Deloitte LLP
Bay Adelaide Centre, East Tower
8 Adelaide Street West
Suite 200
Toronto, ON M5H 0A9
Canada

Tel: +1 416 601 6150
Fax: +1 416 601 6400
www.deloitte.ca

INDEPENDENT ASSURANCE REPORT

To the management of Entrust Corporation ("Entrust"):

Scope

We have been engaged, in a reasonable assurance engagement, to report on Entrust management's statement that for its Certification Authority (CA) operations in Ottawa, Ontario, Canada, Toronto, Ontario, Canada, Denver, Colorado, USA, Dallas, Texas, USA, and Berkshire, United Kingdom, throughout the period 1 March 2021 to 28 February 2022 (the "Period") for its CAs as enumerated in Attachment A, Entrust has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its Certification Practice Statements as enumerated in Attachment B

- maintained effective controls to provide reasonable assurance that Entrust provides its services in accordance with its Certification Practice Statements

- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and certificates it manages is established and protected throughout their lifecycles;
  - the integrity of subscriber keys and certificates it manages is established and protected throughout their lifecycles;
  - subscriber information is properly authenticated (for the registration activities performed by Entrust); and
  - subordinate CA certificate requests are accurate, authenticated, and approved

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

in accordance with the WebTrust Principles and Criteria for Certification Authorities v2.2.1.

Entrust does not escrow its CA keys and does not provide certificate suspension services. Accordingly, our procedures did not extend to controls that would address those criteria.

Certification authority's responsibilities

Entrust's management is responsible for its statement, including the fairness of its presentation, and the provision of its described services in accordance with the WebTrust Principles and Criteria for Certification Authorities v2.2.1.

Our independence and quality control

We have complied with the relevant rules of professional conduct / code of ethics applicable to the practice of public accounting and related to assurance engagements, issued by various professional accounting bodies, which are founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

The firm applies Canadian Standard on Quality Control 1, *Quality Control for Firms that Perform Audits and Reviews of Financial Statements, and Other Assurance Engagements*, and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Practitioner's responsibilities

Our responsibility is to express an opinion on management's statement based on our procedures. We conducted our procedures in accordance with Canadian Standard on Assurance Engagements 3000, *Attestation Engagements Other than*

Deloitte.

Audits or Reviews of Historical Financial Information, set out in the CPA Canada Handbook – Assurance. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, management's statement is fairly stated, and, accordingly, included:

(1) obtaining an understanding of Entrust's key and certificate lifecycle management business practices and its controls over key and certificate integrity, over the authenticity and confidentiality of subscriber and relying party information, over the continuity of key and certificate lifecycle management operations and over development, maintenance and operation of systems integrity;
(2) selectively testing transactions executed in accordance with disclosed key and certificate lifecycle management business practices;
(3) testing and evaluating the operating effectiveness of the controls; and
(4) performing such other procedures as we considered necessary in the circumstances.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Relative effectiveness of controls

The relative effectiveness and significance of specific controls at Entrust 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 effectiveness of controls at individual subscriber and relying party locations.

Inherent limitations

Because of the nature and inherent limitations of controls, Entrust's ability to meet the aforementioned criteria may be affected. For example, controls may not prevent, or detect and correct, error, fraud, unauthorised 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.

Basis for qualified opinion

During our procedures, we noted the following which caused a qualification of our opinion. The qualifications only apply to the locations generating subscriber keys (USA and United Kingdom). The CAs issuing the certificates are not impacted

	Observation	Relevant WebTrust Criteria
1	At sites located in the USA and the United Kingdom, we noted that: • Dual custody access was not always enforced by the access control system (United Kingdom); • Individuals not in approved, trusted roles had physical access to CA facilities (USA); • Audible alarms when facilities are accidentally left open/unlocked for an extended period were not consistently implemented (United Kingdom); and • A generic access credential existed for access to one of the facilities (United Kingdom). This caused WebTrust Principles and Criteria for Certification Authorities v2.2.1, Criterion 3.4 to not be met.	**3.4:** The CA maintains controls to provide reasonable assurance that: • physical access to CA facilities and equipment is limited to authorised individuals, protected through restricted security perimeters, and is operated under multiple person (at least dual custody) control; • CA facilities and equipment are protected from environmental hazards; • loss, damage or compromise of assets and interruption to business activities are prevented; and • compromise of information and information processing facilities is prevented.
2	For services provided out of USA, system monitoring and hardening controls were not consistently implemented across all CA systems during the Period.	**3.5:** The CA maintains controls to provide reasonable assurance that: • the secure operation of CA information processing facilities is ensured; • the risk of CA systems failure is minimised;

