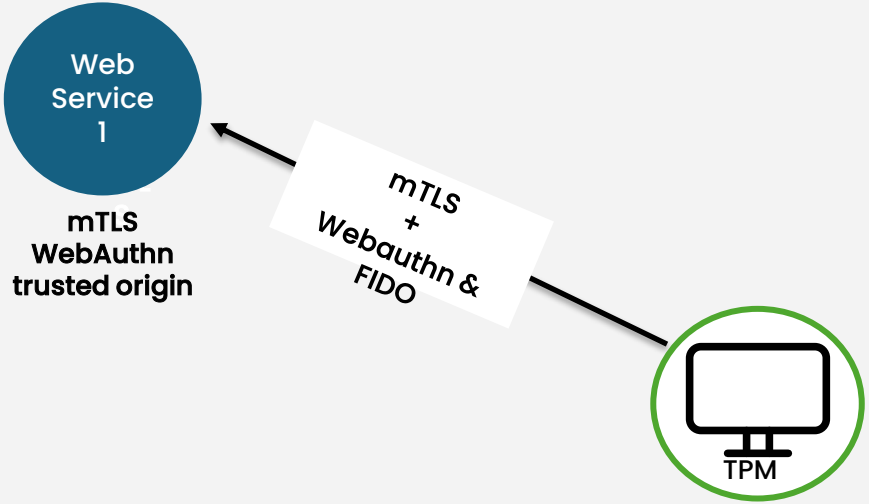
Access Security Building Block

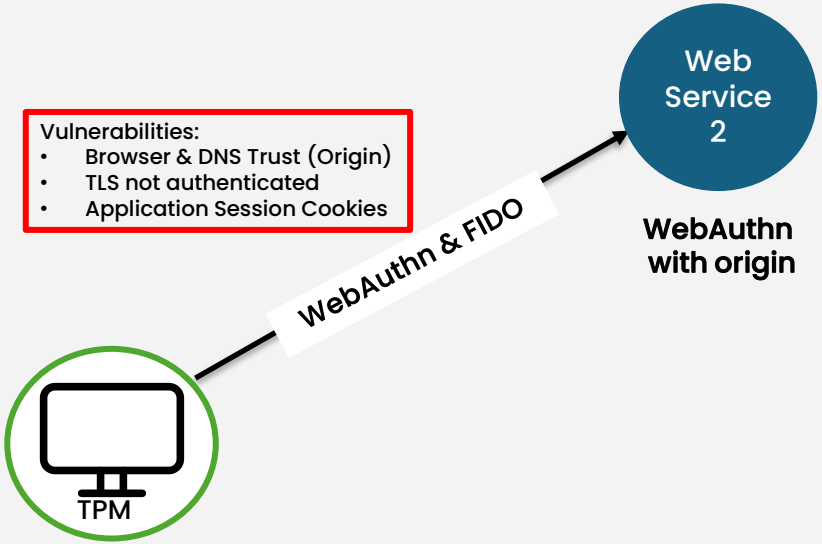
Authenticate device requesting access.

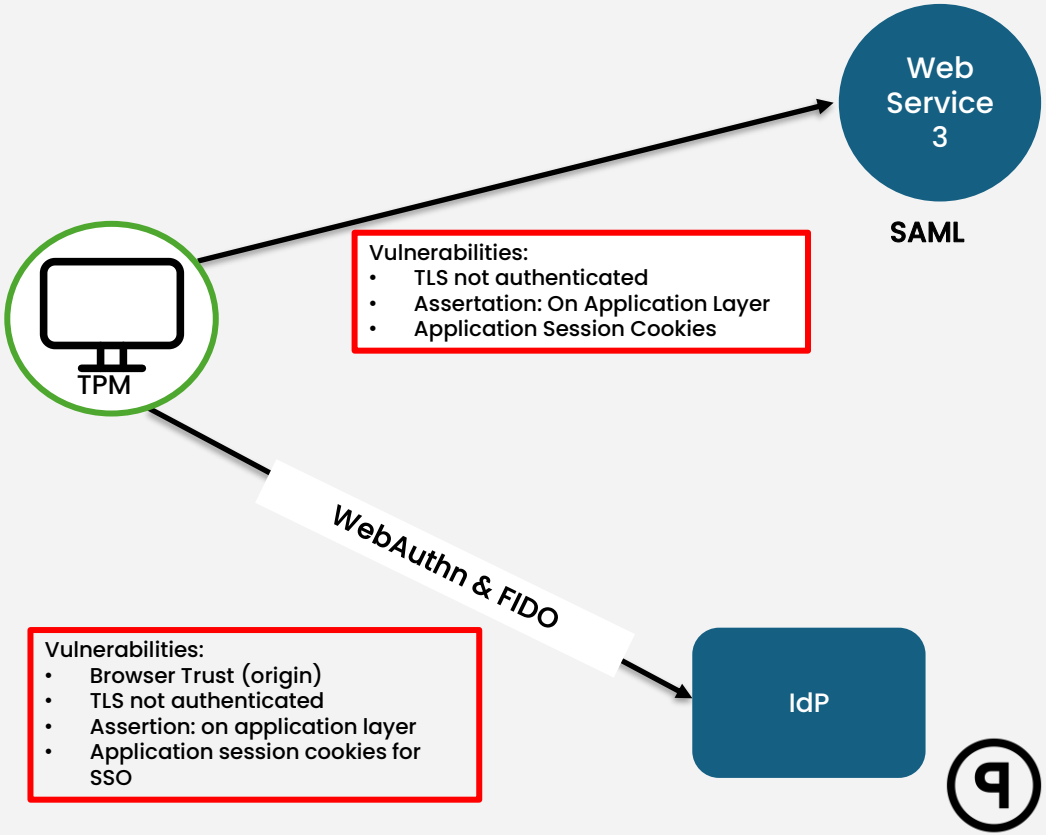
State-of-the-art challenges

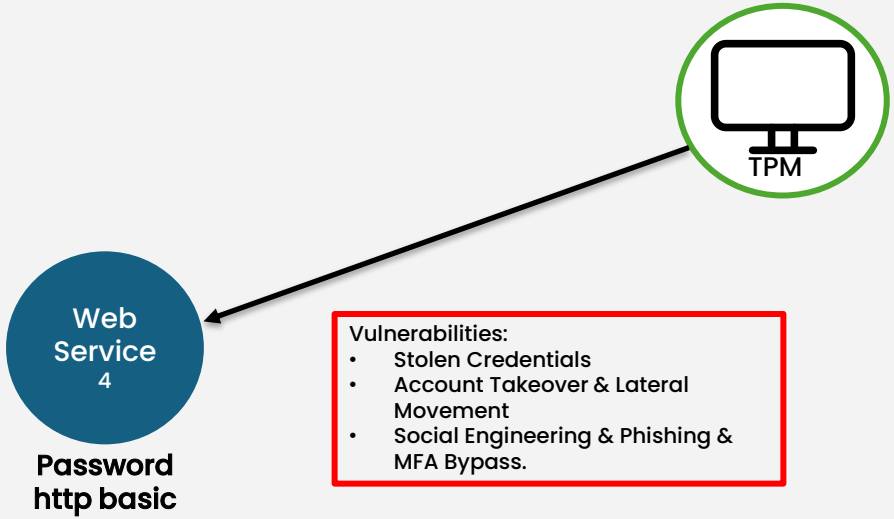
- mTLS
  - Certificate Management, Key Distribution & Security
  - Environment support limited
- FIDO2
  - Decentralized identity proofing ?security?
  - Application layer authentication -> MitM vulnerability challenges
  - Session security out of scope
- Identity Federation Standards
  - Assertion/token & session security out of scope
  - Designed to federate trust!

