

# FIDO Certified Professional

## CANDIDATE HANDBOOK



**Congratulations on taking the first step in enhancing your career.**

**The FIDO Alliance (FIDO) established the FIDO Certified Professional (FCP) program to promote the expertise gained as a professional engaged in identity and access management. By choosing to review this candidate handbook, you have taken the first step toward joining those who have distinguished themselves by earning the FCP credential.**

Thank you for your interest in the FIDO Certified Professional Program (FCP). This handbook summarizes key aspects of the FCP Program and is intended to help you understand why the program was developed, how it is governed, its policies and procedures, and the steps to earning and maintaining the FCP credential.

The handbook is a useful reference to you as you:

- make your decision whether to pursue the FCP
- complete the FCP application

The FCP is a constantly evolving program that continues to grow and be refined in accord with the evolution of due diligence and certification professional practices. You are encouraged to use this handbook as a guide to learn more about the program however, we strongly encourage you to review the material on the [FCP Program website page](#). FCP staff can be reached via email at [fcp@fidoalliance.org](mailto:fcp@fidoalliance.org).

### IS MY INFORMATION KEPT CONFIDENTIAL?

Certification applications and candidates' performance on the FCP review shall remain confidential unless otherwise stipulated by the reviewee or as required by law. The FCP Program will release application and pass/fail information only to the applicant and only in writing. The exception to this is the published list of FCPs that the Board Certification Committee makes available to the public. This statement does not preclude the publishing of any holder's name against whom disciplinary action has been taken.

## ABOUT THE FIDO CERTIFIED PROFESSIONAL PROGRAM

### INTRODUCTION

This handbook contains the application requirements, procedures, and eligibility requirements to sit for the FCP examination. A link to the governing program policies is also provided.

### THE FCP CERTIFICATION

The mission of the FCP Certification program is to advance the identity, authentication, and authorization discipline. Certification through this program proves advanced knowledge and technical skills to analyze, validate, design, deploy, and educate on secure authentication systems using FIDO.

## SCOPE OF THE FCP CERTIFICATION

A FIDO Certified Professional is an identity and authentication expert who helps organizations deploy and integrate FIDO standards by analyzing business requirements and proposing a FIDO architecture that ensures secure authentication processes.

## THE FCP CERTIFICATION GOVERNANCE

The FIDO certified professional program as a whole is the responsibility of the FIDO Board Certification Committee (BCC), with necessary oversights and approvals from the FIDO Board of Directors and collaboration with other FIDO Working Groups where needed. The Certification Secretariat is responsible for implementing, operating, and managing the FIDO Certified Professional program defined by the BCC.

## FCP ELIGIBILITY REQUIREMENTS

---

### PREREQUISITE EXPERIENCE

The FIDO Certified Professional shall have at least two to four (2-4) years of industry experience in at least three (3) of the five (5) domains of knowledge. The domains of knowledge are:

- 1. Analyzing Business Requirements**
- 2. Validating Business and Technical Requirements for Implementation**
- 3. Designing and Implementing Business and Technical Requirements**
- 4. Deploying FIDO Authentication Solutions**
- 5. Educating Others about Authentication**

FIDO Certification professionals generally work in roles such as Technology Architects, System & Operations Engineers, Security Professionals, and Identity & Access Management Professionals.

The certification application will include a section to report years of industry experience.

## DEFINITIONS

### **Applicant:**

An individual who has submitted the application for FCP Certification

### **Candidate:**

An individual who meets the eligibility requirements for FCP Certification

### **Certified Individual:**

An individual who has earned and maintained the FCP Certification and is authorized to use the FCP Mark.

## FCP ACCOUNT AND APPLICATION

To start the certification process, the individual must complete the account registration process on the [FCP Program website page](#). The account will give access to the FCP Dashboard, where individuals seeking FCP certification can complete additional program forms and see deadlines and status updates.

## FCP EXAM FEES

Exam fees are due following Candidate approval. Initial exam fees for FIDO Member participants are \$550 and \$750 for non-FIDO Member participants.

