IBM® **Digital Health Pass**

Administration Guide

Managing verifiers and credential verification

Version 2

Contents

Introduction 1

About this document 1
About Digital Health Pass applications 2
Process overview 2
Introduction to administration 3
Terms and concepts 4
About the administrative console 7
About Basic customers and Enterprise customers 7
About credential verification 8
About supported healthcare QR codes 9
Roles and responsibilities 10

Getting started 11

Automatic organization, verifier setup 11
What you need 11
Using your welcome email 12
Tips for administration 12
Logging in to the console 13

Customer Administrators 14

Adding an organization 14
Adding an Organization Administrator 15
Reviewing Organization Administrators 15
About verification rules for verifier credentials 15
About credential types, processing 16
About rule sets 17
Viewing verifier configurations 20
Adding a verifier configuration to your catalog 20
Testing and production 21
Reviewing verifier metrics 22

Organization Administrators 23

Adding a verifier credential 23
Reviewing, sharing verifier credentials 24

Revoking a verifier credential 24

Verifiers **25**

How it works 25
Getting authenticated for verification 26
Scanning 26

Troubleshooting and support **28**

Copyright information **29**

Index **32**

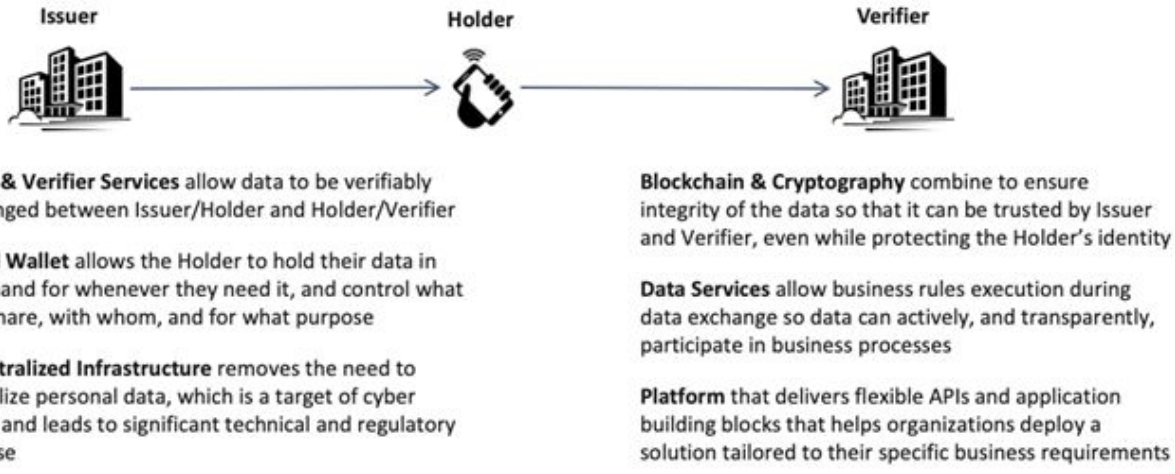
Introduction

Welcome to IBM® Digital Health Pass

IBM Digital Health Pass is a collection of services, mobile applications, and administrative portals that allows organizations to exchange data with individuals through a trusted, secure, and privacy-protecting credential exchange process.

Digital Health Pass is built on IBM decentralized ledger tech to empower an eco-system of credential issuers and verifiers, running on the IBM® Cloud.

Figure: IBM Digital Health Pass concepts



About this document

This document describes the credential verification workflow which is just one of the possible workflows supported by IBM Digital Health Pass.

How the information here is organized

- Overview of administration
- Getting ready for administration, including information that you need to get started
- Procedures in sections by role. For example, for Customer Administrator tasks, see the Customer Administrators topics.

About Digital Health Pass applications

When you as an IBM customer deploy Digital Health Pass, the solution includes these mobile apps. These are available for download from standard app stores, for example, the Apple App Store ↗:

IBM Digital Health Pass Wallet mobile app (iOS and Android versions)

Holders use this app to store and share digital credentials, that is, health cards and passes.

IBM Digital Health Pass Verify mobile app (iOS version only)

Verifiers use this app to scan and check holders' credentials.

IBM Digital Health Pass Administration console

Digital Health Pass customer administrators are specially-designated users that are entrusted to set up and manage organizations, verifiers, and credentials for your company. Administrators use the console to issue credentials that enable the Verifier mobile app to do verification scans of holder credentials.

