JULY 19, 2018

FIDO TechNotes: The Truth about Attestation

DOWNLOAD SPECS

DOWNLOAD SPECS

Adam Powers, FIDO Alliance Technical Director

There is a frequently mentioned but little understood term in FIDO: attestation. Even engineers implementing FIDO products are often confused with how attestation works or why it is needed. This Tech Note is an attempt to clarify attestation and its role in FIDO transactions; the post is largely for the technical community, but hopefully it is clear enough to the lay-person with a basic understanding of FIDO as well.

To start with, every time a user registers with a new service (Google, Facebook, PayPal, GitHub, etc.) the FIDO authenticator generates a new key pair for that service. The keys are necessarily unique to that service and aren't shared across services. This is the keypair most commonly associated with FIDO, and it is referred to as the "credential key pair" or just "the key pair". When a user registers with a service a new key pair is generated, and the public key is sent to the service to be stored and used in the future to authenticate the user. That key pair is not the attestation key pair, and to

MORE BUYING, BUILDING & PARTNERING

fido ALLIANCE simpler stronger authentication

WHAT IS FIDO?
HOW FIDO WORKS
FIDO2 PROJECT
ALLIANCE
OVERVIEW
TERMS OF USE

SPECIFICATIONS
OVERVIEW
CERTIFICATION
OVERVIEW
KNOWLEDGE BASE
PRESS CENTER
PRIVACY POLICY

Join the Community

GET THE LATEST UPDATES

PARTICIPATE IN FIDO-DEV FORUM

DOWNLOAD SPECS