## PREPARING FOR THE EXAM

The FIDO Certified Professional is a computer-based exam that is proctored. Candidates have two hours and forty minutes to complete the examination.

The FCP examination was developed in accordance with best practices in test development and measurement. Working with experts in the development of certification examinations, the resulting FCP certification examination is reliable and valid. To validate the examination, measurement specialists worked with the FIDO Alliance staff, and a committee of Subject Matter Experts (SMEs) to design and conduct a job task analysis study. That analysis resulted in the development of a standardized examination content outline that included the expertise of FIDO SMEs. FIDO SMEs were also called upon to write, review, edit, and approve examination questions under the guidance of experts in testing and measurement.

Candidates are encouraged to prepare for the FCP examination by reviewing the FCP exam matrix and Final Examination Content Outline located in the sections below, as well as resources located on the FCP Program website page.

### EXAMINATION CONTENT

This exam matrix is provided to illustrate the general distribution of questions and the relative weight or emphasis given to a skill or content area on the examination. A successful risk management practitioner should have experience and a fundamental understanding of these five broad topic areas.

For a more specific breakdown of topics, refer to the Final Examination Content Outline.

FIDO Certified Professional		
<b>A</b>	Analyzing Business Requirements	16.67%
<b>B</b>	Validating Business and Technical Requirements for implementation	23.33%
<b>C</b>	Designing and Implementing Business/Technical Requirements	28.33%
<b>D</b>	Deploying FIDO Authentication Solutions	20.00%
<b>E</b>	Educating Others about Authentication	11.67%
	<b>Total</b>	<b>100%</b>

## FCP Examination Content Outline

The task list below describes the activities that a FIDO Certified Professional is expected to perform on the job. All examination questions are linked to these tasks.

Content Domains	Finalized % Weighing
<b>A. Analyzing Business Requirements</b>	<b>16.67%</b>
1. Identify goals of stakeholders	2.50%
2. Identify use cases of specific users	2.50%
3. Map business requirements to available technology	3.33%
4. Determine the risk of not implementing the business requirements	2.50%
5. Determine the limitations of the current system	3.33%
6. Prioritize the value of the requirements	2.50%
<b>B. Validating Business and Technical Requirements for Implementation</b>	<b>23.33%</b>
1. Determine the feasibility of the task	4.17%
2. Ensure regulatory/legal compliance	5.00%
3. Size the system (scale, availability, performance)	2.50%
4. Determine implementation phases	4.17%
5. Build proof of concept (POC)	4.17%
6. Conduct testing	3.33%
<b>C. Designing and Implementing Business/Technical Requirements</b>	<b>28.33%</b>
1. Define features from the technical requirements	5.00%
2. Design user experience	4.17%
3. Investigate integration of FIDO solutions with the existing system and business processes	5.00%
4. Develop identity system architecture	6.67%
5. Implement features from the technical requirements	7.50%
<b>D. Deploying FIDO Authentication Solutions</b>	<b>20.00%</b>
1. Configure the FIDO components	6.67%
2. Test components and applications	4.17%
3. Implement monitoring and technical support	5.00%
4. Measure success	4.17%
<b>E. Educating Others about Authentication</b>	<b>11.67%</b>
1. Give an authentication history lesson	3.33%
2. Teach about FIDO protocols	5.83%
3. Provide decision information to business owners	2.50%

## SCHEDULING THE EXAM

---

### SCHEDULING

All candidates will receive an email, *FCP Authorization-to-Test*, from the FIDO Alliance Certified Professional Secretariat with detailed instructions for scheduling the examination with Pearson VUE. Candidates will have the opportunity to schedule their examination at Pearson VUE testing centers.

The FCP Secretariat makes it possible for candidates to sit for the FCP certification examination at a date and time that is convenient for them. Candidates may schedule their FCP certification examination at any convenient date and time within their eligibility period. Candidates must schedule their exam at least 24 hours in advance but may schedule up to 90 calendar days before their desired examination date for the best selection of dates, times, and testing locations.

