PRODUCT SUPPORT

Entrust Identity Mobile App Privacy Statement

Last Updated 21 October, 2024

Why we have created this Privacy Statement

Entrust Corporation ("**Entrust**") has created this privacy statement to provide an overview of how the Entrust Identity Mobile Application ("**App**") processes personal data relating to someone who uses the App (a "**User**"). However, please note that Entrust is not the controller of personal data collected and processed by the App; Entrust merely acts as processor and service provider on behalf of a Customer, as defined below.

Entrust Customers

Entrust provides its customers with Identity and Access Management ("**IAM**") services that enable customers to authenticate a person (e.g. a member of their workforce, a consumer) before they are permitted to do things like log-in to the customer's website, access their VPN, or complete a financial transaction. The IAM services allow a customer to authenticate a person in a variety of ways - for example, by using a soft token, smart credential, one-time passcode, etc. And a customer may decide to allow a person to authenticate themselves via the App. **It is this Entrust customer (the "Customer") who will be the controller of any personal data that is processed by the App.** Users should contact the Customer directly for full details of how the App processes their personal data.

Personal Data Collection and Processing

Depending on how the Customer has chosen to configure their use of Entrust's IAM services, the App may process the following personal data relating to a User.

Personal Data	**Purpose of Processing**
Creating and Activating Identities in the App To use the App to authenticate themselves, a User must first create and activate an "**Identity**" (e.g. a soft token, smart credential, passcode identity, etc.) within the App. The Customer will provide the User with instructions on how to do this, and the creation and activation may involve processing the following personal data.	
Identity Name and Unique Identifier	Each time a User creates and activates a new Identity, they can choose to give it a name (which they may later edit) and Entrust will also generate a Unique Identifier (e.g. a serial number) for that Identity which is visible to the User within the App. Entrust uses this Unique Identifier to prevent the creation of duplicate Identities and to enable the App to communicate with the IAM service(s).
Mobile Phone Number	To register and activate certain types of Identity (e.g. a passcode identity), a User will need to input their mobile phone number into the App. A one-time passcode is sent via SMS to the mobile number (the Customer determines the content of the SMS), which the User must then input into the App to register and activate the Identity.
Data processed for Onfido's Identity Services	If the Customer has a contract with Onfido (another company within the Entrust group), the Customer may use the App to collect and store the personal data that is required for the Customer to use Onfido's Identity Services. For more information, see the section below headed "Onfido as Customer processor."
Pin Number and Auto-Lock Settings	When the User registers and activates an Identity within the App, the Customer may give the User the option (or require them) to set a pin number to protect that Identity. If a pin number is created, the User will need to enter it in the App in order to "unlock" that Identity before it can be used for authentication. Once the Identity is unlocked, it will remain unlocked for so long as the App remains open, subject to a maximum "auto-lock timeout" period. The User can set and modify an auto-lock timeout period of between 1 and 5 minutes within their App settings.

On-device biometrics	When the User registers and activates certain types of Identity within the App, the Customer may give the User the option to protect it using on-device biometrics (i.e. by configuring the App to require the User's on device biometrics, such as their Touch ID, to unlock the Identity). The App does not gain any access to the User's biometric data - the biometric data remains on the User's device - the App is simply notified if the use of on-device biometrics is successful. The User can switch-off the use of on-device biometric at any time within their App settings.
Device Information	The App will access limited information about the device on which the User has installed the App (e.g. device type and operating system version) and use this to troubleshoot issues and confirm whether the device is compliant with FIPS 140-2 (since the Customer may configure their IAM services to only permit authentication via a FIPS compliant device).
Device Permission Settings	Notifications: The User controls - using the settings on the device on which they have installed the App - whether the App is able to send the User push notifications. Camera access: The User controls - using the settings on the device on which they have installed the App - whether the App is able to access their device camera so that, for example, the User can scan a QR code (something which may be necessary to create and activate a new Identity), enable on-device biometrics (see above), or take and share a photo with the App (something which may be necessary depending on how the Customer has chosen to configure their Entrust IAM services and Onfido services). Bluetooth access: The User controls – using the settings on the device on which they have installed the App - whether the App is able to use that device's Bluetooth to communicate with another device.
Authenticating via the App Once the User has created and activated an Identity, they may use the Identity to authenticate themselves. The Customer decides which events require a User to authenticate themselves (e.g. the Customer may require the User to authenticate themselves when they try to log-in to the Customer's website, complete a financial transaction etc.). The Customer then configures their IAM service to send an "**Authentication Request**" to the App each time a User tries to complete such an event. To complete the authentication, the User will need to open the App and approve/confirm the Authentication Request and this may involve processing the following personal data.	
Push Notifications	If the User has enabled push notifications on their device, they will receive a push notification from the App each time they receive an Authentication Request.
Actions	The Actions section of the App shows the User a list of all outstanding Authentication Requests.

