
Securing Cross-Device Flows Using Zero Trust Principles
identiverse
#identiverse

Pieter Kasselman

Identity Standards Architect

Microsoft

Nick Ludwig

Product Manager

Microsoft

The Next 25 Minutes

Recap: Cross Device Flows

- What are they, why do they matter

Problems with Cross Device Flows

- How are they being exploited

Applying Zero-Trust Principles

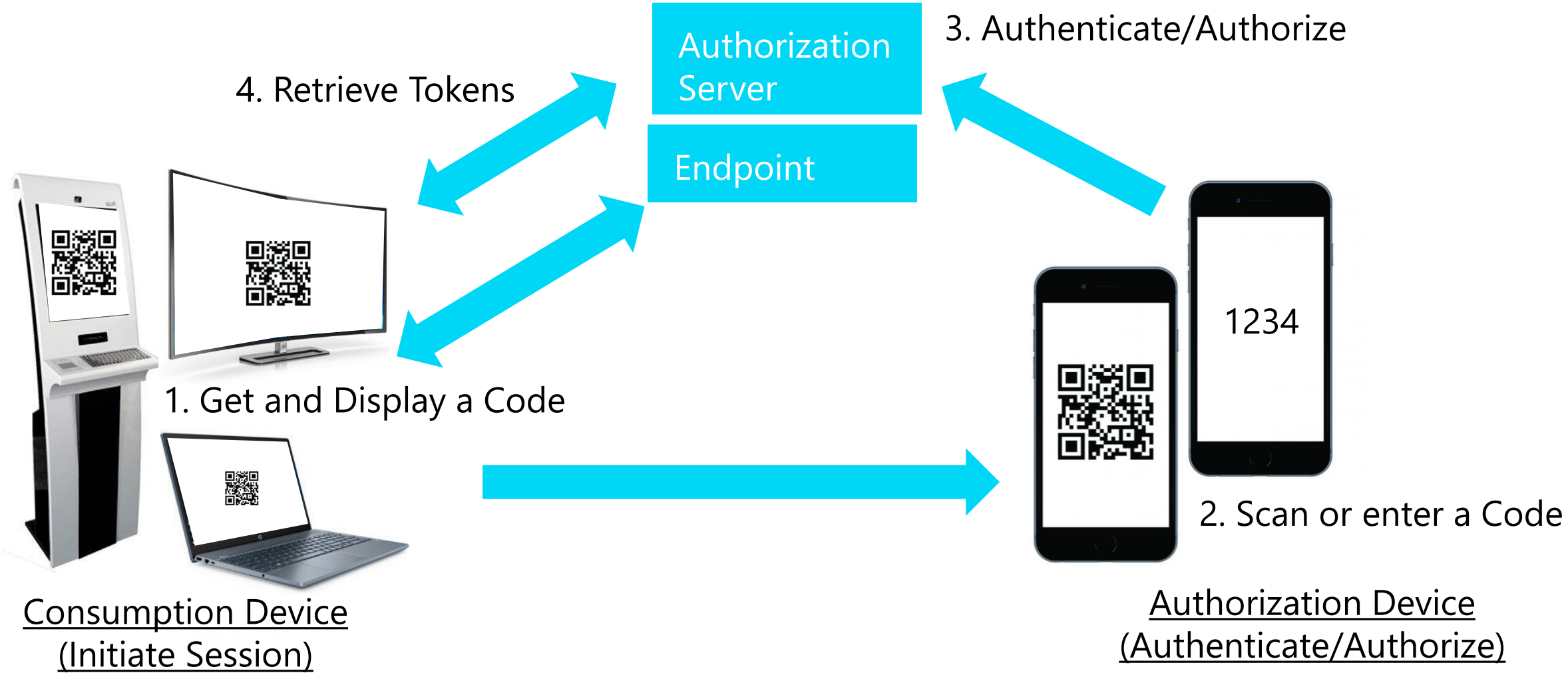
- Verify Explicitly, Least Privilege, Assume Breach