Note that because Pearson VUE testing centers have limited availability, especially during prime testing periods, it is recommended that the candidate schedule their exam early in order to increase the likelihood of receiving their first choice of date, time, and location. Appointments will be made on a first-come, first-served basis, according to availability of testing sites. Neither FIDO Alliance nor the FCP Secretariat is responsible for test center availability.

An extension to schedule FCP certification examination is available up to 180 days. If a candidate fails to schedule their examination within their authorization period a partial refund of the initial exam fee will be processed. Neither FIDO Alliance nor Pearson VUE is responsible if the candidate does not schedule an appointment before their authorization expires. Testing centers can be located by visiting the Pearson VUE website and clicking "For test takers."

### NO SHOWS

Once the examination appointment is scheduled, the candidate will be permitted to make changes to the appointment such as location, rescheduling or cancellation. All changes are made through the Pearson Vue – FIDO Certified Professionals website.

Candidates who show up late and are not admitted, fail to present adequate identification, or refuse to sign the nondisclosure agreement will not be allowed to take the test and will be considered a no-show.

Candidates who are considered no-shows forfeit the full examination fee.

## TAKING THE EXAM

---

### TAKING THE EXAM

All FCP candidates must have prior authorization from the FCP Secretariat to take the examination. Candidates must provide two forms of identification (a list of acceptable forms of identification is below), at least one of which must be government issued, have a photo and a signature. The name on the IDs must match exactly the name submitted on the application or on the web account profile and in the appointment confirmation email.

Additional details on taking the examination are provided to candidates in the email they receive from the FIDO Alliance Certification Team once their application is approved. If candidates experience problems that affect their ability to take the examination, they must notify the test administrator at the testing site immediately. Test administrators cannot answer any questions about test items or content of the examination. However, if candidates have a procedural question, the testing staff will do their best to assist them.

All examination questions are copyrighted property of FIDO Alliance. It is forbidden under federal copyright law to copy, reproduce, record, distribute or display these examination questions by any means, in whole or in part. Doing so may subject the candidate to severe civil and criminal penalties and actions by the FIDO Alliance.

The test administrator will keep the official time and ensure that candidates are given the allotted time of two hours and forty minutes for the examination. If a candidate leaves the room to take a restroom break the examination time will not stop. Candidates are not permitted to leave the examination area to go to their cars, to speak to anyone, or make personal calls.

**The test administrator may dismiss a candidate from the examination for any of the following reasons:**

- If the candidate's admission to the examination is unauthorized.
- If a candidate creates a disturbance or gives or receives help.
- If a candidate attempts to remove examination materials or notes from the testing room.
- If a candidate attempts to take the examination for someone else.
- If a candidate has in his or her possession any prohibited item.
- If a candidate exhibits behavior consistent with memorization or copying of examination items.

## AUTHORIZATION TO TEST

You are strongly urged to schedule your test as soon as convenient after your application is approved. You will receive an "Authorization-to-Test" via email. This authorization will contain the timeframe within which you must test. Your authorization will be valid for 90 days, with extension available up to 180 days.

If you do not request an extension prior to the expiration of your authorization period, you will need to reapply and pay a new examination fee.

## EXAMINATION SECURITY PROCEDURES

Candidates who are taking the FCP examination at a Pearson VUE testing center will be required to provide two forms of valid ID. A primary ID must contain a photo and signature, and one secondary ID with a signature.

### Primary

**The following IDs meet the primary ID requirements:**

- Government-issued driver's license
- State/national identification card
- Passport\*
- Military ID\*
- Alien registration card
- U.S. Passport card
- U.S. Dept of State Driver's license

\*The primary ID must contain a photo and signature unless the signature is embedded in the identification. When this occurs, candidate must present another form of signature identification from the primary or secondary list.

