



## E-Sec Segurança Digital

---

### Manual de Integração – AP - Notificação

Manual de integração Web Service	Versão: 1.0	17/12/2013
----------------------------------	-------------	------------

## Histórico da Revisão

<b>Versão</b>	<b>Descrição</b>	<b>Autor</b>	<b>Aprovação</b>	<b>Data</b>
1.0	Criação do documento	Késsia Barbosa		14/08/2013

## Sumário

1 Introdução.....	3
2 Terminologias.....	4
3 Autenticação.....	4
4 Serviços de Notificação da AP.....	4
4.1 Descrição.....	4
4.2 Fluxos.....	4
4.2.1 Solicitação de Assinatura Assíncrona Servidor - Servidor.....	4
4.3 Formato das Mensagens.....	6
4.3.1 SignatureNotificationReq.....	6
4.3.2 SignatureNotificationResp.....	6
4.4 Status.....	6
4.5 Erros.....	7

## 1 Introdução

Este documento tem por objetivo auxiliar os desenvolvedores à realizarem a integração de suas soluções com o Web Service do Mobile Signature Service (MSS). Este Web Service contém as funcionalidades necessárias que o Application Provider (AP) deve implementar para que o MSS seja capaz de notificá-la sobre a assinatura.

## 2 Terminologias

A fim de facilitar o entendimento deste documento, utilizaremos as seguintes siglas e terminologias:

- WS – Web Service;
- MSS – Mobile Signature Service;
- RSA e ECC – Algoritmos de criptografia assimétrica;
- AP – Application Provider (cliente);

## 3 Autenticação

O processo de autenticação do MSS frente a uma AP não é implementado, fica por conta da AP decidir a autenticação apropriada. A autenticação desses serviços não é necessário, visto que os parâmetros passados são assinados.

## 4 Serviços de Notificação da AP

Esta seção descreve os serviços Web Services de notificação do MSS para o software da AP.

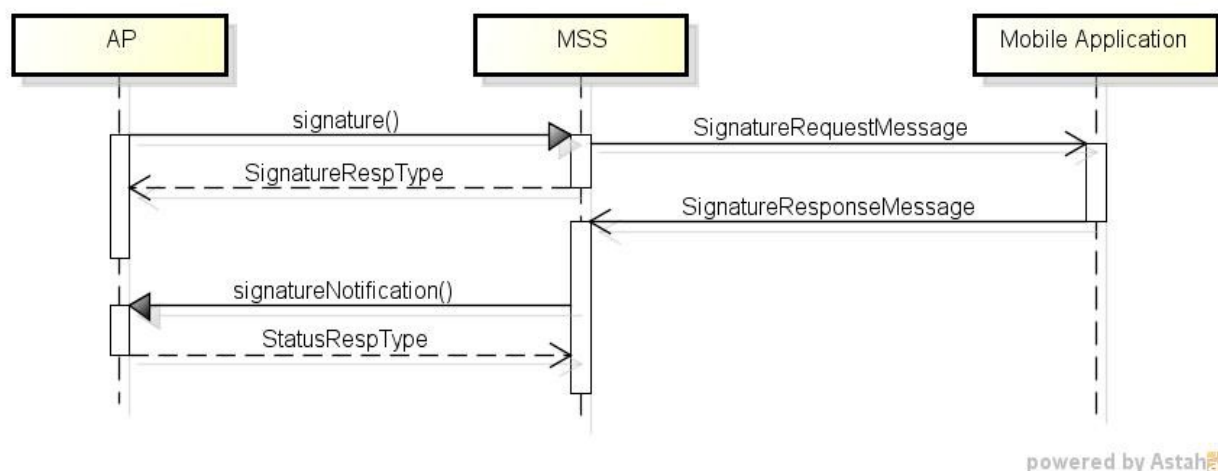
### 4.1 Descrição

Nome do Serviço	Parâmetros	Retorno	Finalidade
SignatureNotification	SignatureNotificationReq	SignatureNotificationResp	Notificar a AP a finalização da requisição de assinatura.

