Frequently asked questions

QUALIFIED WEBSITE AUTHENTICATION CERTIFICATE (QWAC)

Q Which is the right authenticator?

A Depends on the type of banking customer.

Corporate & high-value banking customers:

Consider the Challenge-Response or Camera Token, or our Mobile Smart Credential.

- CR / Camera token: provides independence of elements, something you have (the token) and something you know (the token PIN).
- Mobile Smart Credential: mobile app protected with RASP, something you have (mobile device), something you know (PIN) / something you are (biometric). This also has the advantage of being a digital certificate.

Normal consumer with mobile app:

Our Mobile Soft Token is ideal for most types of online transactions. It provides a very secure onboarding process that can leverage our Device Reputation service. It can also be transparently embedded into your own mobile application, or exist as a standalone identity application leveraged by your banking app. It provides independence of elements when provided as a separate app. It is something you have (mobile device), something you know (PIN) / something you are (biometric).

RASP can be used to protect your mobile app.

Consumer not comfortable with apps:

Dynamically linked SMS OTP may be the right choice. They do not require an app, and function quite well for customers who interact mostly with browser-based transactions. There is an associated cost to sending SMS messages which you may want to consider.

Q Should I use Dynamically Linked SMS OTPS or should I avoid them?

A Can be ideal for certain circumstances.

Several security organizations have recommended against SMS for messaging because of known attacks against the underlying SS7 protocol, and SIM swapping.

The SS7 protocol attacks are sophisticated and difficult to implement, and SIM swapping is costly, so SMS remains a good choice for moderate value transactions.

SMS is also ideal for web-based transactions because no app has to be started, and typically you can display everything the consumer needs from the lock-screen of a mobile device.

Q Do I have to apply SCA to all transactions?

A No, there are instances where SCA is except.

You are exempted from performing SCA / dynamic linking on transactions <= €30 if the cumulative amounts of all transactions since the last SCA do not exceed €100, or fewer than 6 transactions have been performed.

Examples:

- The payer performs 5 €10 transactions with no SCA required. On the 6th €10 transaction, SCA must be applied.
- The payer performs 3 €30 transactions. On the 4th transaction they perform a €15 transaction, SCA must be applied.

Q Can you help identify when an exemption applies?

A Yes.

Our Device Reputation service can help out by keeping track of the number of transactions performed, and by keeping track of the value of past transactions performed.

Even when exemptions apply, we strongly recommend continuing to monitor the risk of each transaction.

Frequently asked questions

QUALIFIED WEBSITE AUTHENTICATION CERTIFICATE (QWAC)

Q When do I need a PSD2 QWAC certificate?

A Read on.

PSD2 QWACs will be required to secure the open APIs used in the open banking framework as specified in the PSD2 requirements. PSD2 certificates provide encryption, security and authentication for the following payment service provider roles:

- ASPSP (Accounts-servicing Payments Service Provider), traditional banks
- AISP (Account Information Service Provider), account aggregator to manage financial services
- PISP (Payment Initiation Service Provider), enables users to make payments directly from their bank
- Issuer of card-based payments instruments

Q How do I apply for a PSD2 QWAC certificate?

A Read on.

Before applying for a PSD2 QWAC certificate a third party must first register as a payment service provider with its National Competent Authority (NCA) and specify its applicable roles. After the third party receives its NCA license, Entrust can complete verification (including all verification required for Extended Validation or EV certificates) and issue the third party with a PSD2 QWAC certificate.

Q Can you tell me the verification requirements for a PSD2 QWAC certificate?

A Read on.

In addition to the extended validation certificate requirements (i.e., name of certificate owner, domain verification, organization identity, legal identity of organization controlling the website, and validity period), PSD2 certificates require the applicant to provide the following information:

1. Authorization Number of the TPP (third-party payment provider), which can be found in the public registers of the national competent authorities.
2. The role(s) of the TPP, which may be one or more of the following:
   - ASPSP
   - PSIP
   - AISP
   - Issuing of card-based payment instruments
3. Name of the competent authorities where the TPP is registered
4. Name of Qualified Trust Service Provider (QTSP)

Q Who can issue PSD2 QWAC certificates?

A Read on.

PSD2 QWAC certificates can only be issued by a Qualified Trust Service Provider (QTSP).

Q When will Entrust start issuing PSD2 QWACs?

A Read on.

We plan to begin issuing QWACs to our customers worldwide once the requirements for EV certificates are revised by the CA/B Forum to support the existing requirements for PSD2 QWACs.

Q Is Entrust recognized as a QTSP?

A Read on.

We are completing the process for designation as a QTSP under eIDAS and ETSI audit requirements. Once that's achieved, we will be able to issue QWAC and PSD2 certificates that validate the business identity and authorized roles of Payment Services Providers (e.g., Financial Service and FinTech firms) that are involved in banking and financial transactions in the EU.