### Secondary

**The following IDs meet the secondary ID requirements:**

Any ID on the primary list  
OR  
Social Security card  
Credit/bank ATM card (signature required)

## Biometrics

Some Pearson VUE testing centers (those designated as Pearson Professional Centers [PPC] and some designated as Select Pearson VUE Testing Centers [PVTC]) may require biometric identification using palm vein capture technology. Palm vein recognition examines the unique patterns in a candidate's palm veins using a safe, near-infrared light source like that in a TV remote control. All centers require electronic signature and a digital photo.

## Erasable Note Board

Standard procedure is that the candidate receives one erasable note board to use as scratch paper during the examination.

## Personal Items

Candidates are not allowed to bring personal items into the testing area. Headsets, mobile phones, electronic devices, watches, wallets, purses, hats, bags, coats, books, notes, or any materials not specifically approved by the certification body are not permitted. Failure to comply with these examination requirements, and the test area or “workspace” not passing a room scan, will result in termination of the exam administration and candidates will need to reschedule and pay a rescheduling fee.

Consideration is made for comfort items (such as a pillow, crutches, and tissues), which the testing center administrator must inspect for exams. A designated area will be provided in the testing area for all personal belongings, but neither Pearson VUE nor the FCP Secretariat is responsible for any personal belongs left in the area before, during or after the examination.

## AFTER THE EXAMINATION

---

### EXAMINATION RESULTS

Candidates will be provided with a printed test receipt at the completion of their examination. The FCP Secretariat will provide exam results once they become available by Pearson VUE. A “cut score” will need to be established once the first 50 exams are completed, resulting a delay in issuing exam results\*. All results are designated as Pass/Fail.

Candidates who failed the examination will be provided a diagnostic analysis of their relative strengths and weaknesses by content area. Diagnostic analysis is not provided onsite. It will be sent in a follow-up email.

Candidates who have successfully passed the examination will be notified of their certification status by the FCP Secretariat. Those who have passed the examination and met all other eligibility requirements will receive a FCP Welcome Packet that includes a FCP certificate and other business and communication items. The individual may then use the FCP initials after their name and use the FCP Mark as allowed by the FCP Code of Ethics and the policies of the FCP Certification. Committee.

**\*NOTE:** Exam results will be delayed for approximately 30-60 days so that we can identify a cut score for the pass/fail rate.

### DISPUTED RESULTS

The FCP Secretariat employs a rigorous process to ensure that no errors occur in the scoring of exams, including a quality control scoring audit and statistical analysis of all questions. Due to the accuracy of electronically scored exams, changes as a result of rescoring are highly unlikely. However, a candidate may request a hand-score of his or her exam by completing and submitting the Application to Hand.

Any disputes must be sent to the FCP Secretariat within 90 days of known incident.

### RETESTS

Candidates who fail the exam may retake it and must pay the retest fee \$150 each time. Candidates who fail may retake the exam 90 days after the first attempt. Candidates who fail on the second attempt may take the exam a third time and must do so 90 days after the second attempt. After the third failure, the candidate will be required to wait 180 days, reapply as a new candidate, and pay all applicable fees.

## CERTIFICATION MAINTENANCE

---

### ANNUAL MAINTENANCE

Annual Maintenance Fees (AMFs) are a required part of certification and are due on an annual basis. The fee covers the cost of certification maintenance and the member benefits that a FIDO Certified Professional will receive as a FCP certificate holder.

The initial AMF fee is included in the initial exam fee. AMFs are prorated for the first year based on the date of certification. Once certified, AMFs will be due January 1st each year. The annual AMF is U.S. \$125.

If the AMF is not paid by the payment deadline the FCP certification will be suspended. If the FCP experiences a hardship during the certification cycle FIDO may allow the FCP a grace period to pay AMFs. If the FCP requires a grace period for their submissions, they must notify the FCP Secretariat on or before the payment deadline.

### CONTINUING PROFESSIONAL EDUCATION

The FCP certification does not require retesting. Instead, the certification program requires FIDO Certified Professionals maintain their knowledge and skills related to their profession. The earning of CPEs is a way for professionals to enhance their knowledge and skills in order to deliver professional services to customers, clients, and community.