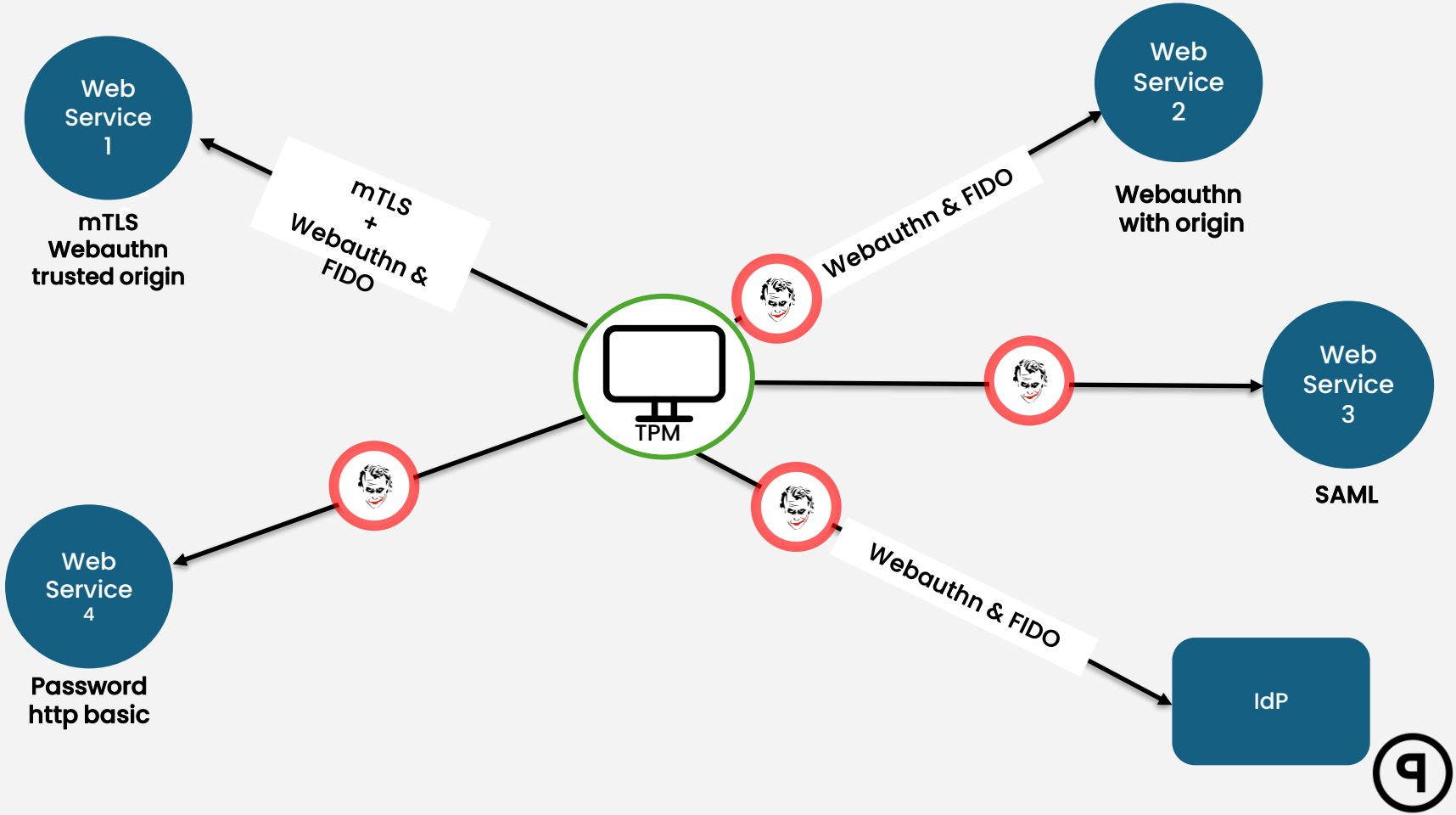

Web Service 1
mTLS
Webauthn
trusted origin
Web Service 2
Webauthn
with origin
TPM
Web Service 3
SAML
Web Service 4
Password
http basic


Web Service 1
mTLS WebAuthn trusted origin
mTLS + Webauthn & FIDO
TPM


Web Service 2
Vulnerabilities:
• Browser & DNS Trust (Origin)
• TLS not authenticated
• Application Session Cookies
WebAuthn & FIDO
WebAuthn with origin
TPM


Web Service 3
SAML
Vulnerabilities:
• TLS not authenticated
• Assertation: On Application Layer
• Application Session Cookies
TPM
WebAuthn & FIDO
Vulnerabilities:
• Browser Trust (origin)
• TLS not authenticated
• Assertion: on application layer
• Application session cookies for SSO
IdP


TPM
Web Service 4
Password http basic
Vulnerabilities:
• Stolen Credentials
• Account Takeover & Lateral Movement
• Social Engineering & Phishing & MFA Bypass.


Web Service 1
mTLS Webauthn trusted origin
mTLS + Webauthn & FIDO
Web Service 2
Webauthn with origin
Webauthn & FIDO
TPM
Web Service 3
SAML
Web Service 4
Password http basic
Webauthn & FIDO
IdP

Workspace Browser: Unified Access Security

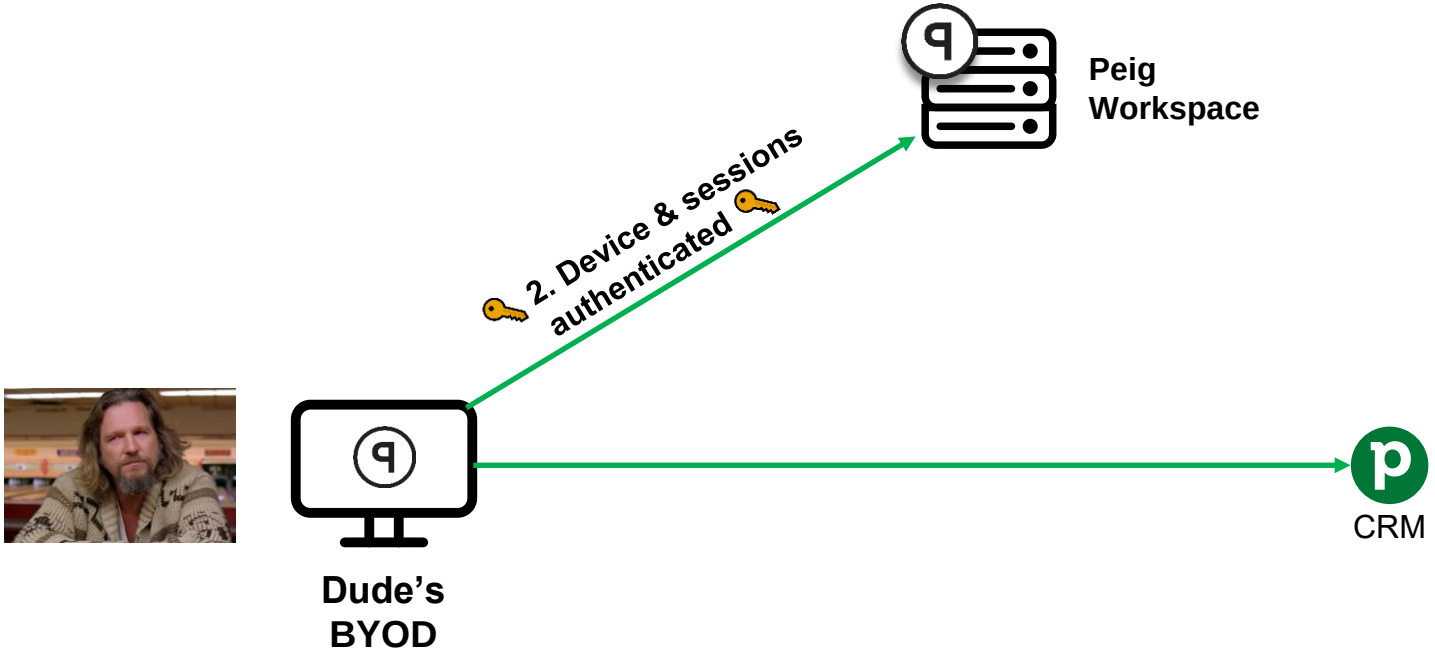
- ✓ Device-bound.
- ✓ Addresses fundamental access threats.
- ✓ No password policy & MFA fatigue.

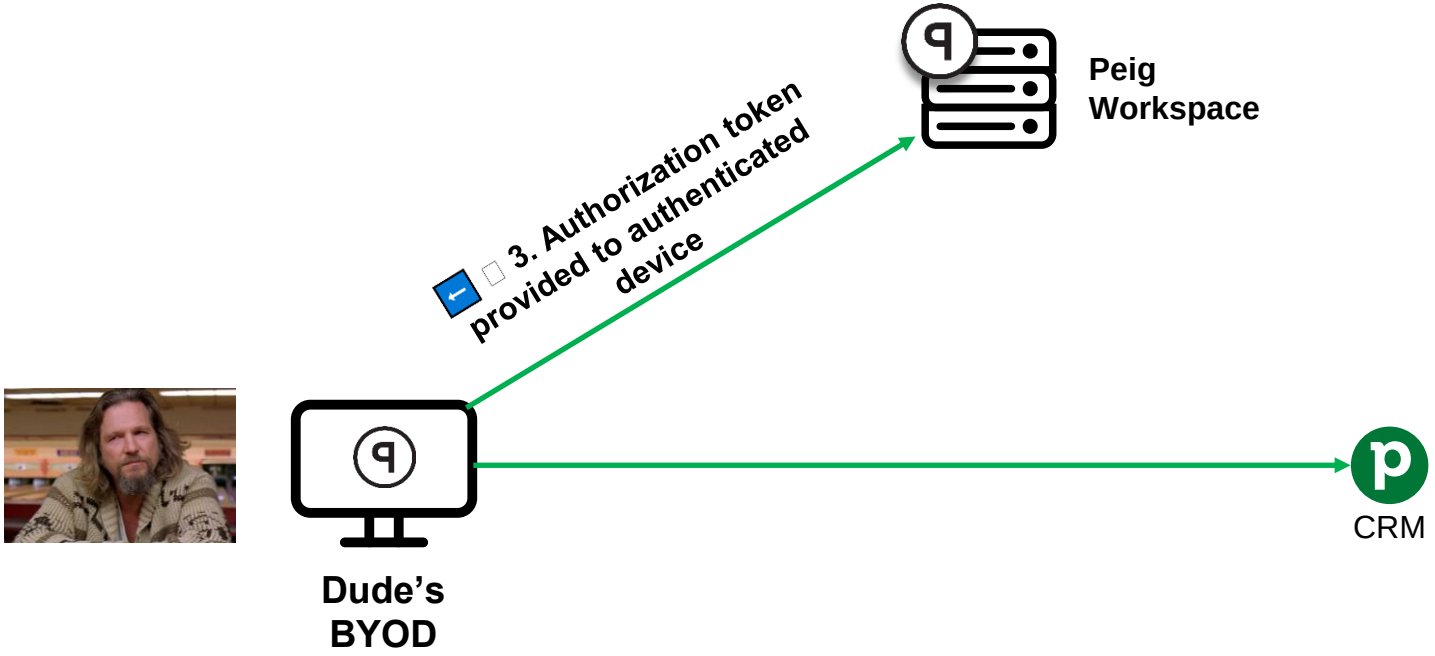
Dude's
BYOD

⬅ 1. https session established

CRM

Peig
Workspace


Peig
Workspace
2. Device & sessions
authenticated
CRM
Dude's
BYOD


Peig
Workspace
3. Authorization token provided to authenticated device
CRM
Dude's
BYOD

