



# QRentry Strong authentication via QR Code

## Strong authentication using a QR Code

Evidian QRentry™ can easily replace traditional authentication methods to protect access to Web portals, Windows sessions and applications.

Evidian QRentry™ replaces the static password by a One-Time Password (OTP). This strong authentication method can be used for internal and external users, including customers, partners and employees.

With Evidian QRentry™, your users authenticate with their smartphone by scanning a QR Code™.

The QRentry™ solution is a multifactor authentication method: I own the smartphone, I know how to unlock it (or I have a dedicated PIN to access the application). This solution supports BYOD, CYOD and non-managed devices.

This authentication method does not rely on network availability - the QRentry™ application on the smartphone is fully autonomous, it works even in airplane mode.

The OTP generator does not rely on the time either. It also avoids the risk of de-synchronization of the traditional methods based on time or on a counter.

QRentry™ is based on the principle of **“Challenge - Response”** and is protected by design against the main attacks; **“man in the middle”, “key logger”, “replay password”, and “phishing”**.

## Multifactor authentication for Web portals

Evidian QRentry™ is an uncomplicated authentication method with a clean user interface.

This strong authentication method reinforces remote user authentication. The confirmation code (OTP) used is by definition not re-playable.

The authentication scenario is the following:.

1. The user navigates to the portal home page
2. The user provides his identity by entering for example his username
3. With his smartphone, the user scans the displayed authentication QR Code™
4. An OTP is displayed on the smartphone. This OTP is automatically sent to the portal or, if the network is not available, the user enters it
5. The user accesses the portal securely.

Once the session is opened, the user benefits from the Single Sign-On (SSO) of the Evidian Web Access Manager (WAM) solution.

Evidian WAM also provides identity federation to your Web applications, as well as access to “Applications As A Service” and Cloud Services.

Evidian WAM is not intrusive (no need to modify your applications). It complies with SAML and many other authentication schemes.

## QRentry for Windows Authentication

With QRentry™, your users log on to their Windows session by scanning a QR Code with their smartphone.

This access is always available, in online or offline mode, connected or not connected to the corporate network and Active Directory.

QRentry™ works even if the PC's network, mouse, USB port and authentication devices are broken. It also works for remote troubleshooting.

## Safety of End-User accounts

QRentry™ drastically reduces the number of helpdesk calls as users can unlock their Windows session themselves. When users lose a password, smartcard or authentication token, they can unlock their Windows session themselves with a smartphone.

A business or personal smartphone can connect in emergency mode and in accordance with safety rules laid down by the company.

QRentry™ is the ideal partner of strong authentication deployments, which often create “lost smartcard” or “biometrics doesn't work” helpdesk calls. The number of helpdesk calls decreases dramatically - there is nothing to memorize. Users can unlock their Windows session themselves even if the helpdesk is out of reach.

## Safety of local Administrator Accounts

By protecting your PC's local administrator accounts, QRentry™ makes technical interventions compliant with your security policy. Technicians must scan a QR Code to access a PC's local administrator account. Such accesses are logged centrally and access privileges can be removed in a few seconds. End-users cannot imitate the technician's actions to get administrator rights. QRentry™ removes the need for quasi-public “admin/admin” passwords that are hard to modify. Local administrator accounts are no longer the “Achilles' heel” of compliance.



# Strong authentication via QR Code

The security system is based on a public/ private key (RSA2048) associated with each user. The public key is stored in a directory.

The private key is securely stored on the smartphone. The data exchanged between the smartphone and the computer is within the QR Code only.

The smartphone enrollment can be a self-enrollment or an enrollment with the presence of an administrator.

## Low-footprint deployment

- ▶ End-users self-registration with their smartphone
- ▶ No additional hardware, nor software to install on the PC or the table
- ▶ No need for network connection on the PC, no need for cellular or data access on the smartphone.

