

Your Security Advantage against Online Banking Fraud

Online Banking has proved to be a popular service with bank customers offering the convenience of anytime access to banking services. However, the growth in sophisticated Online Banking fraud and high profile identity theft attacks can easily undermine consumer confidence in online services.

New security measures including tokens, mutual authentication, one-time-passwords, and consumer education have proven to be successful deterrents against traditional fraud including Phishing attacks. However, more advanced thefts such as Man in the Middle (MitM) and Man in the Browser (MitB) can often bypass existing Online Banking defenses.

The good news is that the advanced PlainPay security features provide a proven and effective deterrent against existing and emerging Online Banking fraud and identity theft. PlainPay is a Mobile APP that runs flawlessly on the main smartphone operating systems and can easily integrate with a bank's existing infrastructure to enhance security and lower operating costs.

With PlainPay consumers have convenient access to a highly secure, second channel authentication tool that provides them with:

- ✓ Greater authentication security when accessing their Online Banking service
- ✓ Greater security when authorising payment instructions or managing their security profile settings



Why use PlainPay?

PlainPay means stronger Security and Control

PlainPay provides all of the benefits of a dedicated hardware security token but without the added costs. In addition, PlainPay works on the consumer's smartphone so there is no inconvenience of having to carry another device around. However, lower cost and greater consumer convenience are not the only advantages. PlainPay also offers superior security advantages over traditional hardware security tokens. For example, when authorising a payment instruction, PlainPay also displays detailed information about the Internet service account and the payment details being authorised. By verifying all of the payment details the consumer enjoys greater peace of mind and the risk of incorrect transactions is greatly reduced.

Easily integrated in the Bank's existing infrastructure

PlainPay's secure authentication features can be easily added to any Internet Banking system to compliment and strengthen the existing security options. PlainPay also includes a guided activation process for the consumer that clearly explains how they can register their PlainPay APP in a few easy steps and educates them on the benefits and usage of the APP for maximum protection and convenience.

Convenient and Easy to Use

A piecemeal response to Online Banking threats can easily result in an unwieldy and complex consumer experience. Auriga's design philosophy is to strengthen security while also promoting consumer convenience and ease of use. As a result, PlainPay has been designed for intuitive use and embraces the increasingly popular QR Code technology. QR codes are now commonplace and are widely recognised and accepted by smartphone users. Consequently consumers are increasingly adopting PlainPay as a secure and convenient banking tool. Adding PlainPay strong authentication to your Online Banking system ensures the maximum protection against attack and the greatest consumer convenience.



Why is PlainPay secure?

PlainPay uses a highly encrypted communication channel between the phone application and the server based on the industry standard SSL protocol and proprietary security algorithms. Every message used by PlainPay is signed with a MAC (Message Authentication Code) and encrypted using a OTP password (One Time Password). This password is generated by a HSM (Hardware Security Module) to ensure the highest security standards. The MAC is based on proprietary algorithms and is regenerated on every transaction for the ultimate in message integrity and security.

In addition to the robust encryption techniques, PlainPay also thwarts the man-in-the-middle (MitM/MitB) attacks by displaying real time information retrieved from the Internet Banking system to the consumer using a second, independent channel. The consumer can easily verify the accuracy of the information on both their Internet Banking and Mobile channels to ensure that no information tampering remains undetected.



How does it work?

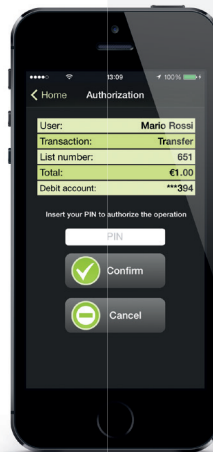
1



Accessing your Online Banking account.
After entering your Online Banking User ID and password a one shot QR code will be displayed on your Online Banking screen. Simply run the PlainPay APP on your phone to capture the QR code and enter your PlainPay PIN to complete the log on Authentication process.



2



Authorising payment instructions.

After confirming the transaction data to be executed, all you need to do is run the PlainPay APP on your smartphone to capture the QR Code displayed by your Online Banking system. Check that the payment instructions displayed by PlainPay match your Online Banking entry and then authorise the payment using your PlainPay PIN.

Headquarters - Bari

Strada Vassallo, 1
70125 Bari - Italy
Phone: +39.080.5692111
Fax: +39.080.5692112
headquarters@aurigaspa.com

Milan office

via Santa Maria Valle, 3
20123 Milano - Italy
Phone: +39.02.00681.583
Fax: +39.02.00681.400
milan@aurigaspa.com

Rome office

via R. Gigante, 20
00143 Roma - Italy
Phone: +39.080.5692111
Fax: +39.080.5692112
rome@aurigaspa.com

London office

Building 3, 566 Chiswick High Road
London W4 5YA - United Kingdom
Phone: +44 (0)208 849 8022
Fax: +39.080.5692112
london@aurigaspa.com

Paris office

88 ter avenue Général Leclerc,
92100 Boulogne Billancourt France
Phone: +33 (0)1.74.31.11.77
Fax: +33.(0)1.74.31.10.00
paris@aurigaspa.com