Process overview

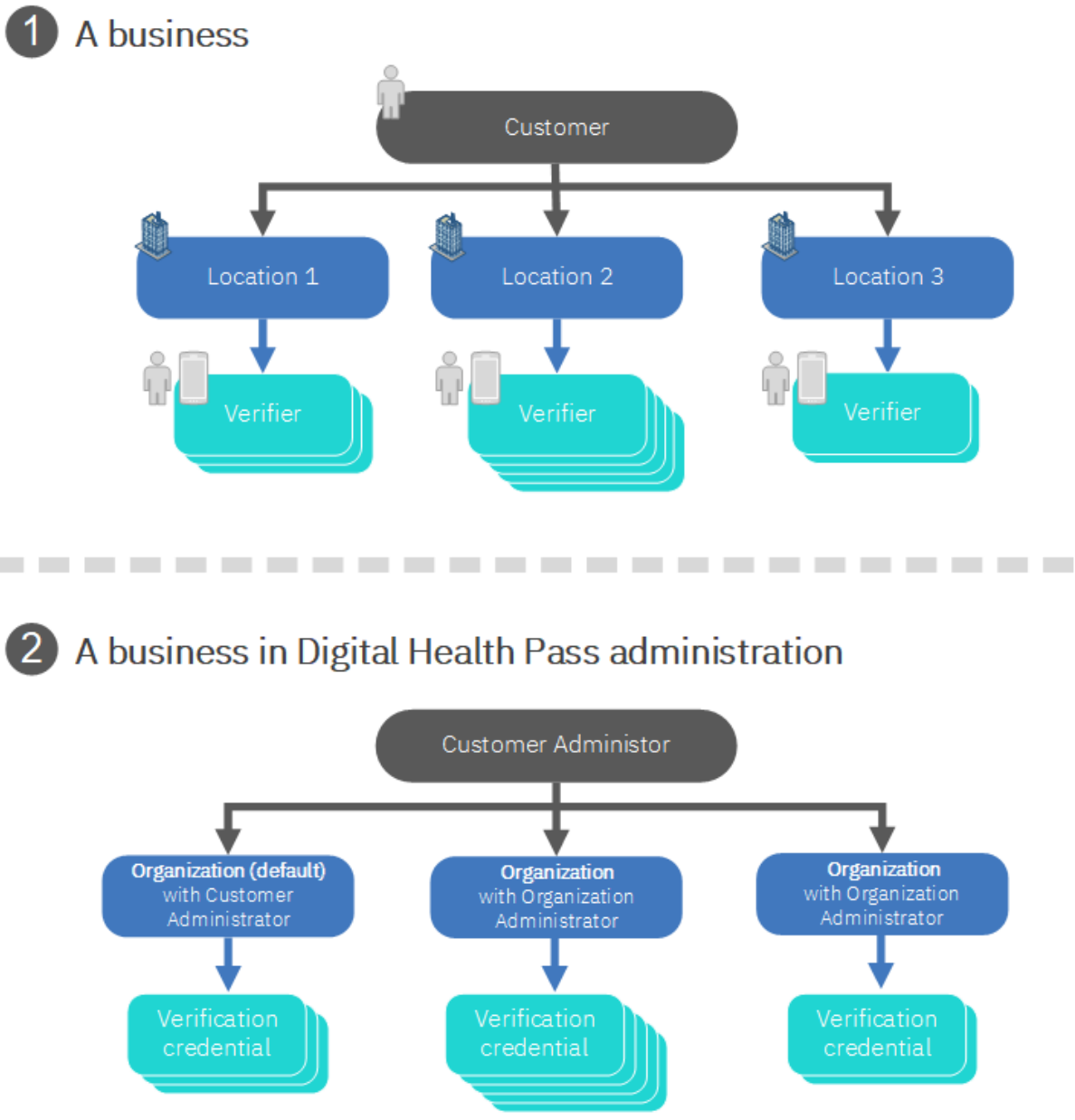
Here's a summary of customer steps in Digital Health Pass onboarding:

1. The Customer Administrator receives a "welcome" email from IBM with information for accessing administration.
2. The Customer Administrator uses the Digital Health Pass administrative console to set up organizations as needed, to add and manage verifiers.
3. The Customer Administrator can manage organizations (initially, only the default organization), create new organizations, and manage verifier credentials for each organization.
4. Verifiers are authenticated per verification session, then use the IBM Digital Health Pass Verify mobile app to scan holder health passes or cards, and determine their validity.

Introduction to administration

This document describes administrative procedures for creating and managing organizations within your company, and creating verifier credentials associated with those organizations.

Figure: Example of organizations and verifiers onsite and in IBM Digital Health Pass



Administrative types and procedures

Digital Health Pass differentiates administrative responsibilities by administrator type. As you use the procedures in this document, it's important that you log in to the Digital Health Pass administrative console using the appropriate administrative credentials. For information about administrator types, see Roles and responsibilities.

Terms and concepts

credentials

In Digital Health Pass Administration, verifiable **credentials** include **health passes** and **cards**. These are electronic documents that prove that a holder has had a test or a vaccination. Credentials include quick response (QR) codes and related information for verification.

Tip: Use the terms **credential**, **pass**, and **card** carefully since they refer to different items. These are not different terms for the same thing.

DCC

Digital COVID Certificate (European Union credentials). For information about supported credential types, see About supported healthcare QR codes.

digital wallets

A mobile app, such as IBM Digital Health Pass Wallet, that offers a secured digital alternative to paper health credentials, for example, vaccination cards or test results for COVID-19. It provides a convenient, voluntary option for individuals to share that they've been vaccinated or tested negative as needed.

Note: Digital wallets may also be referred to as *digital passports*, *digital health passports*, or *vaccine passports*.

GHP

Good Health Pass. For information about supported credential types, see About supported healthcare QR codes.

health pass

A verifiable credential, an electronic document, that displays your health status. Also see *credentials*.

holders

These are end users that present holder credentials, cards, and passes for verification, using the Digital Health Pass Wallet app.

issuers

These issue lab results, vaccination records as digital credentials sent to holders' digital wallets. A testing lab is one example of an issuer.

organizations

Organizations represent subsets within your company, for example, a specific location, region, division or some other classification. By default, your company has a default organization created in Digital Health Pass. As an administrator, you can create more organizations or delete existing organizations.

rule sets

In Digital Health Pass, rule sets control how credentials are processed and assessed. Rule sets processing executes and evaluates multiple rules together against individual credentials. Also see *verifier configurations*.

SHC

Vaccination Credential Initiative SMART Health Cards. For information about supported credential types, see About supported healthcare QR codes.

VC

In IBM Digital Health Pass credential verification, the VC abbreviation identifies the verifiable credential type. Compare this to established credential standards, for example, SMART Health Cards (VCI) and Digital COVID Certificate (European Union).

