## TELIA'S MANAGEMENT'S ASSERTION

Telia Company AB (Telia) operates the Certificate Authority (CA) services as listed in Attachment A, and provides SSL services.

The management of Telia has assessed its disclosure of its certificate practices and controls over its SSL CA services. During our assessment we noted the following deviations which caused the relevant criteria to not be met:

| # | Observation | Relevant WebTrust Criteria |
|---|---|---|
| 1 | The Key Usage extension in the root CA certificates of *TeliaSonera Root CA v1* and *Sonera Class 2 CA* is not marked critical and *TeliaSonera Root CA v1* certificate's subject information does not include subject:countryName. This caused WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3, Principle 2, Criterion 2.3 to not be met.<br><br>However, Telia generated a new root CA, *Telia Root CA v2*, on 29 November 2018, which is planned to eventually replace *TeliaSonera Root CA v1* and *Sonera Class 2 CA*. Extensions, key sizes, and certificate policy identifiers (including Reserved Certificate Policy Identifiers) of the new Telia Root CA v2 certificate conform to the Baseline Requirements. | **Principle 2, Criteria 2.3**<br><br>The CA maintains controls to provide reasonable assurance that the extensions, key sizes, and certificate policy identifiers (including Reserved Certificate Policy Identifiers) of Root CA certificates generated conform to the Baseline Requirements |

Based on that assessment, in Telia management's opinion, except for the matters as described in the preceding table, in providing its SSL and non-SSL Certification Authority (CA) services in Finland and Sweden, throughout the period 1 April 2019 to 31 March 2020, Telia has:

- disclosed its SSL certificate life cycle management business practises in its:
  - Telia Root Certificate Policy and Certification Practice Statement, version 2.5, dated March 2020
  - Telia Production Certification Practice Statement, version 2.8, dated March 2020
  - Telia Server Certificate Policy and Certification Practice Statement, version 2.7, dated March 2020
  - Telia Organizational User Certificate Policy and Certificate Practice Statement, version 1.4, dated March 2020

  including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the Telia website, and provided such services in accordance with its disclosed practices
- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and SSL certificates it manages is established and protected throughout their lifecycles; and

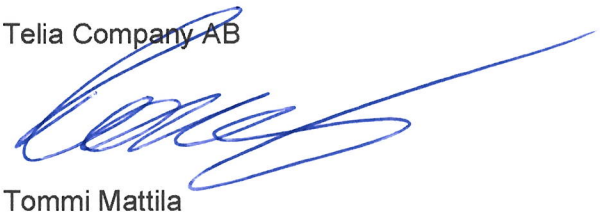
- SSL subscriber information is properly authenticated (for the registration activities performed by Telia)

- 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
- maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum

in accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.4.

Helsinki, 26 June 2020

Telia Company AB



Tommi Mattila

Head of Product Area, IT Services

## Attachment A: List of CAs in scope

The following CAs were in scope for the SSL Baseline Requirements and Network Security Requirements:

