

به نام خدا



همراه اول

دومین دوره همراه نخبگان همراه اول

درآمدی بر Mobile Connect Technology

سبحان ارشدی

فهرست

3.....	مقدمه
4.....	الگوریتم‌ها و پروتکل‌ها
8.....	چالش‌ها
10.....	اپراتورهای استفاده کننده
12.....	مسیر پیش رو
13.....	منابع

مقدمه

MC به منظور ارائه تجربه کاربری راحتتر و امنتر برای کاربران طراحی شده است. اولین بار GSMA (که یک انجمن راهبردی در زمینه تلفن همراه و تکنولوژی های مربوط به آن است) در سال 2014 با هدف احراز هویت از طریق موبایل در سطح جهانی این تکنولوژی را برای اپراتورهای تلفن همراه پیشنهاد داد. این تکنولوژی سعی دارد از طریق اپراتورها و موبایل هر شخص اعتماد بین DSP و کاربر را افزایش دهد. موارد استفاده Mobile Connect فهرستی از نمونه هایی از نحوه بکارگیری راه حل هویت با سرویس های مختلف است. هر مورد استفاده از یک یا چند محصول Mobile Connect استفاده می کند و بینشی در مورد اینکه چگونه رامحل هویت می تواند به کسبوکارها خدمت کند، ارائه می کند. کاربران می توانند هویت خود را با استفاده از تشخیص چهره بیومتریک و پین احراز هویت کنند.



الگوریتم‌ها و پروتکل‌ها

(Open Authorization) OAuth 1.0

پروتکلی است که به طور گسترده مورد استفاده قرار می‌گیرد که مجوز این را برای دسترسی به منابع محافظت شده از طرف کاربران اجازه می‌دهد. این روشی را برای افراد فراهم می‌کند تا دسترسی محدودی به داده‌های خود را بدون به اشتراک گذاشتن اعتبار حساس خود، مانند رمز عبور، با برنامه‌های شخص ثالث فراهم کنند.

OAuth 1.0 از سه موجودیت اصلی تشکیل شده است: کاربر (*resource owner*)، ارائه دهنده خدمات (*server*)، و مصرف کننده (*client application*). کاربر می‌خواهد به مصرف کننده اجازه دسترسی به منابع خود در ارائه دهنده خدمات را بدون اشتراک‌گذاری مستقیم اعتبار خود بدهد.

برای فعال کردن دسترسی این و کنترل شده به منابع محافظت شده در وب استفاده می‌شود. معمولاً زمانی مطرح می‌شود که کاربر بخواهد به یک برنامه شخص ثالث اجازه دهد تا از سرویس دیگری به داده های خود دسترسی داشته باشد. این می‌تواند شامل سناریوهایی مانند ورود از طریق رسانه های اجتماعی، دسترسی به فضای ذخیره سازی ابری یا تعامل با API ها باشد.

فرآیند مجوز OAuth 1.0 شامل چندین مرحله برای اطمینان از دسترسی این به منابع محافظت شده است:

1. Consumer Requests Authorization
2. User Grants Permission
3. Service Provider Issues Request Token
4. User is Redirected
5. Consumer Exchanges Request Token for Access Token
6. Consumer Accesses Protected Resources

OAuth 2.0

پروتکل استاندارد صنعتی برای مجوز است OAuth 2.0. بر سادگی برنامه نویس مشتری تمرکز دارد و در عین حال جریان های مجوز خاصی را برای برنامه های کاربردی وب، برنامه های دسکتاپ، تلفن های همراه و سمتگاه های انتقال نشیمن ارائه می‌دهد. این مشخصات و پسوندهای آن در گروه کاری IETF OAuth در حال توسعه هستند.

OAuth 2.0 از چهار موجودیت اصلی تشکیل شده است: کاربر (*resource owner*), سرور احراز هویت (*Authorization Server*), ارائه دهنده خدمات (*resource server*), و مصرف کننده (*client*). این‌ها باعث تضمین دسترسی این به منابع محافظت شده بدون افشا اعتبر بلندمدت هویت کاربر می‌شوند.

تفاوت OAuth 1.0 با OAuth 2.0

نتیجه :copilot

Terminology and Roles

در OAuth 2.0، ما چهار نقش داریم: مشتری، سرور مجوز، سرور منبع و مالک منبع.