	This caused WebTrust Principles and Criteria for Certification Authorities v2.2.1, Criterion 3.5 to not be met.	• the integrity of CA systems and information is protected against viruses and malicious software; • damage from security incidents and malfunctions is minimised through the use of incident reporting and response procedures; and • media are securely handled to protect them from damage, theft and unauthorised access.
3	On supporting systems providing CA services: • User and system access reviews were not consistently performed (USA and United Kingdom); • Reviews of network and firewall configurations were not consistently performed (United Kingdom); and • Approvals for individuals to gain system access were not consistently obtained or provided prior to access being provisioned (USA). This caused WebTrust Principles and Criteria for Certification Authorities v2.2.1, Criterion 3.6 to not be met.	**3.6:** The CA maintains controls to provide reasonable assurance that CA system access is limited to authorised individuals. Such controls provide reasonable assurance that: • hypervisor, operating system, database, and network device access is limited to authorised individuals with predetermined task privileges; • access to network segments housing CA systems is limited to authorised individuals, applications and services; and • CA application use is limited to authorised individuals.
4	On supporting systems providing CA services, audit logs of relevant events were not consistently captured (USA). This caused WebTrust Principles and Criteria for Certification Authorities v2.2.1, Criterion 3.10 to not be met.	**3.10:** The CA maintains controls to provide reasonable assurance that: • significant CA environmental, key management, and certificate management events are accurately and appropriately logged; • the confidentiality and integrity of current and archived audit logs are maintained; • audit logs are completely and confidentially archived in accordance with disclosed business practices; and • audit logs are reviewed periodically by authorised personnel.

Practitioner's qualified opinion

In our opinion, except for the matters described in the preceding section entitled 'Basis for qualified opinion', throughout the period 1 March 2021 to 28 February 2022, Entrust has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its Certification Practice Statements as enumerated in Attachment B

- maintained effective controls to provide reasonable assurance that Entrust provides its services in accordance with its Certification Practice Statements

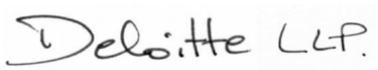
- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and certificates it manages is established and protected throughout their lifecycles;
  - the integrity of subscriber keys and certificates it manages is established and protected throughout their lifecycles;
  - subscriber information is properly authenticated (for the registration activities performed by Entrust); and
  - subordinate CA certificate requests are accurate, authenticated, and approved

- maintained effective controls to provide reasonable assurance that:
  - logical and physical access to CA systems and data is restricted to authorised individuals;

- the continuity of key and certificate management operations is maintained; and
- CA systems development, maintenance, and operations are properly authorised and performed to maintain CA systems integrity

in accordance with the WebTrust Principles and Criteria for Certification Authorities v2.2.1.

This report does not include any representation as to the quality of Entrust's services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities v2.2.1, nor the suitability of any of Entrust's services for any customer's intended purpose.



Deloitte LLP
Chartered Professional Accountants
Toronto, Ontario, Canada
11 May 2022

Deloitte.

ATTACHMENT A

LIST OF IN SCOPE CAs

Root CAs
1. Entrust.net Certification Authority (2048)
2. Entrust Root Certification Authority - G4
3. Entrust Digital Signing Root Certification Authority - DSR1
Intermediate CAs
4. Entrust Certification Authority - AATL1
Document Signing CAs
5. Entrust Class 3 Client CA - SHA256
6. Entrust Certification Authority - ES QSig1
7. Entrust Certification Authority - ES QSig2
8. Entrust Certification Authority - ES QSeal1
9. Entrust Certification Authority - ES QSeal2
10. Entrust Certification Authority - DE QSig1
11. Entrust Certification Authority - DE QSeal1

Deloitte.