Dude's
BYOD

→ 4. Authorization token provided to service over authenticated session

CRM

Peig
Workspace

Dude’s
BYOD

Peig
Workspace

⬅️ 🍪 5. Session cookie
provided to Dude’s BYOD

CRM

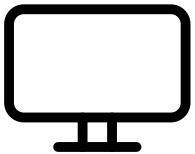
Peig
Workspace

6.Cookie stored
short-term

Dude’s
BYOD

CRM

Dude's BYOD



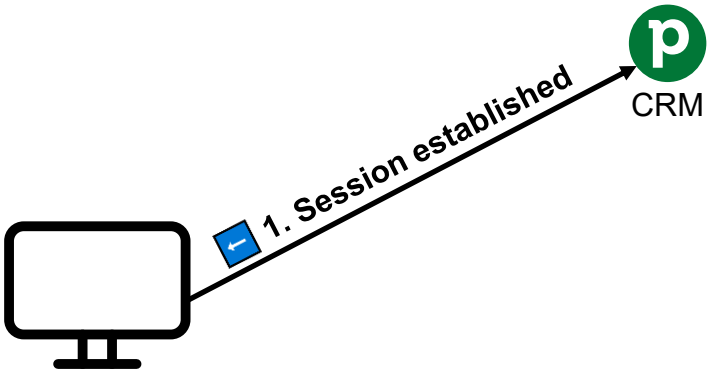
Hacker's device

Peig Workspace

CRM

Dude's
BYOD

Peig
Workspace

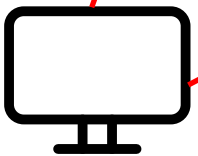


Hacker's
device