From Principles to Practice

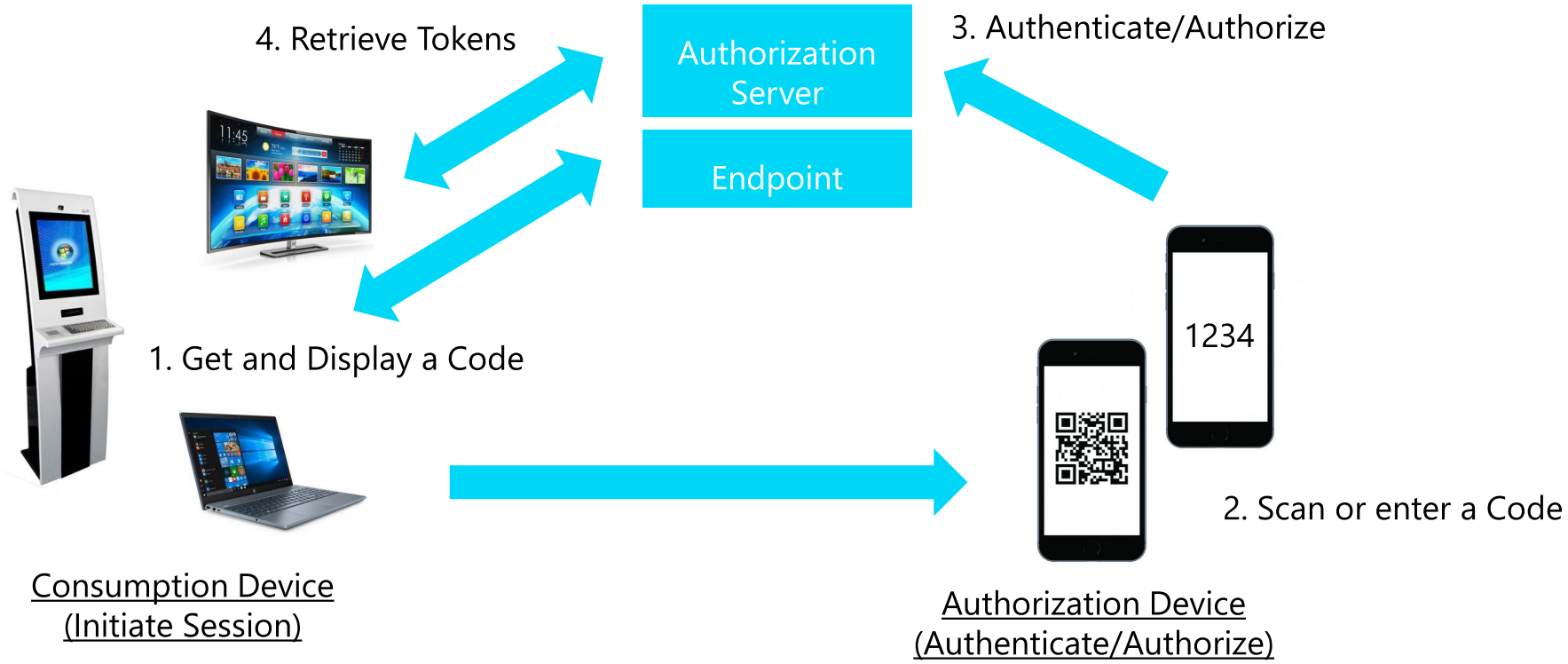
- 15 Practical Mitigations and When to Apply them

Q&A

What is a Cross Device Flow?



What is a Cross Device Flow?



