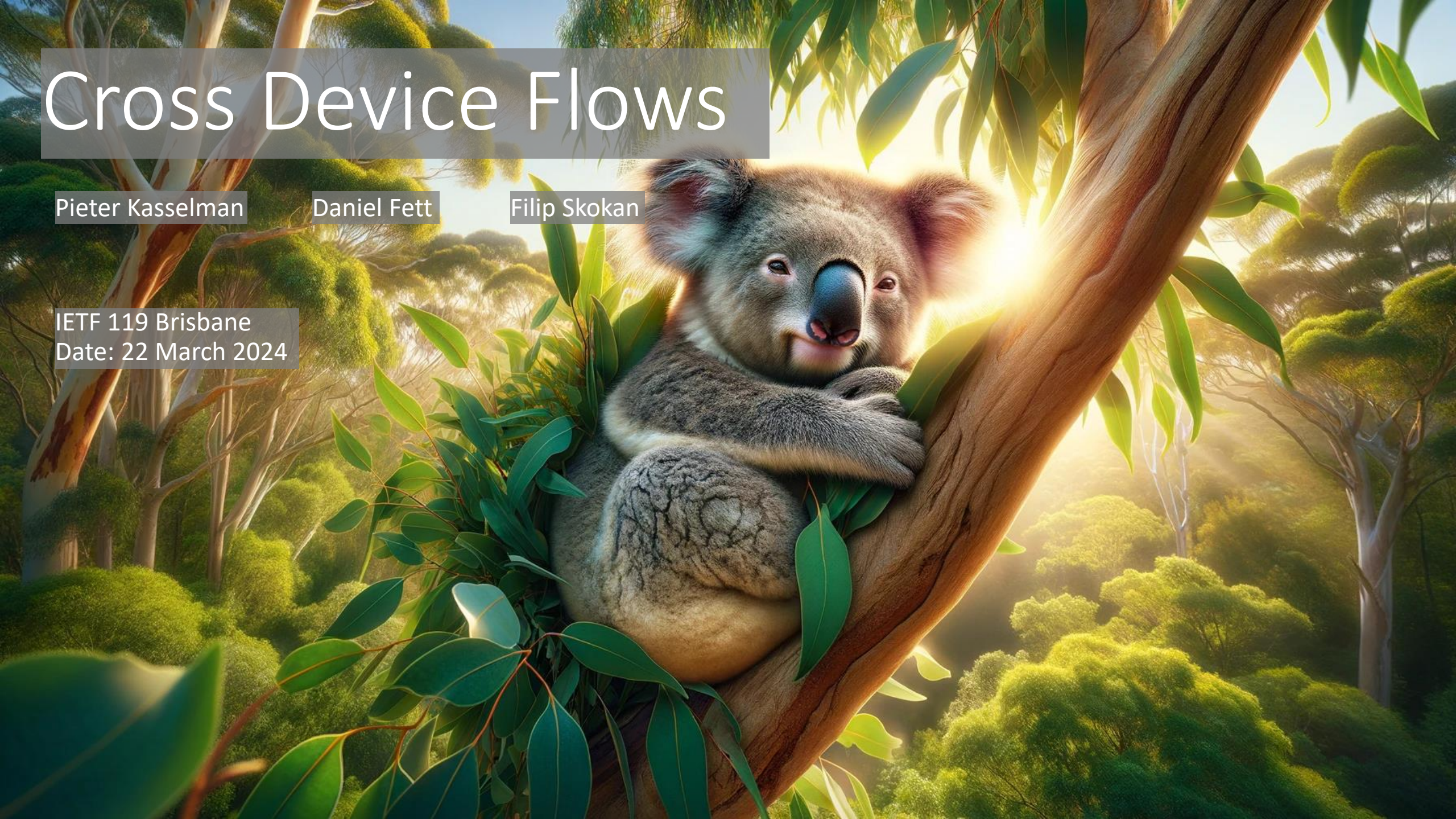
Cross Device Flows

Pieter Kasselman Daniel Fett Filip Skokan

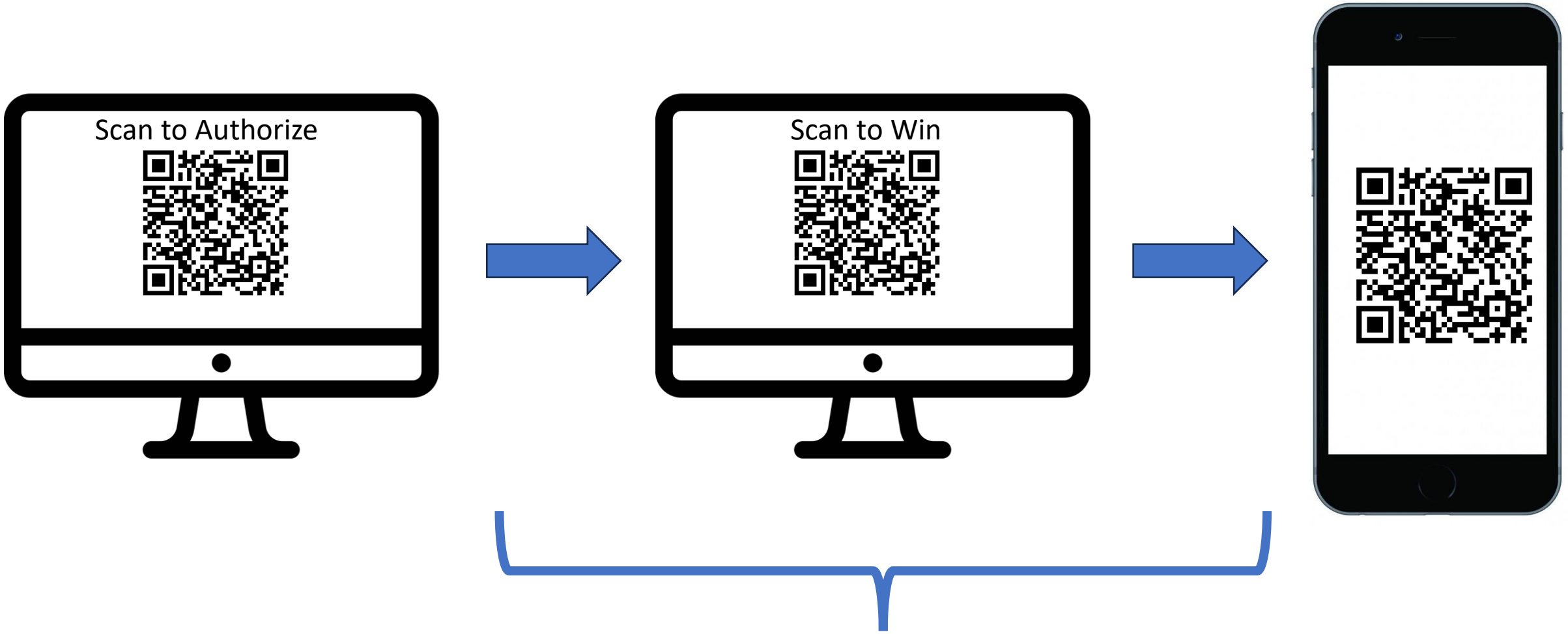
IETF 119 Brisbane
Date: 22 March 2024



Agenda

- Why are we here?
- What’s new?
- Where do we go next?

Why are we here?


Scan to Authorize
Scan to Win
Unauthenticated Channel

What’s new

What’s new in Draft -05

-05

* Added section to provide actionable guidance to implementers on how to use this document.
* Expanded section on formal analysis to include completed research projects.
* Added reference to OpenID for Verifiable Presentations.