Dude's
BYOD

Peig
Workspace

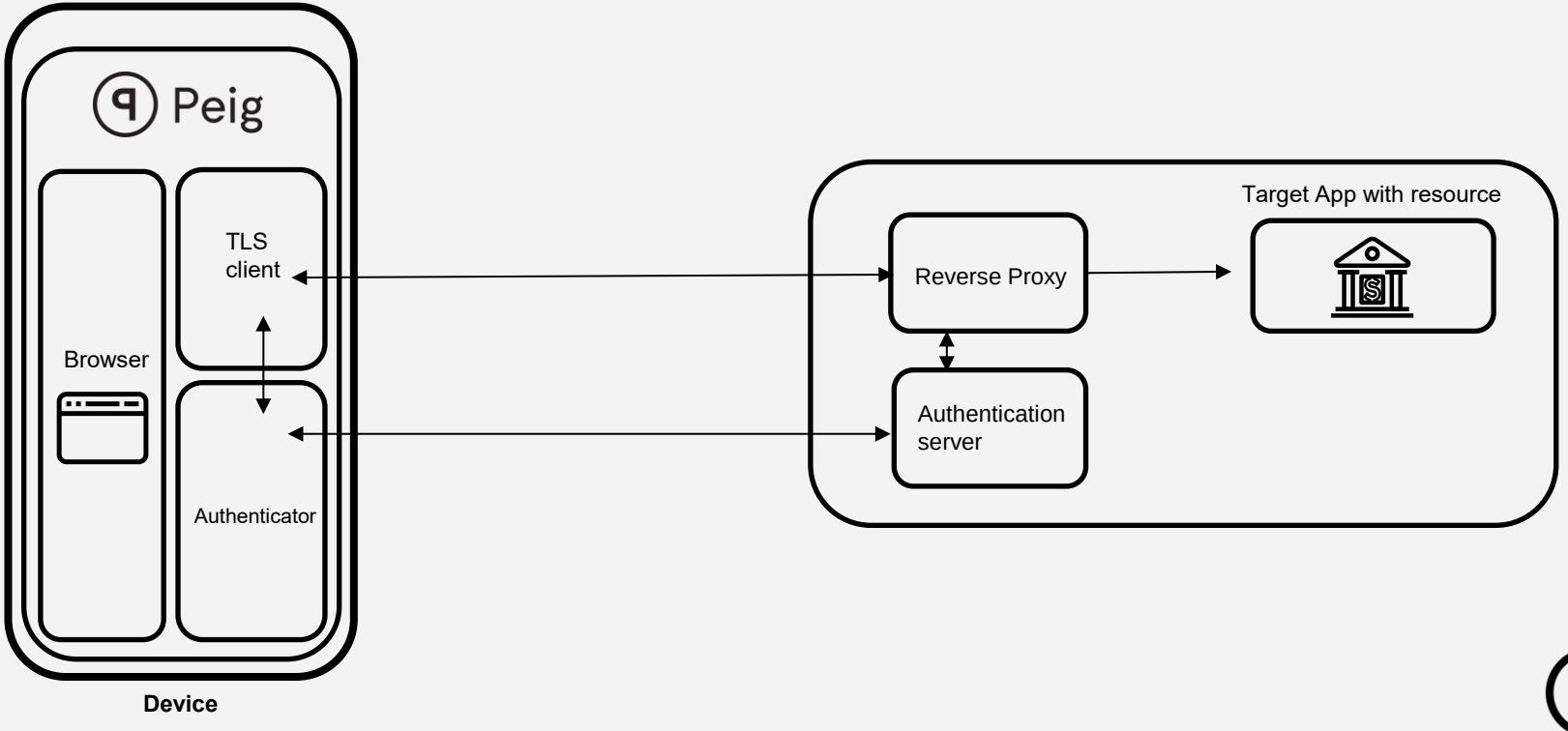
2. Device & sessions not authenticated



Hacker's
device

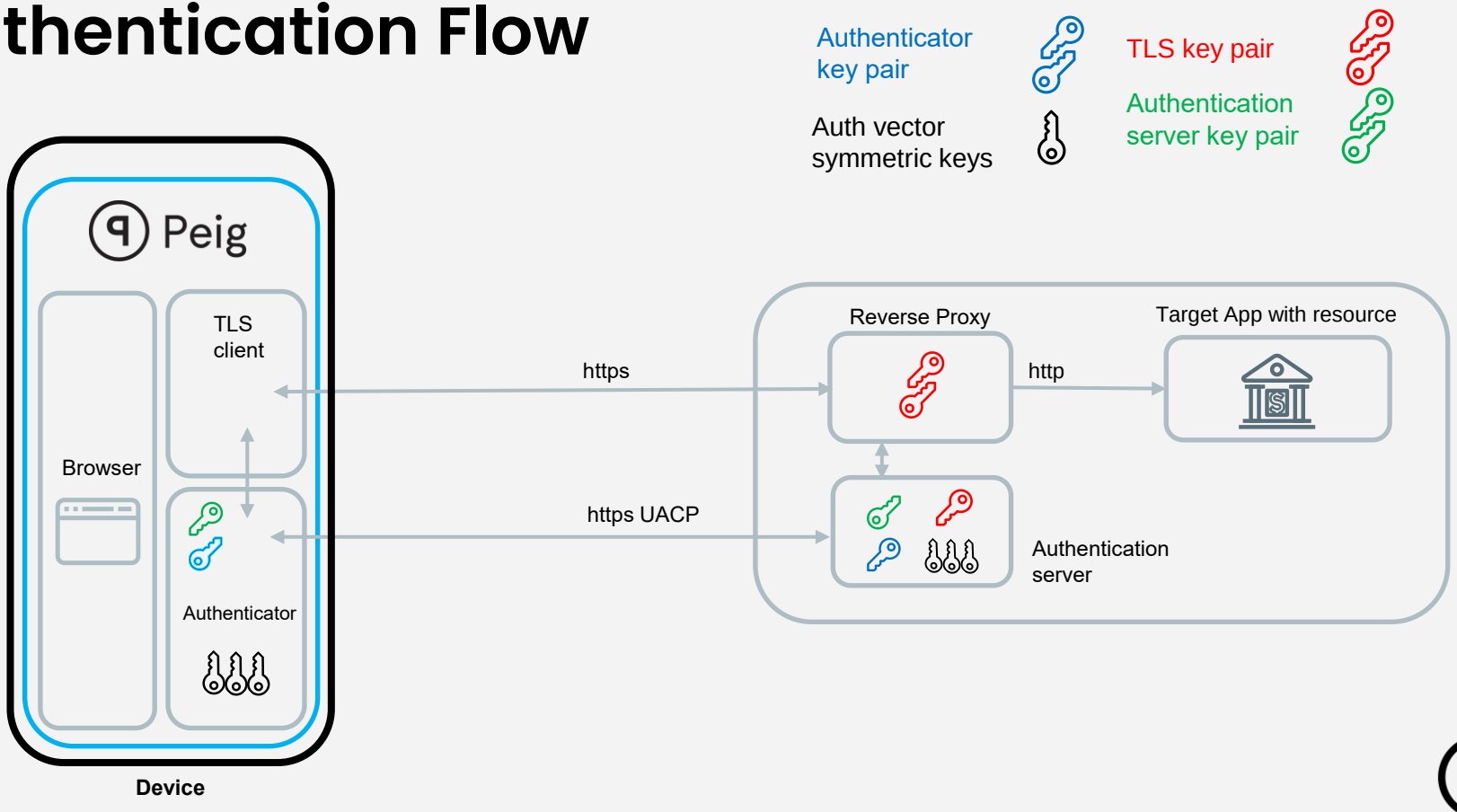
CRM

Authentication Flow



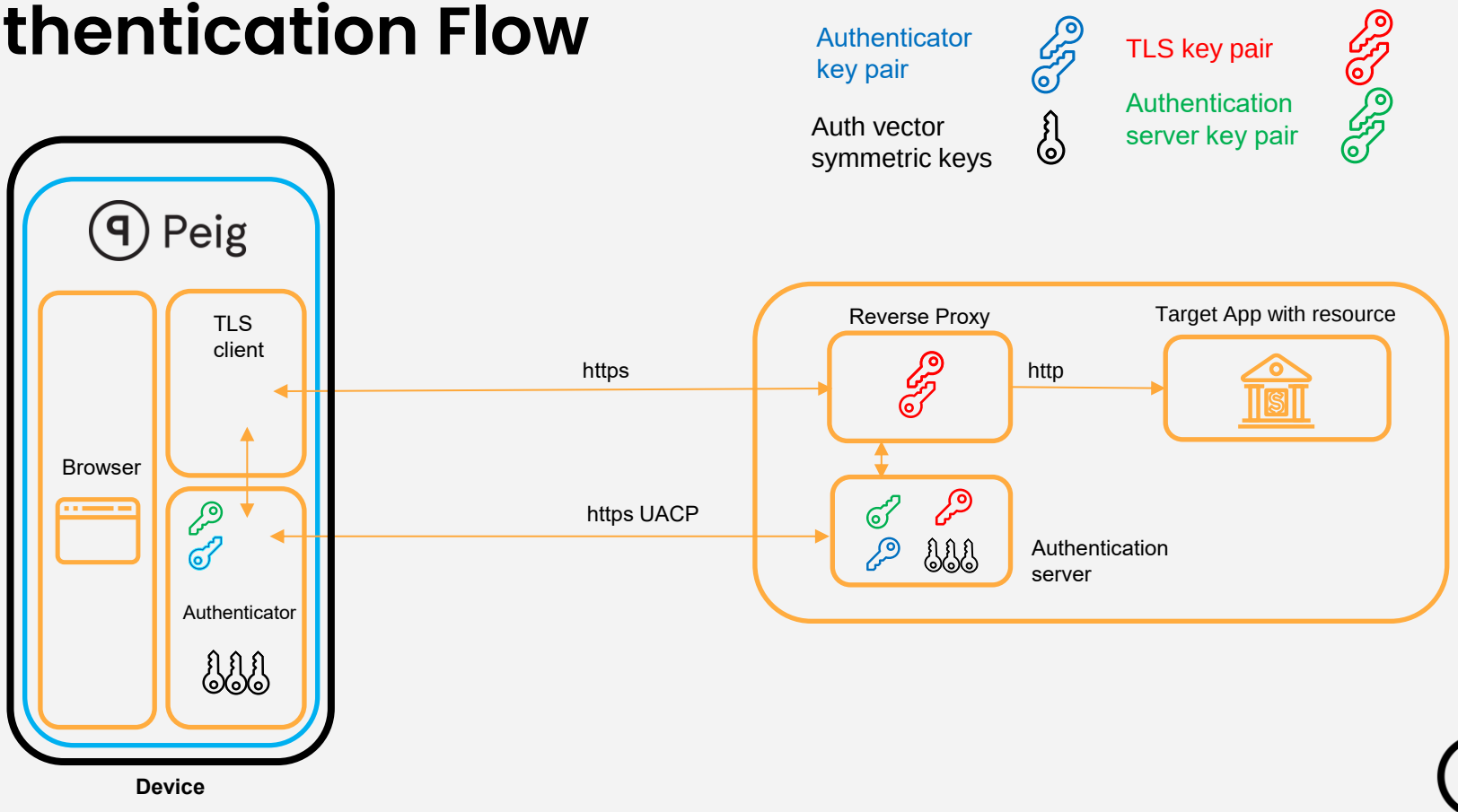
Note: private key is facing up (🗝)

Authentication Flow



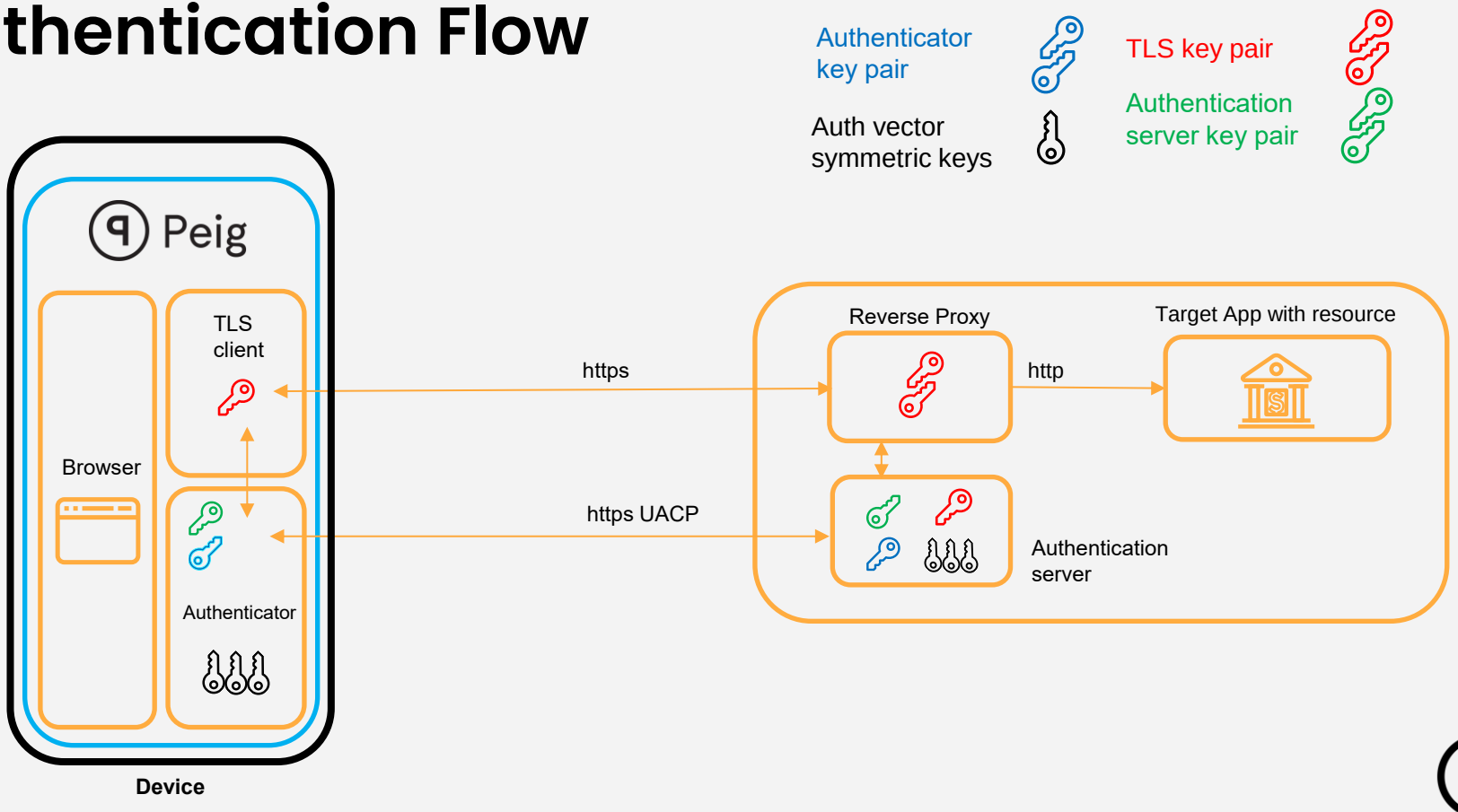
Note: private key is facing up (🗝)

Authentication Flow



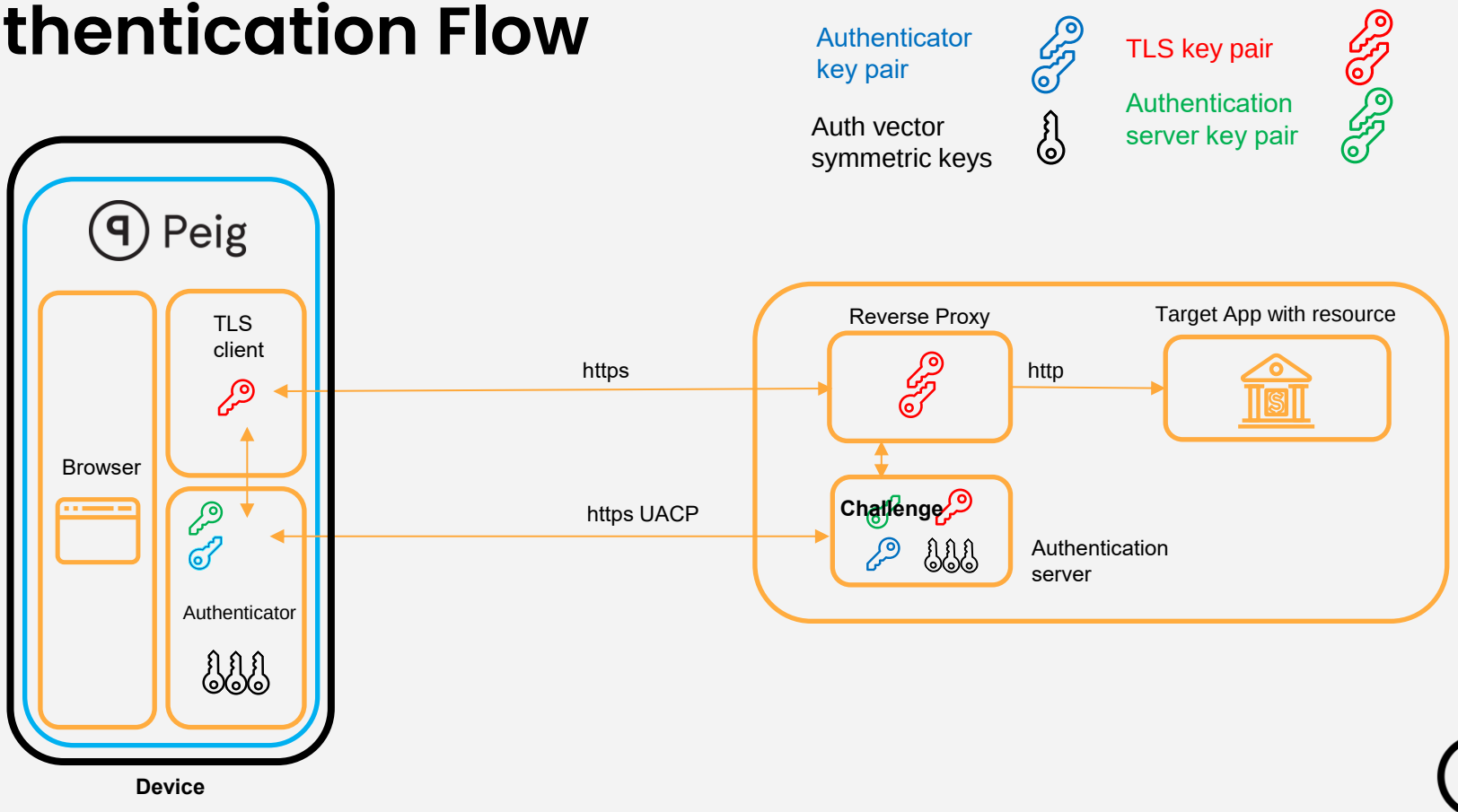
Note: private key is facing up (🗝)

