A tabela abaixo serve para controle de alteração dessa documentação. Ela deve ser removida e depois reinserida para entrega aos clientes.

Date	Descrição
29/07/2025	Primeira versão.

1. Introdução

Esta documentação visa explicar e exemplificar a utilização da `API` de verificação de assinaturas de `PDF`s assinados com Certificados de Assinatura Única (CertAU) ou com certificados tradicionais.

Essa `API` sofrerá modificações sucessivas durante o seu ciclo de vida, de modo que, com o passar do tempo, novas funcionalidades serão adicionadas. Essas modificações podem ser maiores ou menores, resultando ou não em uma quebra de compatibilidade. Ou seja, modificações menores não resultarão em uma mudança de `URL` para consumo, enquanto mudanças maiores podem gerar uma versão que não seja compatível com a anterior, requerendo uma nova `URL` de consumo.

- **Retorno da API de verificação:** Informações referentes à assinatura do documento enviado para validação. Esse retorno é uma estrutura composta por dois elementos principais, detalhadamente tratados na seção **3.2. (Retorno do Verificador)**.

2. URLs do serviço e requisitos para consumo da API

A `URL` da `API` de verificação é a seguinte:

- `https://assinadoravancado.gov.mz/api/verifier/pdf/<version>/verify` (Produção)

O campo `<version>` se refere à versão da `API`. O formato de versionamento segue o padrão semver. Porém, o usuário pode informar apenas a versão `major`.

Exemplos:

- `https://assinadoravancado.gov.mz/api/verifier/pdf/1/verify`: A versão com `major` igual a `1` mais atualizada será chamada.

IMPORTANTE: No momento, apenas a versão `1` está disponível, sendo válidos os exemplos acima.

Para consumir a API de verificação, não há requisitos quanto a tokens de acesso.

3. Utilização do verificador

3.1. Chamada de API

Para o serviço de verificação, deve-se enviar uma requisição para a `URL` de verificação (explicitada na seção 2), na rota `/verify`, enviando o documento a ser assinado. Segue um exemplo dessa requisição via cURL:

```
curl -X POST 'https://assinadoravancado.gov.mz/api/verifier/pdf/1/verify' \
-F file=@assinado.pdf
```

No exemplo acima, um arquivo chamado `assinado.pdf` é enviado para o serviço de verificação em sua versão `1`

3.2. Retorno do verificador

Como retorno do verificador, obter-se-á a seguinte estrutura:


```
[
  {
    "certificate": {
      "SHA1": "afe5e6a9cb0102778be3ef2fe7a0e3ac069eb430",
      "SHA256": "c0d164f8a2703ea5590a4e82d8c02f06637bdc4104b03dac77ca2287ac2c5e61",
      "digest_algo": "sha512",
      "hash_algorithm": "sha256",
      "is_otc": true,
      "issuance_time_reference": 1754762754,
      "issuer": {
        "common_name": "AC CertAU v2",
        "country_name": "MZ",
        "organization_name": "INTIC",
        "organizational_unit_name": "DLC",
        "state_or_province_name": "Maputo"
      },
      "not_valid_after": 4865042828.0,
```

```
    "not_valid_before": 1754762753.0,
    "ots_hash": "ee980ff4362ba... (omitido para brevidade)",
    "raw": "MIIFIDCCBAigAw... (omitido para brevidade)",
    "serial": "1253AC8C439DFFAB8311841ACD8274686E95B2EC",
    "signature_algorithm": "rsassa_pkcs1v15",
    "subject": {
      "common_name": "FREDERICO SCHARDONG",
      "country_name": "MZ",
      "email_address": "frede.sch@gov.mz",
      "nuit": "12312313223"
    },
    "trust_status": "trusted"
  },
  "signature": {
    "auth_time": 808,
    "contact_info": "https://assinadoravancado.gov.mz",
    "coverage": "ENTIRE_FILE",
    "cripto": {
      "digest_algo": "sha512",
      "digest_value_manually_calculated": "ee980ff4362ba... (omitido para brevidade)",
      "signature_algo": "sha512_rsa"
    },
    "reason": null,
    "signature_time": 1754762754.0,
    "signer_software": {
      "name": "Assinador Avançado",
      "version": "1.8.1"
    },
    "validity": {
      "individual_checks": {
        "does_ots_pades_digest_match_signature_digest": true,
        "is_certificate_trusted": true,
        "is_document_modification_permission_respected": true,
        "is_signature_ISO32000_valid": true,
        "is_signature_coverage_ok": true,
        "is_signature_hash_algo_strong": true,
        "is_signature_time_after_certificate_creation": true,
        "is_signature_valid": true
      },
      "invalid_cause": "",
      "is_valid": true
    },
    "verification_time": 1754924356.849538
  },
  "software_version": "1.9.3"
}
]
```