### 4.2 Fluxos

#### 4.2.1 Solicitação de Assinatura Assíncrona Servidor - Servidor

O MSS disponibiliza um serviço de notificação quando a requisição de assinatura for concluída para facilitar a integração da AP.



1. A AP solicita a assinatura de um documento de forma assíncrona pelo método de acordo com o tipo de assinatura que pode ser: WS *signatureRequestMessage()*, WS *signatureComplexDocument()* ou WS *signatureByTemplate()*;
2. O MSS realiza as seguintes verificações:
  1. verifica se a AP solicitante é válida;
  2. verifica se o usuário alvo da solicitação está cadastrado;
  3. verifica se o usuário alvo da solicitação possui um certificado válido do tipo especificado pela AP;
3. O MSS responde à AP com o número da transação gerada (o software de AP deve guardar esse número pois ele deverá ser utilizado para consultar o status da transação);
4. O MSS envia uma mensagem de solicitação de assinatura para a aplicação móvel;
5. A aplicação móvel assina o documento;
6. A aplicação móvel envia a assinatura para o MSS;
7. O MSS verifica a assinatura;
8. O MSS notifica a AP que a assinatura foi realizada com sucesso pelo método WS *signatureNotification()*;
9. A AP recebe a assinatura junto com status da transação.

## 4.3 Formato das Mensagens

### 4.3.1 SignatureNotificationReq

Nome	Formato	Descrição	Obrigatório
TransactionId	Long	Número criado pelo MSS para esta transação	sim
Status	StatusType	Status atual da transação. REQUEST_OK (100) caso a requisição seja válida e aceita pelo MSS SIGNATURE (500) caso o modo seja síncrono e o MSS possui uma assinatura realizada pelo usuário VALID_SIGNATURE (502) caso a assinatura for válida INVALID_SIGNATURE (503) caso a assinatura for inválida	sim
Signature	Base64Binary	Assinatura computada no aparelho móvel	não

### 4.3.2 SignatureNotificationResp

Nome	Formato	Descrição	Obrigatório
Status	StatusType	Status atual da transação.	sim

## 4.4 Status

O MSS utiliza um conjunto de status para informar o resultado de operações diversas. Abaixo estão listados os status utilizados pelo WS de AP, bem como seus códigos e descrições.

Nome	Código	Descrição
REQUEST_OK	100	Requisição recebida com sucesso.
INVALID_CERTIFICATE	432	Problema na verificação do certificado.
SIGNATURE	500	Assinatura realizada.
REVOKED_CERTIFICATE	501	Certificado revogado.
VALID_SIGNATURE	502	Assinatura válida.
INVALID_SIGNATURE	503	Assinatura inválida.
OUTSTANDING_TRANSACTION	504	Transação ainda não processada. Retornada nos serviços de query (ex: mssStatusQuery) quando a resposta da solicitação ainda não está disponível.

## 4.5 Erros

Assim como os status, o MSS também utiliza um conjunto de código de erros para informar situações de inconformidade. O WS de AP utiliza os códigos de erro abaixo:

Nome	Código	Descrição
WRONG_PARAM	101	Erro em algum parâmetro da requisição.
MISSING_PARAM	102	Retornado quando algum parâmetro da requisição não for encontrado.
UNAUTHORIZED_ACCESS	104	A autenticação do requisitante falhou.
UNKNOWN_CLIENT	105	O usuário final não foi encontrado. Por exemplo, no mssFindUser.
EXPIRED_TRANSACTION	208	A requisição expirou.
USER_CANCEL	401	O usuário cancelou a operação.
MOBILE_SIGNATURE_ERROR	406	Erro geral de assinatura.
NO_CERT_FOUND	422	O usuário não possui um certificado do tipo especificado pela AP.
ERROR_CERTIFICATE	425	Erro geral de verificação do certificado.
INTERNAL_ERROR	900	Erro geral do MSS.