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

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

REPORT OF THE INDEPENDENT ACCOUNTANT

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

Scope

We have examined the assertions by the management of SAFE ID and DigiCert, Inc. ("DigiCert"), an independent subservice organization that provides Public Key Infrastructure ("PKI") management services to SAFE ID, that in generating and protecting its key pairs included in the certificates enumerated in Attachment A, on October 28, 2020, in Mountain View, California, SAFE ID has:

- followed the CA key generation and protection requirements in its:
  - SAFE Identity Bridge CA Certification Practice Statement, Version 1.0 and SAFE Identity Trust Anchor Certification Practice Statement, Version 1.0 (the "CPSs"); and
  - SAFE Identity Bridge CA Certificate Policy, Version 1.0 ("CP")

- included appropriate, detailed procedures and controls in its Key Generation Script for SAFE Identity Root Creation + New Bridge CA + Cross Signing Key Ceremony script ("Key Generation Script") dated October 28, 2020

- maintained effective controls to provide reasonable assurance that the key pairs associated with the CAs enumerated in Attachment A were generated and protected in conformity with the procedures described in its CP, CPSs, and Key Generation Script

- performed, during the CA key generation process, all procedures required by the Key Generation Script

- generated the CA keys in a physically secured environment as described in its CP and CPSs

- generated the CA keys using personnel in trusted roles under multiple person control and split knowledge

- generated the CA keys within cryptographic modules meeting the applicable technical and business requirements as disclosed in its CP and CPSs

Certification Authority's Responsibilities

SAFE ID and DigiCert management are responsible for these procedures and for maintaining effective controls based on CA Key Generation Criterion 4.1 of the WebTrust Principles and Criteria for Certification Authorities v2.2.

Independent Accountant'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 assertion is fairly stated, in all material respects. Our examination, included:

(1) obtaining an understanding of SAFE ID's and DigiCert's documented plan of procedures to be performed for the generation of the certification authority key pairs for CAs enumerated in Attachment A;
(2) reviewing the detailed Key Generation Script for conformance with industry standard practices;
(3) testing and evaluating, during the CA key generation process, the effectiveness of controls over the integrity, confidentiality, and availability of all private keys, including back-up copies, and access keys (including physical keys, tokens, and passwords), used in the establishment of the service;
(4) physical observation of all procedures performed during the CA key generation process to ensure that the procedures actually performed on October 28, 2020 were in accordance with the Key Generation Script for the CAs enumerated in Attachment A; and
(5) performing such other procedures as we considered necessary in the circumstances.

Independent Accountant's Opinion

In our opinion, SAFE ID and DigiCert managements' 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 ID's or DigiCert's services other than its CA operations in Mountain View, California, nor the suitability of any of SAFE's services for any customer's intended purpose.

Other Matter

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

February 4, 2021

ATTACHMENT A – IN-SCOPE CAs

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

Cross Signed CAs				
Subject DN	**Issuer DN**	**Serial Number**	**Subject Key Identifier**	**SHA1 Thumbprint**
CN = Trans Sped Mobile eIDAS QCA G2 OU = Individual Subscriber CA O = Trans Sped SRL C = RO	CN = SAFE Identity Bridge CA OU = Certification Authorities O = SAFE Identity C = US	015378124F47D7501E3229F1F15C789B	1D504E458B234014D56B177A17D65A36EBCF4DFD	8A70668CA59A7DA20681CF5EC4A6383C75AD8ADE
CN = SAFE Identity Bridge CA OU = Certification Authorities O = SAFE Identity C = US	CN = SAFE Identity Trust Anchor OU = Certification Authorities O = SAFE Identity C = US	61B7B7837CA05E6859610C78CBD53E	99A41ACDDC6FC6A8083EADB6966C7ED7CF37A4C9	FF7F66CF369194EDD86DF190AB6BA6C1F1A1BAB9
CN = IdenTrust SAFE-BioPharma CA 1 OU = IdenTrust Global Common O = IdenTrust C = US	CN = SAFE Identity Bridge CA OU = Certification Authorities O = SAFE Identity C = US	499F365B92D37AB844648BBA823A4DD7	0C7E4608396BFF2E26BBAE4793F97E2A0FAE70286B	CB023DDEE100C9040C7A9AD60717EBF34AB2106B