CA IDENTIFYING INFORMATION

CA #	Cert #	Subject	Issuer	Serial Number	Key Type	Hash Type	Not Before	Not After	Revoked Date	Extended Key Usage	Subject Key Identifier	SHA256 Fingerprint
1	1	CN=Entrust.net Certification Authority (2048) OU=(c) 1999 Entrust.net Limited OU=www.entrust.net/CPS_2048 incorp. by ref. (limits liab.) O=Entrust.net	CN=Entrust.net Certification Authority (2048) OU=(c) 1999 Entrust.net Limited OU=www.entrust.net/CPS_2048 incorp. by ref. (limits liab.) O=Entrust.net	3863def8	RSA 2048-bits	RSA SHA-1	1999-12-24 17:50:51	2029-07-24 14:15:12			55e481d11180bed889b908a331f9a1240916b970	6dc47172e01cbcb0bf62580d895fe2b8ac9ad4f873801e0c10b9c837d21eb177
2	1	CN=Entrust Root Certification Authority - G4 OU=(c) 2015 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	CN=Entrust Root Certification Authority - G4 OU=(c) 2015 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	00d9b5437fafa9390f000000005565ad58	RSA 4096-bits	RSA SHA-256	2015-05-27 11:11:16	2037-12-27 11:41:16			9f38c45623c339e8a0716ce8544ce4e83ab1bf67	db3517d1f6732a2d5ab97c533ec70779ee3270a62fb4ac4238372460e6f01e88
3	1	CN=Entrust Digital Signing Root Certification Authority - DSR1 O=Entrust, Inc. C=US	CN=Entrust Root Certification Authority - G4 OU=(c) 2015 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	2d37bcd092d2cb88b67f5ccdab71b39b	RSA 4096-bits	RSA SHA-512	2021-11-12 00:00:00	2030-12-30 00:00:00		1.3.6.1.4.1.311.10.3.12, Time Stamping	a6654181f25b87056addfd8a544e8f987bdc23b8	20fc75acb2cad7978c7b006a9b1523bfdaf5490afcf49652c585e4a12f601c85
3	2	CN=Entrust Digital Signing Root Certification Authority - DSR1 O=Entrust, Inc. C=US	CN=Entrust Digital Signing Root Certification Authority - DSR1 O=Entrust, Inc. C=US	6c73c936b185e50b804d5bcec29f83d21a51c1a3	RSA 4096-bits	RSA SHA-512	2021-11-12 18:28:47	2040-12-30 18:28:47			a6654181f25b87056addfd8a544e8f987bdc23b8	e874fe2531eae4a4b6b62f37496bbae90eb1d8fc8cedbebb00a182cfacdc7e61
4	1	C=US O=Entrust, Inc. CN=Entrust Certification Authority - AATL1	CN=Entrust Root Certification Authority - G4 OU=(c) 2015 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	00c727f51f8f922b02000000005565d8ad	RSA 4096-bits	RSA SHA-512	2020-07-20 15:46:21	2037-12-20 16:16:21		1.3.6.1.4.1.311.10.3.12, 1.2.840.113583.1.1.5, E-mail Protection	63f184dd03bea39f64fa767a47c4567ec06da020	839f9b91c2e49218a66416df181b984e9be634d12a95483d98a6199fc0788d74
5	1	CN=Entrust Class 3 Client CA - SHA256 OU=(c) 2015 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	CN=Entrust.net Certification Authority (2048) OU=(c) 1999 Entrust.net Limited OU=www.entrust.net/CPS_2048 incorp. by ref. (limits liab.) O=Entrust.net	551615150000000051ce160e	RSA 2048-bits	RSA SHA-256	2016-02-25 18:08:16	2029-06-25 18:38:16		TLS Web Client Authentication, E-mail Protection, 1.3.6.1.4.1.311.10.3.12, 2.16.840.1.114027.40.11	069f6f4ea2294e0f0cae17bfb69846efadb83b72	33857338361ecfc4858ddff6b9ef6273e3db856ab9cea1c0e2c65925d1c87978
6	1	C=ES O=Entrust Datacard Europe, S.L. organizationIdentifier=VATES-B81188047 CN=Entrust Certification Authority - ES QSig1	C=US O=Entrust, Inc. CN=Entrust Certification Authority - AATL1	4491ca5825be79842b29b0c37286215f	RSA 4096-bits	RSA SHA-512	2020-07-29 16:33:00	2037-12-19 23:59:00		E-mail Protection, 1.3.6.1.4.1.311.10.3.12, 1.2.840.113583.1.1.5	5a53088a6130a90dead54397d3983b951e2e6d02	b2874b588a94034798319d5d329db265f83a47f315ba5831a4970cb57166d594
7	1	CN=Entrust Certification Authority - ES QSig2 organizationIdentifier=VATES-B81188047 O=Entrust EU, S.L. C=ES	CN=Entrust Digital Signing Root Certification Authority - DSR1 O=Entrust, Inc. C=US	3f967d63188a95bf302f82e516cb991d	RSA 4096-bits	RSA SHA-512	2021-11-16 00:00:00	2040-12-29 00:00:00		1.3.6.1.4.1.311.10.3.12, 1.2.840.113583.1.1.5	f5560d69d7da6ac9d8c9a2096e74bedb80c61700	4671fdead3c5b32d834b36591d41496fcb8a0db7d4f9f4cb9d34eabe0947ee87
8	1	C=ES O=Entrust Datacard Europe, S.L. organizationIdentifier=VATES-B81188047 CN=Entrust Certification Authority - ES QSeal1	C=US O=Entrust, Inc. CN=Entrust Certification Authority - AATL1	13ee348e492f8dd6b5c49cf073f714ab	RSA 4096-bits	RSA SHA-512	2020-07-27 14:39:07	2037-12-19 23:59:00		E-mail Protection, 1.3.6.1.4.1.311.10.3.12, 1.2.840.113583.1.1.5	5680152395717fe72d90d0cd063a4f67637d3d75	1701de38124c4458f32b88ae7e62ac15876c427a3ad3bbae8fd1479ff00030f3
9	1	CN=Entrust Certification Authority - ES QSeal2 organizationIdentifier=VATES-B81188047 O=Entrust EU, S.L. C=ES	CN=Entrust Digital Signing Root Certification Authority - DSR1 O=Entrust, Inc. C=US	12f04c327561e6f51e8d39b47e9884e1	RSA 4096-bits	RSA SHA-512	2021-11-16 00:00:00	2040-12-29 00:00:00		1.3.6.1.4.1.311.10.3.12, 1.2.840.113583.1.1.5	3618256ed95df710057c272eb8ecfa414a60ed1f	8c31d9375128d4b107f07678eebfff2cca26a4cabb462f257f31a36fe7bce104
10	1	C=DE O=Entrust Datacard Deutschland GmbH organizationIdentifier=VATDE-119264316 CN=Entrust Certification Authority - DE QSig1	C=US O=Entrust, Inc. CN=Entrust Certification Authority - AATL1	5bb8dd672998a2d5c6f3cdd446aac3a2	RSA 4096-bits	RSA SHA-512	2020-07-29 16:31:03	2037-12-19 23:59:00	2022-02-24 00:00:00	E-mail Protection, 1.3.6.1.4.1.311.10.3.12, 1.2.840.113583.1.1.5	31ec071330c7e2d12d5e11f837a57da9635f5364	84c35fee7a06d0bc61294d411fb4bbef50104596f49688ccaad32cb3b99916d6
11	1	C=DE O=Entrust Datacard Deutschland GmbH organizationIdentifier=VATDE-119264316 CN=Entrust Certification Authority - DE QSeal1	C=US O=Entrust, Inc. CN=Entrust Certification Authority - AATL1	179cc56dc82dbded5573c7999997f646	RSA 4096-bits	RSA SHA-512	2020-07-27 14:42:58	2037-12-19 23:59:00	2022-02-24 00:00:00	E-mail Protection, 1.3.6.1.4.1.311.10.3.12, 1.2.840.113583.1.1.5	6d8665848c526c862f8af7f02e5b9b4572668c7c	a0da9d5628ebcf3d13dd07c92bee9aa2041b4622be29810d517d9ef3ebf9a861