To maintain FIDO Membership and FCP certification, FIDO Certified Professionals must earn a minimum amount of CPE, submitted and reviewed on a yearly basis.

FIDO Certified Professionals are required to earn 90 CPE credits over their 3-year certification cycle and submit annually. All CPE activities must be completed during the three (3) years of each certificate cycle and no later than the certification date (end of certification cycle). Failing to meet the CPE requirements by the annual deadline or 3-year cycle expiration date is grounds for certification suspension.

The FCP is required to keep track of all CPE activities and report them through their FCP Dashboard online. CPE credits are categorized into two groups, Group A and Group B. Group A are activities directly related to the FCP domains of knowledge, and Group B activities are other professional development.

## FIDO CODE OF CONDUCT

---

The FIDO Alliance is a non-profit industry organization that works to replace passwords with simpler, secure methods of authentication. It consists of hundreds of members varying in size and geographical diversity and collaborates with industry partners and regulators around the world.

To help fulfil its mission, the FIDO Alliance has adopted this Code of Conduct, as an ethical framework for its interactions both within the alliance during working group and committee meetings, both online and in person, and for staff, contractors and volunteers representing the FIDO Alliance when meeting with other members, non-members, industry partners and regulators.

The FIDO Alliance believes that compliance with high ethical standards is key to meeting its objectives as well as being to the benefit of all stakeholders.

FIDO Alliance acknowledges that its Member companies may have their own Code of Conduct or equivalent and anticipates that this Code of Conduct shall complement and reinforce those.



This Code of Conduct shall apply to the FIDO Alliance staff and contractors at all times, as well as its Members as their conduct relates to the activities of the FIDO Alliance. For the purposes of this document, 'FIDO Alliance' shall refer to all staff, contractors and all Member volunteers

#### **1. NEUTRALITY**

The FIDO Alliance maintains strict political, religious, and philosophical neutrality.

#### **2. EQUALITY**

The FIDO Alliance and its Members shall respect the principles of equal treatment and equal opportunities between human beings. The FIDO Alliance and its Members abide by the principle of non-discrimination based on, notably, race, origins, social group, sexual orientation, religion, beliefs, abilities, opinions, or language.

#### **3. PROTECTION FROM HARASSMENT**

The FIDO Alliance and its Members bring together individuals from all over the world. All participants shall treat and be treated fairly, politely and with respect by their colleagues. Unacceptable behaviors include any form of harassment (sexual or otherwise), abusive, discriminatory, derogatory, demeaning, offensive, or dangerous conduct, as well as other behaviors that would be considered inappropriate within a professional setting.

#### **4. PRIVACY & CONFIDENTIALITY**

The FIDO Alliance and its Members shall apply the FIDO Alliance Privacy Policy and shall adhere to the applicable legal framework on data protection.

The FIDO Alliance and its Members shall maintain the confidentiality of non-public information, including confidential information provided by third parties, according to the FIDO Alliance Membership Agreement.

#### **5. RESPECT FOR THE RULE OF LAW**

The FIDO Alliance and its Members are committed to respecting the rule of law, in particular the laws, rules and regulations applicable to their activities, whether it is the law of a meeting place, the law of the residence location of a given individual, company or organization, the law of the formation location of a given company or organization, any other law that may apply to the given individual, company or organization and any combination of the above. In doing so, the FIDO Alliance and its Members should take into full consideration prevailing international decisions, treaties, conventions, and trade controls.

#### **6. HONESTY & FAIR COMPETITION**

The FIDO Alliance and its Members are required to adhere to the highest standards of honesty, respect, truth, fairness, and ethical behavior. When communicating to other parties or to the public, the FIDO Alliance and its Members shall use best efforts to ensure the accuracy of statements and shall refrain from providing false, inaccurate, or otherwise misleading information.