In a nutshell

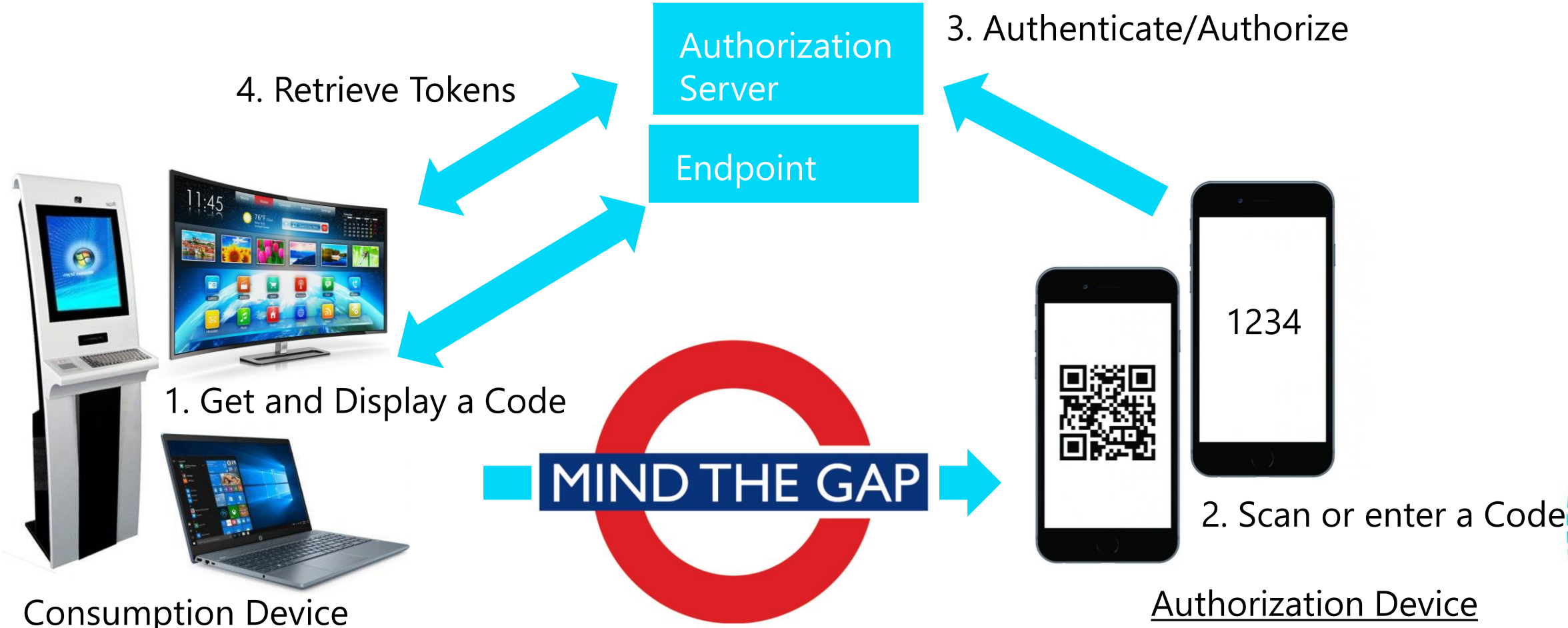
- Initiate session on one device
- Authorize on second device

Benefits

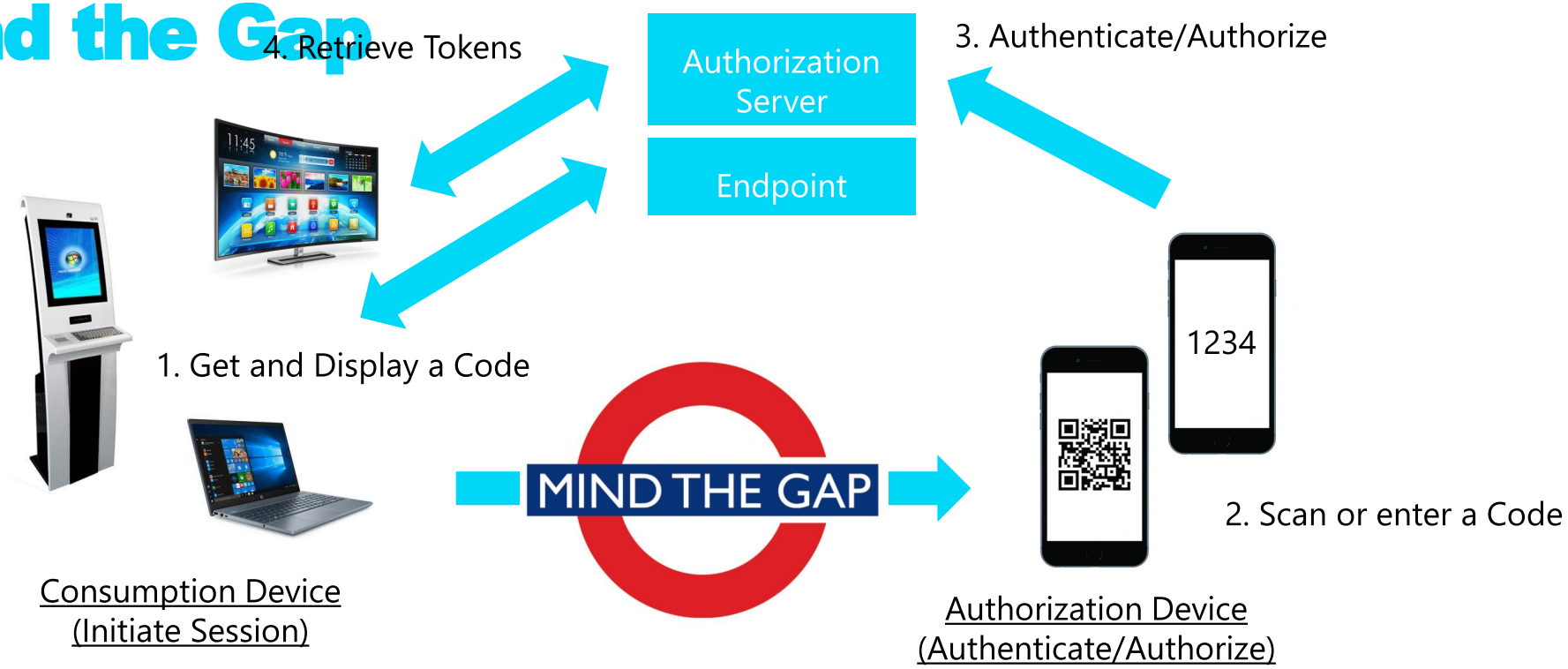
- Authorization for devices with limited input capabilities
- Strong authentication with a personally trusted device