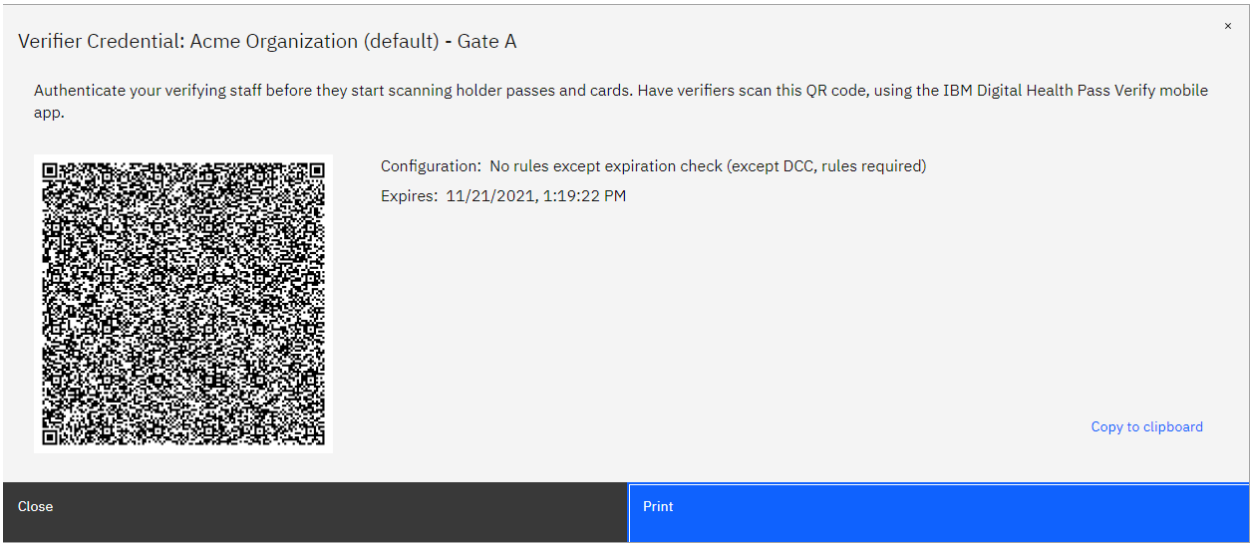
verifier configurations

These configurations determine how to verify holder credentials, using rule sets. You can use Digital Health Pass administration to manage a catalog of verifier configurations. Also see *rule sets*.

verifier credentials

Verifier credentials are a specific type of credential. A verifier credential (figure) is required to allow the Digital Health Pass Verify mobile app to be used by verifiers. Once the verifier app is used to either scan or select a previously-scanned verification credential, the verifier can scan holder credentials, for example, health passes and cards.

Figure: Example of a verifier credential



verifiers

A verifier uses the Verify mobile app to scan holder credentials, cards, and passes. Verifiers determine whether to allow the holder access.

Example: A business has several main offices and many smaller sites. Each office and site can be an organization, with its own **organization administrator**. Each administrator sets up **verifiers** to function as security personnel at each location.

About the administrative console

The administrative console for Digital Health Pass is a web application that allows administrators to perform various tasks, for example, onboarding Digital Health Pass customers (IBM internal only) and managing organizations and verifier credentials.

Note: Customer Administrators can manage both organizations and verifier credentials. Organization Administrators can only manage verifier credentials.

Privacy

The Digital Health Pass solution does not collect specific users' information. In addition, it does not register the exact time of verification scans.

About Basic customers and Enterprise customers

The IBM Digital Health Pass solution is flexible, and scales to meet customer size and needs.

Planning and administration

As a customer, plan both your Digital Health Pass deployment and your approach to administration based on your overall organization size and type. Consider the number of locations you have and the number of verifiers that you'll use.

Example

For Digital Health Pass, an example of a **Basic customer** might be a restaurant. Because there's a single physical location, with one entry and few staff set up as verifiers, the Customer Administrator can manage verifiers using the default organization, which represents a single physical location.

An example of an **Enterprise customer** might be a concert promoter. Let's say that this promoter manages several venues. Here, the deployment is better suited to setting up an organization at each venue. Each of these organizations can in turn manage verifier credentials, for example, to set up a verifier credential for each gate at the venue.

Note: This table lists general criteria for you to consider when getting ready for administration. Because customer needs vary greatly, use these as high-level guidelines.

Table 1 Customer types for IBM Digital Health Pass

	Basic customer	Enterprise customer
Description	Simpler administration	More complex administration
Number of organizations	One organization	Multiple organizations
Staff size	Small staff	Large staff
Locations	One location, few locations	Larger number of locations

	Basic customer	Enterprise customer
Entries (location access)	One entry or few entries	Multiple entries
Verifier management	Performed by Customer Administrator	Delegated to one or more Organization Administrators
Volume of holders	Low volume	High volume

If you have questions about customer types and administration planning, contact your IBM team.

About credential verification

You can use Digital Health Pass administration to apply specific business logic when evaluating the validity of a holder's credential. This logic is critical in determining whether a credential is valid, according to the particular business processes for the customer and organization. The logic involves questions that are specific to the verifier and credential.

Table 2 Questions evaluated when validating of a holder credential

Verifier-specific questions	Is this an issuer that I trust?
	Is this a credential that I accept?
	Does the credential satisfy my business requirements?
Credential-specific questions	Is this credential probably generated by the issuer?
	Is this credential unaltered by the holder?

The answers to these questions will vary among verifying organizations. For example, different organizations might:

- Support different sets of credential types
- Have different business requirements around what criteria must be met for admittance, for example, a negative test
- Trust a different set of issuers

As a verifier, you can apply a **verification configuration** for this situation. In addition, you can associate a configuration with a **verifier credential**. For more information, see About verification rules for verifier credentials.

For information about the types of credentials and QR codes that Digital Health Pass supports, see About supported healthcare QR codes.

About supported healthcare QR codes

IBM Digital Health Pass supports existing data and interoperability standards, and aligns with emerging standards for COVID-19 health passes and digital credentials. The encrypted digital wallet, IBM Digital Health Pass Wallet, allows individuals to maintain control of their personal information and determine what they share, with whom, and for what purpose. When individuals share their health apps with an organization, none of their personal health information leaves the application. Using the Digital Health Pass Wallet and Digital Health Pass Verify, customers manage encrypted, digital health credentials supported through QR codes either in digital wallets or in printed format.

Supported healthcare QR codes

IBM Digital Health Pass

Follows the World Wide Web Consortium (W3C) Decentralized Identifiers (DID) specification and the w3c Verifiable Credentials data model.