The FIDO Alliance is committed to complying with all applicable antitrust laws and regulations, and, by joining the alliance and executing the FIDO Alliance Membership Agreement, its members agree to limit discussions to subjects that relate to the purposes of the FIDO Alliance, whether such discussions take place during formal meetings, informal gatherings, or otherwise.

#### **7. NO CORRUPTION OR CRIMINAL ACTIVITIES**

Neither the FIDO Alliance nor its Members shall use threats, bribes, or other illegal means contrary to national anti-corruption laws to influence the adoption or implementation of laws, rules or regulations, or the content of court decisions. In the absence of national legislation, the FIDO Alliance and its Members shall abide by best international practices on anti-corruption in the private and public sectors.

#### **8. NO CONFLICT OF INTEREST**

FIDO Alliance Members commit to disclose any interest that could reasonably be considered to involve a conflict of interest and to refrain from any activity directly or indirectly giving rise to a conflict of interest.

#### **9. PROHIBITION ON CONDUCT BRINGING THE FIDO ALLIANCE INTO DISREPUTE FIDO**

Alliance and its Members will not engage in any conduct which brings FIDO into disrepute or jeopardizes the integrity of its activities.

## 10. SOCIAL MEDIA

Participants' use of social media can pose risks to the FIDO Alliance's reputation and mission and can even jeopardize the FIDO Alliance's compliance with business rules and laws. To minimize these business and legal risks, the FIDO Alliance expects participants to adhere to the following guidelines and rules regarding social media use.

- Participants are responsible for what they personally communicate in social media and should remember that what they write might be made public, even if they initially intend for the communication to be private. Participants shall make clear in their personal social media activity that they are speaking on their own behalf. They will write in the first person and use their personal addresses and account names when communicating via social media. If a participant discloses their affiliation with the FIDO Alliance, they will also include a disclaimer that their views do not represent those of FIDO Alliance.
- Participants will use good judgment about what they post and remember that anything they say can reflect on the FIDO Alliance, even with the inclusion of a disclaimer.
- Participants must strive to be accurate in their communications about the FIDO Alliance and remember that their statements have the potential to result in liability for themselves or the FIDO Alliance. The FIDO Alliance encourages professionalism, respect and honesty in social media and all other communications. Participants should be mindful that the FIDO Alliance's policies and procedures, and this Code, apply to their social media activity as well, including those policies and standards related to confidentiality, non-discrimination, and harassment.
- If a participant is contacted for comment about the FIDO Alliance for publication, including in any social media or news outlet, they should direct the inquiry to [marketing@fidoalliance.org](mailto:marketing@fidoalliance.org).

## 11. IMPLEMENTATION

The FIDO Alliance is always bound to this Code of Conduct. The FIDO Alliance Members shall adhere to this Code of Conduct, in addition to their own ethical and compliance rules, when conducting any activities associated with the FIDO Alliance. Any external consultants engaged by Members shall also be required to adhere to this Code of Conduct as it relates to their activities concerning the FIDO Alliance.

If any staff member, officer or Member of the FIDO Alliance becomes aware of a breach of the Code of Conduct, he or she may bring it to the attention of the Executive Director in a confidential manner. If this is deemed inappropriate, the complaint may be brought to the President.

## 12. FAILURE TO FOLLOW THE CODE OF CONDUCT

If a participant engages in unacceptable behavior, FIDO may take any action it deems appropriate, up to and including expulsion and/or disqualification from FIDO meetings, events, and programs without warning.

Based on the nature of or continued conduct, failure to adhere to one or more of the principles of the Code of Conduct will be reviewed by the FIDO Board, which may suspend or terminate a staff member, the membership of the Member concerned or require the person concerned to be replaced by the Member with immediate effect.

## REFERENCE MATERIAL

These materials will be useful in helping you study for the FCP Exam. It is not an exhaustive list, and it is recommended that you self-assess according to the domains listed in the FCP Examination Content Outline and study accordingly.