## Security and confidentiality

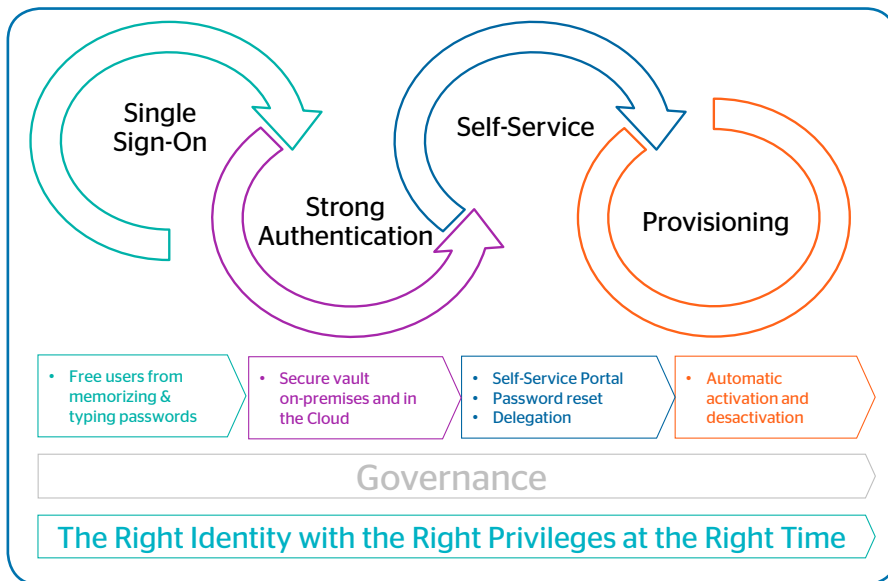
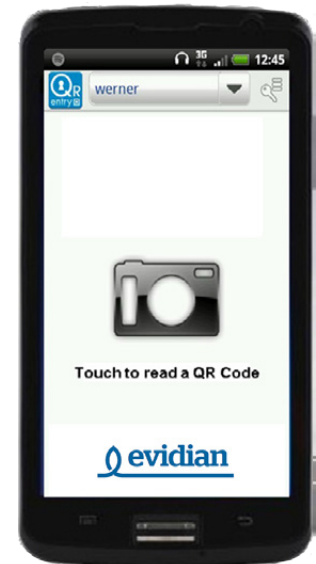
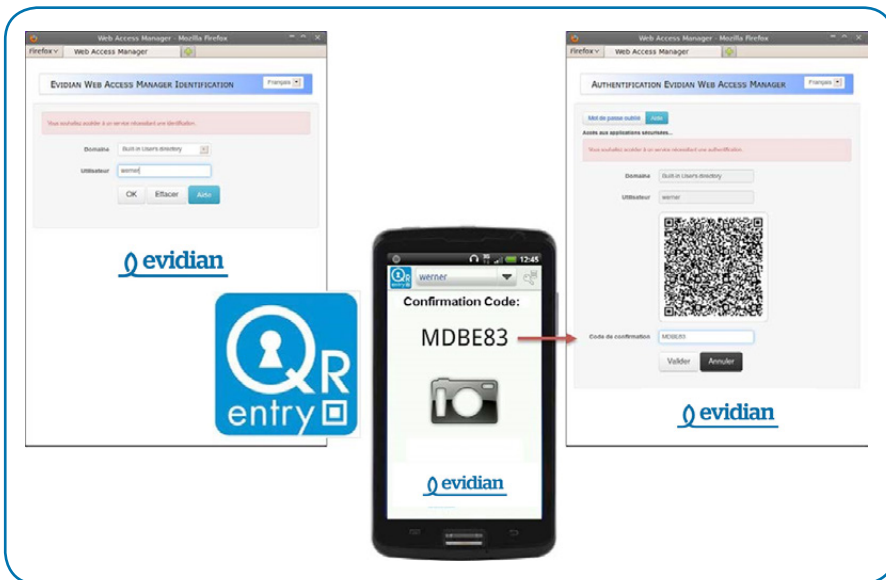
- ▶ Uses a non - re-playable access code
- ▶ All accesses are controlled and logged centrally
- ▶ Access to some applications can be restricted.

## Fast user adoption

- ▶ QR Code usage is widespread among employees
- ▶ 55% of US mobile users own a smartphone (Nielsen 2012).

## Boosts your enterprise's innovation image

- ▶ Evidian QREntry™ for the Web requires Evidian Web Access Manager (WAM).
- ▶ Evidian QREntry™ for Windows requires Evidian Authentication Manager.
- ▶ Evidian QREntry™ is the perfect companion for Evidian Enterprise SSO to strengthen application access privileges with a strong re-authentication.



QREntry™ can be downloaded now on:

- Google Play



- Apple Store



- Blackberry App World



CT\_170413\_LPM\_F-Qrentry\_emi

Atos, the Atos logo, Atos CodeX, Atos Consulting, Atos Workforce, Worldline, Bluewin, Bull, Canopy, the Open Cloud Company, Unify, Yurano, Zero-Email, Zero-Email Certified and The Zero-Email Company are registered trademarks of the Atos group. Atos, Confidential information covered by Atos, to be used by the recipient only. This document, or any part of it, may not be reproduced, copied, circulated and/or distributed nor quoted without prior written approval from Atos. April 2017 © 2017 Atos

www.evidian.com