Problems with Cross-Device Flows

But... Mind the Gap



But... Mind the Gap



Air Gap = Unauthenticated Channel

1. No protocol to establish trust relationship between Consumption Device and Authorization Device
2. Push responsibility for trust decision to the user.
3. Open to abuse by attackers through social engineer to perform illicit consent grant attacks

Common Attack Pattern

5. Retrieve Tokens

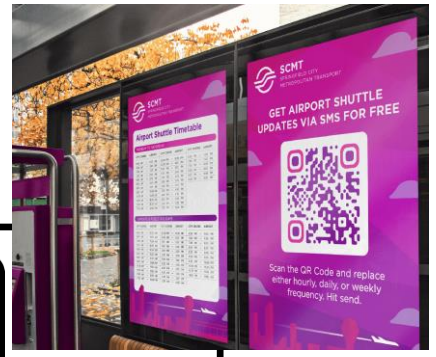
Authorization Server

Endpoint

4. Authenticate/Authorize

1. Get a Code

Attacker Controlled Device
(Initiate Session)



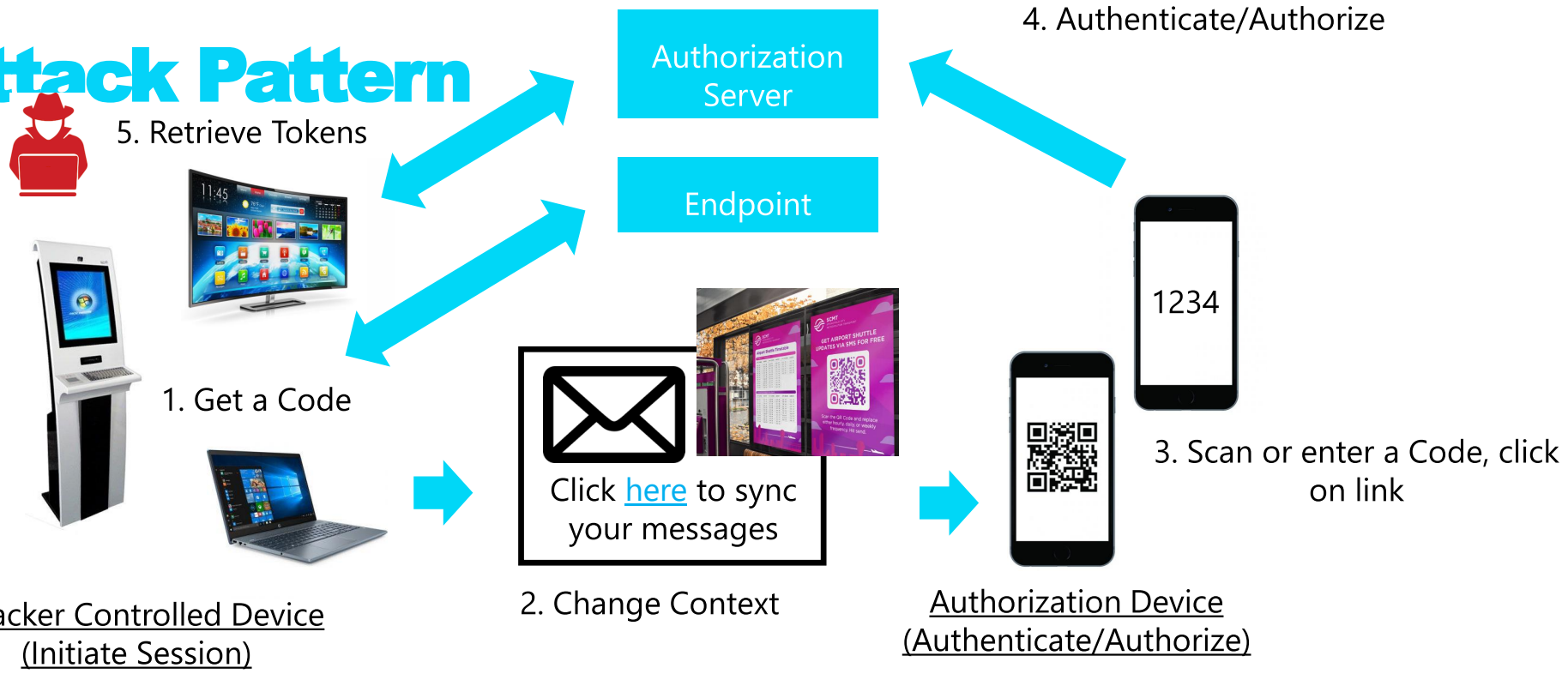
Click here to sync your messages

2. Change Context

3. Scan or enter a Code, click on link

Authorization Device
(Authenticate/Authorize)

Common Attack Pattern



Attack Pattern Summary

1. Initiate the session, retrieve code (QR code, user code)
2. Use social engineering to change context and persuade user to authorize session (illicit consent grant)