IBM Digital Health Pass (https://www.ibm.com/products/digital-health-pass) ↗

w3c Decentralized Identifiers (https://www.w3.org/TR/did-core/) ↗

Digital COVID Certificate (European Union)

Valid in all EU countries. In national language and English. Health data remains with the member state that issues the certificate.

EU Digital COVID certificate (https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/safe-covid-19-vaccines-europeans/eu-digital-covid-certificate_en) ↗

SMART® Health Cards (VCI™)

Based on the World Wide Web Consortium (W3C) Verifiable Credential and Health Level 7 (HL7) SMART on FHIR standards

The VCI Charter (https://vci.org/about) ↗

Good Health Pass

Verifiable credential based on the World Wide Web Consortium (W3C) standard

Good Health Pass Resources (https://www.goodhealthpass.org/resources/) ↗

Roles and responsibilities

This topic provides an overview of IBM Digital Health Pass roles. This overview includes a brief description of common tasks. At your business, one person might fulfill multiple roles.

Table 3 Overview of Digital Health Pass roles

Roles	Description	Where to find information
IBM System Administrators (IBM internal)	Complete onboarding tasks, including creating accounts, adding customers	The IBM internal-only version of the IBM Digital Health Pass Administration Guide
Customer Administrators*	Administer organizations	The IBM Digital Health Pass Administration Guide
Organization Administrators	Administer verifier credentials	The IBM Digital Health Pass Administration Guide
Verifier Coordinators	Manage verifiers	The IBM Digital Health Pass Administration Guide and Verifier Guide
Verifiers	Run app to verify holders	The IBM Digital Health Pass Verifier Guide
Issuers	Issue COVID-19 test results, vaccination status as digital credentials sent to holders' digital wallets	—
Holders	Users that hold health passes, cards (credentials) for verification	—

* Digital Health Pass supports several administrator roles to allow access to features that are appropriate to customer types. In Digital Health Pass administration, roles overlap. A Customer Administrator has all of the same rights and privileges as an Organization Administrator. However, the reverse is not true.

Getting started

Learn how to get started with using Digital Health Pass administration.

Automatic organization, verifier setup

To streamline your deployment, when you're added as a new Digital Health Pass customer, IBM automatically adds a **default organization**. You can quickly proceed with administration, for example, to add organizations and set up verifiers.

Based on your organization's size and complexity, using the default organization and verifier credential might be adequate. For considerations, see About Basic customers and Enterprise customers.

Notes:

- With the default organization, the Customer Administrator is also the Organization Administrator.
- To identify a default organization, look for **(default)** after the name.

What you need

Here's what you need for Digital Health Pass administration.

Administrative account ID and password, console URL

Digital Health Pass customers receive these in a welcome email from IBM.

Web browser

For administration, use the two most-recent desktop versions of either Google® Chrome™ or Mozilla Firefox™

Note: If you have questions about these, contact your IBM team.

Using your welcome email

After IBM adds you as a Digital Health Pass customer, you'll receive a welcome email.

To use your welcome email:

1. In your email inbox, look for the email with a "set password" subject line.
2. Check the email contents. Follow the instructions to set your Digital Health Pass administrative password.

Table 4 Requirements for Digital Health Pass administrator passwords

At least one uppercase character (A - Z)
At least one lowercase character (a - z)
At least one digit (0 - 9)
At least one special character (punctuation)
At least 10 characters
At most 128 characters
Not more than two identical characters in a row (for example, 111 is not allowed)

Tips for administration

Simplify Digital Health Pass administration using these tips.

Find items quickly using filtering.

In the administrative console, lists of items, for example, organizations and credentials, can be lengthy. To quickly locate an item, use filtering.

1. Above a list, click the magnifying glass icon.
2. In the field that appears, type the first few letters of the item's name. The console lists only matching items.

Logging in to the console

Digital Health Pass administrators access the administrative console through its web URL.

Note: Before you log in for the first time, follow the link in the email you received to set up your password.

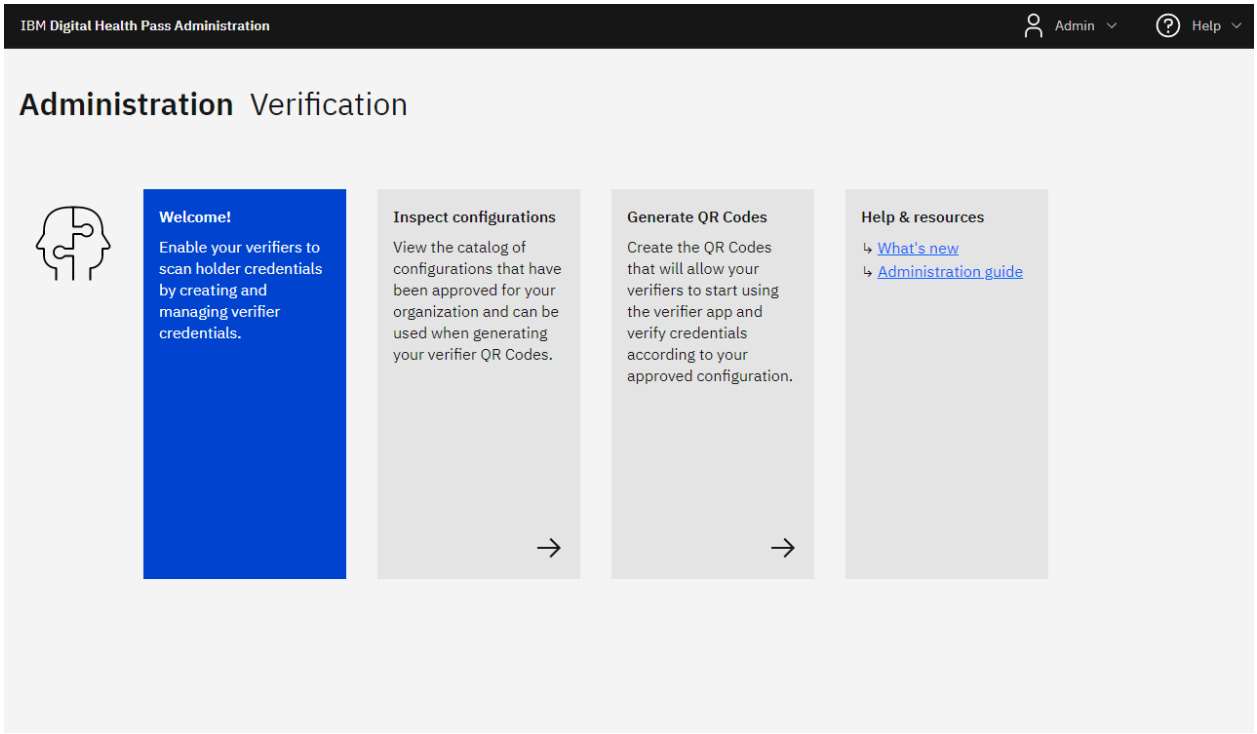
To log in to the console:

1. In a web browser, enter the Digital Health Pass administrative console URL.
2. At the login page, enter your administrative email address and password.
3. Click **Continue**. The console opens.

Notes: Available home page options vary based on the role, for example, System Administrator, Customer Administrator, or Organization Administrator.

To help maintain the security of Digital Health Pass information, always log out. When you're done using the console, in console menu bar, click the profile icon and **Log out**.

Figure: Administration console home page (Organization Administrator version)



Customer Administrators

Learn concepts and procedures that Customer Administrators use to administer the Digital Health Pass application.

Tip: Understand administration basics and capabilities before proceeding. For information, see Roles and responsibilities.

Adding an organization

Add organizations that reflect your business. When IBM sets up a customer to use Digital Health Pass, it also creates a **default organization**. Customer Administrators have the option to define additional organizations.

Each organization has its own administrator, in addition to the Customer Administrator. So, creating additional organizations allows the Customer Administration to delegate the task of managing verifier credentials to other individuals.

Example

Let's say that a national insurance company is using Digital Health Pass in its regional offices. To delegate responsibility of managing verifier credentials, the company can set up an organization in each region.

For more information about organizations, see Introduction to administration.

To add an organization:

1. Log in to the administrative console.
2. On the home page, click the **Manage customers** tile.
3. On the Organizations page, click **Organizations +**.
4. On the Organization page, enter:
    - **Organization name**
    - **Organization administrator:** The first, last names and a valid email address
5. Click **Add Organization**.

Adding an Organization Administrator

You can add an Organization Administrator for a selected Digital Health Pass organization.

For more information about organizations, see Introduction to administration.

To add an Organization Administrator:

1. Log in to the administrative console.
2. On the home page, click the **Manage organizations** tile.
3. On the Organizations page, hover the pointer over the row for the organization that you want.
4. Under **Actions**, click the person icon.
5. On the Administrators page, click **Administrator**.
6. On the Create an Administrator page, enter:
    - The administrator's first, last names
    - A valid email address
7. Click **Add Administrator**.

Reviewing Organization Administrators

Review Organization Administrators set up for a selected Digital Health Pass customer.

To review Organization Administrators:

1. Log in to the administrative console.
2. On the home page, click the **Manage customers** tile.
3. On the Organizations page, in the row for the organization that you want, under **Actions**, click the person icon.
4. On the Administrators page, the console lists the administrators.

Note: The Customer Administrator is the Organization Administrator for the default organization. As a result, information for the default organization does not list any administrators.

About verification rules for verifier credentials

You can use Digital Health Pass administration to define and manage a catalog of **verifier configurations** (standard rule sets). In addition, when you create a verifier credential, you can associate a verifier configuration with it. Each configuration contains:

- **Rule sets:** A list of rules to evaluate against a holder’s credential
- **Trust lists:** A list of issuers which are trusted by the verifier
- **Display fields:** A list of fields from the holder’s credential that are displayed on the verifier application when a holder credential is scanned

The administration console includes a special **Configuration Catalog** of these configurations, from which you can select then associate a configuration with a verifier credential.

Process overview for verification rules, configurations

1. Understand rules in verifier configurations. View them in the configuration catalog.
2. Select configurations from the Master Catalog for use in your own catalog.
3. Add the verifier credentials that you need. Associate a verifier configuration with each credential.
4. Test the configuration, then place in production.

Administrator roles

Permissions related to verifier configuration differ based on the administrator type (table).

Table 5 Administrators and permissions for verifier configurations

Role	Create	View	Associate configurations with verifier credentials
Customer administrators	Yes	Yes	Yes
Organization administrators	—	Yes	Yes

For an overview of credential verification in Digital Health Pass, see About credential verification. For steps that Organization Administrators use to add verifier credentials, see Adding a verifier credential.

About credential types, processing

When IBM Digital Health Pass processes verifiable credentials, the processing tries to identify the credential type. The supported types include those listed in About supported QR codes, processing. In the administration console, the Configuration Catalog also lists these, using an abbreviation for each type, for example, IDHP for IBM Digital Health Pass.

Table 6 Processing based on credential type

Credential type	Processing
Supported credential type Examples: IBM Digital Health Pass, Good Health Pass	Parses more-specific information from the credential Each known credential type has an associated credential schema, which describes how and where information is stored within the credential. This varies based on the type.

Credential type	Processing
Verifiable credential **Note:** In the Configuration Catalog, the **VC** abbreviation identifies the verifiable credential type.	Extracts and verifies limited information from the credential This is in effect fallback parsing, when processing cannot initially identify the verifiable credential as a supported credential type.

About rule sets

As an IBM Digital Health Pass customer, you have specific policies for verifying digital healthcare credentials. These policies include criteria for, for example, whether a credential is supported or expired. In addition, customers need the flexibility to control policies when applied to multiple digital credential standards, for example, the SMART Health Cards (SHC) standard and the Digital COVID Certificate (DCC) European Union standard.