در OAuth 1.0، شرایط متفاوت است: مصرف کننده (مشتری)، کاربر (مالک منبع) و ارائه دهنده خدمات (سرور منبع).
این به صراحت نقش سرور منبع و سرور مجوز را از هم جدا نمی کند.

Authentication and Signatures

OAuth 2.0 الزامات رمزنگاری را ساده کرد. برخلاف OAuth 1.0، پس از تولید توکن، برای تماس‌های API واقعی نیازی به امضای ندارد.

OAuth 1.0 شامل ارسال دو نشانه امنیتی برای هر تماس API است، در حالی که OAuth 2.0 از یک نشانه امنیتی منفرد استفاده می کند.

Performance and Scalability

اجرای OAuth 2.0 سریعتر و آسانتر از OAuth 1.0 است.

OAuth 1.0 دارای محدودیت هایی در مقیاس پذیری بود، در حالی که OAuth 2.0 به این مسائل می پردازد.

به طور خلاصه، OAuth 2.0 یک پیشرفت قابل توجه نسبت به OAuth 1.0 است که تجربه کاربری بهتر، پیاده سازی ساده تر و مقیاس پذیری پیشرفته را ارائه می دهد.

OAUTH 1	OAUTH 2
Doesn't need HTTPS communication.	Demands HTTPS communication.
Request Digital Signature to sign Oauth request messages.	Doesn't need Digital Signature and relies on SSL/TLS.
Only handle web-browser based implementations.	Consider non-web clients as well.
Less Flexible, more complex to design and develop	Easier for 3rd party developers to implement.
Client app signs all OAuth request to OAuth server with its unique consumer secret.	Client application includes client secret with every request.
More secure because of the Digital Signatures for OAuth communication as well.	Relatively less secure than OAuth 1, they are centered around bearer tokens.

:(OIDC) OpenIDConnect

یک پروتکل احراز هویت قابل همکاری است که بر اساس مشخصات چارچوب OAuth 2.0 است که راه را برای تأیید هویت کاربران بر اساس احراز هویت انجام شده توسط یک سرور مجاز و به دست آوردن اطلاعات نمایه کاربر به رویی قابل اجرا و شبیه به REST ساده می کند.

OpenID Connect به برنامه‌نویسان برنامه‌ها و وبسایت‌ها امکان می‌دهد جریان‌های ورود به سیستم را راهاندازی کنند و اظهارات قابل تأییدی را درباره کاربران در میان کلاینت‌های مبتنی بر وب، تلفن همراه و جلاوا اسکریپت دریافت کنند. و مجموعه مشخصات برای پشتیبانی از طیف وسیعی از ویژگی‌های اختیاری مانند رمزگذاری داده‌های هویت و کشف ارائه‌دهنگان OpenID قابل توسعه است.

برای توسعه‌دهنگان، پاسخی مطمئن و قابل تأیید به این سؤال ارائه می‌کند که «هویت شخصی که در حال حاضر از مرورگر یا برنامه تلفن همراه متصل استفاده می‌کند چیست؟» بهتر از همه، مسئولیت تنظیم، ذخیره و مدیریت رمزهای عبور را که اغلب با نقض اطلاعات مبتنی بر اعتبار مرتبط است، از بین می‌برد.

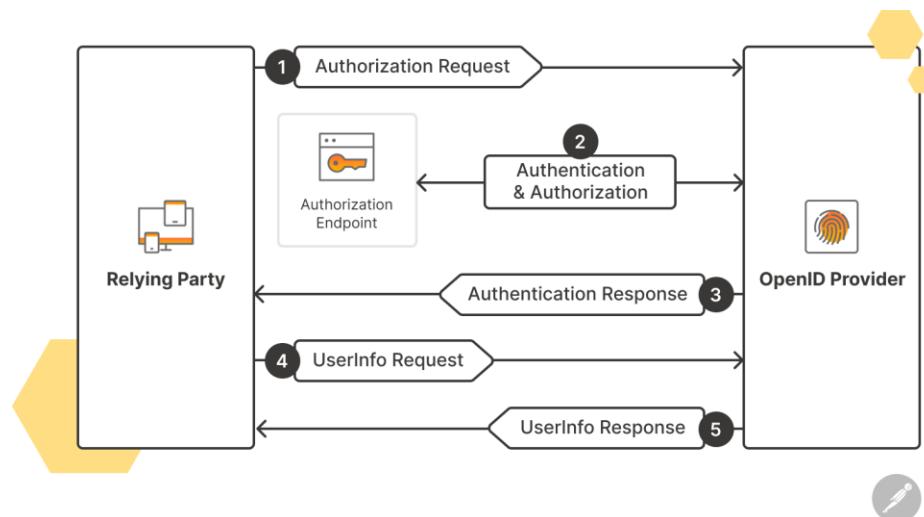
OpenID Connect چندین اصطلاح و مفاهیم کلیدی را معرفی می‌کند که درک آنها ضروری است. این اصطلاحات جدید عبارتند از:

OpenID Provider (OP): سرویسی است که کاربران را احراز هویت می‌کند و اطلاعات هویتی را به طرف‌های متکی (RP) یا برنامه‌های مشتری ارائه می‌دهد.

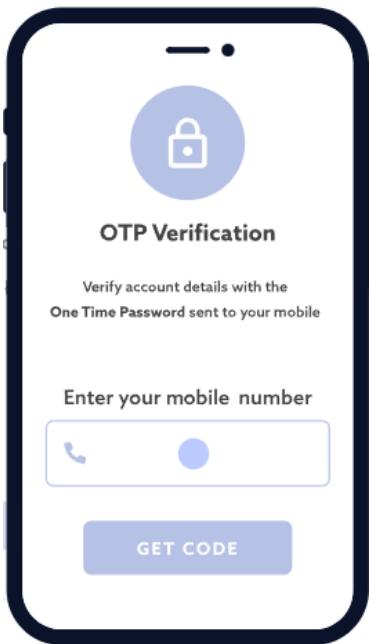
Relying Party (RP): به عنوان یک برنامه مشتری نیز شناخته می‌شود، یک برنامه وب یا تلفن همراه است که برای احراز هویت و اطلاعات هویت کاربر به ارائه دهنده هویت متکی است. RP احراز هویت و اطلاعات کاربر را از OP درخواست می‌کند.

کاربر نهایی: شخصی است که با طرف متکی و تامین کننده هویت تعامل دارد. در OIDC، کاربر نهایی نهادی است که هویت آن احراز هویت می‌شود و اطلاعاتش در حال دسترسی است.

Token ID (JWT): یک توکن وب (JSON) است که پس از احراز هویت موققیت آمیز کاربر توسط ارائه دهنده هویت صادر می‌شود. این شامل اطلاعاتی در مورد کاربر احراز هویت شده، مانند شناسه کاربری و نام آنها است. شناسه توکن اصلی ترین برنامه افزودنی است که OAuth 2.0 به OIDC می‌دهد تا احراز هویت را ممکن کند.



: (Short Message Service One-Time Password) SMS OTP



یک پروتکل امنیتی مهم که برای تأیید هویت کاربر در هنگام ورود به سیستم و تراکنش‌ها استفاده می‌شود. متکی به **رمز عبور یکبار مصرف** است که از طریق متن به تلفن همراه کاربر ارسال می‌شود - این رمز عبور برای تکمیل فرآیندهای ورود یا تراکنش ضروری است - تضمین می‌کند که دسترسی یا مجوز فقط به کاربرانی که دستگاه تلفن همراه ثبت شده دارند اعطا می‌شود.

هنگامی که یک کاربر تلاش می‌کند به یک سرویس امن دسترسی پیدا کند یا یک تراکنش را تکمیل کند، اعتبار ورود خود را وارد می‌کند - بس از ورود موقتیت آمیز به سیستم، سرور احراز هویت یک رمز عبور یک بار مصرف (OTP) تولید می‌کند - دو روش متدال برای تولید OTP :

1- رمز عبور یک بار مصرف مبتنی بر زمان (TOTP) از زمان فعلی به عنوان ورودی برای تولید OTP استفاده می‌کند TOTP ها برای مدت کوتاهی (معمولاً 30 تا 60 ثانیه) معتبر هستند.

2- رمز عبور یک بار مصرف مبتنی بر (HMAC) (HOTP) بر اساس شمارنده ای که با هر نسل OTP جدید افزایش می‌یابد . HOTP ها تا زمان استفاده معتبر باقی می‌مانند. OTP تولید شده به تلفن همراه کاربر پیامک می‌شود (با فرض اینکه شماره تلفن از قبیل ثبت شده و تایید شده باشد) . کاربر OTP را وارد رابط برنامه می‌کند سرور OTP وارد شده را با تولید شده مقایسه می‌کند . اگر مطابقت داشته باشند، احراز هویت ادامه می‌یابد.

