

Chave Móvel Digital

Especificação dos serviços de Assinatura

Versão <V1.11.1>



Agência para a Modernização Administrativa I.P.



CMD - Especificação dos serviços de Assinatura

Referências a outros Documentos

Ref.	Descrição	Autor

Registo de Revisões

Data	Versão	Descrição	Autor
10-05-2016	V0.1	Versão Inicial	Filipe Leitão
11-11-2016	V0.2	Versão Inicial	Jorge Basílio
28-03-2017	V0.3	Versão Inicial	Jorge Basílio
09-11-2017	V0.4	Atualização dos Serviços	Adriano Pires
13-04-2018	V0.9	Revisão e atualização do WSDL Adição de informação de autenticação	Adriano Pires
16-04-2018	V1.0	Revisão documento	André Vasconcelos
08-05-2018	V1.1	Alteração da especificação de assinatura de múltiplos documentos Atualização do WSDL	Bruno Teixeira
08-05-2018	V1.2	Esclarecimento, na introdução, da ordem de invocação das operações do serviço	Bruno Teixeira
24-05-2018	V1.3	Atualização de lista de erros	Adriano Pires
05-06-2018	V1.4	Atualização Serviço CCMovelMultipleSign Atualização ficheiro wsdl	Adriano Pires



CMD - Especificação dos serviços de Assinatura

Data	Versão	Descrição	Autor
24-07-2008	V1.5	Alteração do tipo do campo Pin	Bruno Teixeira
29-09-2008	V1.6	Alteração da ordem dos campos no tipo SignRequest, de forma estarem coerentes com o WSDL	Bruno Teixeira
20-12-2018	V1.7	Novo serviço para receber os valores do PIN, UserId e OTP encriptados	Filipe Leitão
26-03-2019	V1.8	Atualização ficheiro WSDL Alteração do tipo dos campos cifrados	Ricardo Conceição
17-09-2019	V1.9	Esclarecimentos sobre a geração de hash	Bruno Teixeira
23-09-2019	V1.10	Melhoramento códigos erro	Ricardo Conceição
11-12-2019	V1.11	Atualização ficheiro WSDL Atualização de métodos existentes Introdução de novos métodos	Ricardo Conceição
29-04-2021	V1.11.1	Alteração ao serviço SCMDMultipleSign	Ricardo Conceição

Lista de Distribuição

Nome	Organização	email
André Vasconcelos	AMA I.P.	andre.vasconcelos@ama.pt



CMD - Especificação dos serviços de Assinatura

Índice

1	INTRODUÇÃO	5
2	SERVIÇOS	6
2.1	SCMDSERVICE - SERVIÇO DE ASSINATURA QUALIFICADA	7
2.1.1	SCMDSign - Assinatura de Hash	7
2.1.1.1	SignRequest	7
2.1.1.2	SignStatus	8
2.1.2	GetCertificate – Obtém certificado do cidadão	8
2.1.3	ValidateOtp – Validação de código enviado para o cidadão	8
2.1.3.1	SignResponse	9
2.1.3.2	HashStructure	9
2.1.4	SCMDMultipleSign - Assinatura de múltiplos Hash	9
2.1.4.1	MultipleSignRequest	10
2.1.4.2	HashStructure	10
2.1.4.3	SignStatus	10
2.1.5	GetCertificateWithPin – Obtém certificado do cidadão com o PIN de assinatura	11
2.1.6	ForceSMS – Reenvia um SMS com o código de validação para o utilizador	11
3	GERAÇÃO DO HASH DO DOCUMENTO	12
4	ANEXOS	13
4.1	CÓDIGOS DE ERRO	13
4.2	WSDL	13



1 Introdução

A CHAVE MÓVEL DIGITAL VEM MASSIFICAR O PROCESSO DE AUTENTICAÇÃO E ASSINATURA ELETRÓNICA QUALIFICADA DO CIDADÃO.

