OIDC² – A Simple End-to-End User Authentication Method for the Internet

Jonas Primbs
University of Tübingen

Michael Menth
University of Tübingen

36th Crypto Day, 14/15 March 2024

We present Open Identity Certification with OpenID Connect (OIDC²) as a novel end-to-end authentication mechanism for users on the Internet (Primbs & Menth (2023)). OpenID Connect (OIDC) is a protocol for users to log in to different third-party accounts with one Single Sign-On (SSO) account. An SSO account may be, e.g., a Google account. OIDC is widely deployed due to ease of use. OIDC² is a simple extension of OIDC for end-to-end authentication of users who trust each other's OpenID Providers (OPs).

While OIDC issues only ID Tokens (IDTs), OIDC² introduces Identity Certification Tokens (ICTs). Their usage is as follows. An End-User (EU) logs in to his OP and authorizes an application client to obtain an ICT from the OP. Then, the client generates a key pair and includes the public key in the ICT request together with a proof of possession (PoP) of the private key. The OP verifies the public key with the PoP, adds the EU's identity information and the client's public key to a new ICT, signs it, and issues it to the client. The client uses this ICT like a certificate for authentication by another EU's client. That is, EU A's client sends the ICT together with a PoP of the private key to the client of EU B. If the client of EU B is configured to trust the OP, the client verifies the PoP, requests the OP's public key, and uses it to verify the ICT. If PoP and ICT are valid, the identity information is presented to EU B as trustful, otherwise as non-trustful. Ease of use of OIDC² is achieved through short lifetime of ICTs so that neither complex key management nor certificate revocation lists are needed.

We distinguish authoritative OPs and verifying OPs. The first group issues unique identities for EUs whose real-world identity is not necessarily verified; examples are email providers. In contrast, verifying OPs also verify an EU's real-world identity; examples are banks or employers.

OIDC² can solve many authentication problems for which either no authentication standards have evolved, yet, or for which existing solutions fail due to poor usability. Three obvious use cases are instant messaging, video conferencing, and email. Authentication for video conferencing is increasingly important as major incidents due to deepfakes have been recently reported by Oltermann (2022) and Chen & Magramo (2024). Moreover, signed emails are a measure against phishing attacks, but email signatures based on S/MIME and PGP have not been widely adopted by users (Stransky, Wiese, Roth, Acar & Fahl (2022)), probably due to poor usability. With OIDC², emails can be signed with ICTs and verified, without requiring users to deal with long-term certificates.

A deployment strategy for OIDC² is as follows. The most intriguing use case is email. When a large email provider which is also an OP starts issuing ICTs to offer simple email authentication for its users, the ICTs can also be used to sign emails of other email providers. Fast deployment is likely as simple signing and verifying emails is of great value. Once ICTs are available, they may also be used for other services such as instant messaging and video conferencing. If the technology is mature and accepted due to ease of use, other services and OPs will follow.

References

Heather Chen & Kathleen Magramo (2024). Finance Worker Pays out $25 Million after Video Call with Deepfake 'Chief Financial Officer'. https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk, last-accessed: Feb-15-2024.

Philip Oltermann (2022). European Politicians Duped Into Deepfake Video Calls with Mayor of Kyiv. https://www.theguardian.com/world/2022/jun/25/european-leaders-deepfake-video-calls-mayor-of-kyiv-vitali-klitschko, last accessed: Feb-09-2024.

Jonas Primbs & Michael Menth (2023). OIDC^2: Open Identity Certification with OpenID Connect. URL https://dx.doi.org/10.48550/arXiv.2307.16607. Preprint.

Christian Stransky, Oliver Wiese, Volker Roth, Yasemin Acar & Sascha Fahl (2022). 27 Years and 81 Million Opportunities Later: Investigating the Use of Email Encryption for an Entire University. In *2022 IEEE Symposium on Security and Privacy (SP)*, 860–875. URL https://dx.doi.org/10.1109/SP46214.2022.9833755.