Frequently asked questions

QUALIFIED WEBSITE AUTHENTICATION CERTIFICATE (QWAC)

Q What do I get with my PSD2 QWAC certificate?

A Read on.

Our PSD2 QWAC certificates are X.509 compliant and support the PSD2 standard as defined by eIDAS. It includes verification for 1 Domain, and can support up to 250 additional Subject Alternative Names (SANs) for an extra fee.

Q How long is a PSD2 QWAC certificate valid for?

A Read on.

The maximum validity period for a PSD2 QWAC certificate is 24-months.

Q What encryption method is used to support PSD2 QWAC certificates?

A Read on.

RSA encryption will be used to support PSD2 QWAC certificates.

Q What is the minimum key size supported for a PSD2 QWAC certificate?

A Read on.

A minimum key size of 2048 bits will be supported for a PSD2 QWAC certificate.

Q What can a third-party provider do with a PSD2 certificate?

A Read on.

A third-party provider that wants to access customer bank accounts within the EU or their associated data needs to obtain a license and unique PSD identifier from its National Competent Authority (NCA) in the EU member state with regulatory authority over the third-party provider. There are different types of licenses that each determine the data access rights or "roles" of the third-party provider in accordance with their business model.

Q What are the technical requirements for third-party providers and banks?

A Read on.

A third-party provider that wants to gain access to bank accounts, and a bank that is providing third-parties with access to customer account data, must each identify themselves with one or more PSD2 QWAC certificates.

Q What are the requirements for banks?

A Read on.

Banks must also make an API available to third-party Providers that enables access to customer bank accounts or account information. A bank's identity will be confirmed through its own Qualified Website Certificate.

Frequently asked questions

MOBILE APPLICATIONS

Q **Is it easy to integrate your mobile SDKs?**

A Yes, very easy.

We provide sample applications and development guides to ease the process. Both the Mobile Soft Token and Smart Credential SDKs are about the same complexity for integration.

Q **Can I use Xmarin or ReactNative when developing my apps?**

A Yes.

Our mobile SDKs are developed in native code for iOS and Android. There is no restriction on cross-platform development tools.

Q **How secure is your mobile push app?**

A Very Secure.

When our authentication server sends a push notification, it does not contain detailed information about the transaction. The app must make a signed request to the authentication server using a valid Soft Token or Smart Credential before the server will release the transaction details. All communications take place over TLS.

Q **Can my customers have more than one mobile device?**

A Yes.

Each mobile device can register a unique Soft Token or Smart Credential, and all registered devices will receive the push notification. The first one to sign /approve the transaction is the signing device.

Q **Can you tell me about your device reputation and facial recognition SDKs?**

A Of course, read on.

Those two SDKs are optional, and we provide hooks, as required, in our mobile SDKs to support the integration of both into the normal app workflow where appropriate.

Q **Is the shared secret in your mobile soft token securely generated?**

A Yes.

All communication between the MST SDK and our activation server must take place over TLS – the server is not configured for run over unsecured HTTP.

Also, the symmetric key at the heart of the token is created with entropy from both the server and the mobile app. The secret (and other sensitive SDK data) are encrypted in the mobile app space.

Q **Why would I choose Mobile Smart Credential over a Soft Token?**

A Read on.

The soft token relies on a symmetric key, whereas the smart credential relies on asymmetric keys. While very unlikely, a breach of the server cannot affect the smart credential identities because the private key never leaves the mobile device. As well, smart credentials are certificate based and therefore enjoy a higher degree of legality based on their ability to generate true digital signatures.

The mobile smart credential can provide a better UX by providing anonymous login, which eliminates the need for username and password. It also enables new services like digital signing for loans and credit card products.

Frequently asked questions

MOBILE APPLICATIONS

Q Do you support biometrics in your mobile apps?

A Yes.

Our commercial mobile applications support native fingerprint and facial recognition. We also provide a mobile facial recognition SDK for devices “that do not support a native facial biometric.

Our mobile facial recognition SDK can be combined with our Mobile Soft Token and Mobile Smart Credential SDKs in your own app.

Q Can you tell me how biometric data is stored.

A Yes.

All biometric data is stored locally in the app. Native device biometric data is protected by the OS. Our SDK generates a facial template based on scanning different angles of the face during registration. After that the template data is encrypted and stored in the app storage.

Facial data from our SDK is never uploaded from the device, and is therefore GDPR compliant. The end-user can delete it at any time.

Q Do you support iris scan or voice?

A Depends, our SDKs do not limit any restrictions.