چالش‌ها

:Standardization -1

:Consistent Implementation .1

- اطمینان از اجرای یکنواخت در میان اپراتورها و خدمات مختلف تلفن همراه ضروری است.
- GSMA دستورالعمل هایی را ارائه می دهد، اما تغییرات ممکن است به دلیل تفاوت های فنی، شیوه های منطقه ای و الزامات خاص اپراتور رخ دهد.
- دستیابی به یک استاندارد مشترک به حفظ قابلیت همکاری و تجربه کاربری یکپارچه کمک می کند.

:Technical Aspects .2

- Mobile Connect به پروتکل هایی مانند OAuth 2.0 و OpenID Connect متکی است.
- اپراتورها و ارائه دهنگان خدمات باید این استانداردها را برای رفتار ثابت رعایت کنند.
- روش‌های کشف استاندارد به شناسایی اپراتور صحیح برای احراز هویت کمک می‌کنند.

:Regional Differences .3

- مقررات محلی، قوانین حفظ حریم خصوصی و هنجارهای فرهنگی بر اجرا تأثیر می گذارد.
- اپراتورها ممکن است Mobile Connect را برای هماهنگی با نیازهای بازار خود سفارشی کنند.

:User Adoption -2

1. آگاهی و آموزش: بسیاری از کاربران از Mobile Connect به عنوان یک روش احراز هویت بی اطلاع هستند. تشویق پذیرش شامل آموزش کاربران در مورد مزایا، امنیت و سهولت استفاده است. کمپین‌های آگاهی‌بخشی، آموزش‌ها و ارتباطات واضح می‌تواند به پر کردن این شکاف کمک کند.

2. عادت و آشنایی: مردم به ورود نام کاربری و رمز عبور سنتی عادت کرده‌اند. مقاعده کردن کاربران برای تغییر به Mobile Connect مستلزم تأکید بر مزایای آن است. بر جسته کردن جنبه‌های راحتی و امنیتی می‌تواند انگیزه پذیرش را ایجاد کند.

3. اعتماد و اطمینان: ایجاد اعتماد بسیار مهم است. کاربران باید اطمینان داشته باشند که Mobile Connect امن است و به حریم خصوصی آنها احترام می‌گذارد. ارتباط شفاف در مورد حفاظت از داده‌ها و رمزگذاری ضروری است. پذیرش موفقیت آمیز به باور کاربران به قابلیت اطمینان سیستم متکی است.

:Integration -3

1. ادغام پس زمینه: ارائه دهنگان خدمات (مانند بانک ها، پلت فرم های تجارت الکترونیک یا سازمان های دولتی) باید Mobile Connect را در سیستم های موجود خود ادغام کنند. این شامل تطبیق گردش کار احراز هویت برای ترکیب Mobile Connect است - تغییرات Backend ممکن است شامل یکپارچه سازی API های Mobile Connect ، مدیریت جلسات کاربر و مدیریت توکن ها باشد
2. رابط کاربری: طراحی اعلان های کاربر پسند برای Mobile Connect بسیار مهم است - هنگامی که کاربران وارد سیستم می شوند، باید یک پیام واضح و شهودی برای تأیید هویت خود دریافت کنند - رابط کاربری باید به طور یکپارچه آنها را در فرآیند احراز هویت هدایت کند
3. تست و تضمین کیفیت. آزمایش دقیق تضمین می کند که Mobile Connect بدون ایجاد اختلال در خدمات موجود، به خوبی کار می کند - ارائه دهنگان خدمات باید تأیید کنند که Mobile Connect به درستی با برنامه های آنها ادغام می شود - تست سناریوهایی مانند ورود موفقیت آمیز، مدیریت خطاب و مکانیسم های بازگشتی را پوشش می دهد.