3. Bypasses multi-factor authentication (don't need to harvest credentials)

De ecuritus, used b

Homo Securitus

1. A security expert
2. Knows how the protocol should work
3. Detects a social engineering attempt
4. Is laser focused on current context
5. Foolproof mitigation for cross device flows

But is a rare species….

Homo Sapiens

1. “Expertise elsewhere” - not a security expert
2. Busy and in a rush, needs to get things done
3. Worries about breaking things
4. Wants to help

Needs to make fewer decision,
Needs help to make better decisions
Needs protection even if a bad decision is made

Pragmatic Mitigations

- Other.....
- User Experience
- Secure QR
- Trusted Devices
- Sender Constrained Toke
- User Code Meta Data
- Content Filtering
- Proximity

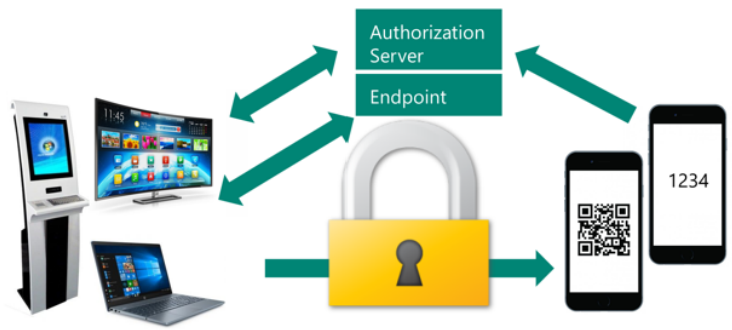
Explore Alternatives

Authenticated Channel

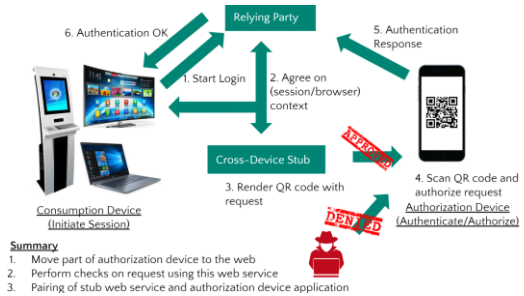
- Authorization Code Grant (WebAuthn, fido)