Deloitte.

ATTACHMENT B

LIST OF ENTRUST CERTIFICATION PRACTICE STATEMENTS

CPS Name	Version	Date
Entrust Certificate Services Certification Practice Statement	3.8	31 Dec 2020
Entrust Certificate Services Certification Practice Statement	3.9	19 Jul 2021
Entrust Certificate Services Certification Practice Statement	3.10	18 Feb 2022
ENTRUST DATACARD EUROPE S.L. Certification Practice Statement (CPS)	1.4	18 Dec 2020
ENTRUST DATACARD EUROPE S.L. Certification Practice Statement (CPS)	1.5	7 May 2021
ENTRUST DATACARD EUROPE S.L. Certification Practice Statement (CPS)	1.5.1	15 Nov 2021
ENTRUST DATACARD EUROPE S.L. Certification Practice Statement (CPS)	1.6	30 Nov 2021
ENTRUST DATACARD DEUTSCHLAND GMBH Certification Practice Statement (CPS)	1.3	18 Dec 2020

ENTRUST MANAGEMENT'S STATEMENT

Entrust Corporation ("Entrust") operates the Certification Authority (CA) services as enumerated in Attachment A, and provides the following CA services:

- Subscriber registration
- Certificate renewal
- Certificate rekey
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate validation
- Subscriber key generation and management
- Subordinate CA cross-certification

The management of Entrust is responsible for establishing and maintaining effective controls over its CA operations, including its CA business practices disclosure on its website, CA business practices management, CA environmental controls, CA key lifecycle management controls, subscriber key lifecycle management controls, certificate lifecycle management controls, and subordinate CA certificate 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 Entrust's Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