Authentication Flow



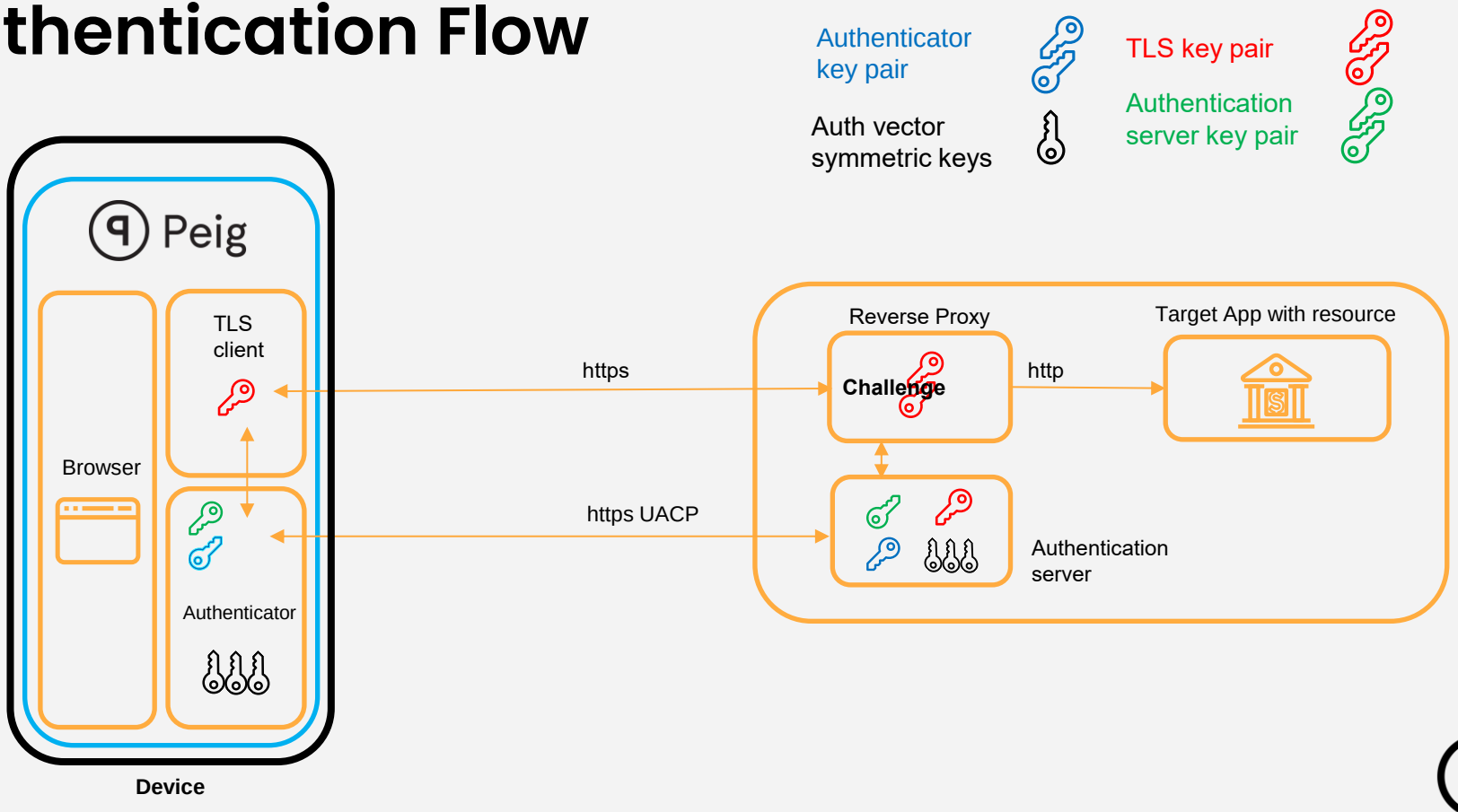
Note: private key is facing up (🗝)

Authentication Flow



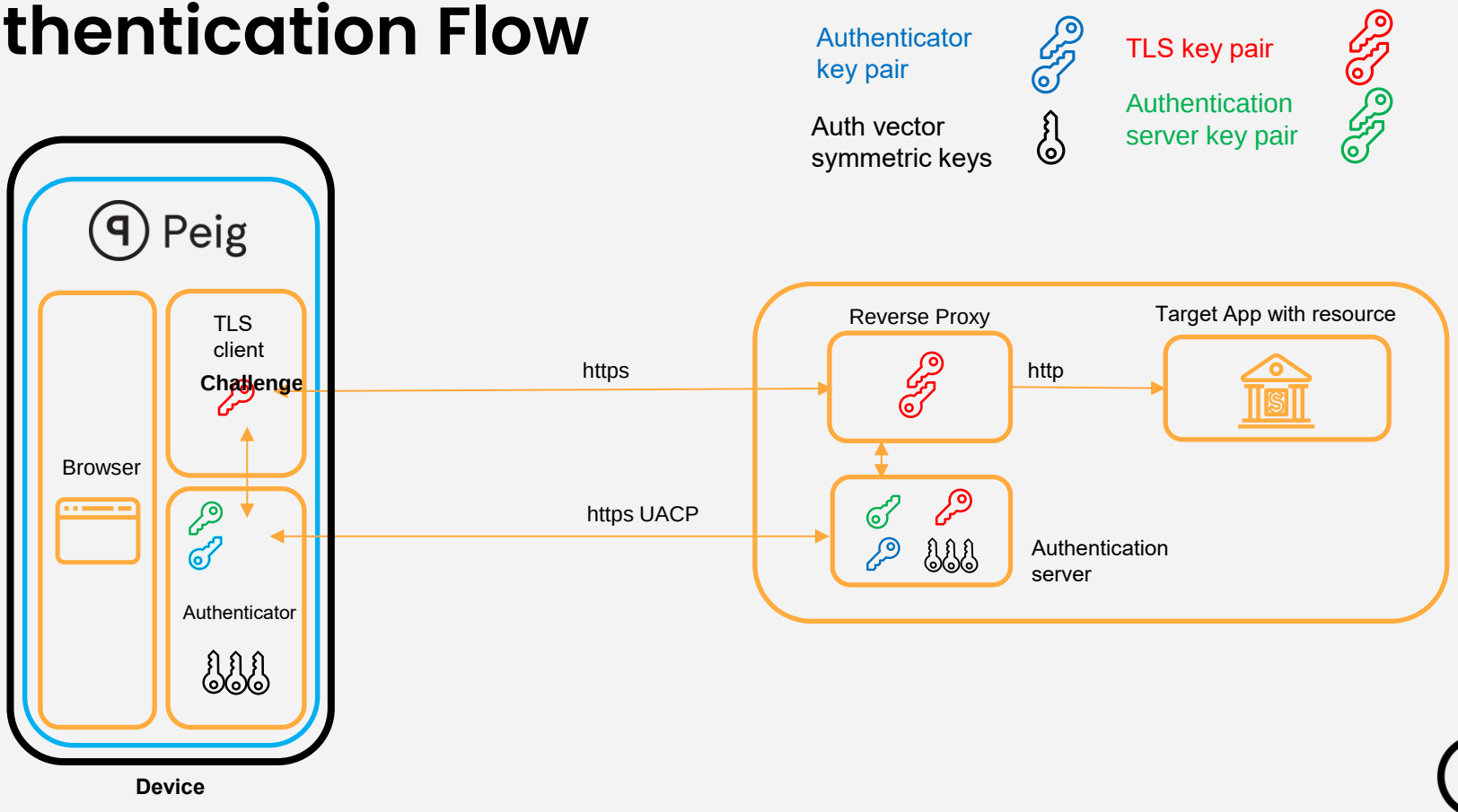
Note: private key is facing up (🔑)