اپراتورهای استفاده کننده

GSMA اعلام کرد که از زمان راهاندازی Mobile Connect در کنگره جهانی موبایل (2014) تاکنون 17 اپراتور شبکه تلفن همراه (MNOs) این سرویس را در 13 کشور راهاندازی کرده‌اند و برنامه‌هایی برای راهاندازی‌های اضافی و آزمایش‌های بتا در پی خواهد داشت. سرویس اتصال موبایل GSMA مشتریان را قادر می‌سازد تا هویت جهانی ایجاد و مدیریت کنند که به طور این‌آنها را احراز هویت کند و به آنها امکان دسترسی این‌به خدمات تلفن همراه و دیجیتال مانند تجارت الکترونیک، بانکداری، سلامت و سرگرمی‌های دیجیتال و همچنین دولت الکترونیک را بدهد.

راه اندازی در بنگلادش توسط Robi (بخشی از گروه Axiata) اعلام شده است. در چین با China Mobile و China Unicom. در اندونزی با Indosat (عضو گروه Ooredoo)، XL Axiata و Telkomsel. در مالزی با DiGi (بخشی از گروه Mobitel) و در سریلانکا با Dialog Axiata و Telenor.

استقرار اتصال تلفن همراه در آینده:

GSMA در حال همکاری نزدیک با اپراتورهای جهانی برای پشتیبانی از استقرار بیشتر Mobile Connect است. اپراتورهای متعهد به راه اندازی عبارتند از: Grameenphone (بنگلادش)، Bouygues Telecom and Telenor (پاکستان)؛ Vodafone و Deutsche Telekom (آلمان)؛ Orange (فرانسه)؛ Vodafone و Telefónica (اسپانیا)؛ Swisscom (سوئیس) و Vodafone (بریتانیا). همچنین متعهد به راه اندازی سرویس Mobile Connect در بلژیک، لهستان، رومانی و در سراسر منطقه Orange در خاورمیانه و آفریقا است. Etisalat، Ooredoo، Zain و STC در سراسر آفریقا و در سراسر بازارهای خود راه اندازی کنند. در ایالات متحده، GSMA توسط مؤسسه ملی استانداردها و فناوری (NIST) به عنوان بخشی از ابتکار عمل دولت ایالات متحده، استراتژی ملی برای هویت‌های مورد اعتماد در فضای سایبری (NSTIC) برای تأمین بودجه یک آزمایش آزمایشی اثبات فناوری مفهومی اعطای شده است.

:Orange-Spain



از سال 2023، Orange España دومین ارائه دهنده تلفن همراه در میان چهار ارائه دهنده اسپانیایی که شامل Vodafone، Yoigo و Movistar می‌شود است. آنها تقریباً 11 میلیون مشتری در اسپانیا را ارائه می‌دهند. در حالی که داده‌های مشخصی از تعداد کل مشتریان تلفن همراه Orange در سراسر جهان به آسانی در دسترس نیست، شایان ذکر است که Orange S.A.، شرکت مادر، به میلیون‌ها مشتری در 26 کشور در سطح جهان خدمات ارائه می‌کند.

نکته مثبت این است که زیرساخت شبکه 5G Orange España در حال حاضر به 58.6٪ از جمعیت اسپانیا رسیده است که 840 شهر را پوشش می‌دهد.

Mobile Connect را بیشتر برای دولت ارائه می‌دهد. خدماتی مانند لایکین به پرتاپل دولت و پرداخت مالیات

: Bangladesh-Grameenphone



یک ارائه دهنده خدمات مخابراتی پیشرو در بنگلادش است. از دسامبر 2023، Grameenphone دارای بیش از 82.20 میلیون مشترک در سراسر کشور است. به صورت سرمایه‌گذاری مشترک بین Telenor and Grameen Telecom فعالیت می‌کند. Telenor دارای 55.8% سهم است، در حالی که Grameen Telecom مالک 34.2% است و 10% باقیمانده در اختیار عمومی است. Grameenphone خدمات صوتی، داده و ارزش افزوده را از طریق قرارداد و طرح‌های پیش‌پرداخت به مشتریان ارائه می‌دهد. این بزرگترین اپراتور تلفن همراه در بنگلادش است که بهترین سرویس اینترنت G4 را در سراسر کشور ارائه می‌کند.

GSMA's Mobile Connect را راهاندازی کرده است، یک رامحل جهانی احراز هویت مبتنی بر تلفن همراه. سرویس Mobile Connect این امکان را به کاربر تلفن همراه می‌دهد تا از تلفن و هویت سیم کارت خود برای ورود آنلاین به برنامه‌های شخص ثالث بدون نیاز به ورود به هر کدام با استفاده از احراز هویت جدگانه استفاده کند.

