PERIODICA
Journal of Modern Philosophy, Social Sciences and Humanities

ISSN NO:2720-4030 Volume 24 November, 2023

FIDO2 Protocol and Biometric Security.

Sultonov Sarvar Mahammadodilovich
Teacher of the ATT department of Fergana branch of TATU

ABSTRACT

The FIDO2 protocol is a cybersecurity protocol designed for user identification and authentication, developed by the FIDO (Fast Identity Online) Alliance. It includes the FIDO U2F (Universal Second Factor) and UAF (Universal Authentication Framework) protocols and aims to make identification and authentication processes on websites, web services or other processes simple, secure, and efficient.

ARTICLE INFO

Received: 24th September 2023
Revised: 24th October 2023
Accepted: 28th November 2023

KEYWORDS: FIDO2, U2F, WebAuthn (Web Authentication), CTAP (Client-to-Authenticator Protocol).

The FIDO2 protocol stands for "Fast Identity Online 2". and work developed FIDO (Fast Identity Online) committee by created _ FIDO committee , users own safety and identification for new and efficient approaches present reach in order to the work take goes _

FIDO2 protocol , by FIDO Alliance his own main goals about , that is passwords or another authentication methods through users identification and authentication of doing easy , safe and efficient approaches Create is simple to do and physical identification tools high level to apply strengthening , advice perform for created _

FIDO Committee , cyber safety branch and identification protocols development for movement doer one series companies and interdisciplinary organizations by organize done in 2012 _ own activities started _ The FIDO Alliance is important networks , organizations and areas physical and online identification and authentication approaches development and of them use for unites _

FIDO2 by FIDO Alliance work developed FIDO U2F (Universal Second Factor) and UAF (Universal Authentication Framework) protocols mutually integration as own development continue makes _ FIDO Alliance companies and organizations , FIDO protocols own services integration to do through to users safe , simple , and reliability increased identification and authentication approaches present to do help are giving

The FIDO2 protocol stands for Fast Identity Online 2 and safety in the field identification and authentication processes easy and safe to do in order to work developed in websites _ and in web services users authentication to do for intended . FIDO2 protocol the following two main from the part consists of :

- WebAuthn (Web Authentication):

- This part is on websites users identification to do for intended web standard represents _ WebAuthn , web browsers and of web services users for passwords and another authentication information to apply stops . Users safe identification to do for from the user received identification through tools (authenticators). authentication do it they get

WebAuthn (Web Authentication) is a FIDO2 protocol within created and on websites users identification to do and authentication to do for intended one is standard . WebAuthn , users passwords or another authentication methods through identification of doing instead of , safe identification tools through themselves identification to do possibility will give .

Main Features :

- Security : WebAuthn , passwords easy empty is safe _ identification through tools (authenticators). identification processes manages _ This method is passwords and another authentication information through surface coming a lot in different ones safety problems to solve the goal does _

- Identification Tools : Users to themselves comfortable and safe identification tools (for example , smartphones , USB keys , biometric devices) choose .

- Safe Communication : WebAuthn , identity tools and website or web services between communication safe and efficient does _

- International Default : WebAuthn , international standards based on created is a lot organization and companies by is used .

WebAuthn , on the web identification and authentication processes simple , effective and safe to do for another authentication methods through created to standards alternative as works _

-CTAP (Client-to-Authenticator Protocol):

CTAP (Client-to-Authenticator Protocol) is part of the protocol created to manage authenticators within FIDO (Fast Identity Online) protocols. This part represents a protocol designed to manage communication between a user device (for example, a smartphone or a USB key) and a web browser. CTAP manages communication between the web browser and the user's device in a secure and efficient manner.

Main features:

Secure Communication: CTAP provides secure communication between the user device and web browsers. This protocol makes secure communication between authentication tools and web browsers easy and efficient.

Convergent Protocol: CTAP ensures that communication between user devices and web browsers is well structured and convergent.

Compatibility with Web Browsers: CTAP is designed to provide compatibility with most web browsers.

Extensive Features: Supports a wide variety of devices, including smartphones, USB keys, and other secure identification devices, in managing identification and authentication processes between user devices and web browsers via FIDO protocols, CTAP.

Intimacy in Use: CTAP ensures that communication between users and web browsers is intuitive and easy.

CTAP was developed by the FIDO Alliance as part of the FIDO2 protocol and is used to manage communication between FIDO2 authenticators and web browsers. This protocol plays an important role in the integration of authentication tools into websites or web services and plays a major role in ensuring secure communication.

The FIDO2 protocol increases security by using authenticators instead of passwords. Users can stop using bad passwords or other authentication information and change them through authentication tools. These tools include smartphones, USB keys, biometric tools (supporters) and other security tools.