Digital Health Pass administration uses **rule sets** to control how credentials are processed and assessed. A rule set definition is a collection of data rule definitions. Rule sets processing executes and evaluates multiple rules together against individual credentials.

Processing and verification

Rule set-based credential processing uses this basic logic: **Rules** → **Trust** → **Display**

Rules

A given credential type uses at least one rule. Rules use if/then statements, where the *if* is the condition and the *then* is the action of the rule. During processing, each rule in a set is applied to each individual credential.

Trust

After completing if/then and test condition assessments, a determination is made on whether to trust the credential, based on the relevant issuers.

Display

Based on successful completion of the previous steps, physically display the appropriate holder information on the credential when issued. This criterion displays selected information based on the credential type.

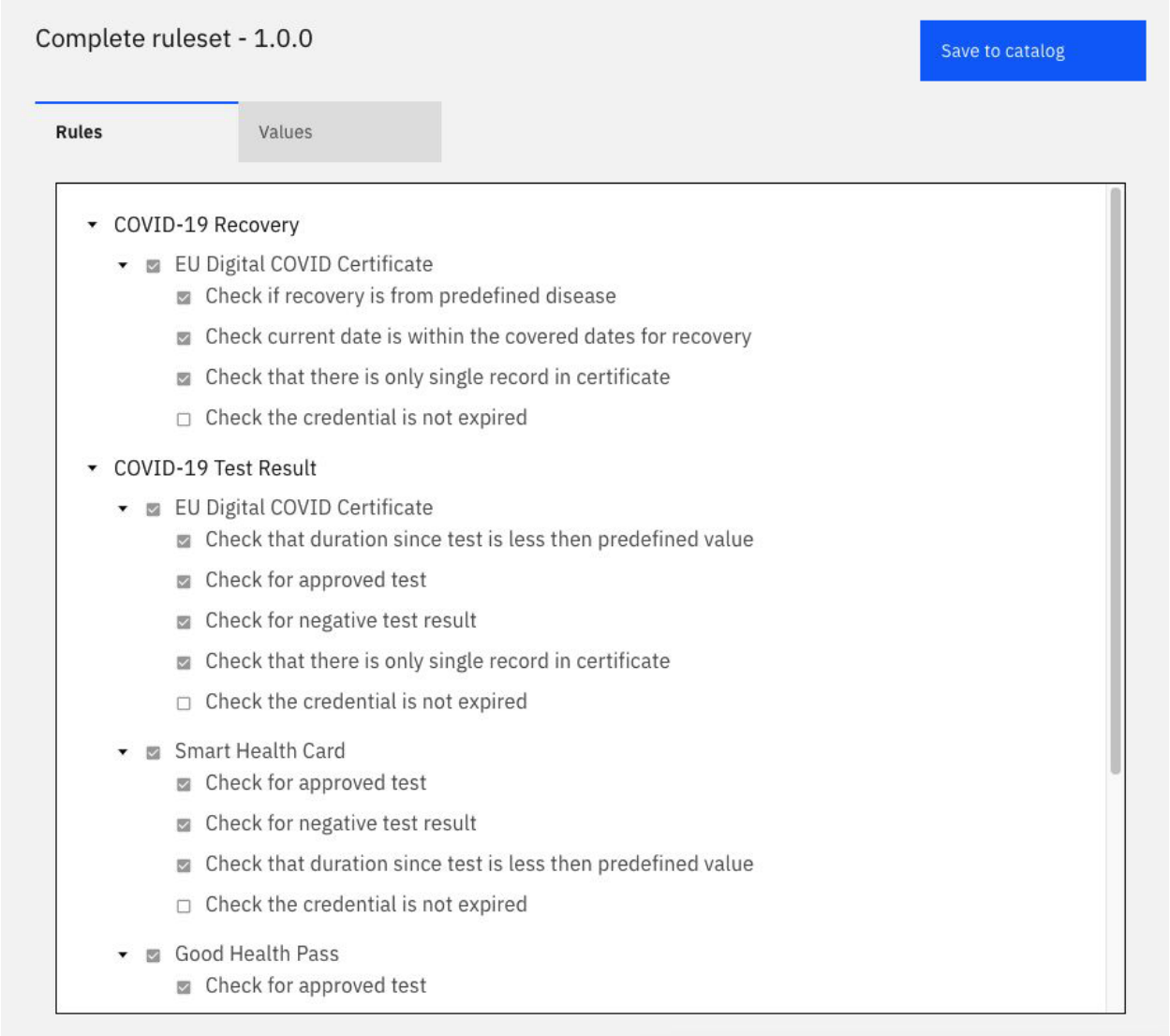
Table 7 Example of credential processing for verification

Credential type	Rule set, →rules	Trust	Display
Digital COVID Certificate (DCC) European Union	**Verify a Vaccination** → Check it is 14 to 365 days since getting the vaccination → Check for approved vaccine → Check for single vaccination record → Check for completed vaccination cycle	Trust all issuers registered in the EU Gateway	Display only minimum identity (name, date of birth)

Verification configurations, rule sets

Digital Health Pass includes several standard rule sets as **verifier configurations**. You'll find these configurations in the administration console's Configuration Catalog. For steps to access the Configuration Catalog, see Viewing verifier configurations.

Figure: Example of a rule set in the Configuration Catalog



Viewing verifier configurations

In Digital Health Pass administration, you can review verifier configurations, for example, prior to associating a configuration with a verifier credential. You'll find configurations in two catalogs:

- **Master Catalog:** By default, this includes several standard configurations.
- **<Customer> Configuration Catalog:** This contains configurations that you've selected for use from the Master Catalog. If needed, you can set up multiple configurations for each supported credential type.