| CA # | Cert # | Subject | Issuer | Serial | Key Algorithm | Key Size | Digest Algorithm | Not Before | Not After | SKI | SHA2 Fingerprint | Other information |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | CN = TeliaSonera Root CA v1 O = TeliaSonera | Self-signed | 0095BE16A 0F72E46F1 7B398272F A8BCD96 | RSA | 4096 bits | sha1RSA | 18 October 2007 | 18 October 2032 | F08F593800B 3F58F9A960C D5EBFA7BAA 17E81312 | DD6936FE21F8F077 C123A1A521C12224F 72255B73E03A72606 93E8A24B0FA389 | |
| 1 | 2 | CN = TeliaSonera Root CA v1 O = TeliaSonera | Sonera Class2 CA | 87ED2E1A2 8264AC519 AA3AEBB90 DA2CB | RSA | 4096 bits | sha256RSA | 5 December 2014 | 5 April 2021 | F08F593800B 3F58F9A960C D5EBFA7BAA 17E81312 | E9563581E712B290F 23A749346535EB0D9 81E3D4A39D56D604 684CD0B1698C89 | Cross-certificate |
| 2 | 1 | CN = Sonera Class2 CA O = Sonera C = FI | Self-signed | 1D | RSA | 2048 bits | sha1RSA | 16 April 2001 | 16 April 2021 | 4AA0AA5884 D35E3C | 7908B40314C138100 B518D0735807FFBF CF8518A0095337105 BA386B153DD927 | |
| 3 | 1 | CN = Telia Root CA v2 O = Telia Finland Oyj C = FI | Self-signed | 01675F27D 6FE7AE3E4 ACBE095B0 59E | RSA | 4096 bits | sha256RSA | 29 November 2018 | 29 November 2043 | 72ACE43379A A4587F6FDA C1D9ED6C72 F86D82439 | 242B69742FCB1E5B2 ABF98898B94572187 544E5B4D991178657 3621F6A74B82C | |
| 3 | 2 | CN = Telia Root CA v2 O = Telia Finland Oyj C = FI | TeliaSonera Root CA v1 | 01675F82B E0017DE89 55A9376EB 1F9 | RSA | 4096 bits | sha256RSA | 29 November 2018 | 18 October 2032 | 72ACE43379A A4587F6FDA C1D9ED6C72 F86D82439 | EF6F29F636F62BDD 4753122F41F3419EE 7C2877587BE4A9807 ADF58946458E7F | Cross-certificate |
| 4 | 1 | CN = TeliaSonera Server CA v2 O = TeliaSonera C = FI | TeliaSonera Root CA v1 | 4C462AF6D BFBF7804F 84C17CFEA 972B6 | RSA | 4096 bits | sha256RSA | 16 October 2014 | 16 October 2032 | 2F493C294FD 70725F9C68C D564F5663D1 2832295 | D721110388CA6F20B BA9FD1A8DBA4EFB8 C16392A3DEBAD97C 553EEAF0ACACAAC | |

| CA # | Cert # | Subject | Issuer | Serial | Key Algorithm | Key Size | Digest Algorithm | Not Before | Not After | SKI | SHA2 Fingerprint | Other information |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 5 | 1 | CN = TeliaSonera Gateway CA v2 O = TeliaSonera C = FI | TeliaSonera Root CA v1 | 00863C7564 1195854FB4 3138A0A0C F8AA3 | RSA | 4096 bits | sha256RSA | 16 October 2014 | 16 October 2032 | 87AAE313129 F118BCA68C D1E2DC429A 8FA101ACB | 46226B7B89E02CA8F 5D85D67ED8CB4B19 C48382058BB162421 99D540CABE9268 | |
| 6 | 1 | CN = Telia Extended Validation CA v3 O = Telia Finland Oyj C = FI | Telia Root CA v2 | 01675FAC7 2994C74BF 1A67EDC1B 3AD | RSA | 4096 bits | sha256RSA | 29 November 2018 | 29 November 2043 | FB36703B5D1 FF07DB22089 C0E92EB7D9 E858A835 | 98C2545A2C05A342E DB22A9F6C7CCC1F E98D87595676E3A29 8ADE97F7B01291D | |
| 7 | 1 | CN = Telia Domain Validation SSL CA v1 O = Telia Finland Oyj C = FI | TeliaSonera Root CA v1 | 0161AE200 5CE3F127E F88DD7251 BB1 | RSA | 4096 bits | sha256RSA | 19 February 2018 | 16 October 2032 | 496C32537C5 DED2BE3A2A B9C0BC95DE 495D4925F | D75F8BC0DB4B2938 2145499A61148659C F29A967E2AE470B49 8A1799788A8284 | Revoked 17 April 2020 |
| 8 | 1 | CN = Telia Domain Validation CA v3 O = Telia Finland Oyj C = FI | Telia Root CA v2 | 01675FFDE 7E41811E2 CD76B0CD B50A | RSA | 4096 bits | sha256RSA | 29 November 2018 | 29 November 2043 | 5BF1EE298D 31B23B3AE01 7CBA407E93 F82421FA3 | A7E83056E9B3D9DD B1816B95518F6A5E5 A1DFDFA28F60533B 1C850855EAA4263 | |
| 9 | 1 | CN = Telia Domain Validation CA v2 O = Telia Finland Oyj C = FI | TeliaSonera Root CA v1 | 016584E34 A38D9E963 EBEED2174 784 | RSA | 4096 bits | sha256RSA | 29 August 2018 | 18 October 2032 | ED3D749C2C 53BB71937B4 B11F6B891E2 82F992DB | 5B312B7E11B70D07 C14E0AB99F08D007 48966098C52AA85A0 6A0822BBE59A02C | |