3.2.1 Sobre a estrutura retornada

A esturura retornada é uma lista de dois elementos no formato `JSON-like` ou dicionário (chave e valor) em que cada elemento possui uma série de chaves que reúnem informações importantes acerca da análise da assinatura, processada pelo verificador. Um dos dicionários se refere ao certificado utilizado para a assinatura e o outro possui informações sobre a assinatura propriamente.

Primeiramente, tem-se a chave `certificate`.


```
  "certificate": {
     "SHA1": "afe5e6a9cb0102778be3ef2fe7a0e3ac069eb430",
     "SHA256": "c0d164f8a2703ea5590a4e82d8c02f06637bdc4104b03dac77ca2287ac2c5e61",
     "digest_algo": "sha512",
     "hash_algorithm": "sha256",
     "is_otc": true,
     "issuance_time_reference": 1754762754,
     "issuer": {
       "common_name": "AC CertAU v2",
       "country_name": "MZ",
       "organization_name": "INTIC",
```

```
      "organizational_unit_name": "DLC",
      "state_or_province_name": "Maputo"
    },
    "not_valid_after": 4865042828.0,
    "not_valid_before": 1754762753.0,
    "ots_hash": "ee980ff4362ba... (omitido para brevidade)",
    "raw": "MIIFIDCCBAigA... (omitido para brevidade)",
    "serial": "1253AC8C439DFFAB8311841ACD8274686E95B2EC",
    "signature_algorithm": "rsassa_pkcs1v15",
    "subject": {
      "common_name": "FREDERICO SCHARDONG",
      "country_name": "MZ",
      "email_address": "frede.sch@gov.mz",
      "nuit": "12312313223"
    },
    "trust_status": "trusted"
  }
```


Esse dicionário possui informações sobre o certificado do usuário ou entidade que assinou o documento:

- `SHA1`: *Hash* do documento utilizando a função SHA-1, com 160 bits.
- `SHA256`: *Hash* do documento utilizando a função SHA-256, com 256 bits.
- `digest_algo`: Algoritmo de resumo criptográfico utilizado para cálculo do resumo do documento.
- `hash_algorithm`: Algoritmo de *hash* utilizado no certificado.
- `is_otc`: valor booleano que indica se o certificado que está assinando o documento é um Certificado de Assinatura Única.
- `issuer`: Contém informações sobre o emissor do certificado (Nome da AC, nome do país, nomes da organização e da unidade da organização)
- `not_valid_after` e `"not_valid_before"`: período em que o certificado é valido.
- `ots_hash`: Hash da assinatura OTS (*One-Time Signature*). Nesse caso, utiliza a função `SHA-512`
- `issuance_time_reference`: Momento exato da geração do certificado (se o certificado não tiver, então este campo não existirá)
- `raw`: O certificado em *bytes* puros.
- `serial`: Número de série do certificado.
- `signature_algorithm`: Algoritmo de assinatura utilizado. Nesse caso, foi usado RSA com assinatura anexada (SSA = *Signature Scheme with Appendix*), no padrão PKCS#1V1.5.
- `subject`: Dados do usuário que assinou o documento (nome, endereço de e-mail, CPF, data de nascimento (DDMMAAAA), nome da organização e nome da unidade da organização).
- `trust_status`: informa se o certificado utilizado para assinatura é confiável (está na lista de certificados confiáveis). Possíveis valores são:
  - **trusted**: o certificado é confiado.
  - **revoked**: o certificado está na lista de Certificados Revogados da Raiz.
  - **unstrusted**: o certificado não é confiável, pois nenhum certificado da sua cadeia está na lista de certificados confiáveis.