O presente documento visa especificar o serviço para integração de sistemas externos para realização de assinaturas qualificadas através da Chave Móvel Digital (CMD). Este serviço irá disponibilizar as seguintes operações, que devem ser invocados pela ordem indicada abaixo:

1. GetCertificate: obtém certificado do cidadão;
2. SCMDSign: quando se pretende assinar um único documento, deve ser utilizada esta operação que recebe o hash do documento a assinar;
3. SCMDMultipleSign: quando se pretende assinar vários documentos, deve ser utilizada esta operação que recebe a lista dos hash dos documentos a assinar. Este serviço tem um limite de 100 documentos por operação, caso seja efetuado um pedido com mais documentos, irá ser retornado o erro 900, com a mensagem associada de demasiados documentos para assinar;
4. GetCertificateWithPin: obtém o certificado do cidadão com o pin de assinatura associado;
5. ForceSMS: força o envio de um SMS com um novo código OTP, associada a uma operação em processo;
6. ValidateOtp: último passo do processo, que valida o código de segurança enviado e devolve o hash assinado, uma lista de hash assinados ou o certificado do cidadão, conforme ter sido invocada anteriormente a operação SCMDSign, SCMDMultipleSign ou GetCertificateWithPin.



CMD - Especificação dos serviços de Assinatura

2 Serviços

Nesta secção é descrita a especificação do serviço SCMDService. Os sistemas externos que desejem efetuar a integração com este serviço devem implementar os seguintes protocolos para a comunicação:

- Comunicação HTTPS com basic authentication;
- Mensagem SOAP;

As credenciais para a autenticação serão disponibilizadas pela AMA aquando dos trabalhos de integração.

As operações descritas, irão implementar criptografia assimétrica para encriptação e descriptação dos dados sensíveis introduzidos pelo Cidadão (nº de Telemóvel, PIN de Assinatura e OTP). A CMD irá disponibilizar a chave pública através de um certificado X.509 para que os sistemas externos efetuem a encriptação da informação, com RSA, que será descriptada pela CMD com a chave privada.

Endpoints

DEV	Serviço: https://dev.cmd.autenticacao.gov.pt/Ama.Authentication.Frontend/SCMDService.svc Certificado: a definir (apenas acessível dentro da rede da AMA)
PPR	https://preprod.cmd.autenticacao.gov.pt/Ama.Authentication.Frontend/SCMDService.svc Certificado: a definir
PRD	https://cmd.autenticacao.gov.pt/Ama.Authentication.Frontend/SCMDService.svc Certificado: a definir



CMD - Especificação dos serviços de Assinatura

2.1 SCMDService - Serviço de Assinatura Qualificada

O serviço *SCMDService* irá disponibilizar 6 operações, a operação de assinatura de hash de 1 documento, a operação de assinatura de várias hash, a operação de validação de código de segurança OTP (*One Time Password*), a operação de obter o certificado do cidadão, a operação de obter o certificado do cidadão com recurso a PIN, e a operação de forçar um SMS para um processo em curso.

2.1.1 SCMDSign - Assinatura de Hash

Operação	SCMDSign
Parâmetro de Entrada	SignRequest (2.1.1.1)
Parâmetro de Saída	SignStatus (0)

2.1.1.1 SignRequest

Parâmetros	Tipo	Obrigatório?	Descrição
ApplicationId	byte[]	Sim	Identificador da aplicação que efetua o request
DocName	string	Não	Nome do Documento ou identificador para permitir ao Cidadão identificar o ato que vai originar a assinatura
Hash	byte[]	Sim	Hash da informação sobre a qual vai ser gerada a assinatura
Pin	base64String(cifrado)	Sim	Código PIN do utilizador
UserId	base64String(cifrado)	Sim	Identificador da conta do utilizador (ex.: Nº de Telemóvel: "+351 966666666")



CMD - Especificação dos serviços de Assinatura

2.1.1.2 SignStatus

Parâmetros	Tipo
ProcessId	string
Code	string
Message	string
Field	string
FieldValue	string

