Instant ID as a Service (IIDaaS) Mobile Flash Pass

Driving the convergence of digital and physical credentials

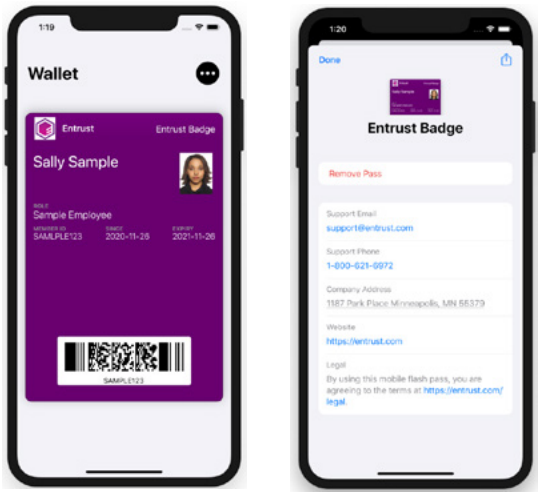
With the widespread adoption of smartphones, smart watches, and other mobile devices, organizations around the globe are now offering digital credentials to complement their physical credentials. This provides a convenient, secure way to issue dynamically provisioned credentials to employees, students, visitors, and vendors.

Entrust Instant ID as a Service (IIDaaS™) is enabling this convergence of digital and physical credentials through support of the mobile flash pass. This enables you to issue digital badges to your end-users that include biographic data as well as a photograph and/or bar code.

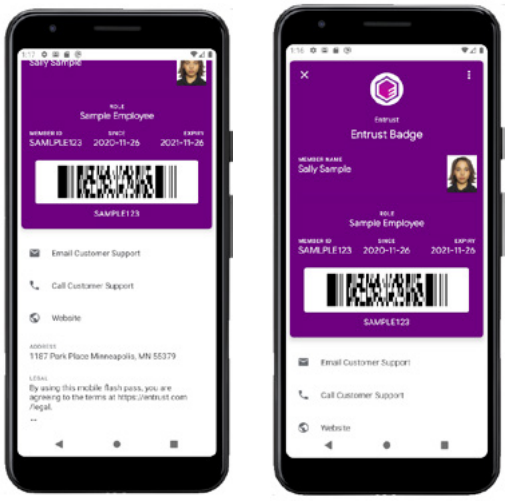
COMPATIBLE WITH APPLE AND ANDROID

Mobile flash pass credentials can be saved to either an Apple Wallet or Google Pay application as a “Pass,” or “Membership Card” resource.

IIDaaS Mobile Flash Pass



Mobile flash pass in Apple Wallet



Mobile flash pass in Google Pay

Mobile flash pass designs

Mobile flash passes issued through IIDaaS allow customization of various fields and branding. You can even have multiple mobile flash pass designs for different applications.

With IIDaaS, the enrollment captures all the required information and then is transformed into a printed card and/or a mobile flash pass. This process allows you to link the physical credential design to the mobile flash pass design and map the fields to populate data into the mobile flash pass. You can specify the background color and add a corporate logo on top of the mobile flash pass.

The mobile flash pass has the following user fields:

- User Full Name
- User Role
- Since Date
- User Number (or ID)
- User Photo
- Expiry Date
- Bar code Value (likely the User Number)
  - Bar code type options: QRCODE, PDF417, CODE128, or NONE

The mobile flash pass also includes additional company information. With the exception of the company name, this information is on the back of an Apple Wallet Pass or at the bottom of a Google Wallet Pass:

Required fields

- Company Name
- Company Address
- Company Support Email

Optional fields

- Company Support Phone
- Company Website
- Legal Information

IIDaaS Mobile Flash Pass

Issuing a mobile flash pass

1. The issuing organization must first register for Apple Developer accounts and Google Merchant accounts in order to generate credentials that allow the cloud solution to seamlessly issue mobile flash passes.

2. End-user within the organization enrolls with the administrator (just as they would with a physical ID badge).

3. The administrator sends the mobile flash pass claim link to end-user via email. Administrator can specify a deadline for the claim token link, after which time the end-user will no longer be able to claim the mobile flash pass.

4. End-user claims their mobile flash pass token for Apple Wallet and/or Google Pay using the links in the email.

Sending a mobile flash pass

The issuer administrator uses the enrollment form to enter the email address where the mobile flash pass will be delivered. It will show the following details about the claim status of the mobile flash pass.

- **Claim token expiry:** The date the claim token will expire. If this date passes without the end-user claiming the mobile flash pass, a new email with a new claim token will need to be sent.
- **Claim date:** The date when the mobile flash pass was claimed by the user.
- **Claim status:**
  - **<Blank> or UNCLAIMED:** The user hasn't been sent a mobile flash pass email.
  - **SENT:** The user has been sent a mobile flash pass email but hasn't yet claimed it.
  - **CLAIMED:** The user has clicked the link in the email to claim the mobile flash pass.

IIDaaS Mobile Flash Pass

Mobile flash pass vs. mobile credential

A mobile flash pass issued through Entrust IIDaaS is a "static digital ID." It includes the end-user data (name, ID, role, date) and photo in the digital credential. This credential data is stored in the secure element of the mobile device. Consequently, the mobile flash pass is ideal for visual verification of the user and for applications where scanning of the QR code or bar code are required.

Today, the mobile flash pass has fewer capabilities than a smart mobile credential. A mobile flash pass issued through IIDaaS does not access the wireless radio Bluetooth low energy (BLE), Near Field Communication (NFC), or 802.11x (WiFi) of the mobile device.

	Mobile Flash Pass	Mobile Credential
Visual Identification	X	X
IOS and Android	X	X
Mobile and Watch	X	X
Bar Code/QR Code Scanning and Swiping	X	
Smart Card Capabilities		X
NFC Technology		X
Access Control		X
POS Terminals		X

ENTRUST

ELLIOTT DATA SYSTEMS, INC.
www.elliottdata.com

Local Identification, Secure Access & Accountability Solutions Provider

St. Louis, MO | Memphis, TN
1-888-345-8511