Observação importante: Diferentemente dos certificados digitais convencionais, o certificado contém informações sobre o documento a ser assinado (mais especificamente o *hash* do documento) justamente por se tratar de um Certificado de Assinatura Única, CertAU.

O dicionário contido na chave `signature` reúne informações sobre a assinatura.


```
  "signature": {
    "auth_time": 808,
    "contact_info": "https://assinadoravancado.gov.mz",
    "coverage": "ENTIRE_FILE",
    "cripto": {
      "digest_algo": "sha512",
      "digest_value_manually_calculated": "ee980ff4362ba... (omitido para brevidade)",
      "signature_algo": "sha512_rsa"
    },
    "reason": null,
    "signature_time": 1754762754.0,
    "signer_software": {
      "name": "Assinador Avançado",
      "version": "1.8.1"
    },
    "validity": {
      "individual_checks": {
        "does_ots_pades_digest_match_signature_digest": true,
        "is_certificate_trusted": true,
        "is_document_modification_permission_respected": true,
        "is_signature_ISO32000_valid": true,
        "is_signature_coverage_ok": true,
        "is_signature_hash_algo_strong": true,
```

```
        "is_signature_time_after_certificate_creation": true,
        "is_signature_valid": true
      },
      "invalid_cause": "",
      "is_valid": true
    },
    "verification_time": 1754924856.897747
}
```


- `auth_time`: Tempo decorrido, em segundos, da última autenticação do usuário no sistema antes da realização da assinatura.
- `contact_info`: Contato do sistema de assinatura, para que o recebedor do documento possa verificar o mesmo caso necessário.
- `coverage`: Cobertura da assinatura em relação ao arquivo.
  - **LTA_UPDATES**: As únicas atualizações são do tipo que seria permitido como parte do processamento de assinatura de arquivamento de longo prazo (LTA). Ou seja, atualizações no armazenamento de segurança do documento ou novos carimbos de data/hora do documento. Para fins de avaliação, se um documento foi modificado no sentido definido nas normas PAdES e ISO 32000-2, essas atualizações não contam.
  - **ENTIRE_FILE**: Assinatura cobre todo o arquivo.
  - **FORM_FILLING**: As únicas atualizações são assinaturas extras e atualizações para formar valores de campos ou seus fluxos de aparência, além dos níveis anteriores.
  - **ENTIRE_REVISION**: Assinatura cobre a revisão do arquivo.
  - **ERROR**: Cobertura da assinatura violada: não permite assinaturas posteriores.
  - **SKIPPED**: Não foi possível determinar a cobertura da assinatura.
- `cripto`: Informações criptográficas (algoritmo de *hash* utilizado, valor de *hash* gerado na análise, algoritmo de assinatura)
- `reason`: Consentimento da assinatura/a razão pela qual tal assinatura foi feita no documento. Mostra o comprometimento do assinante perante o documento.
- `signature_time`: *Timestamp* do momento da assinatura, no formato *Unix Timestamp*.
- `signer_software`: Informações sobre o sistema que assinou o documento (nome e versão do software assinador)
- `validity`: dicionário que contém duas entradas.
  - `individual_checks`: Análises de validação específicas realizadas sobre a assinatura.
    - `does_ots_pades_digest_match_signature_digest`: Checagem essencial para o certificado de Assinatura Única (CertAU). Essa checagem confere se o *hash* do documento é idêntico ao *hash* informado no certificado.
    - `is_certificate_trusted`: Informa se o certificado é confiável (se reconstruindo o sua cadeia de certificação, se chega em um certificado que pertence à lista de confiança do sistema).
    - `is_document_modification_permission_respected`: Se a política de modificação do documento é respeitada, segundo a ISO-32000.
    - `is_signature_coverage_ok`: Se a cobertura da assinatura respeita as especificações.
    - `is_signature_hash_algo_strong`: Se o algoritmo DE *hash* usado na assinatura é forte. Algoritmos como o `MD5` e `SHA1` são considerados criptograficamente fracos e por isso invalidam a assinatura.
    - `is_signature_ISO32000_valid`: É realizada uma verificação geral da assinatura na biblioteca pyhanko em que vários atributos da assinatura são validados.
    - `is_signature_time_after_certificate_creation`: Se a assinatura foi realizada após a emissão do certificado.
    - `is_signature_valid`: Se a assinatura é criptograficamente intacta.
  - `invalid_cause`: Causa de `is_valid` estar apontando uma assinatura inválida. Caso a assinatura seja, válida, o valor desse campo é uma *string* vazia. Caso seja inválida, dará mais detalhes acerca da invalidade.
  - `is_valid`: Retorna `true` se todas as checagens de `individual_checks` forem bem sucedidas. Caso contrário, retorna `false`.
- `verification time`: informa o *timestamp* do momento em que a verificação foi realizada.