2.1.2 GetCertificate – Obtém certificado do cidadão

Operação	GetCertificate
Parâmetro de Entrada	byte[] applicationId base64String userId (cifrado)
Parâmetro de Saída	string certificate

2.1.3 ValidateOtp – Validação de código enviado para o cidadão

Operação	ValidateOtp
Parâmetro de Entrada	base64String code (cifrado) string processId byte[] applicationId
Parâmetro de Saída	SignResponse (2.1.3.1)



CMD - Especificação dos serviços de Assinatura

2.1.3.1 SignResponse

Parâmetros	Tipo
Signature	Byte[]
ArrayOfHashStructure	List<HashStructure>
SignStatus	Objecto referido no ponto 2.1.1.2
certificate	String

2.1.3.2 HashStructure

Parâmetros	Tipo	Obrigatório?	Descrição
Signature	byte[]	Sim	Assinatura do documento
Name	string	Sim	Nome do documento
id	string	Sim	Indentificador do documento

2.1.4 SCMDMultipleSign - Assinatura de múltiplos Hash

Operação	CCMoveIMultipleSign
Parâmetro de Entrada	MultipleSignRequest List<HashStructure>
Parâmetro de Saída	SignStatus (0)



CMD - Especificação dos serviços de Assinatura

2.1.4.1 MultipleSignRequest

Parâmetros	Tipo	Obrigatório?	Descrição
ApplicationId	byte[]	Sim	Identificador da aplicação que efetua o <i>request</i>
Pin	base64String (cifrado)	Sim	Código PIN do utilizador
UserId	base64String (cifrado)	Sim	Identificador da conta do utilizador (Nº Telemóvel: "+351 966666666")

2.1.4.2 HashStructure

Parâmetros	Tipo	Obrigatório?	Descrição
Hash	byte[]	Sim	Hash da informação sobre a qual vai ser gerada a assinatura
Name	String	Sim	Nome do documento
id	String	Sim	Identificador do documento

2.1.4.3 SignStatus

Parâmetros	Tipo
ProcessId	string
Code	string
Message	string
Field	string
FieldValue	string



CMD - Especificação dos serviços de Assinatura

2.1.5 GetCertificateWithPin – Obtém certificado do cidadão com o PIN de assinatura

Operação	GetCertificateWithPin
Parâmetro de Entrada	byte[] applicationId base64String userId (cifrado) Base64String pin (cifrado)
Parâmetro de Saída	SignStatus (0)

2.1.6 ForceSMS – Reenvia um SMS com o código de validação para o utilizador

Operação	ForceSMS
Parâmetro de Entrada	byte[] applicationId base64String userId (cifrado) String processId
Parâmetro de Saída	SignStatus (0)





3 Geração do Hash do documento

.....

A geração do hash deve ser feita conforme o “PKCS #1: RSA Cryptography Specifications Version 2.2”, ponto 9.2 até ao passo 2:

- <https://tools.ietf.org/html/rfc8017#page-45>

A título de exemplo, o AlgorithmIdentifier para um hash SHA-256 seria o seguinte:

```
unsigned char[] sha256SigPrefix =  
  
    { 0x30, 0x31, 0x30, 0x0d, 0x06, 0x09,  
  
      0x60, 0x86, 0x48, 0x01, 0x65, 0x03, 0x04, 0x02, 0x01,  
  
      0x05, 0x00, 0x04, 0x20};
```

O hash enviado para os serviços deve ser o prefixo seguido do hash do documento.





4 Anexos

4.1 Códigos de Erro

Código	Descrição
200	OK
500's	Erros de sistema
800's	Parâmetros inválidos
801	Pins não correspondem
802	OTP inválido
817	Ocorre quando o serviço de assinatura do SCMD está inativo. O cidadão não recebe o OTP.
900	Erro genérico

4.2 WSDL



SCMDService.wsdl