Unauthenticated Channel

- Client Initiated Back Channel Authentication (OpenID)
- Device Authorization Grant (OAuth 2)



Foundational Underpinnings



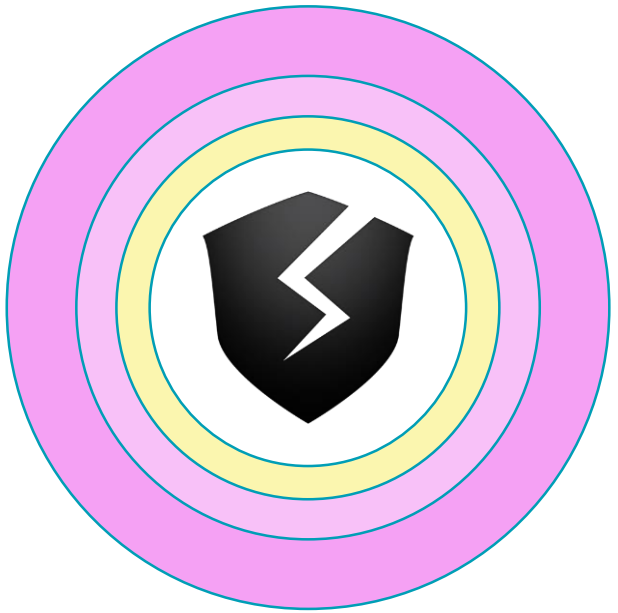
Applying Zero-Trust Principles

Zero Trust Principles and Cross-Device Flows

Verify Explicitly

Least Privilege

Assume Breach



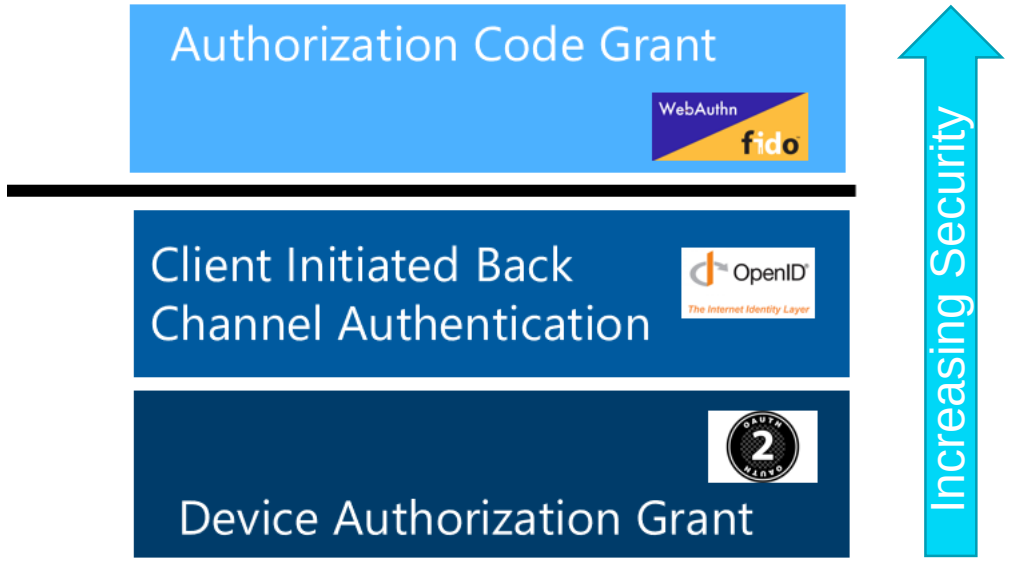
From Principles to Practice

“Start by doing what’s necessary; then do what’s possible; and suddenly you are doing the impossible.” – **St. Francis of Assisi**