No caso de documentos com múltiplas assinaturas, a validação é calculada sobre cada uma delas. Ou seja, a lista do retorno conterá validação de certificado e assinatura (apresentados acima) para cada assinatura. Abaixo, há um exemplo de validação de um documento assinado duas vezes.

```
curl -X POST 'https://assinadoravancado.gov.mz/api/verifier/pdf/1/verify' \
-F file=@assinado_2_vezes.pdf
```


```
[
  {
    "certificate": {
      "SHA1": "9635156994ac93e7b18f586ede4c79e1aa754127",
      "SHA256": "ceffdfac0e2473f442ccfa56c71da42b3c6a2c3ccacb2e019f37c55f0e3029ee",
      "digest_algo": null,
      "hash_algorithm": "sha256",
      "is_otc": false,
      "issuer": {
        "common_name": "AC SAFEWEB RFB v5",
        "country_name": "BR",
        "organization_name": "ICP-Brasil",
        "organizational_unit_name": "Secretaria da Receita Federal do Brasil - RFB"
      },
      "not_valid_after": 1747236279.0,
```

```
      "not_valid_before": 1715700279.0,
      "ots_hash": null,
      "raw": "MIIHvDCCBaSgAw... (omitido para brevidade)",
      "serial": "722E437432E94923",
      "signature_algorithm": "rsassa_pkcs1v15",
      "subject": {
        "common_name": "ARTHUR GONCALVES PUCCINELLI:05727915937",
        "country_name": "BR",
        "email_address": "ARTHURPUCCINELLI@HOTMAIL.COM",
        "organization_name": "ICP-Brasil",
        "organizational_unit_name": [
          "Secretaria da Receita Federal do Brasil - RFB",
          "RFB e-CPF A1",
          "(EM BRANCO)",
          "01579286000174",
          "videoconferencia"
        ]
      },
      "trust_status": "untrusted"
    },
    "signature": {
      "auth_time": null,
      "contact_info": null,
      "coverage": "ENTIRE_REVISION",
      "cripto": {
        "digest_algo": "sha256",
        "digest_value_manually_calculated": "1b8747be9a... (omitido para brevidade)",
        "signature_algo": "sha256_rsa"
      },
      "reason": null,
      "signature_time": 1740051163.0,
      "signer_software": {
        "name": "DocuSign®",
        "version": "20.2.0.200505"
      },
      "validity": {
        "individual_checks": {
          "does_ots_pades_digest_match_signature_digest": null,
          "is_certificate_trusted": false,
          "is_document_modification_permission_respected": false,
          "is_signature_ISO32000_valid": false,
          "is_signature_coverage_ok": true,
          "is_signature_hash_algo_strong": true,
          "is_signature_time_after_certificate_creation": true,
          "is_signature_valid": true
        },
        "invalid_cause": "assinatura é inválida. Confira as checagens individuais",
        "is_valid": false
      },
      "verification_time": 1754924857.051126
    },
    "software_version": "1.9.3"
  },
  {
    "certificate": {
      "SHA1": "afe5e6a9cb0102778be3ef2fe7a0e3ac069eb430",
      "SHA256": "c0d164f8a2703ea5590a4e82d8c02f06637bdc4104b03dac77ca2287ac2c5e61",
      "digest_algo": "sha512",
      "hash_algorithm": "sha256",
      "is_otc": true,
      "issuance_time_reference": 1754762754,
      "issuer": {
        "common_name": "AC CertAU v2",
        "country_name": "MZ",
        "organization_name": "INTIC",
        "organizational_unit_name": "DLC",
        "state_or_province_name": "Maputo"
```

```
    },
    "not_valid_after": 4865042828.0,
    "not_valid_before": 1754762753.0,
    "ots_hash": "ee980ff4362ba... (omitido para brevidade)",
    "raw": "MIIFIDCCBAigAwI... (omitido para brevidade)",
    "serial": "1253AC8C439DFFAB8311841ACD8274686E95B2EC",
    "signature_algorithm": "rsassa_pkcs1v15",
    "subject": {
      "common_name": "FREDERICO SCHARDONG",
      "country_name": "MZ",
      "email_address": "frede.sch@gov.mz",
      "nuit": "12312313223"
    },
    "trust_status": "trusted"
  },
  "signature": {
    "auth_time": 808,
    "contact_info": "https://assinadoravancado.gov.mz",
    "coverage": "ENTIRE_FILE",
    "cripto": {
      "digest_algo": "sha512",
      "digest_value_manually_calculated": "ee980ff4362ba... (omitido para brevidade)",
      "signature_algo": "sha512_rsa"
    },
    "reason": null,
    "signature_time": 1754762754.0,
    "signer_software": {
      "name": "Assinador Avançado",
      "version": "1.8.1"
    },
    "validity": {
      "individual_checks": {
        "does_ots_pades_digest_match_signature_digest": true,
        "is_certificate_trusted": true,
        "is_document_modification_permission_respected": true,
        "is_signature_ISO32000_valid": true,
        "is_signature_coverage_ok": true,
        "is_signature_hash_algo_strong": true,
        "is_signature_time_after_certificate_creation": true,
        "is_signature_valid": true
      },
      "invalid_cause": "",
      "is_valid": true
    },
    "verification_time": 1754924856.897747
  },
    "software_version": "1.9.3"
  }
]
```


