Tel: 314-889-1100
Fax: 314-889-1101
www.bdo.com

101 S Hanley Rd, Suite 800
St. Louis, MO 63105

REPORT OF THE INDEPENDENT ACCOUNTANT

To the management of SAFE Identity LLC ("SAFE Identity"):

Scope

We have examined the assertions by the management of SAFE Identity and DigiCert, Inc. ("DigiCert"), an independent subservice organization that provides Public Key Infrastructure ("PKI") management services to SAFE Identity, that for its Certification Authority ("CA") operations in California and Utah, in the United States of America, as of November 2, 2020 for its CAs enumerated in Attachment B, SAFE Identity and DigiCert have:

- disclosed SAFE Identity's business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its SAFE Identity Bridge CA Certificate Policy ("CP") (including sections 1 through 9), and SAFE Identity Bridge CA Certification Practice Statement ("CPS") (including sections 1 through 9), and Memorandum of Agreement between the United States Federal Public Key Infrastructure Policy Authority and SAFE Identity ("MOA") (including sections 1 through 9), as enumerated in Attachment A

- suitably designed, and placed into operation, its CA services in accordance with its disclosed practices, including:
  - SAFE Identity's ("CP") (including sections 1 through 9);
  - SAFE Identity's CPS (including sections 1 through 9) that is consistent with SAFE Identity's CP; and
  - the MOA (including sections 1 through 9)

- suitably designed, and placed into operation, controls to provide reasonable assurance that:
  - the integrity of keys and certificates it manages is established and protected throughout their lifecycles; and
  - subordinate CA certificate requests are accurate, authenticated, and approved

- suitably designed, and placed into operation, effective controls to provide reasonable assurance that:
  - logical and physical access to CA systems and data is restricted to authorized individuals;
  - the continuity of key and certificate management operations is maintained; and
  - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity

based on the WebTrust Principles and Criteria for Certification Authorities v2.2.1.

SAFE Identity does not escrow its CA keys, does not provide subscriber key lifecycle management controls, does not provide subscriber registration, and does not provide certificate suspension services. Accordingly, our examination did not extend to controls that would address those criteria.

Certification Authority's Responsibilities

SAFE Identity and DigiCert management are responsible for their respective assertions, including the fairness of their presentation, and the provision of their described services in accordance with the WebTrust Principles and Criteria for Certification Authorities v2.2.1.

Practitioner's Responsibilities

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether management's assertions are fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risks of material misstatement of management's assertions, whether due to fraud or error. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

The suitability of the design of the controls at SAFE Identity and DigiCert and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other factors present at individual subscriber and relying party locations. We have performed no procedures to evaluate the suitability of the design of the controls at individual subscriber and relying party locations. We did not perform any procedures regarding the operating effectiveness of the aforementioned controls for any period and, accordingly, do not express an opinion thereon.

Inherent Limitations

Because of the nature and inherent limitations of controls, SAFE Identity's and DigiCert's ability to meet the aforementioned criteria may be affected. For example, controls may not prevent, or detect and correct, error, fraud, unauthorized access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

Independent Accountant's Opinion

In our opinion, as of November 2, 2020, SAFE Identity's and DigiCert's management assertions, as referred to above, are fairly stated, in all material respects.

This report does not include any representation as to the quality of SAFE Identity's or DigiCert's services other than its CA operations in California and Utah, in the United States of America, nor the suitability of any of SAFE Identity's or DigiCert's services for any customer's intended purpose.

Other Matters

Without modifying our opinion, we noted the following other matter during our procedures:

Matter Topic	Matter Description
Key Recovery Policy ("KRP")	As of November 2, 2020, SAFE ID had not finalized its KRP. The KRP was finalized on February 25, 2021.

The World Health Organization classified the COVID-19 outbreak as a pandemic in March 2020. Based on the continued increase in exposure globally, the gravity or length of the impact of the COVID-19 outbreak cannot be estimated at this time.

BDO USA, LLP

April 6, 2021

ATTACHMENT A – POLICIES IN-SCOPE

Certification Practice Statement Versions In-Scope

CPS Name	Version	Effective Date
SAFE Identity Bridge CA Certification Practice Statement	1.0	October 21, 2020
SAFE Identity Trust Anchor Certification Practice Statement	1.0	October 21, 2020

Certificate Policy Version In-Scope

The SAFE Identity Certificate Policy is published on the SAFE Identity website.