Entrust management has assessed its disclosures of its certificate practices and controls over its CA services. Based on that assessment, in Entrust management's opinion, in providing its Certification Authority (CA) services at Ottawa, Ontario, and Toronto, Ontario, throughout the period 1 March 2021 to 28 February 2022 Entrust has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environment control practices in its Certification Practice Statements as enumerated in Attachment B

- maintained effective controls to provide reasonable assurance that Entrust provides its services in accordance with its Certification Practice Statements

- maintained effective controls to provide reasonable assurance that:
    - the integrity of keys and certificates it manages is established and protected throughout their lifecycles;
    - the integrity of subscriber keys and certificates it manages is established and protected throughout their lifecycles;
    - subscriber information is properly authenticated (for the registration activities performed by Entrust); and
    - subordinate CA certificate requests are accurate, authenticated, and approved

- maintained 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

in accordance with the WebTrust Principles and Criteria for Certification Authorities v2.2.1, including the following:

CA Business Practices Disclosure

- Certification Practice Statement (CPS)

CA Business Practices Management

- Certification Practice Statement Management

CA Environmental Controls

- Security Management
- Asset Classification and Management
- Personnel Security
- Physical and Environmental Security
- Operations Management
- System Access Management
- System 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

Subscriber Key Lifecycle Management Controls

- CA-Provided Subscriber Key Generation Services
- CA-Provided Subscriber Key Storage and Recovery Services
- Integrated Circuit Card (ICC) Lifecycle Management
- Requirements for Subscriber Key Management

Certificate Lifecycle Management Controls

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

Subordinate CA and Cross Certificate Lifecycle Management Controls

- Subordinate CA and Cross Certificate Lifecycle Management

Entrust does not escrow its CA keys and does not provide certificate suspension services. Accordingly, our statement does not extend to controls that would address those criteria.

Entrust management has also reported or responded to the following 'bugs' on Mozilla's Bugzilla reporting system:

Bug ID	Summary	Opened	Closed
1696227	Entrust – Incorrect Jurisdiction Country Value in an EV Certificate	2021-03-03	2021-07-15
1712106	Invalid localityName	2021-05-20	2021-12-13
1728796	Incorrect value in Business Category field for Government Entities	2021-09-02	2021-12-13
1731887	Test Website Certificates Expired	2021-09-21	2021-10-20
1737057	CRLs and OCSP responses not issued as specified in the CPS	2021-10-21	2022-03-08
1744827	SSL Certificates issued with Unverified IP Addresses	2021-12-07	2022-01-14
1748634	Late Revocation for SSL Certificates issued with Unverified IP Addresses	2022-01-05	2022-03-08

Bruce Morton
Director, Entrust Certificate Services
10 May 2022

ATTACHMENT A

LIST OF IN SCOPE CAs

Root CAs
1. Entrust.net Certification Authority (2048)
2. Entrust Root Certification Authority - G4
3. Entrust Digital Signing Root Certification Authority - DSR1
Intermediate CAs
4. Entrust Certification Authority - AATL1
Document Signing CAs
5. Entrust Class 3 Client CA - SHA256
6. Entrust Certification Authority - ES QSig1
7. Entrust Certification Authority - ES QSig2
8. Entrust Certification Authority - ES QSeal1
9. Entrust Certification Authority - ES QSeal2
10. Entrust Certification Authority - DE QSig1
11. Entrust Certification Authority - DE QSeal1

ATTACHMENT B

LIST OF ENTRUST CERTIFICATION PRACTICE STATEMENTS

CPS Name	Version	Date
Entrust Certificate Services Certification Practice Statement	3.8	31 Dec 2020
Entrust Certificate Services Certification Practice Statement	3.9	19 Jul 2021
Entrust Certificate Services Certification Practice Statement	3.10	18 Feb 2022
ENTRUST DATACARD EUROPE S.L. Certification Practice Statement (CPS)	1.4	18 Dec 2020
ENTRUST DATACARD EUROPE S.L. Certification Practice Statement (CPS)	1.5	7 May 2021
ENTRUST DATACARD EUROPE S.L. Certification Practice Statement (CPS)	1.5.1	15 Nov 2021
ENTRUST DATACARD EUROPE S.L. Certification Practice Statement (CPS)	1.6	30 Nov 2021
ENTRUST DATACARD DEUTSCHLAND GMBH Certification Practice Statement (CPS)	1.3	18 Dec 2020