IoT : l'alliance FIDO veut renforcer la sécurité

L'alliance FIDO (Fast IDentity Online) officialise la création de l'IoT Technical Working Group afin d'élaborer un *framework* pour l'authentification des objets connectés sans mot de passe.

Trois axes de travail ont été définis : l'interopérabilité avec les fournisseurs de services, l'association d'applications et d'utilisateurs ainsi que le provisionnement *via* les routeurs et les hubs IoT.

> *We are thrilled to be partnering with our members to address this critical area of authentication. https://t.co/lR68AoGE3f*
>
> *— The FIDO Alliance (@FIDOAlliance) 26 juin 2019*

Sécuriser la récupération de comptes

Au sein de l'IoT Technical Working Group, on trouve des représentants d'ARM, Qualcomm, Intel, Google, Lenovo ou encore Microsoft.

Intel n'est pas impliqué dans l'autre groupe de travail officiellement constitué cette semaine : l'Identity Verification and Binding Working Group.

Son objectif : renforcer la sécurité des systèmes de création et de récupération de comptes protégés par un dispositif FIDO. À ces fins, il définira des critères pour la validation d'identité à distance et développera un programme de satisfaction.

Une douzaine d'organisations sont membres de ce groupe de travail à la tête duquel on trouve MasterCard et Onfido.

En toile de fond, des attaques IoT dont le volume augmente plus nettement que les investissements consentis pour les juguler.

Au-delà des budgets se pose la question de la sécurité même des objets connectés. Notamment la difficulté d'installer des correctifs : certains ne peuvent tout simplement pas être mis à jour ou requièrent une intervention spécifique du fournisseur.