CP Name	Version	Effective Date
SAFE Identity Bridge CA Certification Policy	1.1	November 2, 2020

Memorandum of Agreement Version In-Scope

The Memorandum of Agreement pertains to the SAFE Identity Bridge CAs and is restricted to authorized program members.

Memorandum Name	Effective Date
Memorandum of Agreement between the United States Federal Public Key Infrastructure Policy Authority and SAFE-BioPharma Association, LLC	May 25, 2018

ATTACHMENT B – LIST OF CAs IN-SCOPE

Root & Bridge CAs			
Subject DN	**Serial Number**	**Subject Key Identifier**	**SHA1 Thumbprint**
CN = SAFE Identity Trust Anchor OU = Certification Authorities O = SAFE Identity C = US	1B2603F85D6CF13D6240B07AA05636F9	5AFB570A6F9AF07F0CE5665E9C62C12430D13A18	6DF7EE37FC8FE4E833A40A60721775EE54479C7E
CN = SAFE Identity Bridge CA OU = Certification Authorities O = SAFE Identity C = US	3989585F78174960AC3830C8D14C59EF	99A41ACDDC6FC6A8083EADB6966C7ED7CF37A4C9	834FFE2112652722909A6F4CA7AA6C5D7F4D1021

SAFE IDENTITY LLC MANAGEMENT'S ASSERTION

SAFE Identity LLC ("SAFE Identity") and DigiCert, Inc. ("DigiCert"), an independent subservice organization that provides Public Key Infrastructure ("PKI") management services to SAFE Identity, operate the Certification Authority ("CA") services for the CAs enumerated in Attachment B, and provide the following CA services:

- Certificate renewal
- Certificate rekey
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate validation
- Subordinate CA and cross certificate lifecycle management

The management of SAFE Identity is responsible for establishing controls over its CA operations, including its CA business practices disclosure on its website, CA business practices management, applicable CA environmental controls, CA key lifecycle management controls, and subordinate CA lifecycle management controls. These controls contain monitoring mechanisms, and actions are taken to correct deficiencies identified.

There are inherent limitations in any controls, including the possibility of human error, and the circumvention or overriding of controls. Accordingly, even effective controls can only provide reasonable assurance with respect to SAFE Identity's CA operations.

SAFE Identity's management has assessed its disclosure of its certificate practices and controls over its CA services. Based on that assessment, in SAFE Identity management's opinion, in providing its CA services in California and Utah, in the United States of America, as of November 2, 2020, SAFE Identity has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its SAFE Identity Bridge CA Certificate Policy ("CP") (including sections 1 through 9), SAFE Identity Bridge CA Certification Practice Statement ("CPS") (including sections 1 through 9), and Memorandum of Agreement between the United States Federal Public Key Infrastructure Policy Authority and SAFE Identity ("MOA") (including sections 1 through 9), as enumerated in Attachment A

- suitably designed, and placed into operation, its CA services in accordance with its disclosed practices, including:
  - SAFE Identity's CP (including sections 1 through 9);
  - SAFE Identity's CPS that is consistent with SAFE Identity's CP (including sections 1 through 9); and
  - the MOA (including sections 1 through 9)

- suitably designed, and placed into operation, controls to provide reasonable assurance that subordinate CA certificate requests are accurate, authenticated, and approved

based on the WebTrust Principles and Criteria for Certification Authorities v2.2.1, including the following:

CA Business Practices Disclosure

- Certification Practice Statement (CPS)
- Certificate Policy (CP)

CA Business Practices Management

- Certification Practice Statement Management
- Certificate Policy Management
- CP and CPS Consistency

CA Environmental Controls

- Security Management
- Personnel Security
- Disaster Recovery, Backups, and Business Continuity Management
- Monitoring and Compliance
- Audit Logging

CA Key Lifecycle Management Controls

- CA Public Key Distribution

Subordinate CA Certificate Lifecycle Management Controls

- Subordinate CA and Cross Certificate Lifecycle Management

SAFE Identity does not escrow its CA keys, does not provide subscriber key lifecycle management controls, does not provide subscriber registration, and does not provide certificate suspension services. Accordingly, our assertion does not extend to controls that would address those criteria.

SAFE Identity

DocuSigned by:
Kyle Neuman
16E5C44BC12B434...