To view verifier configurations:

1. Log in to the administrative console.
2. On the home page, click the **Set up configurations** tile.
3. On the Organizations page, click the row for the organization that you want.
4. On the Configuration catalog page, under **Actions**, for the configuration that you want, click the open model icon (arrow).
5. Under **Name**, click the row for the configuration that you want.
6. On the configuration page, click the **Rules** tab, then drill down to the detail that you want.
7. To display rules and their settings, click the **Values** tab, then drill down to the detail that you want.

Adding a verifier configuration to your catalog

You can build your own catalog of verifier configurations by selecting from standard, IBM-supplied configurations. Once a configuration is in your catalog, you customize its settings.

For steps to associate a verifier configuration with a verifier credential , see Adding a verifier credential.

To add a verifier configuration to your catalog:

1. Log in to the administrative console as a customer administrator.
2. On the home page, click the **Set up configurations** tile.
3. On the Configuration catalog page, click the **Master Catalog** tab.
4. In the catalog, locate the one that you want, and click its row.
5. Click **Save to catalog**.
6. In the Save Configuration dialog box, type a configuration name. Make sure that each configuration uses a unique name, to clearly differentiate them.
7. Click **Save**.

Testing and production

Testing verifier configurations

You can complete testing if you have several different credentials of each type.

Placing a configuration in production

After you use Digital Health Pass administration to create a verifier configuration, it is immediately available for production use.

Reviewing verifier metrics

You can review verification-related statistics for a selected organization. Easy-to-understand donut charts summarize verifier activity by credential type, scan results, and issuer for a specified time range.

To review verifier metrics:

1. Log in to the administrative console.
2. On the home page, click the **Manage organizations** tab.
3. On the Organizations page, in the row for the organization that you want, under **Actions**, click the chart icon.
4. On the Verification metrics page, review the charts.
5. As needed, under **Time range**, adjust the time period for which you want to review metrics.

Organization Administrators

Learn concepts and procedures that Organization Administrators use to administer the Digital Health Pass application.

Tip: Understand administration basics and capabilities before proceeding. For information, see Roles and responsibilities.

Adding a verifier credential

A valid, non-expired **verifier credential** is required for verifiers to use the Digital Health Pass Verify mobile application to scan and verify holder health passes and cards. In addition, the credential enables the Verify app to submit metrics for completed scans. You can:

- Issue a single verifier credential to all verifiers
- Issue each verifier their own verifier credentials
- Issue different groups of verifiers different verifier credentials

With the Verify app, the verifier can scan, store, and switch between multiple verifier credentials.

Each credential has an **expiration date**, which you can set based on your organization's needs. For example, for a sports event, one-day expiration might be suitable. Alternately, if your organization sets up a verifier annually, you can set credential expiration to 365 days.

Example

Let's say that an event management company is using Digital Health Pass to verify attendees at events. The company can add a verifier credential for each gate at a venue, and either assign all verifiers at that gate the same credential, or assign each individual verifier their own verifier credentials. For each verifier credential, the company can specify an expiration date for the verifier credential, based on the event date. When a gate staff member starts work, he'll typically scan a credential to start a verification session, and the credential will remain valid through its expiration date.

For an example of a verifier credential, see Terms and concepts.

To add a verifier credential:

1. Log in to the administrative console.
2. On the home page, click the **Generate QR codes** tile.
3. On the Verification Credentials page, click **Verification Credential +**.
4. At the Create a Verification Credential page:
    a. Type a name for the credential.

b. Specify the expiration time period, in days.

c. Under **Configuration**, select the verification configuration that you want for the credential. For information about verification configurations, see About verification rules for verifier credentials.

d. If there is more than one version of the configuration, select the **Use specific version** check box. From the **Version** drop-down list box that appears, select the version that you want.

Note: For the time period, type a whole number. Do not include a decimal or fraction.

5. Click **Save credential**.

Reviewing, sharing verifier credentials

Display and, if needed, share a copy of a Digital Health Pass verifier credential. The copy you display includes the credential's QR code, name, configuration, company, organization and expiration date.

To review, share a verifier credential:

1. Log in to the administrative console.
2. On the home page, click the **Generate QR codes** tile.
3. On the Verifier credential page, under **Name**, click the credential that you want.
4. After the credential appears, review the details.
5. To share a copy of the credential, for example, with a verifier:
   - To print a copy, click **Print**.
   - To share a file copy:
     a. Click **Copy to clipboard**.
     b. Paste the credential image into a graphics program, for example, Windows Paint.
     c. Save the image to the file format that you want, for example, .jpg.

Revoking a verifier credential

You can revoke (disable) a verifier credential when, for example, it is no longer used.

To revoke a verifier credential:

1. Log in to the administrative console.
2. On the home page, click the **Generate QR codes** tile.
3. On the Verification Credentials page, in the row for the configuration that you want to delete, under **Actions**, click the revoke (circular) icon.
4. In the Revoke Verifier Credential dialog box, click **Revoke Credential** to confirm.

Verifiers

Learn concepts and procedures that verifiers use with the Digital Health Pass solution.

Note: Administrators can use the information here when training verifiers on standard Digital Health Pass procedures.

How it works

You'll verify that holders have valid credentials (health cards or passes), for example, for access to a business or venue. To verify, you'll use IBM Digital Health Pass to scan the credentials.

Figure: Scanning a verifier credential

1. Get ready.

Before scanning, get prepared. Use the IBM Digital Health Pass Verify app and get authenticated.

To set up your app, scan the QR code provided by your organization.

Figure: Scanning a QR code

2. Holders present health passes, cards for scanning.

With the individual's QR code open on their telephone (or using their paper QR code), hold the smartphone with the Verify app over the individual's QR code.

Make sure the code is clearly visible within the screen of the smartphone that has the Verify app.

Wait while verification completes.

Figure: Checking validity

3. Verifiers check for validity.

Check information on the pass or card to determine whether it's valid. Follow any special guidance from your organization.

To scan another individual's QR code, tap **Scan Next Pass**.

Getting authenticated for verification

Prior to verifying — for example, if you're going to start work and scan health passes for customers at a restaurant — make sure that you have a current, valid verifier credential.

