



simple, secure, affordable authentication

Technical Overview

Every phone call generates data for routing, billing and call logging. identrica uses this information, generated by a user's phone call at time of login, to authenticate the user and control access to resources.

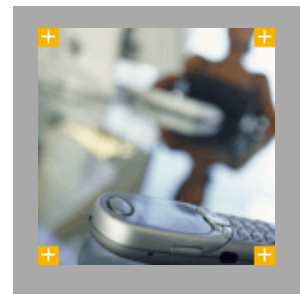
A standard unmodified mobile phone or landline and an internet connection are the only two components. Therefore there are no requirements for any additional or non-standard equipment.

identrica can control access to applications and resources from any device – desktop, laptop, pda, hspda – using any mobile handset anywhere in the world to make a free call to the identrica service number.

identrica can be used to provide 2-factor authentication for:

- Enterprise-level access solutions – e.g. Citrix.
- Enterprise-level and project-specific remote access gateways to applications, which include all the SSL/VPN solutions.
- Other access gateways which are not specifically SSL/VPN products; for example Fortigate, Cisco PIX.
- Microsoft remote access products, where users require access to Microsoft applications remotely – e.g. Outlook Web Access, ISA2004.
- User authentication to Wireless networks at Wireless Access Points, using Radius and Active Directory, with most vendors, including Trapeze and Nortel.
- PDA-based client-server applications, where user authentication is built into the 'Windows Mobile' or Symbian application and calls identrica without user intervention.
- Windows terminal services

identrica



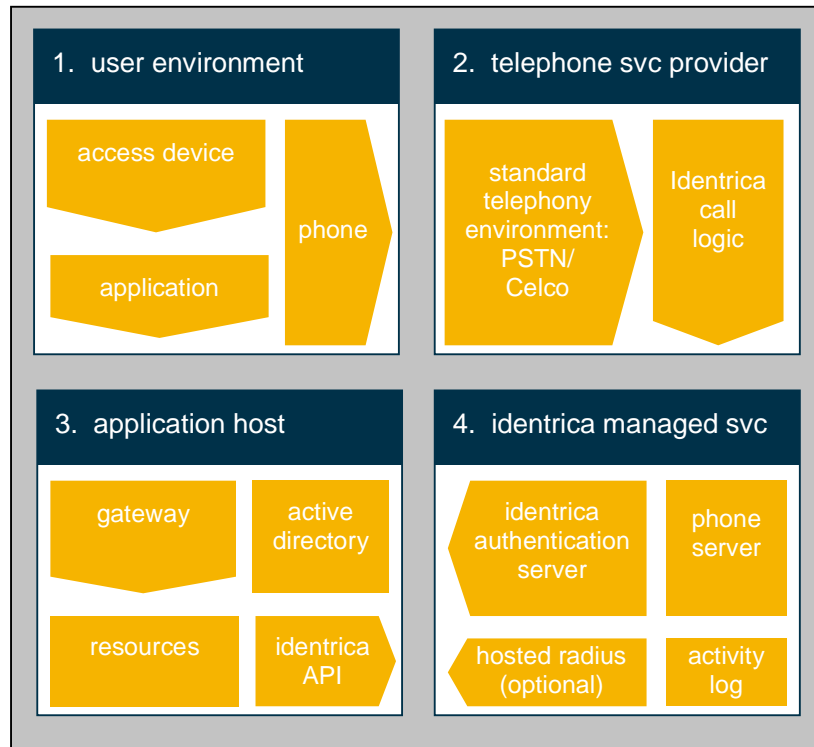
How identrica works

1. A user accesses web-based applications running in a browser on his device, as normal.

The user has a phone – multiple phone numbers may be registered to their name (e.g. mobile, landline, pda). The phone numbers are typically registered in Active Directory.

As part of the login process, the user is asked to provide their registered phone number and call the identrica service from that phone. The call is not answered so costs nothing.

2. The user's call to the identrica server is delivered by the phone company using standard telephony protocols, up to the point where it leaves the public network.



At this stage identrica's "terminating" telephone switch applies the 'identrica call logic' to validate the call – ensuring, for example, that the Caller Line Identification (CLI) is not spoofed. If everything is validated the switch delivers the call, as SIP, over a secure IP connection to the identrica authentication server.

3. The application gateway (Citrix, SSL VPN or other specialised device) uses an identrica API to ask the identrica authentication server whether a call has been made.

4. If a 'clean' call has been received, the server confirms this to the API, and logs the transactions for activity reporting (also optionally for billing, compliance or traceability).

When confirmation is received, the application host checks that the user's phone number is registered and completes the authentication by checking the password.

Infrastructure

identrica has been designed for simple integration into your chosen access infrastructure. Your existing gateway or web application logon pages require only the addition of an extra text box for the user to enter their telephone number.

Interface is via a range of identrica APIs which are typically Radius based but include custom interfaces e.g. for Citrix. The identrica APIs manage connectivity to the identrica service, monitoring availability of two separate managed service sites. The APIs also interface with the database to check user phone numbers. The user's phone number (or numbers) can be simply registered in, and retrieved from, your existing Active Directory, an equivalent database or the identrica user management facility.

Gateways are typically enterprise level remote web access gateways like Citrix Access Platform, or SSL/VPN devices such as AEP/Netilla, Aventail or NetScreen. They may of course also be project or application specific, or more specialised devices like Cisco PIX, routers or firewalls.



simple, secure, affordable authentication

Identrica Ltd, Cipher House, Silver End, Olney, Bucks, MK46 4AL
T: +44 (0)1234 714138 E: info@identrica.com