Authentication Flow



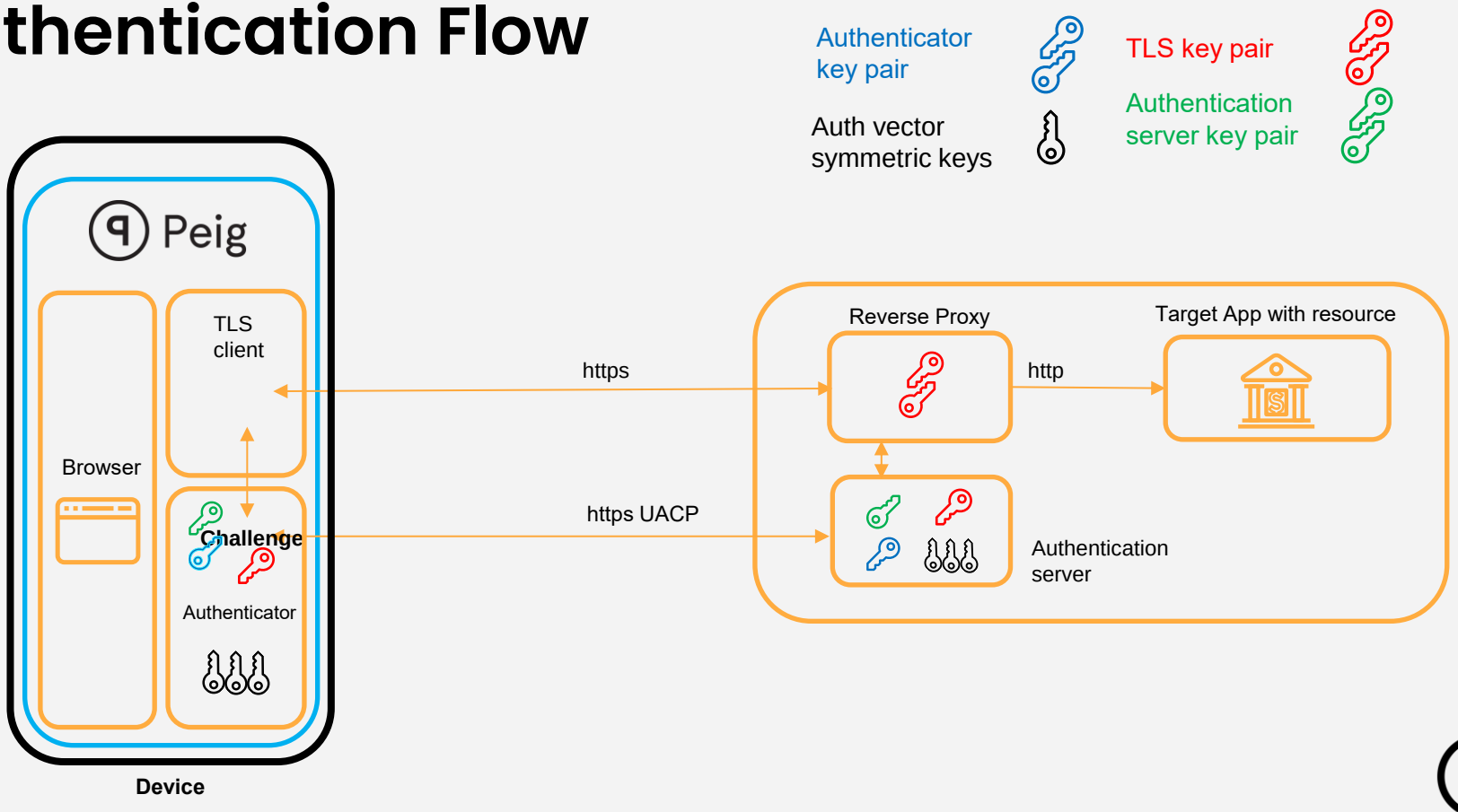
Note: private key is facing up (🗝)

Authentication Flow



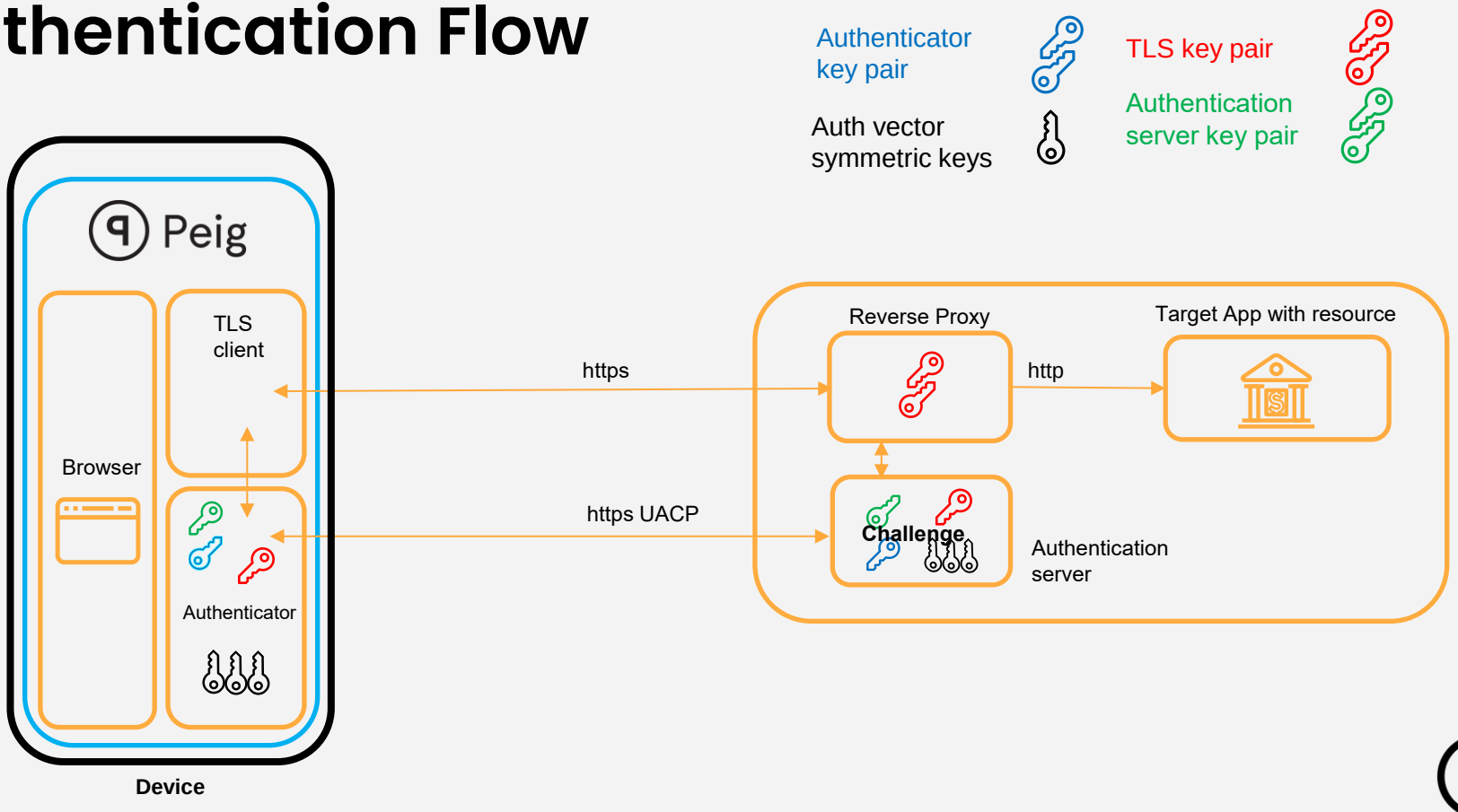
Note: private key is facing up (🗝)

Authentication Flow



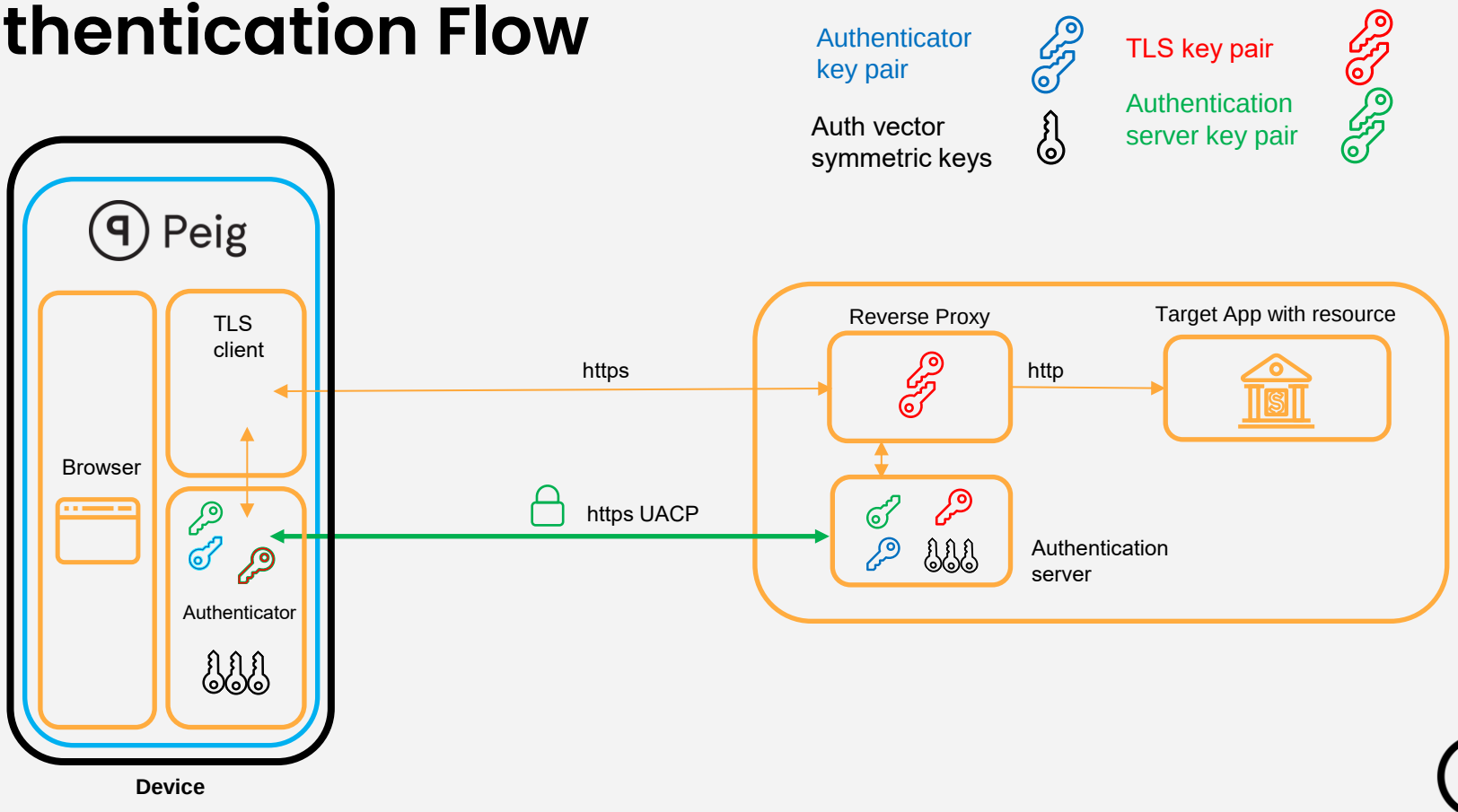
Note: private key is facing up (🗝)