To get authenticated for verification:

1. Using the Digital Health Pass Verify app, scan the QR code for your verifier credential. Your organization provides you with the verifier credential.

   Where you'll find your credential differs. For example, your organization might email your credential, which you can scan from a computer display. Alternately, your organization might print your credential and post at it your workplace, where you can scan the copy.
2. Check the credential for validity. Make sure you're using it prior to its expiration date.

If the Verify app displays an error message

If you scan a QR code and Verify displays a **No Organization** or **You don't have a valid organization...** message, make sure that you're scanning:

- A current, valid credential (not expired)
- A verifier credential (not another type of QR code)

If you have questions, contact your onsite Verifier Coordinator.

Scanning

To start scanning holder health cards and passes (credentials), use the Digital Health Pass Verify mobile app.

Note: Before scanning, make sure that you're authenticated.

To scan health passes, cards:

1. At the start of a verification session:
   a. Open the Verify app and open the app settings.

b. Select the appropriate verifier credential, either from a previous scanned verifier credential or scan a new verifier credential QR code.

2. Get ready for holders to present credentials (health card or pass) for verification.

   With the IBM Digital Health Pass Wallet mobile app, holders tap a pass or card to display its QR code.

Note: Alternately, rather than displaying a credential from a digital wallet, holders might present a printed credential instead.

3. With the Pass Verify app open, point and center your device's camera at the QR code.

   When the app detects a valid QR code, it automatically scans and evaluates the credential.

4. Check the validation message and color.
5. If your organization's policies require any additional verification steps, complete those.
6. When you're done scanning, close the Verify app to maintain data security.

Troubleshooting and support

You can resolve many issues with IBM Digital Health Pass by trying troubleshooting procedures.

IBM Digital Health Pass Verify mobile app

Troubleshooting IBM Digital Health Pass Verify on IBM Support (https://www.ibm.com/support/pages/node/6447133) ↗

Product documentation

IBM® Digital Health Pass documentation on IBM Support (https://www.ibm.com/support/pages/node/6447523) ↗

Privacy policy

IBM® Digital Health Pass documentation on IBM Support (https://www.ibm.com/support/pages/node/6447523) ↗

Copyright information

Notices

This information was developed for products and services offered in the US. This material might be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Terms and conditions

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

The terms and conditions are in addition to any terms of use for the IBM website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside of your enterprise, without the express consent of IBM.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

Index

A

access, 6
accounts, 11
administration
  accessing, 13
  administrative account, 11
  administrator types, 7
  console, 2
  introduction, 2, 3
  overview, 7
administrators
  password, 12
  types, 10
  types and procedures, 4
app stores, 2
authentication, 26

B

Basic customers, 7
browser versions, 11

C

cards, 4
colors
  in validation, 27
concepts, 11
configuration catalog, 18
  adding configurations, 20
  overview, 16
console, administrative, 2
  logging in, 13
  overview, 7
  roles and features, 7
coordinators, verifier, 10
copyrights
  legal, 29
credentials
  cards, 4
  health passes, 4
  verifier credentials, 8
Customer Administrators
  procedures, 14
  responsibilities, 10
customers
  types, 7

D

DCC, Digital COVID Certificate (European Union credentials), 9
default organization, 11, 14
digital wallet, 4
display fields, 15, 17
document organization, 1, 25
documentation, 28
downloading

apps, 2

E

email notification, 12
Enterprise customers, 7
European Union credentials, 9
expiration date, 23

F

filtering, 12

G

GHP, Good Health Pass, 9
glossary, 4
Good Health Pass, 9

H

health passes, 4
  credentials, 4
  overview, 9
holders
  about, 4, 10
  presenting cards, passes, 27
home page, 13

I

IDHP, IBM Digital Health Pass, 9
if/then statements, 17
introduction
  administration overview, 3
  document, 1
  process overview, 2
issuers
  overview, 4
  responsibilities, 10
  trusted, 18

L

legal, 29
logging in, 13

M

Master Catalog
  rule sets, 16
  verifier configurations, 20
metrics, verifier, 22
mobile applications
  product, 2

O

onboarding
  example, 3
Organization Administrators
  adding, 15
  procedures, 23
  responsibilities, 10
  reviewing, 15
organizations
  about, 5
  adding, 14
  default organization, 11, 14

P

passes, 4
  digital wallet, 2
  overview, 9

password, administrative, 12
planning, 7
privacy, 7
privacy policy, 28
process overview, 2
production, 21

Q

QR codes, 4
  health cards, passes, 4
  in credentials, 5
  scanning, 26
  supported types, 9
quick response (QR) codes, 4

R

requirements, 11
revoking verifier configurations, 24
roles and responsibilities
  administrative console, 7
  overview, 10
rule sets, 17
  definition, 5
rules, verification, 15, 16, 17

S

scanning
  mobile app, 2
  overview, 25
  procedure, 26
security
  logging out, 13
SHC, Vaccination Credential Initiative SMART Health Cards, 9
signing in, 13
statistics, verifier, 22
support, 28

T

terms, 4
testing verifier configurations, 21
tips, 12
trademarks, 29
troubleshooting, 28
trust lists, 15, 17

V

Vaccination Credential Initiative SMART Health Cards, 9
valid, invalid, 27
validation, scanning, 26
VC, Vaccination Credential Initiative SMART Health Cards, 9
VC, verifiable credential type, 5, 17
verifier configurations
  definition, 5
  production, 21
  revoking, 24
  rule sets, 18
  testing, 21
  viewing, 20
verifiers
  about, 6
  metrics, 22
  procedures, 25
  responsibilities, 10

verifier configurations, 8
Verifier Coordinators, 10
verifier credentials
about, 5
adding, 23
expiration date, 23
printing, 24
reviewing, 24
Verify mobile app, 2
verifying
authentication, 26
preparation, 25
procedures, 25
verification rules, 15, 16

W

Wallet mobile app, 2
web browser, 11
welcome email, 12
what you need, 11