Grameenphone در ابتدا 1000 کاربر را از وب سایت طبقه بندی شده - www.ekhanei.com - برای پروژه آزمایشی انتخاب کرده است و قصد دارد با سایر سایت‌ها، آگهی‌ها و برنامه‌های تجارت الکترونیک پیشرو ارتباط برقرار کند. کاربران می‌توانند با کلیک بر روی نشانواره Mobile Connect و تایپ شماره تلفن همراه (GP) Grameenphone به‌طور این‌از لپتاپ یا دسکتاپ خود به www.ekhanei.com وارد شوند.

مسیر پیش رو

هم اکنون شرکت‌ها در تلاش اند که امنیت این روش و بوزر فریندلی بودن MC را افزایش دهند. سعی دارند که از فناوری‌هایی مثل FIDO2 و WebAuthn برای بهبود امنیت استفاده کنند.

FIDO2 یک استاندارد باز برای احراز هویت کاربر است که هدف آن تقویت روش ورود افراد به خدمات آنلاین برای افزایش اعتماد کلی است. FIDO2 امنیت را تقویت می‌کند و از افراد و سازمان‌ها در برابر جرایم سایبری با استفاده از اعتبار رمزگاری مقاوم در برابر فیشنینگ برای تأیید هویت کاربران محافظت می‌کند.

آخرین استاندارد احراز هویت باز است که توسط FIDO Alliance، یک کنسرسیوم صنعتی از مایکروسافت و سایر سازمان‌های فناوری، تجاری و دولتی توسعه یافته است. این اتحاد استانداردهای احراز هویت FIDO 1.0 را منتشر کرد - که احراز هویت چندعاملی مقاوم در برابر فیشنینگ (MFA) را معرفی کرد.

نحوه ثبت نام برای یک سرویس پشتیبانی شده توسط FIDO2:

مرحله 1: هنگام ثبت نام در یک سرویس، از شما خواسته می‌شود که یک روش تأیید کننده FIDO پشتیبانی شده را انتخاب کنید.

مرحله 2: احراز هویت FIDO را با یک حرکت ساده که احراز هویت کننده از آن پشتیبانی می‌کند، فعال کنید، چه با وارد کردن پین، لمس یک خواننده اثر انگشت، یا قرار دادن کلید امنیتی FIDO2.

مرحله 3: هنگامی که احراز هویت فعال شد، دستگاه شما یک جفت کلید خصوصی و عمومی ایجاد می‌کند که منحصر به دستگاه، حساب و سرویس شما است.

مرحله 4: دستگاه محلی شما کلید خصوصی و هر گونه اطلاعات محروم‌انه مربوط به روش احراز هویت، مانند داده‌های بیومتریک شما را به طور ایمن ذخیره می‌کند. کلید عمومی رمزگذاری شده و همراه با یک شناسه اعتباری که به طور تصادفی تولید می‌شود، در سرویس ثبت شده و در سرور احراز هویت آن ذخیره می‌شود.



منابع

[OAuth 1.0 Explained: Understanding the Key Components for Secure API Access — Part 1 | by Arman Karapetyan | System Weakness](#)

[OAuth 2.0 — OAuth](#)

[What's the difference OAuth 1.0 and OAuth 2.0? | by Himaanshu Shukla | Medium](#)

[What Is OpenID Connect? | Postman Blog](#)

[How OpenID Connect Works - OpenID Foundation](#)

[What Is SMS OTP? Benefits, Implementation and Use Cases \(textmagic.com\)](#)

[GSMA | Mobile Connect Factsheet - Mobile Identity](#)

[GSMA | GSMA MOBILE CONNECT LAUNCHED BY 17 MOBILE OPERATORS IN 13 COUNTRIES - Newsroom](#)

[Orange mobile customers Europe 2017-2023 | Statista](#)

[Orange España - Wikipedia](#)

[Grameenphone - Wikipedia](#)

[Grameenphone Launches GSMA's Mobile Connect Service Pilot in Bangladesh \(thefastmode.com\)](#)

[What Is FIDO2? | Microsoft Security](#)

[FIDO and Mobile Connect - FIDO Alliance](#)

[How SecureAuth FIDO2 WebAuthn works](#)