Most PSD2 customers will be developing their own apps and leveraging our SDKs – including the facial recognition SDK. Our SDKs do not impose any restrictions on the types of biometric authenticators you want to support.

As well, because GDPR imposes such high barriers to storing biometric data off-device, no server-side work is required to integrate your preferred biometric option if data is stored device-local.

MOBILE RASP

Q Am I required to protect my apps with RASP?

A No.

The short answer is “no”. The RTS section which is typically used to justify RASP is under Article 9, Independence of Elements in the RTS.

It must be noted that current mobile OSs cannot provide complete assurance that a rogue mobile application is not masquerading as a legitimate one.

RASP provides the tools to ensure that it is extremely difficult for reverse engineering to happen.

Q Should I bother using RASP?

A Absolutely.

RASP does more than just protect your application from being compromised. It also provides protections against debuggers, emulators, and rooted mobile devices from being used. It can also provide components like secure keyboards to protect against key-loggers masquerading as value added 3rd party keyboards.

Q Is RASP easy to adopt?

A Yes.

It is usually run on the app after it has been built, but before being signed, meaning no work for your developers to integrate any SDKs.

Frequently asked questions

TRANSACTION RISK ANALYSIS

Q **What type of risks should we consider for TRA?**

A **Read on.**

Some examples include:
– Any kind of fraud or attacks related to the user's device.
– Unusual device inputs such as fingerprint or geolocation.
– Unusual transaction details such as large money transfers

Q **Can your solutions help address TRA?**

A **Yes.**

Our authentication solutions (whether on-premise or cloud) – in conjunction with device reputation – helps prevent fraud without adding friction to the end user. We have a sophisticated risk analytics engine that can inject contextual (risk) information from 3rd parties and output data via CSV to SIEM systems. Plus, device reputation provides a deep inspection of device information, incorporating financial transaction details,a database of over 3B devices, and web relations with billions of accounts. This allows our customers to learn about potential device threats much sooner than systems that don't connect multiple sources.

Q **What is Device Reputation?**

A **Read on.**

Device Reputation is about the interconnects between devices, the accounts they access, and the transactions they attempt.

It all starts with detailed information being collected about a device. This information is checked inside a cloud database to try and identify the device. Once that is done, an analysis is run to see if the device can be trusted. The trust analysis is based on a simple but powerful rules engine.

Q **Can you describe how Device Reputation works?**

A **Read on.**

The cloud service maintains a database of devices, accounts, and transactions. Devices are related to accounts through transactions. As devices perform transactions against accounts, a rules engine compares the device information against a known database of devices looking for bad behavior, or relationships to other devices with bad behavior. This impacts the trust in the device.

Q **How does device reputation uniquely identity a device?**

A **Read on.**

The Device Reputation looks at several dozens of device characteristics for web browsers, iOS and Android apps. It then uses this information to try an identify matching devices in its database. More importantly, Device Reputation is about identifying risk rather than just devices.

Q **Who do you partner with to provide Device Reputation?**

A **iovation.**

The partnership combines Entrust's adaptive authentication solution with iovation's device- and risk-based authentication services which tap into a knowledge base of more than 3.5 billion devices. The packaged solution allows organizations to provide users with a transparent, secure experience that enables step-up authentication when a user's registered device is identified as a risk, thereby providing a deeply intelligent, frictionless approach to authentication and fraud prevention.

Integrations exist for web browser (Javascript), iOS and Android.

Frequently asked questions

ENTRUST

TRANSACTION RISK ANALYSIS

Q Is it easy to integrate Device Reputation into my transaction workflow?

A Yes.

We have integrated the features of Device Reputation into our Entrust Identity Fingerprint SDK for browser, iOS, and Android.

Q What about integrating Device Reputation into my mobile workflow?

A Read on.

Our Mobile Soft Token SDK has callbacks for collecting Device Reputation during the creation of the soft token, as well as during the loading of transactions. The Entrust Identity server can be configured to enforce Device Reputation checks before it will allow the mobile device to create the soft token, or to receive a transaction for approval.

Authenticator Options Review

MOBILE SMART CREDENTIAL

- Support PKI signing
- Private key on mobile device
- Dynamic linking through PKI signature

CHALLENGE RESPONSE (CR) TOKENS AND CAMERA TOKEN

- Symmetric shared secret
- Token has a numeric key-pad
- Sign a transaction
- Dynamic linking through hash with shared secret

MOBILE SOFT TOKEN

- Supports OATH OCRA
- Symmetric shared secret
- Dynamic linking through OCRA hash with shared secret

SMS OTP – DYNAMICALLY LINKED

- Symmetric shared secret
- Token has a numeric key-pad
- Sign a transaction
- Dynamic linking through hash with shared secret

Learn more at **entrust.com**

ENTRUST

U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223
info@entrust.com