Authentication Flow



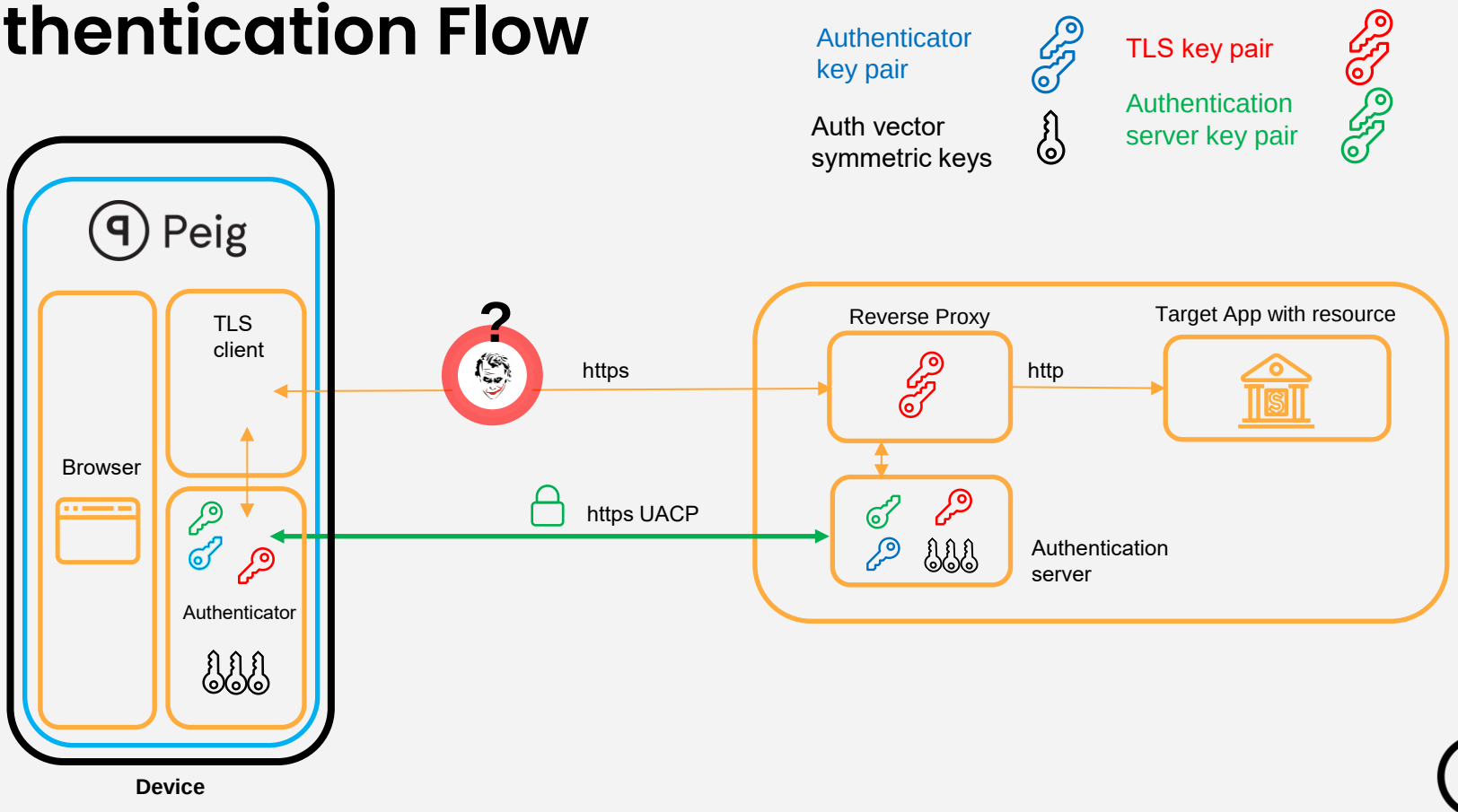
Note: private key is facing up (🗝)

Authentication Flow



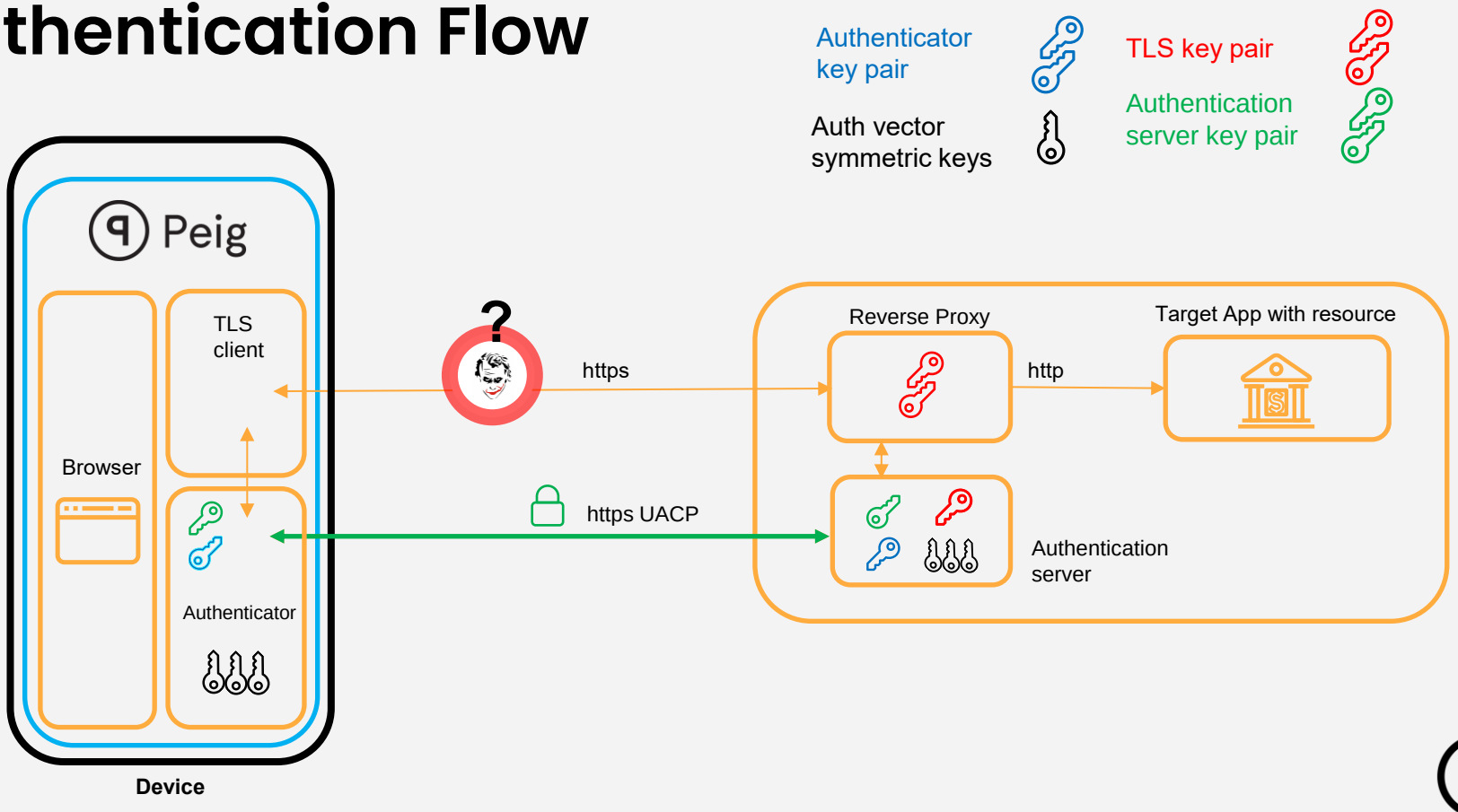
Note: private key is facing up (🗝)

Authentication Flow



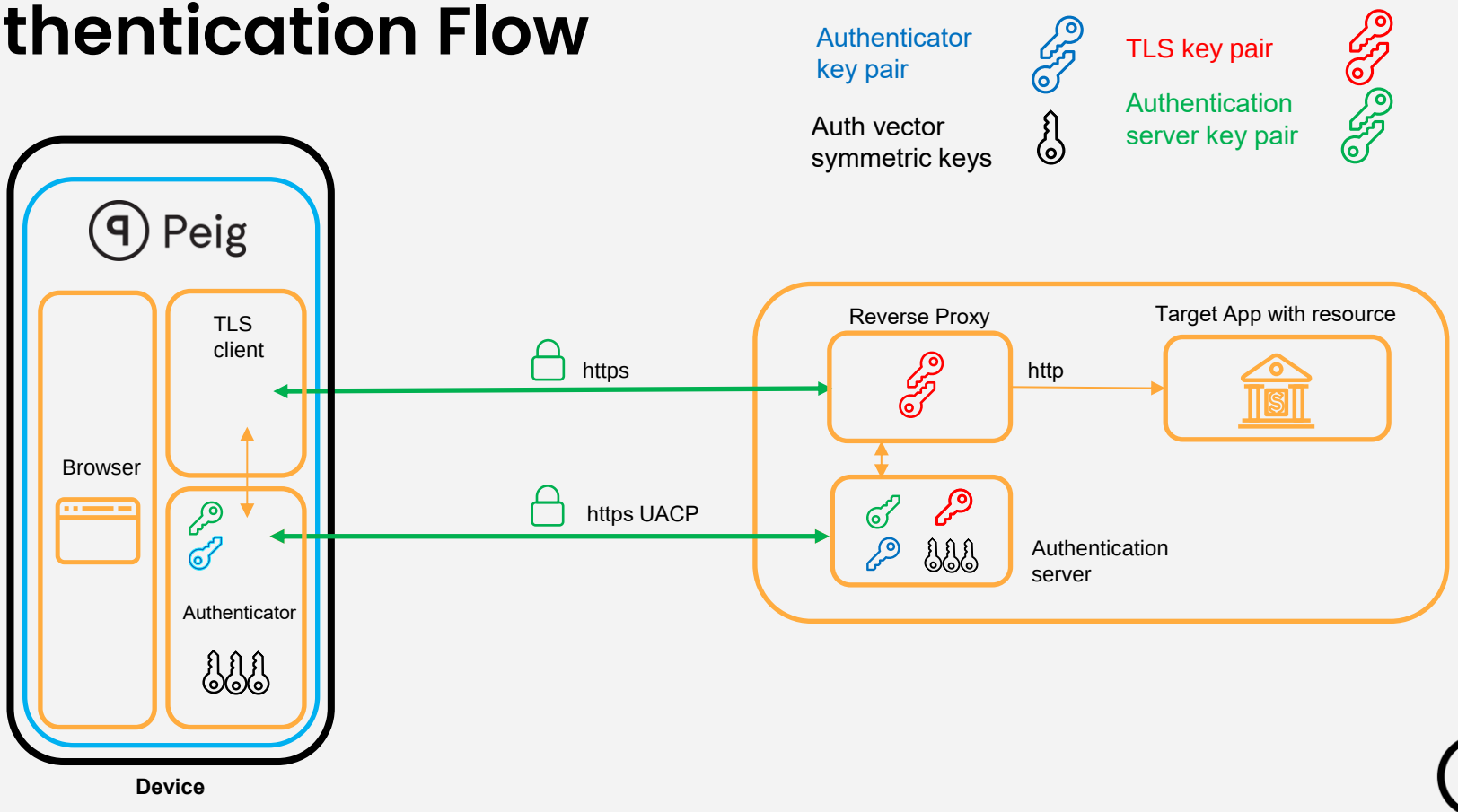
Note: private key is facing up (🗝)