Name	Source
<b>FIDO Protocol v2.1</b>	<a href="https://fido-uaf--v1.2-ps-20201020/fido-uaf-protocol-v1.2-ps-20201020.html">fido-uaf--v1.2-ps-20201020/fido-uaf-protocol-v1.2-ps-20201020.html</a>
<b>FIDO UX Guidelines</b>	<a href="http://fidoalliance.org/wp-content/uploads/2021/06/FIDO-UX-Guidelines_Final_June2021.pdf">http://fidoalliance.org/wp-content/uploads/2021/06/FIDO-UX-Guidelines_Final_June2021.pdf</a>
<b>How to FIDO</b>	<a href="https://fido-alliance.github.io/how-to-fido/HowToFIDO.html">https://fido-alliance.github.io/how-to-fido/HowToFIDO.html</a>
<b>WebAuthn Support Matrix</b>	<a href="https://fidoalliance.org/fido2/fido2-web-authentication-webauthn/">https://fidoalliance.org/fido2/fido2-web-authentication-webauthn/</a>
<b>FIDO Authenticator Security Requirements</b>	<a href="https://fidoalliance.org/specs/fido-security-requirements/fido-authenticator-security-requirements-v1.4.1-fd-20210510.html">https://fidoalliance.org/specs/fido-security-requirements/fido-authenticator-security-requirements-v1.4.1-fd-20210510.html</a>
<b>FIDO UAF Architecture Overview</b>	<a href="https://fidoalliance.org/specs/fido-uaf-v1.2-ps-20201020/fido-uaf-overview-v1.2-ps-20201020.html">https://fidoalliance.org/specs/fido-uaf-v1.2-ps-20201020/fido-uaf-overview-v1.2-ps-20201020.html</a>
<b>FIDO Security Reference</b>	<a href="https://fidoalliance.org/specs/fido-v2.0-id-20180227/fido-security-ref-v2.0-id-20180227.html">https://fidoalliance.org/specs/fido-v2.0-id-20180227/fido-security-ref-v2.0-id-20180227.html</a>
<b>FIDO Server Spec</b>	<a href="https://fidoalliance.org/specs/fido-v2.0-rd-20180702/fido-server-v2.0-rd-20180702.html#authentication-examples">https://fidoalliance.org/specs/fido-v2.0-rd-20180702/fido-server-v2.0-rd-20180702.html#authentication-examples</a>
<b>WebAuthn Spec</b>	<a href="https://fidoalliance.org/specs/fido-v2.0-rd-20180702/fido-server-v2.0-rd-20180702.html#intro">https://fidoalliance.org/specs/fido-v2.0-rd-20180702/fido-server-v2.0-rd-20180702.html#intro</a>
<b>FIDO CTAP 2.1</b>	<a href="https://fidoalliance.org/specs/fido-v2.1-ps-20210615/fido-client-to-authenticator-protocol-v2.1-ps-20210615.html">https://fidoalliance.org/specs/fido-v2.1-ps-20210615/fido-client-to-authenticator-protocol-v2.1-ps-20210615.html</a>
<b>WebAuthn spec</b>	<a href="https://fidoalliance.org/specs/fido-v2.1-rd-20210309/#user-consent">https://fidoalliance.org/specs/fido-v2.1-rd-20210309/#user-consent</a>
<b>FIDO Metadata Statement v3</b>	<a href="https://fidoalliance.org/specs/mds/fido-metadata-statement-v3.0-ps-20210518.html">https://fidoalliance.org/specs/mds/fido-metadata-statement-v3.0-ps-20210518.html</a>
<b>U2F and Phishing Attacks</b>	<a href="https://fidoalliance.org/tech-target-how-can-u2f-authentication-end-phishing-attacks/">https://fidoalliance.org/tech-target-how-can-u2f-authentication-end-phishing-attacks/</a>
<b>GDPR</b>	<a href="https://gdpr-info.eu">https://gdpr-info.eu</a>