https://datatracker.ietf.org/doc/draft-ietf-oauth-cross-device-security/

Best Practices Section – How to use the draft

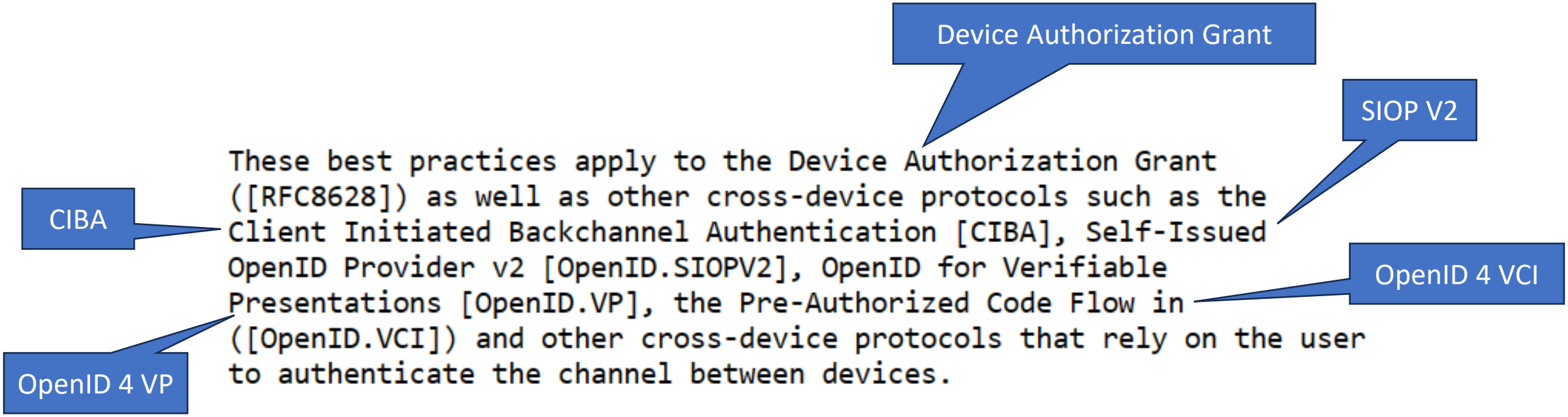
2. Best Practices

This section describes the set of security mechanisms and measures to secure cross-device protools against Cross-Device Consent Phishing and Cross-Device Session Phishing attacks that the OAuth working group considers best practices at the time of writing.

1. Risk Assessment
2. Don’t use without mitigations
3. Minimise risk with protocol selection
4. Implement appropriate mitigations
5. Implement proximity checks

1. Implementers MUST perform a risk assessment before implementing cross-device flows, weighing the risks from Cross-Device Cosnsent Phishing and Cross-Device Session Phishing attacks against benefits for users.
2. Implementers SHOULD avoid cross-device flows if risks cannot be sufficiently mitigated.
3. Implementers SHOULD follow the guidance provided in Section 6.2 for protocol selection.
4. Implementers MUST implement practical mitigations as listed in Section 6.1 that are appropriate for the use case, architecture, and selected protocols.
5. Implementers SHOULD implement proximity checks as defined in Section 6.1.1 if possible.

Best Practices Section – Protocols it applies to



Formal Methods Summary

"Trusted Device Relationship" (Section 6.1.17)

In "Formal analysis of self-issued OpenID providers" [Bauer2022], the protocol of [OpenID.SIOPV2] was analyzed using the Web Infrastructure Model (WIM). The WIM is specifically designed for the analysis of web authentication and authorization protocols. While it is a manual (pen-and-paper) model, it captures details of browsers and web interactions to a degree that is hard to match in automated models. In previous works, previously unknown flaws in OAuth, OpenID Connect, and FAPI were discovered using the WIM. In the analysis of a cross-device SIOP V2 flow in [Bauer2022], the request replay attack already described in Section 13.3 of [OpenID.SIOPV2] was confirmed in the model. A mitigation was implemented based on a so-called Cross-Device Stub, essentially a component that serves to link the two devices before the protocol flow starts. This can be seen as an implementation of a trusted device relationship as described in Section 6.1.7. The mitigation was shown to be effective in the model.

"CDCP against Backchannel Transferred Sessions"

In "The Good, the Bad and the (Not So) Ugly of Out-of-Band Authentication with eID Cards and Push Notifications: Design, Formal and Risk Analysis" [MPRCS2020], Pernpruner et al. formally analysed an authentication protocol relying on push notifications delivered to an out-of-band device to approve the authentication attempt on the primary device (Backchannel-Transferred Session Pattern, Section 3.1.2). The analysis was performed using the specification language ASLan++ and the model checker SATMC. According to the results of the analysis, they identified and defined the category of *implicit attacks*, which manage to deceive users into approving a malicious authentication attempt through social engineering techniques, thus not compromising all the authentication factors involved; these attacks are aligned with the definition of Cross-Device Consent Phishing (CDCP) attacks.

In "Security analysis of the Grant Negotiation and Authorization Protocol" [Helmschmidt2022], an analysis of a draft of the Grant Negotiation and Authorization Protocol (GNAP) [I-D.ietf-gnap-core-protocol] was performed using the Web Infrastructure Model. The same attack as in [Bauer2022] was found to apply to GNAP as well. In this case, a model of a "careful user" (see Section 6.1.13) was used to show that the attack can be prevented (at least in theory) by the user.

"User Education" (Section 6.1.13)

In "An Automated Multi-Layered Methodology to Assist the Secure and Risk-Aware Design of Multi-Factor Authentication Protocols" [PCRSM2023], Pernpruner et al. defined a multi-layered methodology to analyze multi-factor authentication protocols at different levels of granularity. They leveraged their methodology to formally analyze a protocol relying on a QR code that has to be scanned on a secondary device to approve the authentication attempt on the primary device (User-Transferred Session Data Pattern, Section 3.1.1). Given the results of the analysis, they proposed some practical mitigations either to prevent or reduce the risk of successful attacks, such as those described in Section 6.1.13 and Section 6.1.17.

"User Education" and "Trusted Device Relationship" (Section 6.1.13 and Section 6.1.17)

Where do we go Next?

Next Steps

- We need reviewers!

Questions