Cross Signed CAs				
Subject DN	**Issuer DN**	**Serial Number**	**Subject Key Identifier**	**SHA1 Thumbprint**
CN = Federal Bridge CA G4 OU = FPKI O = U.S. Government C = US	CN = SAFE Identity Bridge CA OU = Certification Authorities O = SAFE Identity C = US	296AA3F84B617E281B3452DAAE216E26	79F00049EB7F77C25D410265348A90239B1E076F	1B5633FD2D4FC9F3A519AB494D206AA89832FAFC
CN = Carillon PKI Services G2 Root CA 3 OU = Certification Authorities O = Carillon Information Security Inc. C = CA	CN = SAFE Identity Bridge CA OU = Certification Authorities O = SAFE Identity C = US	38070F5E7452F00803E82E5DDC123D31	5E3774AA41289E1A3D75BAED4A090DDBC41093E9	2DF9D20203CFB0CE1EF48CDC03A16FE7B46E0ACA

SAFE IDENTITY, LLC MANAGEMENT'S ASSERTION

SAFE Identity, LLC ("SAFE ID") and DigiCert, Inc. ("DigiCert"), an independent subservice organization that provides Public Key Infrastructure ("PKI") management services to SAFE ID, have deployed a PKI. As part of this deployment, it was necessary to create a hierarchy consisting of a self-signed root CA, a bridge CA, and cross signed CAs, as enumerated in Attachment A. These CAs will perform client certificate services. In order to allow the CAs to be installed in a final production configuration, a key generation ceremony was conducted, the purpose of which was to formally witness and document the creation of the CAs' private signing keys. This helps assure the non-refutability of the integrity of the SAFE ID CAs' key pairs, and in particular, the private signing keys.

SAFE ID management has securely generated key pairs, each consisting of a public and private key, in support of its CA operations. The key pairs were generated in accordance with procedures described in the SAFE Identity Bridge CA Certificate Policy, Version 1.0 ("CP"), SAFE Identity Bridge CA Certification Practice Statement, Version 1.0, SAFE Identity Trust Anchor Certification Practice Statement, Version 1.0 (the "CPSs"), and SAFE Identity Root Creation + New Bridge CA + Cross Signing Key Ceremony Script ("Key Generation Script"), which are based on CA Key Generation Criterion 4.1 of the WebTrust Principles and Criteria for Certification Authorities v2.2.

SAFE ID management established and maintained effective controls over the generation of these keys. These controls were designed to provide reasonable assurance of adherence to the above-mentioned practices throughout the CA key generation process.

SAFE ID management is responsible for establishing and maintaining procedures over its CA key generations, and over the integrity and confidentiality of all private keys and access keys (including physical keys, tokens, and passwords) used in the establishment of the key pairs associated with the CAs enumerated in Attachment A, and for the CA environmental controls relevant to the generation and protection of its CA keys.

SAFE ID management has assessed the procedures and controls for the generation of the CA keys. Based on that assessment, in management's opinion, in generating and protecting its CA keys enumerated in Attachment A, on October 28, 2020, in Mountain View, California, in the United States of America, SAFE ID has been assured DigiCert:

- followed the CA key generation and protection requirements in its CP and CPSs
- included appropriate, detailed procedures and controls in its Key Generation Script dated October 28, 2020
- maintained effective controls to provide reasonable assurance that the key pairs associated with the root, bridge, and cross signed CAs enumerated in Attachment A were generated and protected in conformity with the procedures described in its CP, CPSs, and Key Generation Script
- performed, during the CA key generation process, all procedures required by the Key Generation Script
- generated the CA keys in a physically secured environment as described in its CP and CPSs

- generated the CA keys using personnel in trusted roles under multiple person control and split knowledge
- generated the CA keys within cryptographic modules meeting the applicable technical and business requirements as disclosed in its CP and CPSs

based on CA Key Generation Criterion 4.1 of the WebTrust Principles and Criteria for Certification Authorities v2.2.

DocuSigned by:
Kyle Neuman
16E5C44BC12B434...