<b>Trusted Certificates</b>	<a href="https://gist.github.com/CMCDragonkai/f5f76b8eb13e7579aba3">https://gist.github.com/CMCDragonkai/f5f76b8eb13e7579aba3</a>
<b>WebAuthn without user gesture</b>	<a href="https://github.com/w3c/webauthn/issues/1293">https://github.com/w3c/webauthn/issues/1293</a>
<b>NIST SP 800-63-3</b>	<a href="https://pages.nist.gov/800-63-3/sp800-63-3.html">https://pages.nist.gov/800-63-3/sp800-63-3.html</a>
<b>WebAuthn Attestation</b>	<a href="https://w3c.github.io/webauthn/#attestation-conveyance">https://w3c.github.io/webauthn/#attestation-conveyance</a>
<b>WebAuthn Gesture</b>	<a href="https://w3c.github.io/webauthn/#authorization-gesture">https://w3c.github.io/webauthn/#authorization-gesture</a>
<b>WebAuthn Spec RP ID</b>	<a href="https://w3c.github.io/webauthn/#rp-id">https://w3c.github.io/webauthn/#rp-id</a>
<b>WebAuthn Spec Modality</b>	<a href="https://w3c.github.io/webauthn/#sctn-authenticator-attachment-modality">https://w3c.github.io/webauthn/#sctn-authenticator-attachment-modality</a>
<b>Cookie Blocking</b>	<a href="https://webkit.org/blog/10218/full-third-party-cookie-blocking-and-more/">https://webkit.org/blog/10218/full-third-party-cookie-blocking-and-more/</a>
<b>WebAuthn Spec Public Key</b>	<a href="https://www.w3.org/TR/webauthn/#public-key-credential">https://www.w3.org/TR/webauthn/#public-key-credential</a>
<b>WebAuthn Spec Attestation Types</b>	<a href="https://www.w3.org/TR/webauthn/#sctn-attestation-types">https://www.w3.org/TR/webauthn/#sctn-attestation-types</a>
<b>WebAuthn Spec Automation</b>	<a href="https://www.w3.org/TR/webauthn/#sctn-automation">https://www.w3.org/TR/webauthn/#sctn-automation</a>
<b>WebAuthn Spec credential Storage</b>	<a href="https://www.w3.org/TR/webauthn/#sctn-credential-storage-modality">https://www.w3.org/TR/webauthn/#sctn-credential-storage-modality</a>
<b>WebAuthn - excludeCredentials</b>	<a href="https://www.w3.org/TR/webauthn-2/#dom-publickeycredentialcreationoptions-excludecredentials">https://www.w3.org/TR/webauthn-2/#dom-publickeycredentialcreationoptions-excludecredentials</a>
<b>Domain Bound Credential</b>	<a href="https://www.w3.org/TR/webauthn-2/#GetAssn-DetermineRpId">https://www.w3.org/TR/webauthn-2/#GetAssn-DetermineRpId</a>
<b>FIDO GDPR</b>	<a href="https://www.w3.org/TR/webauthn-2/#sctn-authenticator-data">https://www.w3.org/TR/webauthn-2/#sctn-authenticator-data</a> <a href="https://cdn2.hubspot.net/hubfs/4723359/FIDO_Alliance_GDPR_FAQ_September2018.pdf">https://cdn2.hubspot.net/hubfs/4723359/FIDO_Alliance_GDPR_FAQ_September2018.pdf</a>
<b>WebAuthn Spec User Presence</b>	<a href="https://www.w3.org/TR/webauthn-2/#sctn-registering-a-new-credential">https://www.w3.org/TR/webauthn-2/#sctn-registering-a-new-credential</a> (step 14) and <a href="https://www.w3.org/TR/webauthn-2/#sctn-verifying-assertion">https://www.w3.org/TR/webauthn-2/#sctn-verifying-assertion</a> (step 16)
<b>Use of signcount</b>	<a href="https://www.w3.org/TR/webauthn-2/#sctn-sign-counter">https://www.w3.org/TR/webauthn-2/#sctn-sign-counter</a>