Authentication Flow



Note: private key is facing up (🗝)

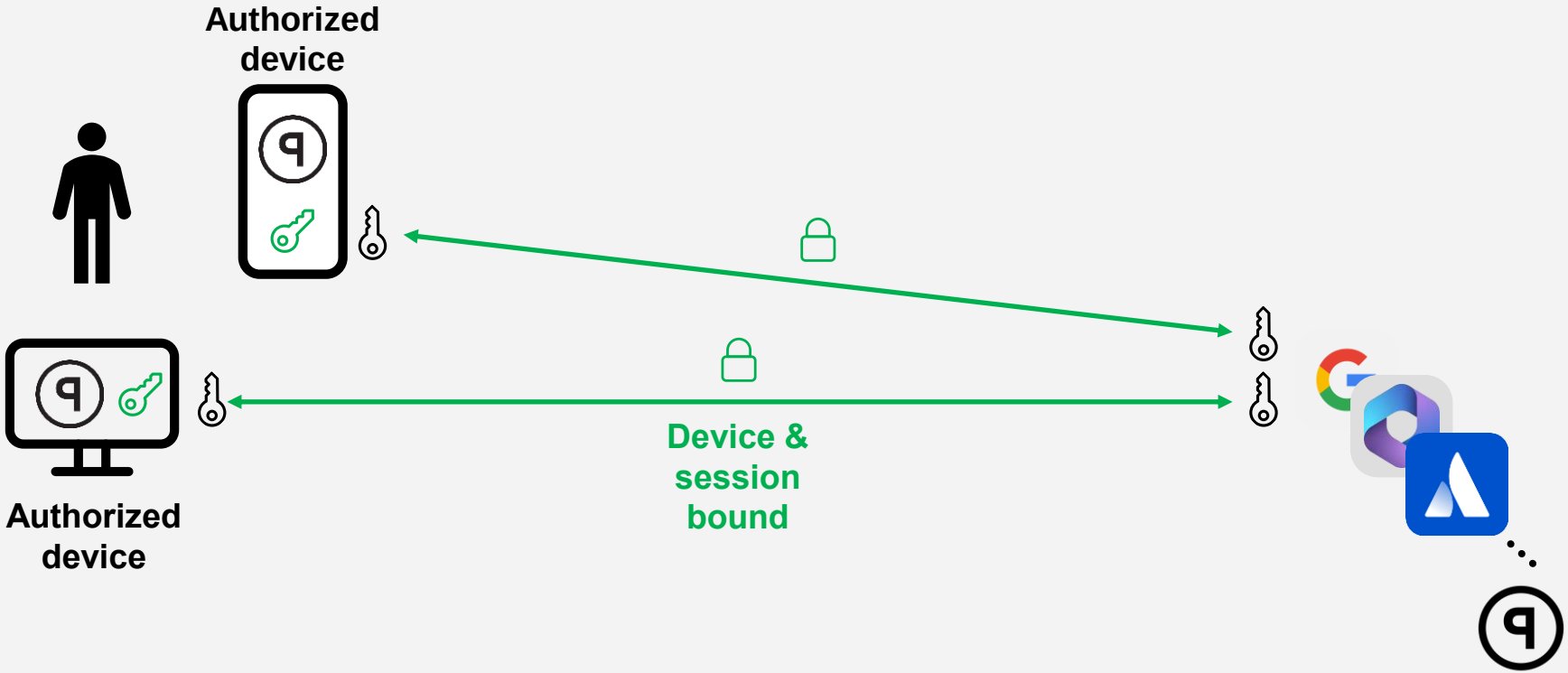
Authentication Flow



Dude's authenticator

The dude in coffee shop

Device-bound Access Security model



Device-bound access security

- **Credential theft protection**
  - No passwords & traditional MFA
  - Device-bound cryptography
- **Session theft prevention**
  - Phishing & **MitM resistant** authentication
  - **Persistent cookies** not stored in filesystem
- **Controls apply in different environments**

  (e.g SSO, or where mTLS not applicable)

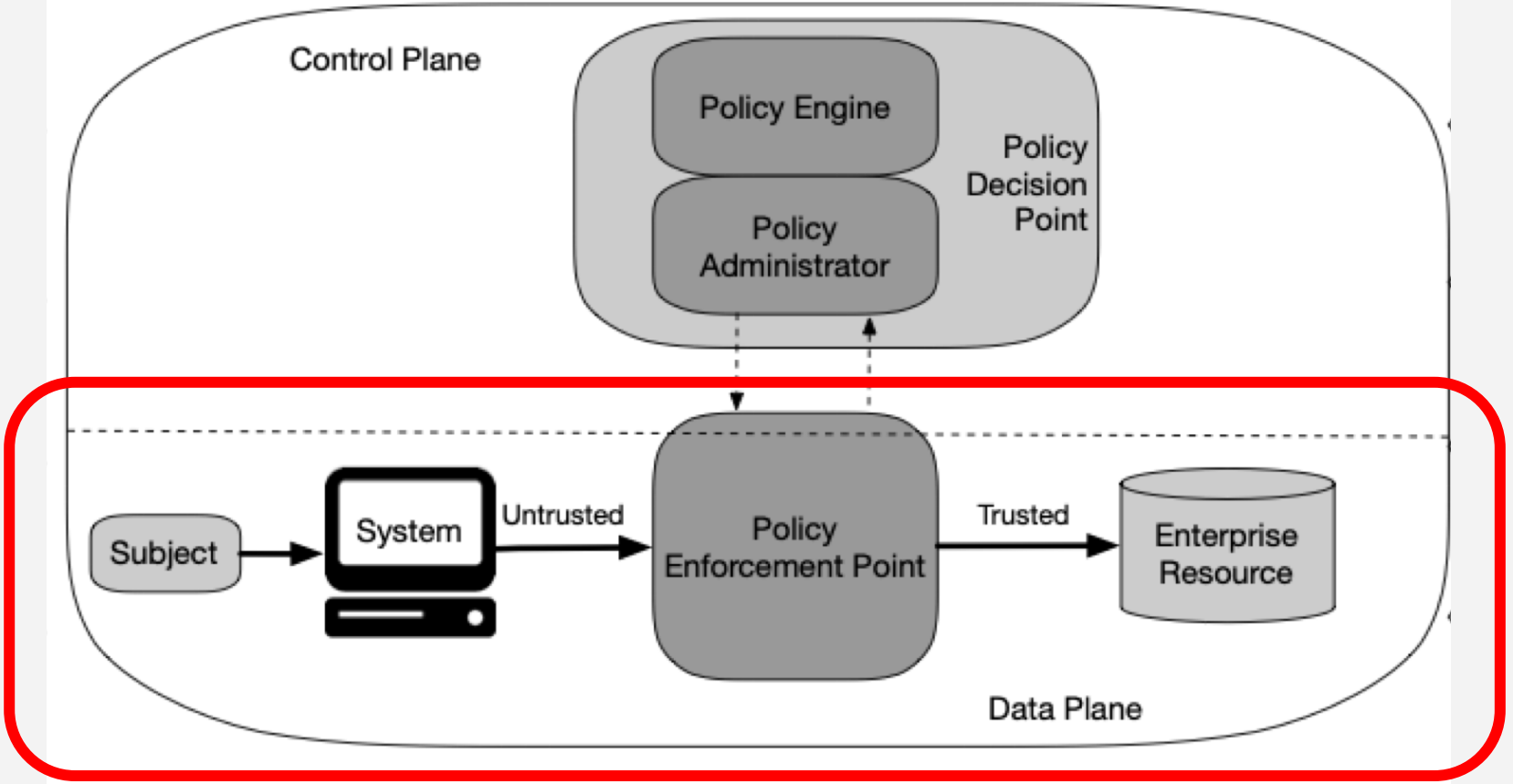


Figure 2: Core Zero Trust Logical Components

Is that all?

- Cryptography lifecycle
1. Validity
2. Change & update controls
- Crypto agility
1. Cryptography system algorithm agnostic
2. Cryptography implementation agnostic
- Layered key security

Let’s discuss!

Connect with Us

Peig

peig.io

LinkedIn

@ Peig | Passwordless Access

@ David Rihak

channel program

@ Peig

Our mission is to protect yours.