4/6/2021

Kyle Neuman
Managing Director

ATTACHMENT A – POLICIES IN-SCOPE

Certification Practice Statement Versions In-Scope

CPS Name	Version	Effective Date
SAFE Identity Bridge CA Certification Practice Statement	1.0	October 21, 2020
SAFE Identity Trust Anchor Certification Practice Statement	1.0	October 21, 2020

Certificate Policy Version In-Scope

The SAFE Identity Certificate Policy is published on the SAFE Identity website.

CP Name	Version	Effective Date
SAFE Identity Bridge CA Certification Policy	1.1	November 2, 2020

Memorandum of Agreement Version In-Scope

The Memorandum of Agreement pertains to the SAFE Identity Bridge CAs and is restricted to authorized program members.

Memorandum Name	Effective Date
Memorandum of Agreement between the United States Federal Public Key Infrastructure Policy Authority and SAFE-BioPharma Association, LLC	May 25, 2018

ATTACHMENT B – LIST OF CAs IN-SCOPE

Root & Bridge CAs			
Subject DN	**Serial Number**	**Subject Key Identifier**	**SHA1 Thumbprint**
CN = SAFE Identity Trust Anchor OU = Certification Authorities O = SAFE Identity C = US	1B2603F85D6CF13D6240B07AA05636F9	5AFB570A6F9AF07F0CE5665E9C62C12430D13A18	6DF7EE37FC8FE4E833A40A60721775EE54479C7E
CN = SAFE Identity Bridge CA OU = Certification Authorities O = SAFE Identity C = US	3989585F78174960AC3830C8D14C59EF	99A41ACDDC6FC6A8083EADB6966C7ED7CF37A4C9	834FFE2112652722909A6F4CA7AA6C5D7F4D1021

DIGICERT, INC. MANAGEMENT'S ASSERTION

DigiCert, Inc. ("DigiCert") provides Public Key Infrastructure ("PKI") management services to SAFE Identity LLC ("SAFE Identity"), who operates the Certification Authority ("CA") services for the CAs enumerated in Attachment B. DigiCert provides the following PKI services to SAFE Identity:

- Certificate renewal
- Certificate rekey
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate validation

The management of DigiCert is responsible for establishing controls over its operations, to support SAFE Identity's CA business practices disclosures on SAFE Identity's website, applicable CA environmental controls, CA key lifecycle management controls, and subordinate CA lifecycle management controls. These controls contain monitoring mechanisms, and actions are taken to correct deficiencies identified.

There are inherent limitations in any controls, including the possibility of human error, and the circumvention or overriding of controls. Accordingly, even effective controls can only provide reasonable assurance with respect to DigiCert's PKI services.

DigiCert's management has assessed SAFE Identity's disclosure of its certificate practices and DigiCert's controls to provide its PKI services to SAFE Identity. Based on that assessment, in DigiCert management's opinion, in providing its PKI services in California and Utah, in the United States of America, as of November 2, 2020, DigiCert has:

- suitably designed, and placed into operation, controls to provide reasonable assurance that the integrity of keys and certificates it manages is established and protected throughout their lifecycles

- suitably designed, and placed into operation, controls to provide reasonable assurance that:
    - logical and physical access to CA systems and data is restricted to authorized individuals;
    - the continuity of key and certificate management operations is maintained; and
    - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity

based on the WebTrust Principles and Criteria for Certification Authorities v2.2.1, including the following:

CA Environmental Controls

- Security Management
- Asset Classification and Management
- Personnel Security
- Physical and Environmental Security
- Operations Management
- System Access Management
- Systems Development, Maintenance, and Change Management
- Disaster Recovery, Backups, and Business Continuity Management
- Monitoring and Compliance
- Audit Logging

CA Key Lifecycle Management Controls

- CA Key Generation
- CA Key Storage, Backup, and Recovery
- CA Public Key Distribution
- CA Key Usage
- CA Key Archival
- CA Key Destruction
- CA Key Compromise
- CA Cryptographic Hardware Lifecycle Management
- CA Key Transportation
- CA Key Migration

Certificate Lifecycle Management Controls

- Certificate Renewal
- Certificate Rekey
- Certificate Issuance
- Certificate Distribution
- Certificate Revocation
- Certificate Validation

DigiCert, Inc.

DocuSigned by:
Jeremy Rowley
CFF89E6506D0438...

4/6/2021

Jeremy Rowley
Executive VP of Product