

# RealMe

## Authentication and Transaction Signing

Proprietary and Confidential

### Overview

GlobalCrypto offers the ability to digitally sign elements on a web page. A good example of this is signing financial transactions presented and manipulated within a web widget.

### Attack Surface

As financial institutions increase their defenses against online crime, attacks are becoming more insidious. Criminals are performing Man-In-The-Middle (MITM) network attacks to hijack authenticated sessions--note that this was their first response to the use of OTP tokens . Since network attacks are hard to maintain, criminals subsequently evolved to using Man-In-The-Browser (MITB) attacks to modify transactions. MITB type attacks typically manifest as javascript code injection attacks or a drive-by BHO download. Both of these type attacks seek to modify HTML forms as they are entered by a customer before they are transmitted to the web server.

### Elements of the Solution

There are answers to MITM and MITB attacks which use a combined approach including applied cryptography and the use of flash web widgets to offer users a protected surface to enter transaction information.

MITM type attacks are easily mitigated through the use of PKI-style bi-directional encryption of critical information as it flows between a web widget and the web application. The customer and the web application use each other's (unpublished) public key to encrypt critical information for transmission on the wire. If there is a Man in the Middle the details of the information flow are unobservable and the session is immune from information injection on the network including DNS poisoning and Certificate Spoofing attacks. Our web widget unpacks information from the web application which can only be decrypted using a user's unlocked credential and the web application only receives information encrypted by a web widget using the same unlocked credential.

**GLOBAL  
CRYPTO**

MITB attacks are more insidious because they wait for a user to authenticate and then simply modify HTML fields before they are transmitted to the web application. The answer to MITB is to transmit a transaction digital signature with the transaction to ensure integrity. The fear with signing a transaction entered through an HTML form is that a MITB virus might change values in the HTML form at opportune moments in the transaction. If the signing routine is contained in a javascript method it is simple for MITB or injected code attacks to hook the submission of the transaction, modify the fields, compute a new signature for the modified transaction and then send up the transmission.