Authentication Request Information	Each Authentication Request presented to the User will contain certain information regarding the request (so the User knows the origin of the request and can confirm its authenticity). The Customer decides what information is shared, but the list may include: • User ID (this is a User ID created by the Customer for each individual User); • The date and time the request was submitted; • The status of the request (e.g. pending); • The application from which the request was made; • The name of the browser from which the request was made (e.g. Firefox); • The IP address from which the request was made; • The state, city or country level location from which the request was made (including a map depicting the same) based on IP address; and • The operating system of the device from which the request was made.
Data processed for Onfido's Identity Services	If the Customer has a contract with Onfido (another company within the Entrust group), the Customer may use the App to collect and store the personal data that is required for the Customer to use Onfido's Identity Services. For more information, see the section below headed "Onfido as Customer processor."
Action History	When the User opens each Identity within the App, they will be able to view the history of the previous 100 Authentication Requests made in respect of that Identity. For each request, the User will be able to see the Authentication Request Information described above plus details of whether the User approved/confirmed the Authentication Request.

Data Retention

Neither Entrust nor the Customer can remotely delete data from the App – the User is the only person able to control this. At any time, a User may delete the App entirely (in which case all of the information stored within the App will be promptly deleted) or delete a specific Identity from the App (in which case all of the information stored within the App in respect of that Identity is promptly deleted).

Data Privacy Rights

If you are a User seeking to exercise your data privacy rights in respect of the personal data that is collected and processed by the App, you should contact the Customer (who, as explained above, is the controller for all personal data collected and processed by the App). Entrust, as the processor/service provider, will assist the Customer, to the extent reasonable and practicable, in responding to data subject requests from Users that relate to the processing of personal data collected and processed by the App. Please note, however,

Data Protection Measures

Entrust, as the processor/service provider, will process the personal data described in the table above on behalf of the Customer and in accordance with the Customer's instructions as set out in the Data Processing Addendum ("**DPA**") found at https://www.entrust.com/-/media/documentation/licensingandagreements/dpa---entrust-acting-as-processor.pdf.

Onfido as Customer Processor

As explained above, a Customer will invite a User to download and use the App in connection with the Customer's use of Entrust's IAM services. If the Customer is also a customer of Onfido (another company in the Entrust group), the Customer may also use the App to collect and store the personal data that is required for the Customer to use Onfido's Identity Services.

The Customer continues to be the controller of this personal data and it is Onfido – and not Entrust – that is the processor and service provider. A User should contact the Customer for specific information about the processing of personal data for the purposes of Onfido's Identity Services (since it is for the Customer to choose how to use and configure Onfido's Identity Services). However, by way of example the Customer may configure the App to: (i) collect an image or video of the User and/or their government issued identity document; and (ii) store a token that contains an encrypted face embedding. More information about how Onfido may process personal data (as processor and service provider) on behalf of its customers is available here.

Contact Information

For questions about this privacy statement, please contact privacy@entrust.com. For Entrust Corporation's general privacy statement, please see here https://www.entrust.com/legal-compliance/data-privacy/privacy-statement.