Note que, para cada assinatura, teremos todas as validações realizadas com seus respectivos resultados sendo retornados.

3.2.2. Erro na verificação

Podem acontecer dois erros específicos:

- **Erro ao obter a Lista de Serviços Confiáveis (LSC):** Por algum erro de rede ou na disponibilidade da *URL* da *LSC*, o verificador não consegue obtê-la e, portanto, não confia em nenhum certificado para validar assinaturas.
  - **Código de status HTTP retornado**: 500
  - **Mensagem de erro:**

```
{"error": "Erro obtendo a LSC"}
```

- **Estrutura do PDF corrompida**: O PDF não possui uma estrutura válida, impossibilitando a verificação de suas assinaturas.
  - **Código de status HTTP retornado**: 533

- **Mensagem de erro:**

```
"PDF mal estruturado"
```

- **Erro geral:** Em caso de erro geral durante o processo de verificação.
  - **Código de status HTTP retornado**: 422
  - **Mensagem de erro:**

```
{
  "error": "Erro validando assinatura"
}
```

4. Validando Certificados CertAU

A validação de documentos assinados com CertAUs herda todos os passos de uma verificação de assinaturas com certificados tradicionais. Porém, um passo adicional é necessário: O *hash* do documento original (documento no estado imediatamente anterior à assinatura que está sendo verificada), calculado em tempo de verificação, deve ser igual ao *hash* que está presente na extensão `OneTimeCertificateHash` do CertAU.

Note, nos exemplos de retorno do verificador, ao longo da presente documentação, que o campo `does_ots_pades_digest_match_signature_digest` deve ser `true` para que a assinatura seja considerada válida. O valor desse campo é exatamente o resultado do passo adicional comentado no parágrafo anterior e é consequência de uma igualdade entre os valores dos campos `digest_value_manually_calculated` e `ots_hash`, pois note que ambos devem coincidir para que se tenha uma assinatura válida.

Outra consideração muito importante acerca das assinaturas geradas por CertAUs é que, por definição, a validação dessas assinaturas deve ser feita não considerando o horário atual, mas sim o momento de geração do certificado, que ocorre imediatamente antes da geração da assinatura. Isso é uma consequência desse modelo de certificação, que desconsidera artefatos de marcação temporal e revogação presentes no modelo tradicional. Para mais informações, leia o artigo sobre CertAU.

Comments