| CA # | Cert # | Subject | Issuer | Serial | Key Algorithm | Key Size | Digest Algorithm | Not Before | Not After | SKI | SHA2 Fingerprint | Other information |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 10 | 1 | CN = Telia Server CA v3<br>O = Telia Finland Oyj<br>C = FI | Telia Root CA v2 | 01675FE78 F10F349257 F16B3731F 7A | RSA | 4096 bits | sha256RSA | 29 November 2018 | 29 November 2043 | 46668D0E072 316B0EA4F05 EB965ADEA5 EEC97EA4 | 1281AD8FABE883F2 09E9636448D1A80C3 73DAA7686C813A270 FAD48F5F5E589A | |

**KPMG Advisory N.V.**
P.O. Box 74500
1070 DB Amsterdam
The Netherlands

Laan van Langerhuize 1
1186 DS Amstelveen
The Netherlands
Telephone +31 (0)20 656 7890
www.kpmg.com/nl

**To the Management of Telia Company AB (Telia)**

Amstelveen, 26 June 2020

**Subject:** Independent Auditor's Report WebTrust for CAs Baseline Requirements

We have been engaged, in a reasonable assurance engagement, to report on Telia' management's assertion that for its Certification Authority (CA) operations in Finland and Sweden, throughout the period 1 April 2019 through 31 March 2020 for its CAs as enumerated in Attachment A, Telia has:

- disclosed its SSL certificate lifecycle management business practices in its:
    - Telia Root Certificate Policy and Certification Practice Statement, version 2.5, March 2020
    - Telia Production Certification Practice Statement, version 2.8, March 2020
    - Telia Server Certificate Policy and Certification Practice Statement, version 2.7, March 2020
    - Telia Organizational User Certificate Policy and Certificate Practice Statement, version 1.4, March 2020

  including its commitment to provide SSL Certificates in conformity with the CA/Browser Forum Guidelines, as published on the Telia website, and provided such services in accordance with its disclosed practices
- maintained effective controls to provide reasonable assurance that:
    - the integrity of keys and SSL certificates it manages is established and protected throughout their lifecycles; and
    - SSL subscriber information is properly authenticated (for the registration activities performed by Telia)
- 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.

And, for its CAs as enumerated in Attachment A

- maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum in accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.4.

**Certification Authority's responsibilities**

Telia' management is responsible for its assertion, including the fairness of its presentation, and the provision of its described services in accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.4.

**Our independence and quality control**

We have complied with the independence and other ethical requirements of the *Code of Ethics for Professional Accountants* issued by the International Ethics Standards Board for Accountants, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour. Therefore, we are independent of Telia and complied with other ethical requirements in accordance with the Code of Ethics of NOREA and the Code of Ethics for Professional Accountants (a regulation with respect to independence) of the NBA, Royal Netherlands Institute of Chartered Accountants.

We apply the International Standard on Quality Control 1, 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. We also apply the Regulations for Quality management systems of the NBA and, accordingly, maintain a comprehensive system of quality control, including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

**Auditor's responsibilities**

Our responsibility is to express an opinion on management's assertion based on our procedures. We conducted our procedures in accordance with International Standard on Assurance Engagements (ISAE) 3000, *Assurance Engagements Other than Audits or Reviews of Historical Financial Information,* issued by the International Auditing and Assurance Standards Board and the related Dutch Directive 3000A 'Attestation engagements', as issued by NOREA, the IT Auditors Association in The Netherlands.

These standards requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, management's assertion is fairly stated, and, accordingly, included:

1. obtaining an understanding of Telia' SSL certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of SSL

certificates, and obtaining an understanding of Telia's network and certificate system security to meet the requirements set forth by the CA/Browser Forum;

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 Telia 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, Telia' 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.