2/4/2021

Kyle Neuman
Managing Director, SAFE ID

ATTACHMENT A – IN-SCOPE CAs

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

Cross Signed CAs				
Subject DN	**Issuer DN**	**Serial Number**	**Subject Key Identifier**	**SHA1 Thumbprint**
CN = Trans Sped Mobile eIDAS QCA G2 OU = Individual Subscriber CA O = Trans Sped SRL C = RO	CN = SAFE Identity Bridge CA OU = Certification Authorities O = SAFE Identity C = US	015378124F47D7501E3229F1F15C789B	1D504E458B234014D56B177A17D65A36EBCF4DFD	8A70668CA59A7DA20681CF5EC4A6383C75AD8ADE
CN = SAFE Identity Bridge CA OU = Certification Authorities O = SAFE Identity C = US	CN = SAFE Identity Trust Anchor OU = Certification Authorities O = SAFE Identity C = US	61B7B7837CA05E6859610C78CBD53E	99A41ACDDC6FC6A8083EADB6966C7ED7CF37A4C9	FF7F66CF369194EDD86DF190AB6BA6C1F1A1BAB9
CN = IdenTrust SAFE-BioPharma CA 1 OU = IdenTrust Global Common O = IdenTrust C = US	CN = SAFE Identity Bridge CA OU = Certification Authorities O = SAFE Identity C = US	499F365B92D37AB844648BBA823A4DD7	0C7E4608396BFF2E26BBAE4793F97E2A0FAE7028	CB023DDEE100C9040C7A9AD60717EBF34AB2106B
CN = Federal Bridge CA G4 OU = FPKI O = U.S. Government C = US	CN = SAFE Identity Bridge CA OU = Certification Authorities O = SAFE Identity C = US	296AA3F84B617E281B3452DAAE216E26	79F00049EB7F77C25D410265348A90239B1E076F	1B5633FD2D4FC9F3A519AB494D206AA89832FAFC

Cross Signed CAs				
Subject DN	**Issuer DN**	**Serial Number**	**Subject Key Identifier**	**SHA1 Thumbprint**
CN = Carillon PKI Services G2 Root CA 3 OU = Certification Authorities O = Carillon Information Security Inc. C = CA	CN = SAFE Identity Bridge CA OU = Certification Authorities O = SAFE Identity C = US	38070F5E7452F00803E82E5DDC123D31	5E3774AA41289E1A3D75BAED4A090DDBC41093E9	2DF9D20203CFB0CE1EF48CDC03A16FE7B46E0ACA

DIGICERT, INC. MANAGEMENT'S ASSERTION

DigiCert, Inc. ("DigiCert") provides Public Key Infrastructure ("PKI") management services to SAFE Identity, LLC ("SAFE ID"). As part of its services agreement, it was necessary to implement and maintain effective controls in generating and protecting CA keys enumerated in Attachment A for the deployment of a PKI. These CAs will serve as the root, bridge, and cross signed CAs for client certificate services. In order to allow the CAs to be installed in a final production configuration, a Key Generation Ceremony was conducted, the purpose of which was to formally witness and document the creation of the CAs' private signing keys. This helps assure the non-refutability of the integrity of the CA key pairs, and in particular, the private signing keys.

DigiCert management has securely generated key pairs, each consisting of a public and private key, in support of SAFE ID's CA operations. The key pairs were generated in accordance with procedures described in the SAFE Identity Bridge CA Certificate Policy, Version 1.0 ("CP"), SAFE Identity Bridge CA Certification Practice Statement, Version 1.0, SAFE Identity Trust Anchor Certification Practice Statement, Version 1.0 (the "CPSs"), and SAFE Identity Root Creation + New Bridge CA + Cross Signing Key Ceremony Script ("Key Generation Script"), which are based on CA Key Generation Criterion 4.1 of the WebTrust Principles and Criteria for Certification Authorities v2.2.

DigiCert management established and maintained effective controls over the generation of these keys. These controls were designed to provide reasonable assurance of adherence to the above-mentioned practices throughout the CA key generation process.

DigiCert management is responsible for establishing and maintaining procedures over the CA key generations, and over the integrity and confidentiality of all private keys and access keys (including physical keys, tokens, and passwords) used in the establishment of the root, bridge and cross signed CAs enumerated in Attachment A, and for the CA environmental controls relevant to the generation and protection of the CA keys.

DigiCert management has assessed the procedures and controls for the generation of the CA keys. Based on that assessment, in management's opinion, in generating and protecting the SAFE ID CA keys enumerated in Attachment A, on October 28, 2020, in Mountain View, California, in the United States of America, DigiCert has:

- followed the CA key generation and protection requirements in SAFE ID's CP and CPSs
- included appropriate, detailed procedures and controls in its Key Generation Script dated October 28, 2020
- maintained effective controls to provide reasonable assurance that the key pairs associated with the root, bridge and cross signed CAs enumerated in Attachment A were generated and protected in conformity with the procedures described in its CP, CPSs, and Key Generation Script
- performed, during the CA key generation process, all procedures required by the Key Generation Script

- generated the CA keys in a physically secured environment as described in SAFE ID's CP and CPSs
- generated the CA keys using personnel in trusted roles under multiple person control and split knowledge
- generated the CA keys within cryptographic modules meeting the applicable technical and business requirements as disclosed in SAFE ID's CP and CPSs

based on CA Key Generation Criterion 4.1 of the WebTrust Principles and Criteria for Certification Authorities v2.2.

DocuSigned by:
Jeremy Rowley
CFF89E6506D0438...

2/4/2021

Jeremy Rowley
Chief Product Officer