14 Practical Mitigations

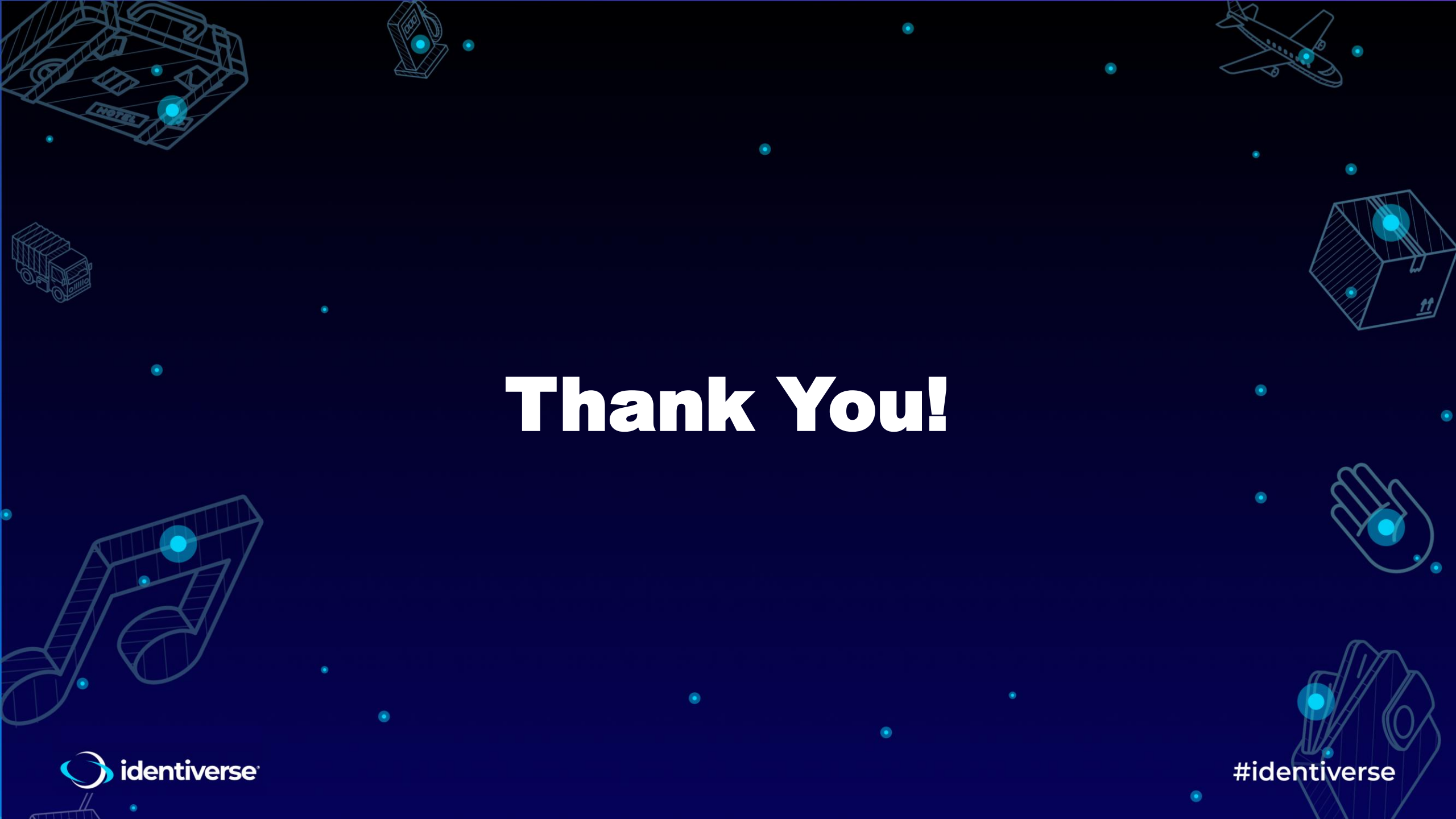
Practical Mitigation	Verify explicitly	Least privilege	Assume breach
Establish proximity	✓		
Trusted devices	✓		
Trusted networks	✓		
Authenticated flow	✓		
User experience	✓		✓
Short lived tokens		✓	
Limited scopes		✓	
One-time or limited user codes			✓
Short lived/timebound user codes			✓
Unique codes			✓
Content filtering			✓
Detect and Remediate			✓
Sender constrained tokens			✓
Rate limits			✓
Block the flow			✓

Protocol Selection



Learn More...

Cross-Device Flows: Security Best Current Practice: draft-ietf-oauth-cross-device-security-01 - Cross-Device Flows: Security Best Current Practice



Thank You!

identiverse

#identiverse