*Subject: Independent Auditor Report WebTrust for CAs Baseline Requirements*
*Amstelveen, 26 June 2020*

## Basis for qualified opinion

During our procedures, we noted the following that caused a qualification of our opinion:

| | Observation | Relevant WebTrust Criteria |
|---|---|---|
| 1 | The Key Usage extension in the root CA certificates of *TeliaSonera Root CA v1* and *Sonera Class 2 CA* is not marked critical and *TeliaSonera Root CA v1* certificate's subject information does not include subject:countryName. This caused WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3, Principle 2, Criterion 2.3 to not be met.<br><br>However, Telia generated a new root CA, *Telia Root CA v2*, on 29 November 2018, which is planned to eventually replace *TeliaSonera Root CA v1* and *Sonera Class 2 CA*. Extensions, key sizes, and Certificate Policy Identifiers (including Reserved Certificate Policy Identifiers) of the new Telia Root CA v2 certificate conform to the Baseline Requirements. | **Principle 2, Criteria 2.3**<br><br>The CA maintains controls to provide reasonable assurance that the extensions, key sizes, and certificate policy identifiers (including Reserved Certificate Policy Identifiers) of Root CA certificates generated conform to the Baseline Requirements |

## Qualified opinion

In our opinion, except for the matters described in the basis for qualified opinion section above, throughout the period 1 April 2019 through 31 March 2020, Telia has, in all material respects:

- disclosed its SSL certificate life cycle management business practices in its:
  - Telia Root Certificate Policy and Certification Practice Statement, version 2.5, March 2020
  - Telia Production Certification Practice Statement, version 2.8, March 2020
  - Telia Server Certificate Policy and Certification Practice Statement, version 2.7, March 2020
  - Telia Organizational User Certificate Policy and Certificate Practice Statement, version 1.4, March 2020

  including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the Telia website, and provided such services in accordance with its disclosed practices
- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and SSL certificates it manages is established and protected throughout their lifecycles; and

  - SSL subscriber information is properly authenticated (for the registration activities performed by Telia)

- 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

- maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum

in accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.4.

This report does not include any representation as to the quality of Telia' services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.4, nor the suitability of any of Telia' services for any customer's intended purpose.

**Use of the WebTrust seal**

Telia' use of the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security Seal constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.

On behalf of KPMG Advisory N.V.

Amstelveen, 26 June 2020

(originally signed by)

drs. ing. R.F. Koorn RE CISA
Partner

*Subject: Independent Auditor Report WebTrust for CAs Baseline Requirements*
*Amstelveen, 26 June 2020*

## Attachment A: List of CAs in scope

The following CAs were in scope of the engagement:

| CA # | Cert # | Subject | Issuer | Serial | Key Algorithm | Key Size | Digest Algorithm | Not Before | Not After | SKI | SHA2 Fingerprint | Other information |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | CN = TeliaSonera Root CA v1 O = TeliaSonera | Self-signed | 0095BE16A0F72E46F17B398272FA8BCD96 | RSA | 4096 bits | sha1RSA | 18 October 2007 | 18 October 2032 | F08F593800B3F58F9A960CD5EBFA7BAA17E81312 | DD6936FE21F8F077C123A1A521C12224F72255B73E03A7260693E8A24B0FA389 | |
| 1 | 2 | CN = TeliaSonera Root CA v1 O = TeliaSonera | Sonera Class2 CA | 87ED2E1A28264AC519AA3AEBB90DA2CB | RSA | 4096 bits | sha256RSA | 5 December 2014 | 5 April 2021 | F08F593800B3F58F9A960CD5EBFA7BAA17E81312 | E9563581E712B290F23A749346535EB0D981E3D4A39D56D604684CD0B1698C89 | Cross-certificate |
| 2 | 1 | CN = Sonera Class2 CA O = Sonera C = FI | Self-signed | 1D | RSA | 2048 bits | sha1RSA | 16 April 2001 | 16 April 2021 | 4AA0AA5884D35E3C | 7908B40314C138100B518D0735807FFBFCF8518A0095337105BA386B153DD927 | |
| 3 | 1 | CN = Telia Root CA v2 O = Telia Finland Oyj C = FI | Self-signed | 01675F27D6FE7AE3E4ACBE095B059E | RSA | 4096 bits | sha256RSA | 29 November 2018 | 29 November 2043 | 72ACE43379AA4587F6FDAC1D9ED6C72F86D82439 | 242B69742FCB1E5B2ABF98898B94572187544E5B4D9911786573621F6A74B82C | |
| 3 | 2 | CN = Telia Root CA v2 O = Telia Finland Oyj C = FI | TeliaSonera Root CA v1 | 01675F82BE0017DE8955A9376EB1F9 | RSA | 4096 bits | sha256RSA | 29 November 2018 | 18 October 2032 | 72ACE43379AA4587F6FDAC1D9ED6C72F86D82439 | EF6F29F636F62BDD4753122F41F3419EE7C2877587BE4A9807ADF58946458E7F | Cross-certificate |
| 4 | 1 | CN = TeliaSonera Server CA v2 O = TeliaSonera C = FI | TeliaSonera Root CA v1 | 4C462AF6DBFBF7804F84C17CFEA972B6 | RSA | 4096 bits | sha256RSA | 16 October 2014 | 16 October 2032 | 2F493C294FD70725F9C68CD564F5663D12832295 | D721110388CA6F20BBA9FD1A8DBA4EFB8C16392A3DEBAD97C553EEAF0ACACAAC | |

