

Webhook Signing

When you register for webhooks we will assign a "secret". This should be kept securely (do not commit to source control).

We will create a signature using this secret and a timestamp each time we send you a webhook. You should use the secret to validate this signature so you are sure the message is from us.

We add the following headers, which you will need to extract:

```
'Content-Type' => 'application/json',  
'X-Webhook-Signature' => $signature,  
'X-Webhook-Timestamp' => (string)$timestamp,  
'X-Webhook-ID' => $webhookId,  
'User-Agent' => 'NRSDB-Webhooks/1.0',
```

You can use the \$webhookId to make sure you don't process the same event twice.

The raw data is added to the body of the message as a JSON string. Decode it to access the details.

```
$body = (string)$request->getBody();  
$payload = json_decode($body, true, 512, JSON_THROW_ON_ERROR);
```

Sample PHP code to validate the message (\$body) using the signature, timestamp and your secret is shown below;

```
/**  
 * Verify signature with timestamp (for recipients)  
 */  
public static function verifyWebhookWithTimestamp(  
    string body,  
    string $signature,  
    string $secret,  
    int $timestamp  
): bool {  
    $signedData = $body . $timestamp;  
    $expectedSignature = hash_hmac('sha256', $signedData, $secret);  
  
    return hash_equals($expectedSignature, $signature);  
}
```

}

Revision #2

Created 26 February 2026 13:06:06 by Simon Gilhooly

Updated 26 February 2026 14:07:09 by Simon Gilhooly