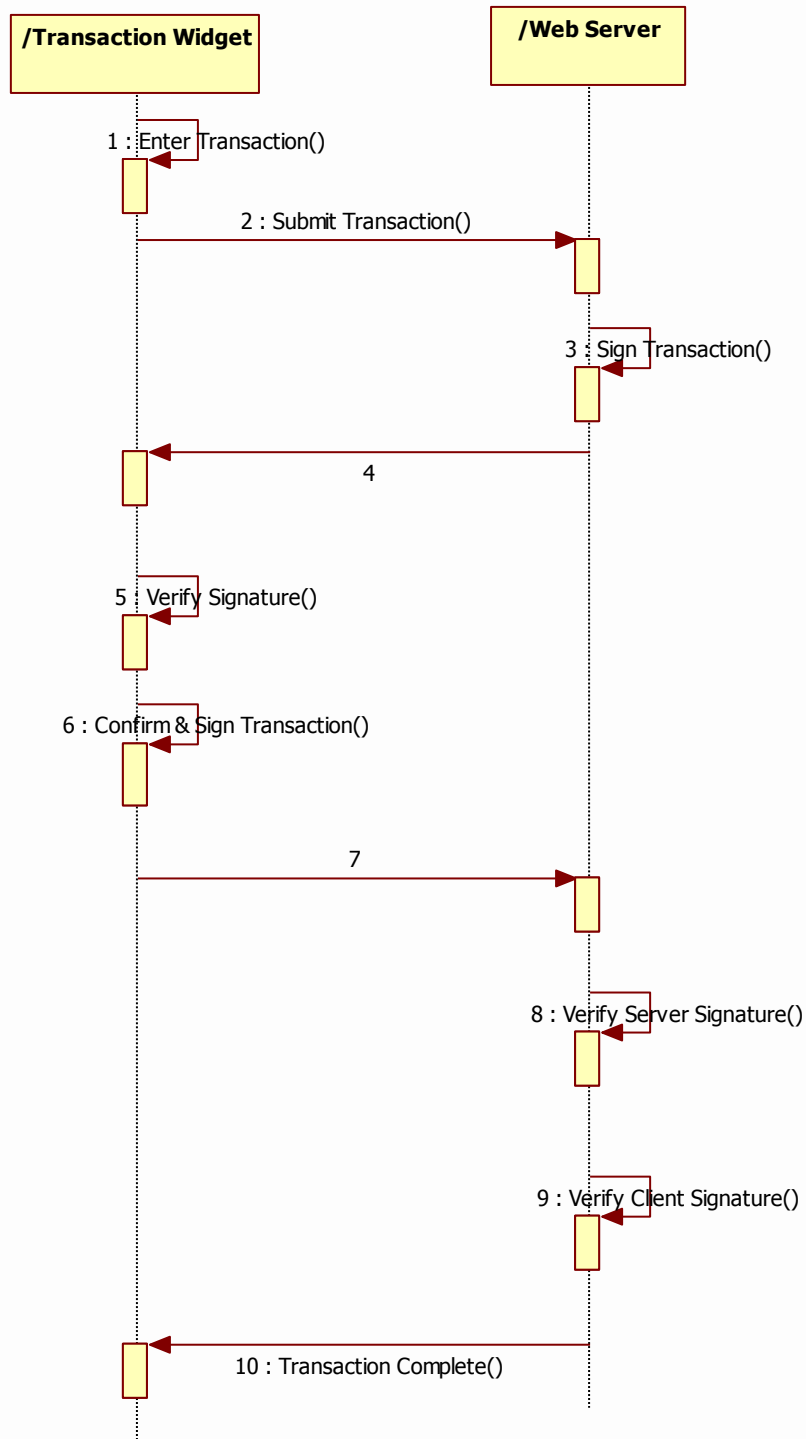
One answer to the above scenario is to introduce hardware transaction signature calculators. However, clever MITB malware can still affect the HTML form elements (eg. Destination account number) at a point before the user enters numerical values into the transactional calculator. The user copies the modified HTML fields into the hardware calculator, enters a correct signature for the modified transaction and the transaction is sent up to the web application. In any case, the weak point in transaction signing is the fact that HTML elements can be programmatically modified and HTML forms can be automatically submitted by a variety of actors.

The GlobalCrypto RealMe system uses Flash web widgets to mitigate the weaknesses in HTML forms illustrated above. Flash offers a rich user experience but also offers protected input surfaces as well as non-mutable displays of information. Note that input into flash web widgets can not be automated directly from javascript or BHO actors.

The RealMe system allows a user to input transaction details into a web widget then sends the recorded transaction to the web server using the public key methods discussed above. The web server then has confidence that a proposed transaction came from a RealMe web widget. A server signature is calculated over the transaction and the proposed transaction with the server signature is returned to the web widget for customer approval. The flash web widget displays a non-mutable form of the transaction to the end user who must then approve the transaction as displayed by clicking a button on the web widget. By clicking on the widget the user guarantees that the widget is in focus and is visible to the end user. Upon approval by the customer the web widget digitally signs the transaction and submits it to the server for processing. The server finally checks the two signatures to make sure they are both valid, proving that the transaction is intact and that the user saw the transaction correctly.

Below is a flow diagram that expresses the information exchange involved in a transaction signing using the RealMe system.





*NOTE: All communications between the widget and the web server are encrypted.*



1. User enters transaction information into the RealMe Transaction Widget.
2. Transaction is uploaded to the widget.
3. The server signs the transaction.
4. The server returns the original transaction and the signature to the widget.
5. The client verifies the server signature.
6. The user confirms the information returned by the server and the widget signs the transaction.
7. The confirmed transaction and the two signatures are uploaded to the server.
8. The server verifies that its signature has not been altered.
9. The server verifies the client signature.
10. The transaction is completed and the user is notified.