*Subject: Independent Auditor Report WebTrust for CAs Baseline Requirements*
*Amstelveen, 26 June 2020*

| CA # | Cert # | Subject | Issuer | Serial | Key Algorithm | Key Size | Digest Algorithm | Not Before | Not After | SKI | SHA2 Fingerprint | Other information |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 5 | 1 | CN = TeliaSonera Gateway CA v2<br>O = TeliaSonera<br>C = FI | TeliaSonera Root CA v1 | 00863C75641195854FB43138A0A0CF8AA3 | RSA | 4096 bits | sha256RSA | 16 October 2014 | 16 October 2032 | 87AAE313129F118BCA68CD1E2DC429A8FA101ACB | 46226B7B89E02CA8F5D85D67ED8CB4B19C48382058BB16242199D540CABE9268 | |
| 6 | 1 | CN = Telia Extended Validation CA v3<br>O = Telia Finland Oyj<br>C = FI | Telia Root CA v2 | 01675FAC72994C74BF1A67EDC1B3AD | RSA | 4096 bits | sha256RSA | 29 November 2018 | 29 November 2043 | FB36703B5D1FF07DB22089C0E92EB7D9E858A835 | 98C2545A2C05A342EDB22A9F6C7CCC1FE98D87595676E3A298ADE97F7B01291D | |
| 7 | 1 | CN = Telia Domain Validation SSL CA v1<br>O = Telia Finland Oyj<br>C = FI | TeliaSonera Root CA v1 | 0161AE2005CE3F127EF88DD7251BB1 | RSA | 4096 bits | sha256RSA | 19 February 2018 | 16 October 2032 | 496C32537C5DED2BE3A2AB9C0BC95DE495D4925F | D75F8BC0DB4B29382145499A61148659CF29A967E2AE470B498A1799788A8284 | Revoked 17 April 2020 |
| 8 | 1 | CN = Telia Domain Validation CA v3<br>O = Telia Finland Oyj<br>C = FI | Telia Root CA v2 | 01675FFDE7E41811E2CD76B0CDB50A | RSA | 4096 bits | sha256RSA | 29 November 2018 | 29 November 2043 | 5BF1EE298D31B23B3AE017CBA407E93F82421FA3 | A7E83056E9B3D9DDB1816B95518F6A5E5A1DFDFA28F60533B1C850855EAA4263 | |
| 9 | 1 | CN = Telia Domain Validation CA v2<br>O = Telia Finland Oyj<br>C = FI | TeliaSonera Root CA v1 | 016584E34A38D9E963EBEED2174784 | RSA | 4096 bits | sha256RSA | 29 August 2018 | 18 October 2032 | ED3D749C2C53BB71937B4B11F6B891E282F992DB | 5B312B7E11B70D07C14E0AB99F08D00748966098C52AA85A06A0822BBE59A02C | |

*Subject: Independent Auditor Report WebTrust for CAs Baseline Requirements*
*Amstelveen, 26 June 2020*

| CA # | Cert # | Subject | Issuer | Serial | Key Algorithm | Key Size | Digest Algorithm | Not Before | Not After | SKI | SHA2 Fingerprint | Other information |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 10 | 1 | CN = Telia Server CA v3<br>O = Telia Finland Oyj<br>C = FI | Telia Root CA v2 | 01675FE78F10F349257F16B3731F7A | RSA | 4096 bits | sha256RSA | 29 November 2018 | 29 November 2043 | 46668D0E072316B0EA4F05EB965ADEA5EEC97EA4 | 1281AD8FABE883F209E9636448D1A80C373DAA7686C813A270FAD48F5F5E589A | |