The FIDO2 protocol makes it possible to use those identification tools instead of passwords or other authentication information to provide better security for websites and online services.

The implementation of the FIDO2 protocol consists of the following steps:

-Choose Identification Means:

It is necessary to choose the means of identification (authenticators) through the FIDO2 protocol. These identification tools are used by the user and include smartphones, USB keys, biometric tools (supporters), and other security tools.

-Install FIDO2 Protocol For Website or Web Service:

A website or web service administrator must be ready to add the FIDO2 protocol. This process allows users of the website or service to use FIDO2 authentication tools.

-Using the WebAuthn API:

When implementing the FIDO2 protocol on a website or web service, you must use the WebAuthn API. This API allows web browsers to select authentication tools, send authentication requests to them, and manage the authentication processes that have been performed.

-Using CTAP:

The Client-to-Authenticator Protocol (CTAP) is used to manage communication between web browsers and FIDO2 authentication devices (such as USB keys or smartphones). CTAP provides secure communication between authentication tools and web browsers.

-User Selection of Identification Means:

Users choose the means of identification and make settings to use them on websites or services related to their devices.

-Managing Authentication Processes:

The FIDO2 protocol provides the ability to manage the authentication processes associated with the use of identification tools. These processes are carried out through authentication requests sent by the website or web service administration server.

The FIDO2 protocol enables the use of secure means of identification instead of identifying users with passwords or other authentication information. This method is used to increase security and make identification processes simpler and more efficient.

References.

1. Sultanov Sarvarjon Mahammadodilovich , Otakhonova Zamirakhon Muratovna , Abdukarimov Shahislam Believe me son _ (2023). DETECTION AND PREVENTION OF PHISHING ATTACKS. Science Promotion, 3(2), 160–164. Retrieved from https://sciencepromotion.uz/index.php/sp/article/view/315
2. Khurshid Khusanboevna Rajabova , Sarvarjon Sultanov Mahammadodilovich . (2023). PSYCHOLOGICAL TYPES OF INTERNET INFLUENCE AND DIFFERENT APPEARANCES OF RESISTANCE TO INFLUENCE. Science Promotion, 3(2), 35–40. Retrieved from https://sciencepromotion.uz/index.php/sp/article/view/285
3. Sultanov Sarvarjon Mahammadodilovich , Khurshida Khusanboevna Rajabova , Rahmonjon Foziljanov Victorious his son _ (2023). Protection in systems intellectual from systems use _ Science Promotion, 3(2), 154–159. Retrieved from https://sciencepromotion.uz/index.php/sp/article/view/314
4. Sarvarjon Sultanov Mahammadodilovich , Sharobiddin Israelov Makhammadyusufovich , Abduvahobov Abdulaziz Jahangir son _ (2023). Types of malware and harmful from programs protection . Science Promotion, 3(2), 88–91. Retrieved from https://sciencepromotion.uz/index.php/sp/article/view/297
5. Abdurakhmonov , S., Sayitov , S., Mirzajonov , M., Bilolov , I., & Khaydarov , A. (2023, April). Research of terminal soldering technology for auto glass heating systems. In E3S Web of Conferences (Vol. 389, p. 01036).
6. Inomjon , B. (2023). METHODS OF DOCUMENT CAMERA USE IN GENERAL SECONDARY SCHOOLS. Engineering problems and innovations.
7. Abdullajonova , N. (2023). SIMPLE LINEAR REGRESSION METHODS IN PYTHON PROGRAMMING LANGUAGE. Engineering problems and innovations.
8. Sultanov Sarvarjon Mahammadodilovich , Khurshida Khusanboevna Rajabova , Rahmonjon Foziljanov Victorious his son _ (2023). Developing of the state important infrastructure in the sector cyber security opportunities . Science Promotion, 3(2), 149–153. Retrieved from https://sciencepromotion.uz/index.php/sp/article/view/313
9. Sultanov Sarvarjon Mahammadodilovich , Hasanboy Kadyrov Oribjonovich , Rahmonjon Foziljanov Victorious his son _ (2023). USE OF NEW PEDAGOGICAL TECHNOLOGIES IN WEB PROGRAMMING. Science Promotion, 3(2), 144–148. Retrieved from https://sciencepromotion.uz/index.php/sp/article/view/312
10. _Sultanov , S. , & Umarova , M. (2023). CYBER SECURITY: PROTECTING YOUR DATA IN THE DIGITAL AGE. Science and Innovation, 1(28), 49–52. izvlecheno ot https://in-academy.uz/index.php/si/article/view/22350